Veritas InfoScale™ Support for VMware Cloud™ on AWS

Deployment use case and validation

VERITAS

The truth in information.

Scope

Veritas InfoScale™ Enterprise offers a complete suite of storage and clustering capabilities for applications that are running on virtual machines in a VMware vSphere ESXi environment, containerized environments, and in various cloud provider platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

This document describes a use case featuring Veritas InfoScale deployment in a VMware Software-Defined Data Center (SDCC) running on AWS infrastructure. InfoScale is installed on virtual machines in the SDCC environment and various deployment scenarios have been configured and tested.

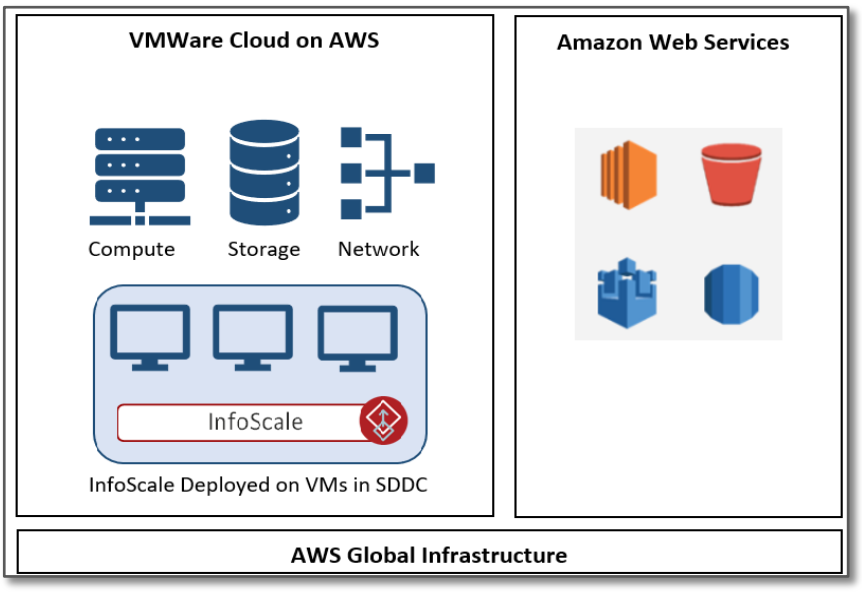
The objective is to showcase InfoScale functionality with various VMware features such as vMotion, vSAN Datastore for Storage, using VMware VMDK with Multi-Writer Flag enabled, Shared SCSI Bus, and enabling Disk UUID. These tests were run on Linux and Microsoft Windows platforms.

Introduction to VMware Cloud™ on AWS

VMware Cloud™ on AWS is a VMware-powered cloud offering jointly developed by Amazon Web Services (AWS) and VMware. It is a cloud service that provides customers with dedicated VMware vSphere-based Software-Defined Data Center (SDDC) on underlying AWS architecture.

VMware provides three important infrastructural components in a deployed SDDC – VMware vSphere, VMware Virtual SAN, and VMware NSX. These components provide virtualization technologies for compute, storage, and network respectively.

The hardware facilities are provided by AWS. The SDDC runs on dedicated, elastic, bare-metal AWS infrastructure. The SDDC has access to the in-house cloud services provided by AWS. Customers have an option to deploy a hybrid or a private cloud environment.

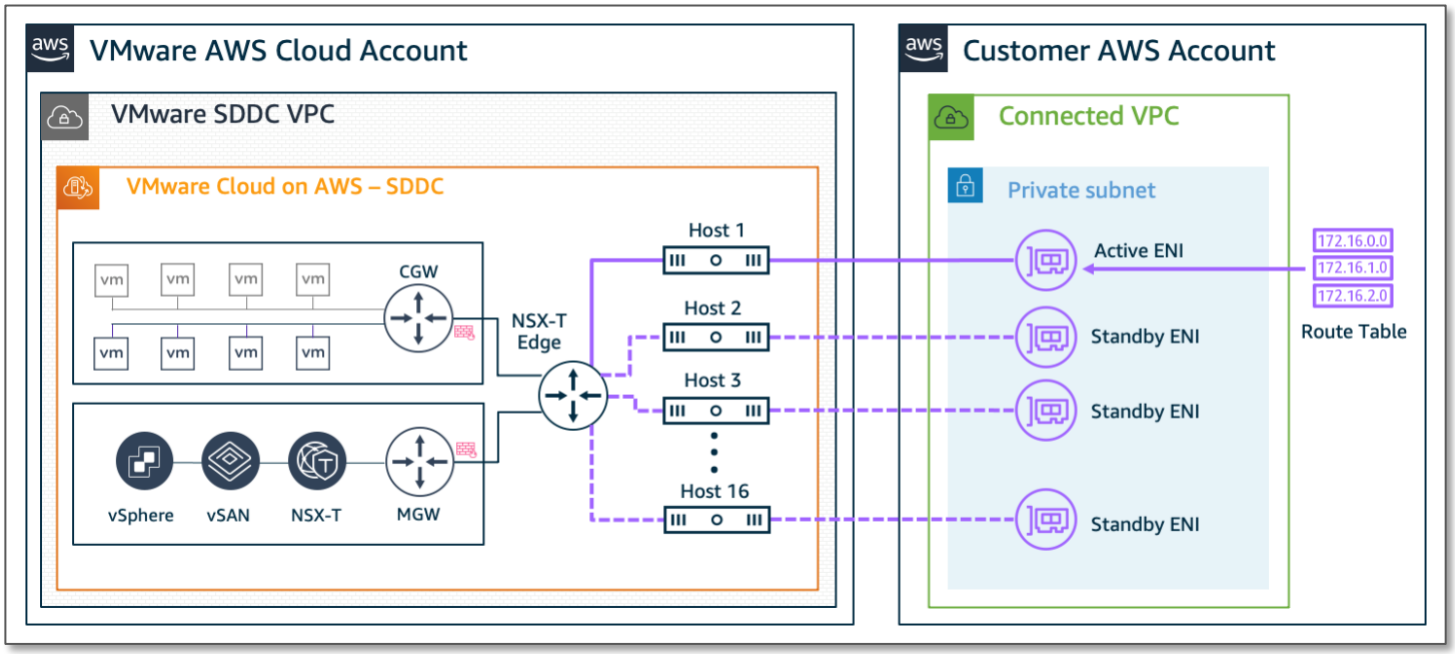


VMware Cloud on AWS is an ideal solution for some common seen industrial use cases:

- **Cloud Migration** – With VMware Cloud Foundation services, customers can seamlessly migrate their critical workloads to SDDCs deployed on AWS cloud platform.
- **Disaster Recovery** – With VMware Site Recovery Manager, VMware DR Technologies combined with High Availability, Scalability provided by AWS.
- **Sustainability** – Reduction of dependent hardware resources, rapid scalability provided by AWS increases power, resource usage effectiveness; hence reducing carbon footprint and increasing sustainability of the environment.

Architectural Overview

The following figure shows connectivity between a deployed SDDC and a Customer Account VPC configured during the deployment process. Using the Amazon Virtual Private Cloud (VPC), virtual machines (VMs) deployed in the SDDC can be integrated with the various services offered by AWS.

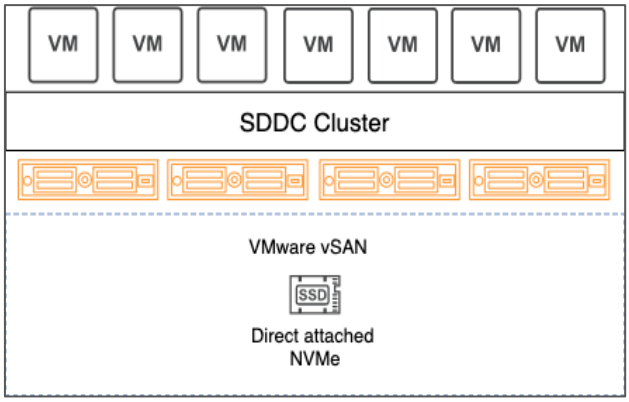


Elastic Network Interface (ENI) provided in the SDDC is responsible for this connection between the workload VMs and AWS services present in the VPC. ENI also has some restrictions; it does not allow to connect the SDDC to other VPC as well as to the internet. There are some solutions provided by AWS if you require to connect your SDDC to other configured VPCs.

Here we can also see the NSX virtually distributed into compute gateway and management gateway. Workload VMs are configured to the compute gateway whereas management components (vSphere, vSAN, NSX) are configured on the management gateway.

Storage Design

The following figure is an architectural diagram of Direct Attached Storage (DAS) using VMware vSAN, one of the four storage options offered by VMware Cloud on AWS. vSAN provides storage with high performance and consistency that proves to be helpful in cloud migration or as an extension to your existent data center.



On the AWS front, vSAN uses Amazon Elastic Compute Cloud (EC2) bare-metal instances. Underlying locally attached Non-Volatile Memory Express (NVMe) flash storage is present. A single distributed vSphere datastore is made by pooling together the storage offered by the EC2 instances. This datastore is then logically divided into two parts, vsandatastore and WorkloadDatastore. These datastores can be seen in the deployed SDDC. Datastore vsandatastore hosts the management components such as vSphere and NSX, whereas WorkloadDatastore is used for storing your Workload virtual machines, corresponding vmdk files, and configuration files. This unique segregation feature provided by vSAN is specifically aimed towards restricting permissions towards the management components present in vsandatastore.

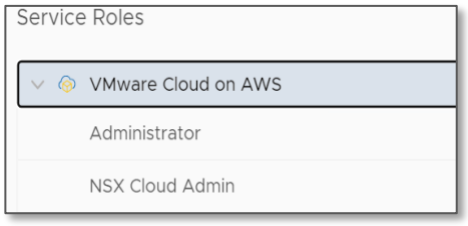
SDCC Deployment Prerequisites

The following are required for deploying a SDDC in VMware Cloud on AWS:

- **MyVMware Account**
  An up-to-date MyVMware account is required.
  You can create an account here: https://vmc.vmware.com/home

- **AWS Account**
  All deployed SDDCs must be linked to an AWS account.

- **VMware Cloud on AWS Account Roles**
  The following roles must be enabled for the account:
  - Administrator
  - NSX Cloud Administrator



- **SDDC Architectural Requirements**
  For SDDC planning and deployment, refer to the following:
  https://docs.aws.amazon.com/whitepapers/latest/sddc-deployment-and-best-practices/account-requirements.html

Creation of SDDC

Log into the VMC Console: https://vmc.vmware.com

The first section allows you to configure the following SDDC properties:

- **AWS Region**
  An AWS region must be selected for the SDDC to be deployed in. VMware Cloud on AWS is not supported in all AWS regions. Refer to the following: AWS Region and Availability Zone Support (vmware.com)

- **Deployment**
  Deployment type can be Single-Host, Multiple Hosts, or Stretched Cluster. This service offers you clusters between 2 and 16 hosts with up to 20 clusters per SDDC. You can also create stretched clusters between Multiple Availability Zones.

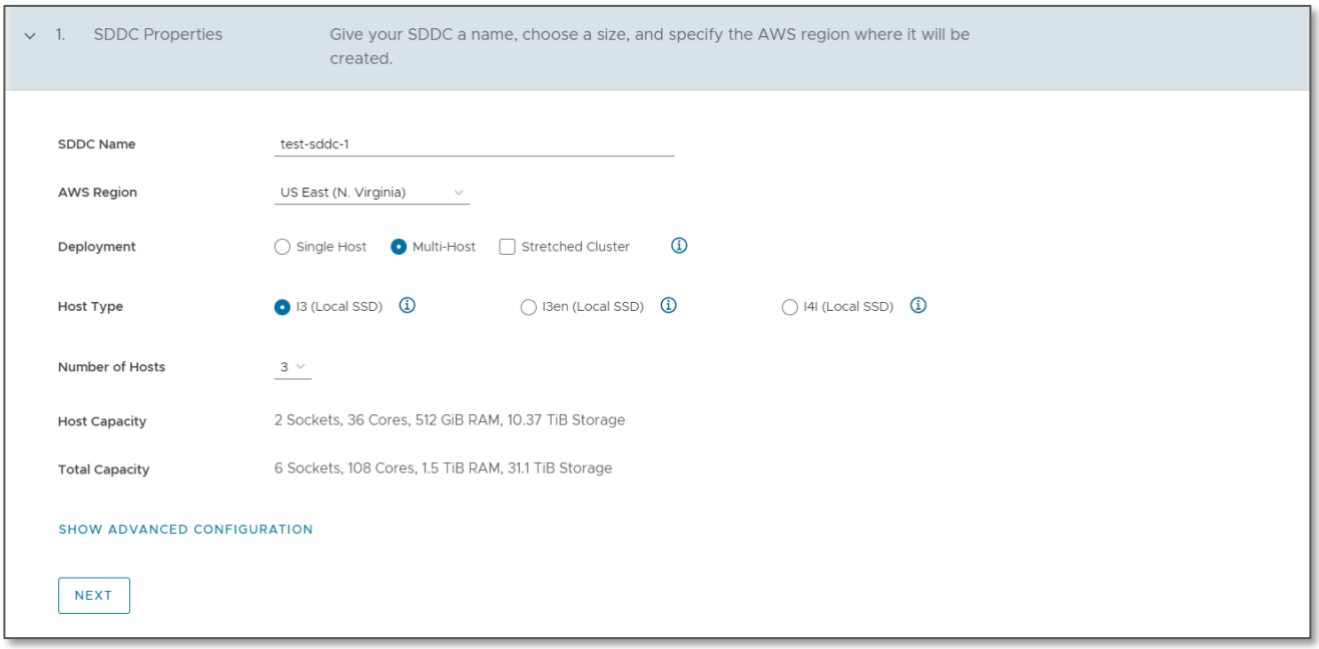
- **Host Type**
  You can select i3, i3en or i4l depending on the number of resources you need. i3 is the default option. For data intensive workloads, i3en is an optimal choice.

- **SDDC Name**
  You must provide a Display name for the SDDC. It does not reflect the vCentre or the cluster name.

- **Number of Hosts**
  If multi-host deployment is selected, the number of hosts must be mentioned here. Hosts can be added or removed later.

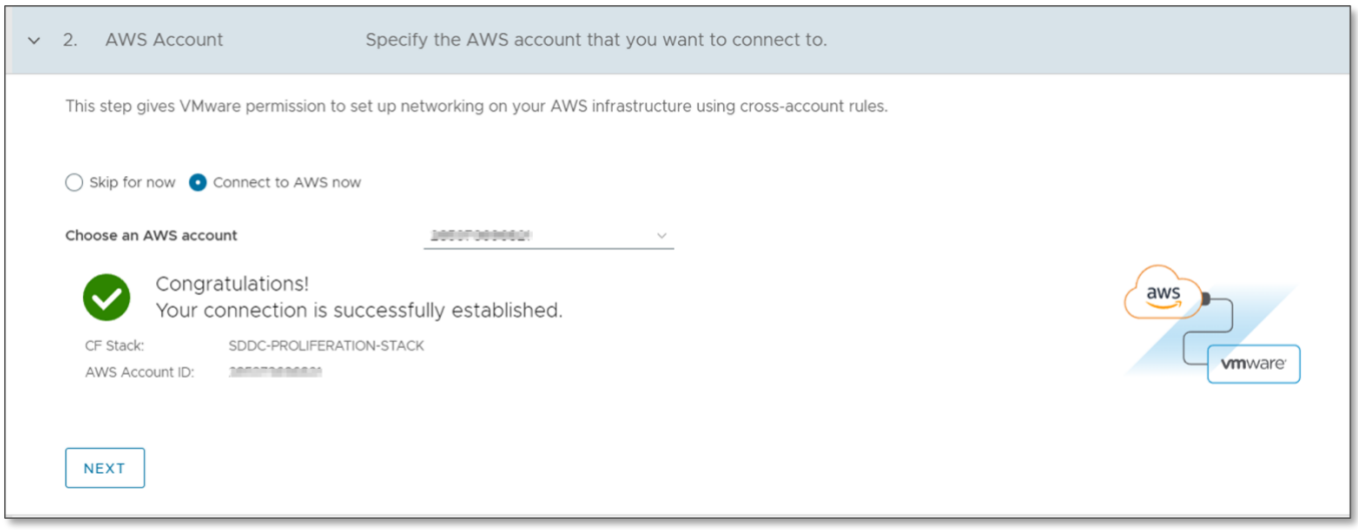
- **Host Capacity and Total Capacity**
  Changes will be reflected here depending on the number of hosts mentioned in the previous section.

- **Show Advanced Configuration**
  This is an optional section to configure the size (Medium or Large) of the SDDC. The default option is Medium. If you plan to deploy more than 30 hosts, or 3000 desktops, you can choose the Large option.



The next section is to configure the AWS Account:

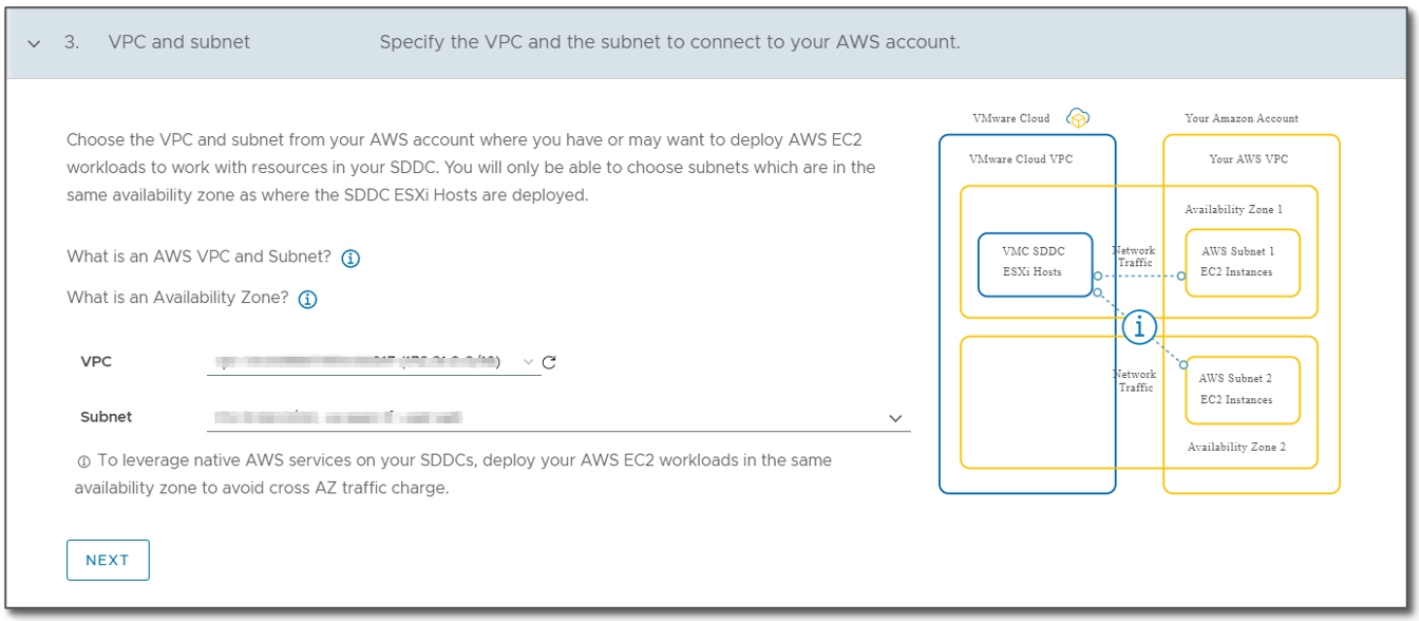
- **Connect to a new AWS Account**
  Select an AWS account from the drop-down menu. This allows networking between this SDDC and the AWS infrastructure.



The next section is to configure Virtual Private Cloud (VPC) and subnet to connect to the AWS Account:

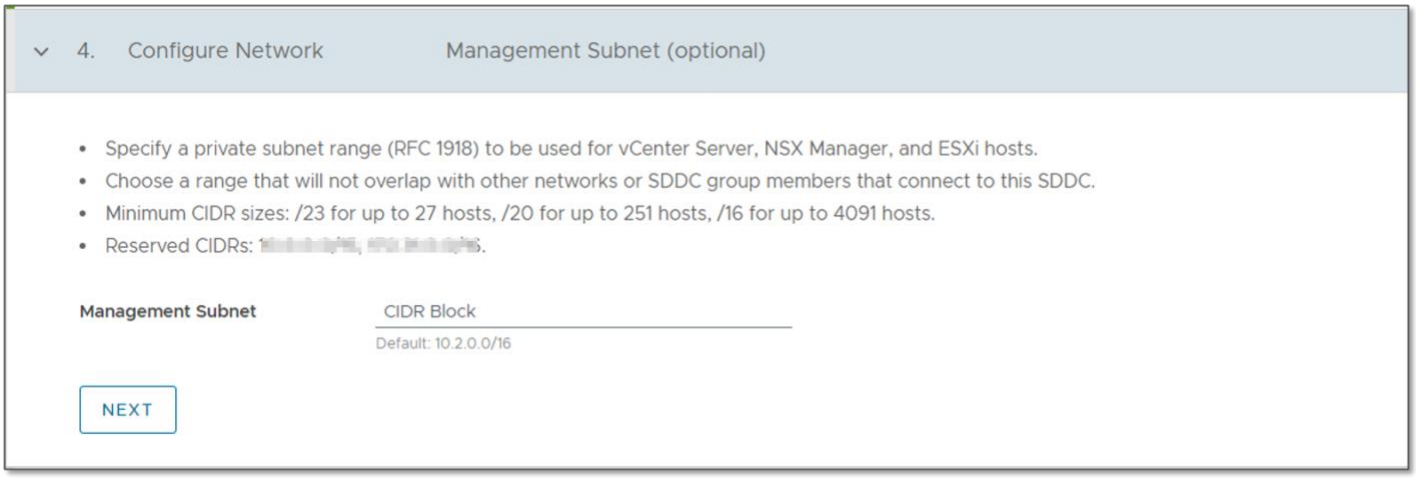
- **VPC**
  Choose a VPC from the drop-down menu. This enlists all the VPCs associated with the AWS account mentioned earlier.

- **Subnet**
  Select the required subnet. The available options in the drop-down menu will be auto-generated depending on the VPC selected.

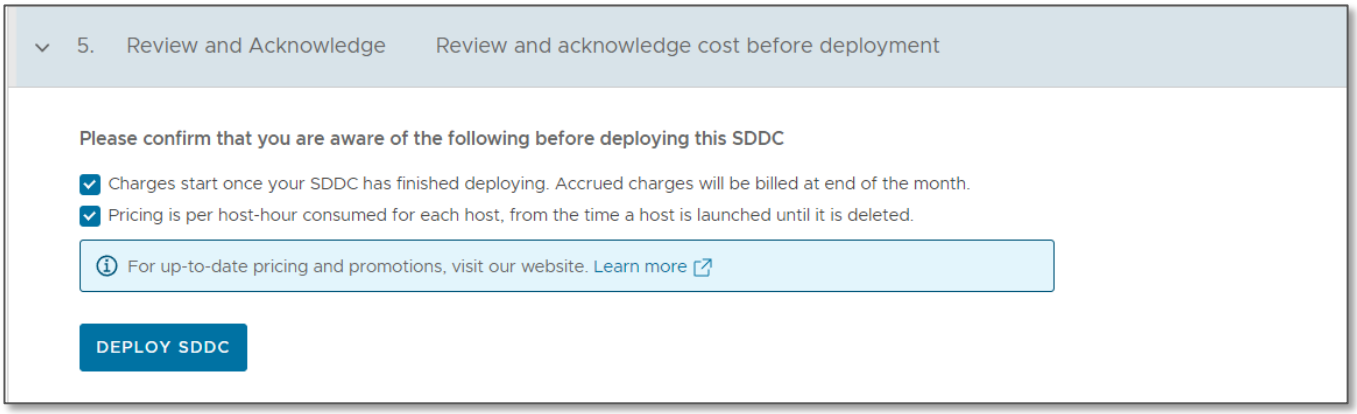


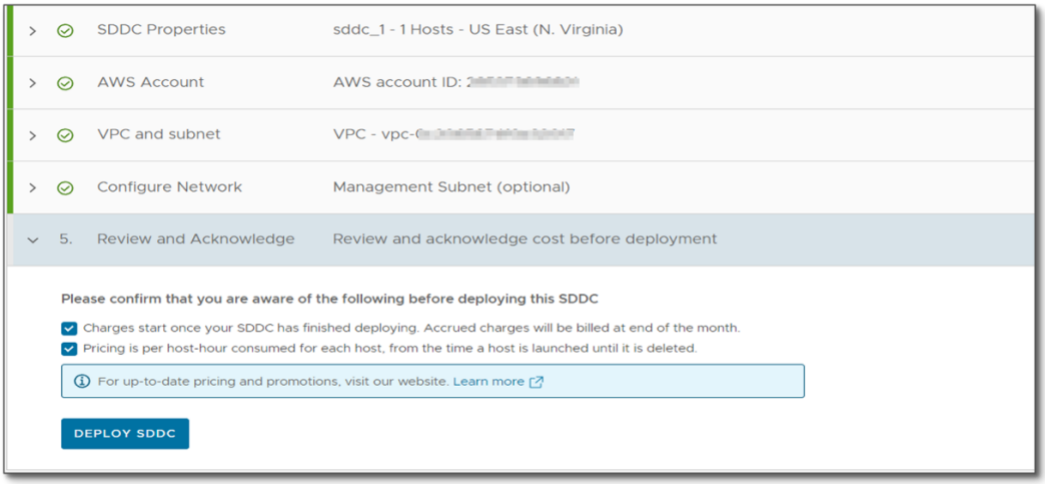
The next section is to configure the network:

- **Management Subnet**
  This is an optional step where you can specify a private subnet range that will be used for the vCenter Server, NSX Manager, and the ESXi hosts. There are few reserved CIDR used by VMware which should not be used.

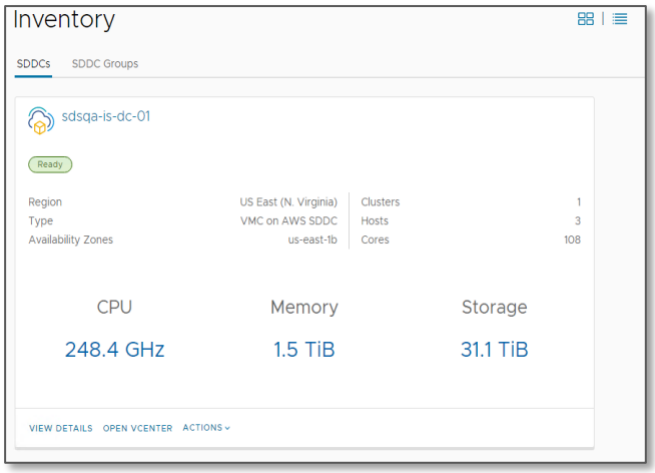


The next section is to review all the selected options and then acknowledge the cost before deployment:





After a successful deployment, you can see the SDDC in the inventory section:



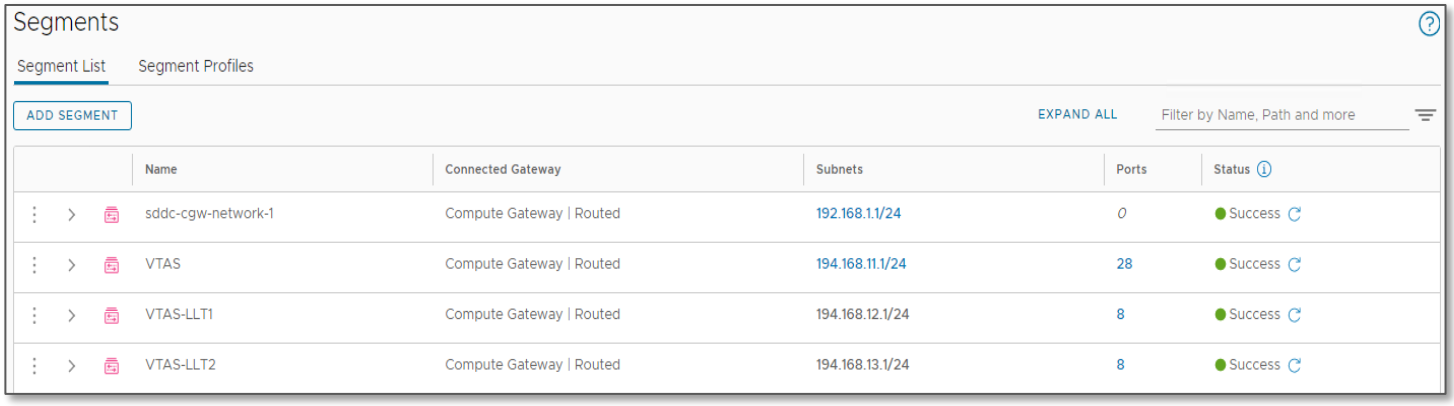
On-Prem vSphere vs VMC SDDC vSphere

On-prem vSphere	SDDC vSphere
Administrator privileges are present with user.	The highest level of privilege provided is cloudadmin. The administrator access is restricted to VMware.
Can access and perform operations on the ESXi hosts present in the SDDC.	No privilege to access the ESXi host operating system. Procedures that require this kind of access are performed by VMware staff.
Can create Virtual Switches, Datastores, and can also add RDMP disks in the SDDC.	Privileges are restricted to virtual machines itself. Segments can be created, like virtual switches. No privileges to create datastores. Does not support creation of RDMP disks.
No firewall rules required to be set by the user.	Firewall rules, inbound and outbound rules for access to the virtual machines, vCentre must be set by the user.
VMware and InfoScale coexistent features such as vSphere HA, vSphere DRS, vMotion on storage level can be tested here.	Due to restricted access to ESXi hosts and datacenter, tests with features such as vMotion on storage level, vSphere HA, and vSphere DRS cannot be performed as in an on-premises environment.

Network and Security Configurations

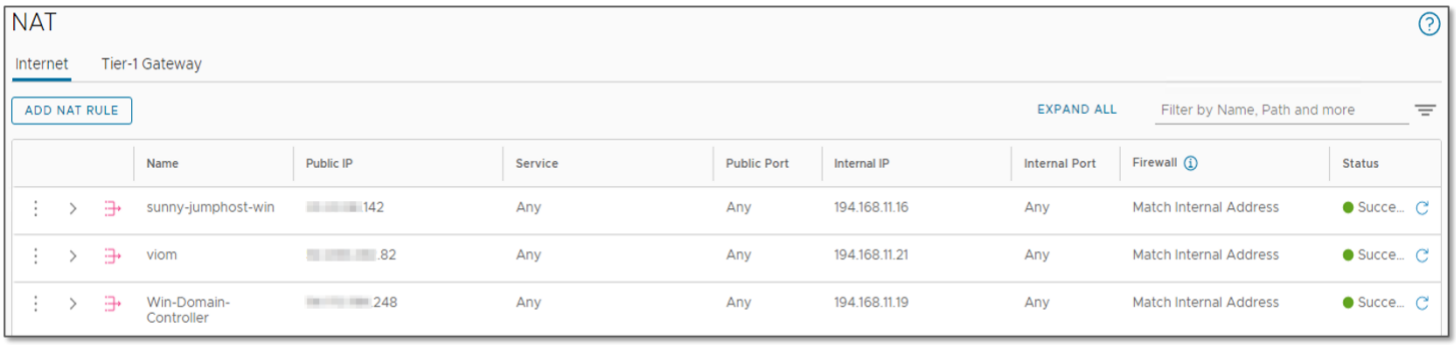
Segments

- Network Segments work as logical networks and are used by the workload VMs.
- A single Host Starter SDDC comes with a single routed network segment named sddc-cgw- network-1.
- Multi-host SDDCs do not have a default network segment. You must create at least one for your workload VMs.
- Three types of network segments can be configured – Routed (Default), Extended, Disconnected.
- You can also delete or modify the parameters of an existing segment.



NAT

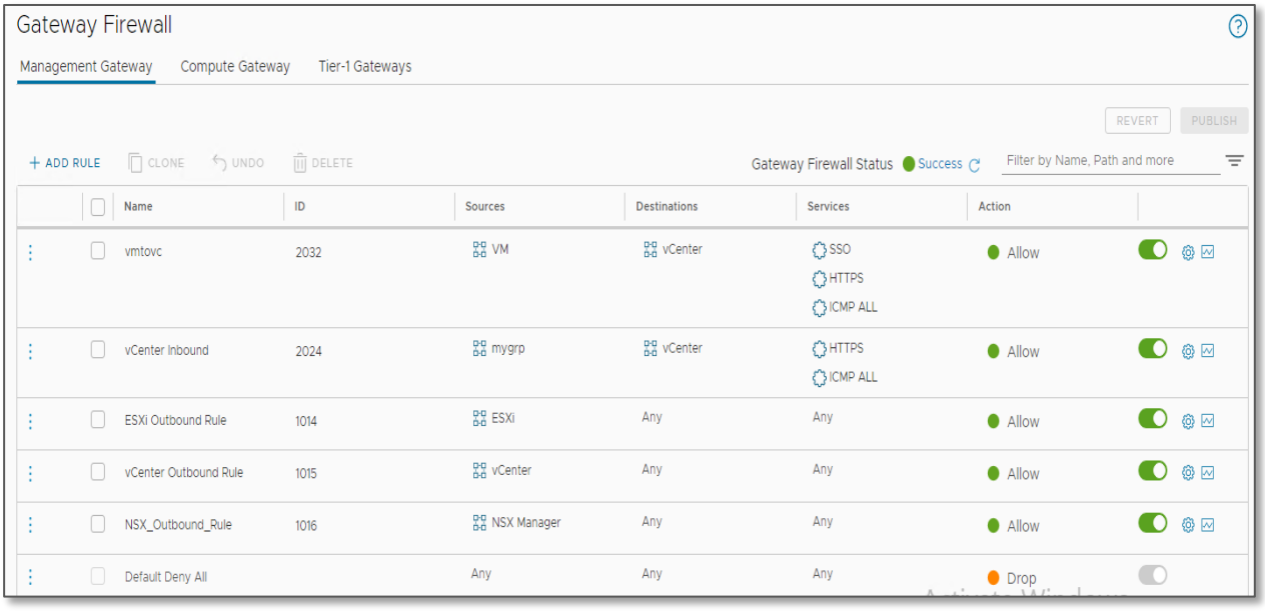
- Network Address Translation (NAT) controls how IP addresses in packet headers appear on either side of a gateway.
- Internet interface (the Compute Gateway) maps internal source or destination IP addresses on packets from compute network segments to addresses that are usable on the public Internet.
- Tier-1 gateways map traffic between the gateway and other SDDC network interfaces.
- You provide an existing internal IP of a machine and map it to an external IP of your choice.



Gateway Firewall

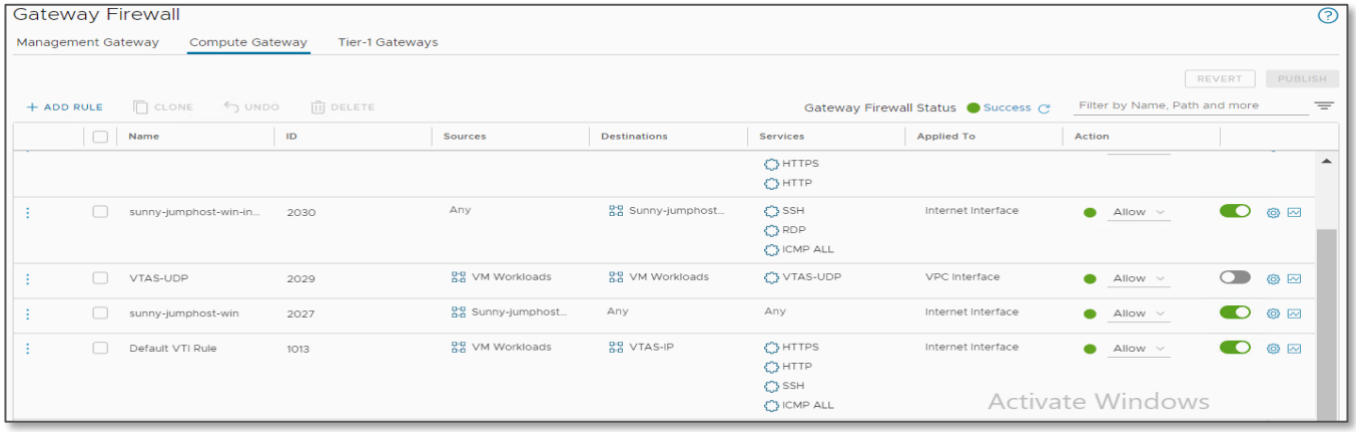
1. Management Gateway

    - Blocks traffic to all management network destinations from all sources.
    - Specify actions to take on network traffic from a specified source to a specified destination. Either the source or destination must be a system-defined inventory group such as vCentre, NSX Manager, or ESXi Hosts.



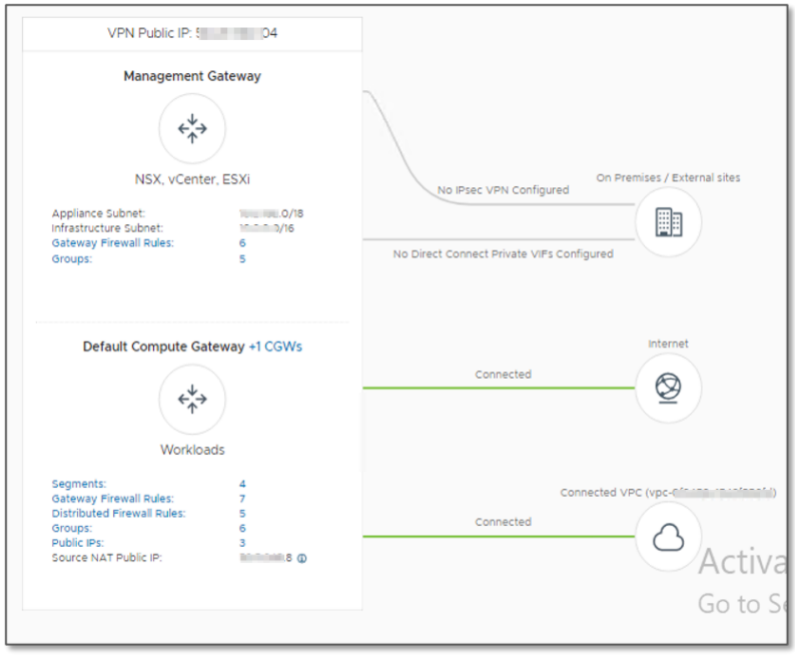
2. Compute Gateway

    - Specify actions to take on network traffic from a specified source to a specified destination. Sources and destinations can be chosen from a list of a physical network interfaces.
    - Actions can be either Allow or Drop.



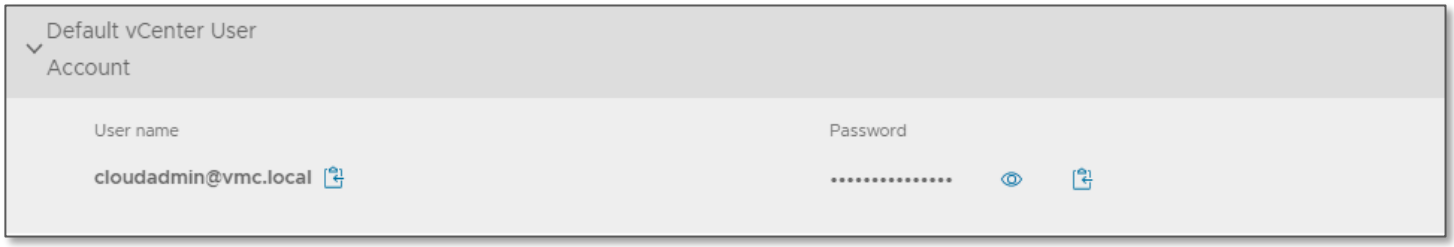
- **Groups** - Management, Compute inventory groups
- **Services** - ICMP, HTTP, HTTPS, etc.
- **Public IPs** – Raise a request to generate public IP addresses. These IP addresses will then be used to create NAT rules.

The following diagram in the vCentre server displays all the network configurations:



vCentre Details

- On the VMware Cloud on AWS console, we can find the public IP and vCenter FQDN that can be used to access the vCentre after a successful deployment.
- The default login credentials for the vCentre are also mentioned here. The username is CloudAdmin. This is the highest privilege given to user in VMware Cloud on AWS. Administrator privileges remain with VMware.
- CloudAdmin can create, clone, and modify network rules, Workload virtual machines. This user cannot configure management components like hosts, cluster, or ESXi. These are managed solely by VMware.



InfoScale Installation and Configuration

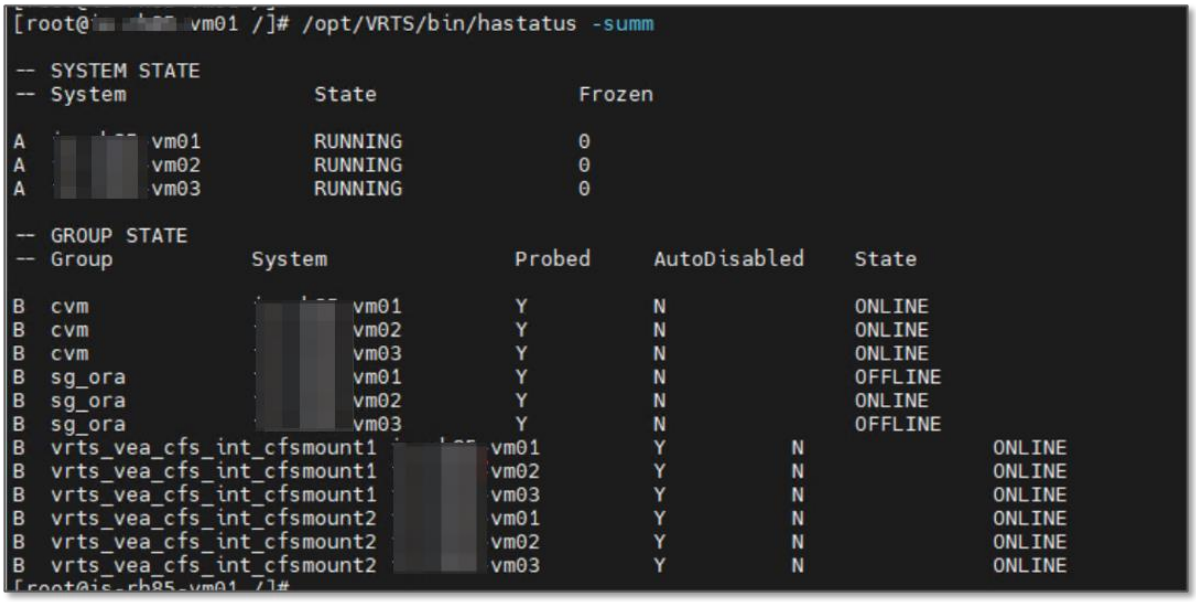
Use the Common Product Installer (CPI) to install InfoScale Enterprise on the systems that you want to configure as the InfoScale cluster nodes. For details on InfoScale installation, refer to the *Veritas InfoScale Installation Guide*.

After the successful installation and configuration of InfoScale Enterprise and the application, you can obtain the details about all the service groups, including the application service groups.

Configure an InfoScale cluster by configuring LLT using UDP protocol. LLT uses UDP sockets for communication among the cluster nodes and creates one UDP socket for each LLT link.

In Flexible Storage Sharing (FSS) environments, read-write operations may be performed on remote disks, and one socket per LLT link may not be enough for large data volumes.

The following screenshots can be referred as they are taken from a test bed created in VMC running in AWS cloud:



```
vm-0001.novalocal:/root>lltstat -nvv active
LLT node information:
    Node                 State    Link  Status  Address
   * 0                   vm-0001 OPEN
                                  eth1    UP      [redacted].55
                                  eth2    UP      [redacted].55
     1                   vm-0002 OPEN
                                  eth1    UP      [redacted].56
                                  eth2    UP      [redacted].56
                         vm-0001.novalocal:/root>gabconfig -a
GAB Port Memberships
===============================================================
Port a gen     9802 membership 01
Port b gen     9805 membership 01
Port d gen     9801 membership 01
Port f gen     9843 membership 01
Port h gen     9839 membership 01
Port m gen     983b membership 01
Port u gen     9841 membership 01
Port v gen     983d membership 01
Port w gen     983f membership 01
Port y gen     983c membership 01
```

```
[root@[redacted]-01 ~]# vxfenadm -d

I/O Fencing Cluster Information:
================================

 Fencing Protocol Version: 201
 Fencing Mode: Customized
 Fencing Mechanism: cps
 Cluster Members:

        * 0 ([redacted]-01)
          1 ([redacted]-02)
          2 ([redacted]-03)

 RFSM State Information:
        node   0 in state  8 (running)
        node   1 in state  8 (running)
        node   2 in state  8 (running)
```

Implemented Test Scenarios on Linux

3-node SFCFSHA Cluster - FSS Setup

- Oracle Fast Failover with / without workload
- vMotion with workload

3-node SFCFSHA Cluster - Shared disks

- CFSMount with Workload
- CPS Based Fencing

2-node SFCFSHA Cluster

- VMware Disk Agent with Oracle

Implemented Test Scenarios on Windows

2 Node MSCS cluster with MSSQL - SCSI-3 disks

- Failover failback of SQL server

2 Node VCS cluster with MSSQL - SCSI-3 disks

- MSSQL resource, VMDG and MountV resource testing with failover failback

2 Node VCS cluster with fileshare application - SCSI-3 disks

- Shared disks - VMDG and Mountv
- Non-Shared disks - VMNSDG and Mountv

All the above systems have been tested for Splitbrain, reboot, shutdown and panic node scenarios

- Additionally, Veritas InfoScale Operations Manager (VIOM) is also deployed on a virtual machine and all the InfoScale clusters mentioned earlier have been added to it.

Conclusion

This document discussed the process of designing and deploying a SDDC on VMWare Cloud on AWS environment and then further deploying InfoScale Enterprise on virtual machines prepared on the SDDC.

It is intended to help understand the extent to which Veritas InfoScale is supported on VMware Cloud on AWS. This will assist in a seamless cloud migration of workloads from on-prem to VMware Cloud as well as in scenarios where disaster recovery is required. A reduction in hardware dependency further improves the sustainability in the organization.

Furthermore, various VMware InfoScale coexistent features have been tested on both Linux and Windows machines. All clusters have also been added to VIOM deployed in the same vCentre.

Prerequisites, requirements, and steps involved in the SDDC deployment have been included. Necessary configurations related to networking and security to be performed by the user have also been mentioned. There are some limitations when it comes to VMware Cloud on AWS, which have been discussed.

As organizations are moving towards incorporating cloud environments for their deployments and workloads, VMware Cloud on AWS is one such environment where SDDCs are deployed on underlying AWS infrastructure. Veritas InfoScale can help use the storage effectively in such cloud deployments and further increase resiliency of applications present there.

References

VMware Cloud on AWS Documentation

https://aws.amazon.com/blogs/architecture/augmenting-vmware-cloud-on-aws-workloads-with-native-aws-services/

Storage options and designs for VMware Cloud on AWS | AWS Storage Blog (amazon.com)

VMware Cloud on AWS Networking and Security - VMware Cloud on AWS

Roles and Permissions in the SDDC (vmware.com)

VMware Cloud on AWS Networking and Security - VMware Cloud on AWS

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at veritas.com or follow us on Twitter at @veritastechllc.

Veritas World Headquarters
2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices
and contact numbers,
please visit our website.