WHITE PAPER – **AUGUST 2017**

VMWARE CLOUD™ ON AWS TECHNICAL OVERVIEW

vmware®

Contents

Introduction

VMware Cloud™ on AWS brings VMware enterprise-class Software-Defined Data Center (SDDC) software to the AWS Cloud. It enables customers to run production applications across private, public, and hybrid cloud environments based on VMware vSphere®, with optimized access to AWS services. It is delivered, sold, and supported by VMware as an on-demand service. IT teams manage their cloud-based resources with familiar VMware tools—without the difficulties of learning new skills or utilizing new tools.

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.

The VMware Cloud on AWS solution enables customers to have the flexibility to treat their private cloud and public cloud as equal partners and to easily transfer workloads between them—for example, to move applications from DevTest to production or burst capacity. Users can leverage the global AWS footprint while getting the benefits of elastically scalable SDDC clusters, a single bill from VMware for its tightly integrated software plus AWS infrastructure, and on-demand or subscription services.

Computing – VMware vSphere Cluster Configuration

Initial Availability Compute Cluster Configuration

At initial availability, the VMware Cloud on AWS base cluster configuration contains 2TB of memory and four 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 144. 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 Scheduler Configuration

The VMware vSphere Distributed Resource Scheduler™ (vSphere DRS) cluster uses a default configuration The migration threshold is set to the default vSphere DRS level three to avoid excessive VMware vSphere vMotion® operations. VMware creates and operates a separate resource pool to manage customer workloads. Customers have the option to create child resource pools but cannot configure cluster affinity rules at initial availability.

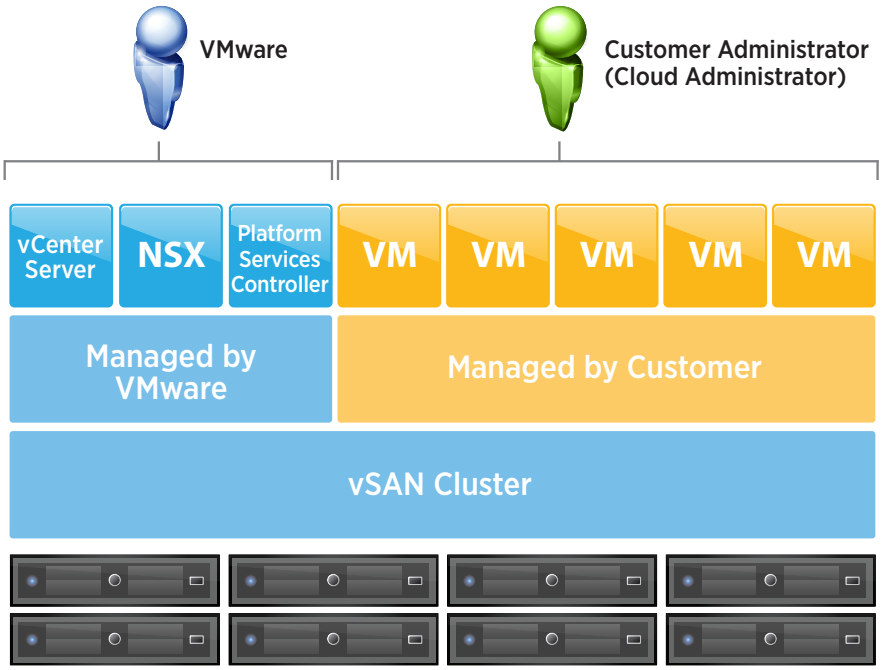

Figure 1. Separation of Virtual Machine Management

VMware vSphere High Availability Cluster Configuration

VMware vSphere High Availability (vSphere HA) provides high availability for VMs by leveraging hosts and resources of a cluster to reserve capacity so workloads can fail over in case of host failures. Hosts in the cluster are monitored; in the event of a failure, the VMs on a failed host are restarted on alternative hosts. Host failure remediation is the responsibility of VMware.

It is important to consider vSphere HA settings when determining consolidation ratio. The following default vSphere HA settings are applied to the SDDC cluster, maximizing productivity while minimizing overhead as well as providing the best balance between economics and availability:

- Host monitoring enabled
- Percentage-based admission control policy
- Host failures tolerated: 1
- VM and application monitoring enabled
- Host isolation response: power off and restart VMs

Storage – VMware vSAN

vSAN Host and Cluster Configuration

The SDDC cluster includes a vSAN all-flash array. At initial availability of VMware Cloud on AWS, 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 four-host cluster configuration, 40TB of raw capacity, comprising all 32 encrypted NVMe devices, is available for the VMs to consume. The management VMs consume .9 percent of the vSAN datastore capacity. 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.

vSAN Architecture

As was mentioned in the previous section, 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.

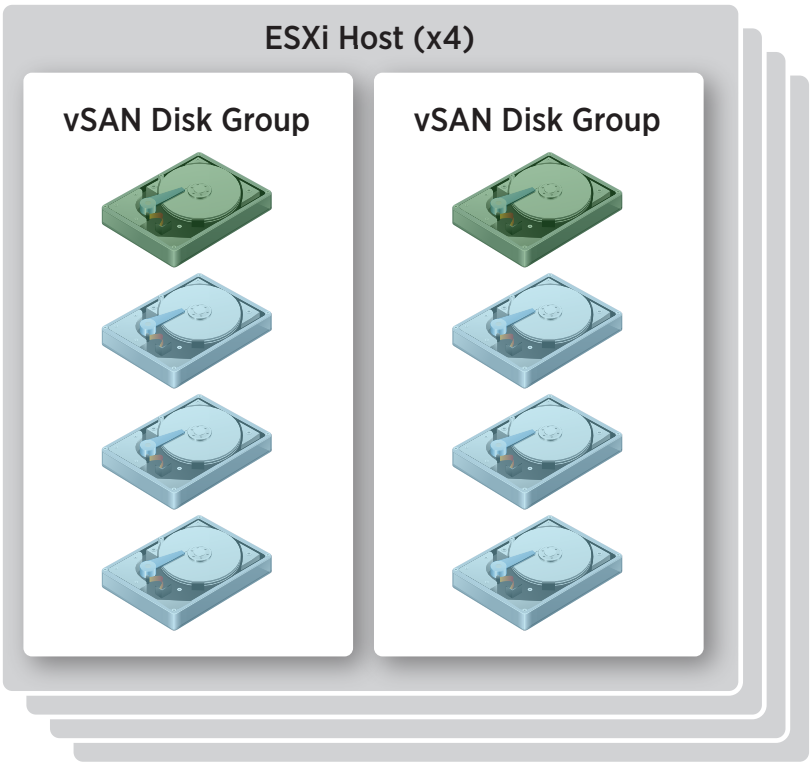

Figure 2. Composition of vSAN Disk Groups

Although default storage policy configuration settings are in place, users can configure their 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 users can select RAID 5 or RAID 6 instead, depending on the number of hosts in the cluster. VMware monitors the health and performance of the vSAN datastore; therefore, vSAN Health Monitoring and vSAN Performance Service are not exposed to the end user.

Storage Encryption

Datastore-level encryption with vSAN encryption, or VM-level encryption with vSphere VM encryption, is not available at initial availability of VMware Cloud on AWS. To provide data security, all local storage NVMe devices are encrypted at the firmware level by AWS. The encryption keys are managed by AWS and are not exposed to or controlled by VMware or VMware Cloud on AWS customers.

vSAN Datastore

All VMs running inside the cloud SDDC consume storage capacity and leverage storage services from the vSAN datastore. Management workloads, and the workloads belonging to a single VMware Cloud on AWS customer, are located on the same vSAN cluster. However, the cloud SDDC introduces a new vSAN capability that provides two logical datastores instead of one. One of these datastores is used to store the management VMs; the other datastore is used for the customer VMs.

Cluster Configuration

At initial availability, clusters are restricted to a single AWS region and availability zone (AZ). Failed hardware can be automatically detected, and automated remediation enables failed hosts to be automatically replaced by other cloud hosts and vSAN datastores to be automatically rebuilt—without user intervention.

Networking – VMware NSX

NSX in VMware Cloud on AWS

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, and the version used in VMware Cloud on AWS provides compatibility between it and other vSphere products used on premises, such as vSphere vMotion.

Simplified Networking Configuration

VMware has introduced a basic networking service to ease the learning curve and enable everyone who uses vSphere to consume VMware Cloud on AWS as readily as possible. Cloud network administrators log in to the VMware Cloud on AWS portal and configure the network ("pre-creating"). They perform tasks such as establishing VPN connectivity and configuring firewall access rules. Next, cloud administrators log in to the vCenter Server platform with a VMware vSphere Web Client instance and consume the networks that the cloud network administrator created ("creating"). Although the cloud administrator can perform tasks such as creating logical networks and connecting VMs, the cloud network administrator permits traffic through the firewall and across the VPN networks.

This mode of consumption utilizes a prescriptive network topology, within which the network and its components are preconfigured and cannot be changed by the customer. Customers provide their own subnets and IP ranges.

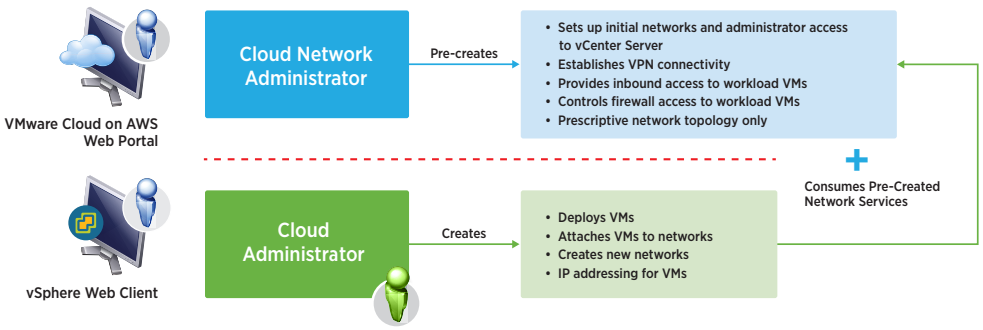

Figure 3. Separation of Networking Capabilities

Network Connectivity

To provide connectivity to VMware Cloud on AWS, two gateways are created. The management edge gateway (MGW) utilizes VMware NSX Edge™ to enable users to connect to the vCenter Server instance. They 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. Users 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.

An IPsec layer 3 VPN is set up to securely connect the on-premises vCenter Server instance with the management components running on the in-cloud SDDC cluster. A separate IPsec layer 3 VPN is set up to create connectivity between the on-premises workloads and the VMs running inside the in-cloud SDDC cluster. NSX is used for all networking and security and is decoupled from Amazon VPC networking. The compute gateway and DLR are preconfigured as part of the prescriptive network topology and cannot be changed by the customer. Customers must provide only their own subnets and IP ranges.

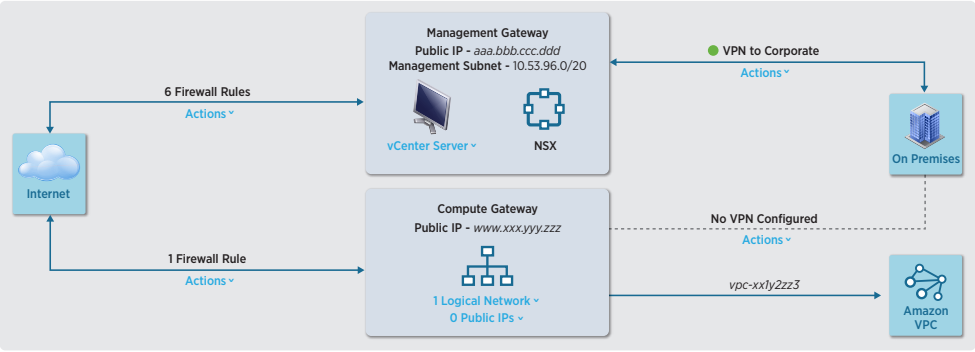

Figure 4. Networking Logical View

Encrypted vMotion

The Encrypted vMotion feature was introduced in VMware vSphere 6.5. It does not require a third-party key manager. It is set on a per-VM basis as one of the VM options. Encrypted vMotion encrypts the data traversing the vSphere vMotion network—not the network itself. It therefore requires no special configuration other than enabling it in the VM options. Encrypted vSphere vMotion migration between hosts inside the cloud SDDC is offered at initial availability of VMware Cloud on AWS.

Host Capacity and Availability Management Features

Instant Provisioning of Host Capacity

Clusters are one of the basic building blocks of managing traditional infrastructure and are used by more than 99 percent of our customers. Typically, administrators create a cluster, add hosts, configure clustering services (e.g., vSphere HA, vSphere DRS, and so on), and start running workloads (i.e., VMs). This approach has been widely adopted as the de facto clustering model in private data centers.

However, if there are host failures, or VMs that demand more capacity, VM availability or performance might be compromised until the administrator adds more hosts to the cluster. Historically, it can take from 6 to 12 weeks for IT to order, rack, stack, and configure a new server, creating opportunities for SLAs to be breached.

To avoid long-term resource availability issues, some customers overprovision their clusters with spare hosts that are available to provide capacity if needed. However, this approach might not be the most economically efficient, because the cluster then tends to be underutilized during routine operation.

With VMware Cloud on AWS, customers have access to a large pool of server resources that exist in AWS data centers. These servers are available on demand and can be joined to existing customer clusters in minutes. If the capacity of a cluster is greater than necessary for the given time, servers can be removed from the customer's cluster and scrubbed before being returned to the general pool of resources. This ability can be utilized to provide unique features that are not available anywhere else.

Automatic Cluster Configuration

As hosts are added to the cluster, VMware Cloud on AWS automatically configures every VMkernel and logical network. After additional hosts are connected to the network, the vSAN datastore automatically expands, enabling the clusters to consume the new storage capacity.

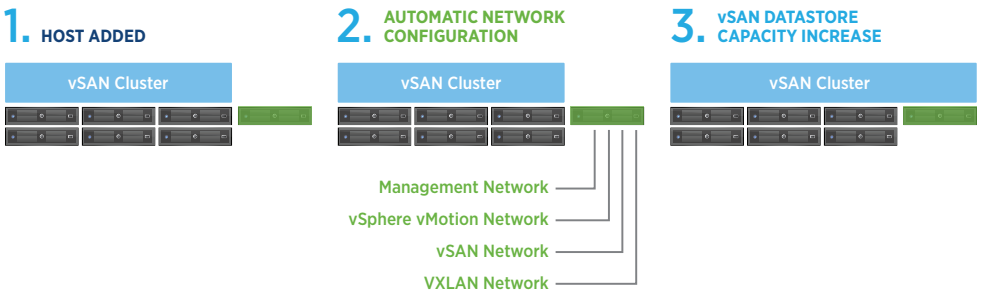

Figure 5. Automatic Cluster Configuration

Automated Cluster Remediation

VMware Cloud on AWS uses vSphere HA to ensure that outages are minimized. In the case of a failed host, VMs are automatically restarted on the surviving hosts. vSAN software ensures that any VM configured with a policy of one or more host failures does not lose data. VMware Cloud on AWS then examines the host and either reboots it, in the case of a transient failure, or replaces it, in the case of hardware fault. In either case, the SDDC continues to run and vSphere DRS optimizes VM placement to minimize impact on the running VMs. In the case of a degraded host, such as a failed disk, VMware Cloud on AWS efficiently removes the host by putting it in maintenance mode before eliminating it from the cluster. Customers are never billed for hosts that are added to a cluster for maintenance or fault tolerance reasons.

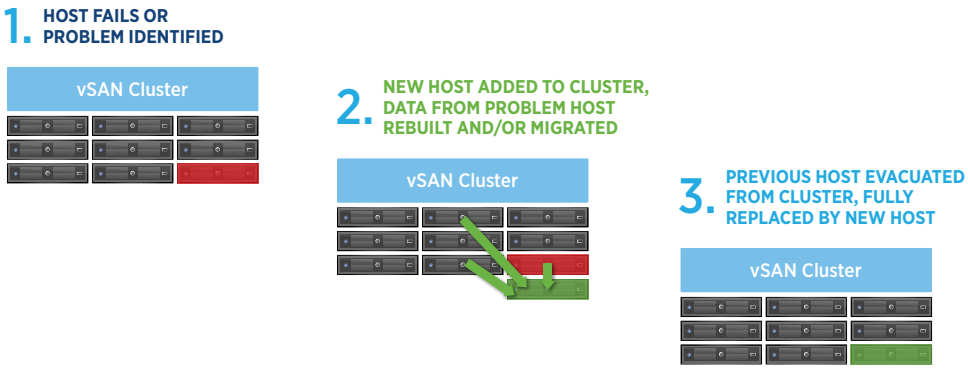

Figure 6. Automatic Cluster Remediation

Hybrid Cloud Operations

Workload Mobility

At initial availability, only cold migration is available to transfer workloads to the cloud SDDC. However, cross-cloud vSphere vMotion migration will be available in future VMware Cloud on AWS releases, as well as per-VM Enhanced vMotion Compatibility, to provide proper vSphere vMotion compatibility between the in-cloud ESXi host's CPU architecture and the customer's on-premises ESXi host's CPU architecture.

vCenter Server Hybrid Linked Mode

VMware Cloud on AWS is designed to provide single pane of glass monitoring for hybrid cloud management. The new Hybrid Linked Mode (HLM) feature enables on-premises and in-cloud vCenter Server instances to share data while maintaining some level of administrative separation. It also enables the linking of vCenter Server instances across different single sign on (SSO) domains, versions, and topologies. In addition, it provides operational consistency between vSphere environments on premises and multiple SDDC vCenter Server instances.

Hybrid Linked Mode enables users to complete the following functions:

- Log in to the vCenter Server instance in their SDDC using their on-premises credentials
- View and manage the inventories of both their on-premises data center and the cloud SDDC from a single vSphere client interface
- Cold-migrate workloads between their on-premises data center and the cloud SDDC

To run HLM, users must have on-premises vCenter Server 6.5d or later, as well as layer 3 network connectivity. Because of the restrictive access model of VMware Cloud on AWS, HLM is restricted to connecting one on-premises Enhanced Linked Mode domain and does not have synchronized roles.

VMware vCenter Content Library

The VMware vCenter® content library feature effortlessly distributes and automatically synchronizes content—such as OVAs, ISO images, and scripts—between on-premises and cloud SDDC deployments. In addition, template support will be available in future VMware Cloud on AWS releases.

By adopting a vCenter content library now, customers will be ready to use VMware Cloud on AWS to its full potential from day one.

Operations Model

VMware Cloud on AWS is sold and operated as a service. To ensure that all environments perform correctly, VMware manages the systems exclusively. Likewise, VMware is the sole contact point for customers. In case of hardware failure, VMware interacts with AWS on the customer's behalf, streamlining communication and remediation.

To enable the monitoring and management of the lifecycle of the cloud SDDC software stack, the VMware Cloud on AWS service retains the administrator rights on the SDDC to deploy and configure the AWS infrastructure and the SDDC software. It is responsible for adding and removing hosts and networks due to a failure or if cluster-scaling operations require more or fewer resources. The VMware Cloud on AWS service is also responsible for cloud SDDC software patching and for the application of updates.

The VMware Cloud on AWS service introduces a new cloud administrator role to the traditional vCenter Server user model and extends the roles and permissions scheme. This is to ensure that the cloud SDDC infrastructure is configured in a prescriptive deployment architecture and that the customer cloud administrator cannot reconfigure the management appliances. Within this model, the customer cloud administrator has full control over their workload while having a read-only view of management workloads and infrastructure.

Due to the restricted access model, the cloud SDDC vCenter Server instance is used only to manage the cloud SDDC environment and does not support management of on-premises SDDC environments. Customers cannot use root access or install VIBs. They can log in to the vCenter Server instance and use it to operate and manage their environment. They do not, however, have direct access to the appliance and cannot make any changes to the vCenter Server instance itself. Customers using a third-party vendor on premises for particular services should consult their partner and ask if they have plans to support the VMware Cloud on AWS model.

Conclusion

The agility to use a private, public, or hybrid environment is one of the main drivers in adopting the cloud. Customers can leverage a hybrid cloud environment in any number of ways. The common denominator is that VMware Cloud on AWS empowers them to focus on consuming resources and managing their VMs rather than spend their time and energy dealing with host-based operations.

FIND OUT MORE

For more information, visit http://cloud.vmware.com/VMC-AWS.
For detailed specifications and requirements, visit http://cloud.vmware.com/VMC-AWS/resources.

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

8/17