Oracle Workloads on VMware Hybrid Multi-Clouds

REFERENCE ARCHITECTURE

vmware®

Table of contents

Oracle Workloads on VMware Hybrid Multi-Clouds

Customers have successfully run business-critical Oracle workloads with high performance demands on VMware® vSphere® for many years.

Customers deploying business-critical Oracle workloads must often do so while managing to stringent SLAs, continuing to deliver high levels of performance, and maintaining application availability. Managing data storage in this context is a significant challenge, as traditional storage solutions for business-critical applications come with a variety of issues to overcome, including inadequate performance and scalability, storage inefficiency, management complexity, and excessive deployment and operating costs.

With more and more production servers being virtualized, the demand for highly converged server-based storage is surging. VMware vSAN™ is designed to provide highly scalable, available, reliable, and high-performance storage using cost-effective hardware (i.e., direct-attached disks in VMware ESXi™ hosts). vSAN adheres to a new policy-based storage management paradigm, simplifying and automating the complex management workflows of traditional enterprise storage systems with respect to configuration and clustering.

vSAN Stretched Cluster enables active/active data centers that are separated by metro distance.

VMware Cloud™ on AWS is an on-demand service that enables customers to run applications across VMware vSphere cloud environments with access to a broad range of AWS services. Powered by VMware Cloud Foundation™, this service integrates vSphere, vSAN and VMware NSX® along with VMware vCenter® management, and is optimized to run on dedicated, elastic, bare-metal AWS infrastructure. ESXi hosts in VMware Cloud on AWS reside in an AWS availability zone (AZ) and are protected by vSphere High Availability (HA).

Stretched Clusters for VMware Cloud on AWS is designed to protect against an AWS AZ failure. With Stretched Clusters for VMware Cloud on AWS, business-critical Oracle workloads with exceptionally high SLA, performance, and application availability requirements can take advantage of cloud deployment while simultaneously achieving high availability across multiple AZs.

Solution Overview

This paper describes the deployment, migration, and configuration of business-critical Oracle workloads on VMware Cloud on AWS and Stretched Clusters for VMware Cloud on AWS.

Key Results

The following highlights summarize the deployment and migration strategies available for moving Oracle workloads to VMware Cloud on AWS:

- Deploying Oracle workloads on VMware Cloud on AWS
- Migrating Oracle workloads from VMware on-premises to VMware Cloud on AWS
- Deploying Oracle workloads on Stretched Clusters for VMware Cloud on AWS

Introduction

Purpose

This paper describes the strategies and best practices for deploying or migrating Oracle workloads from on-premises to VMware Cloud on AWS and Stretched Clusters for VMware Cloud on AWS.

Scope

This reference architecture outlines the deployment and migration strategies and use cases involved in movement of Oracle workloads to VMware Cloud on AWS.

- Deploying Oracle workloads on VMware Cloud on AWS
- Migrating Oracle workloads from VMware on-premises to VMware Cloud on AWS
- Deploying Oracle workloads on Stretched Clusters for VMware Cloud on AWS

Audience

This reference architecture is intended for Oracle database administrators, virtualization and storage architects, or others involved in planning, architecting, and administering Oracle workloads on a VMware SDCC platform, with plans to transition to VMware Cloud on AWS.

Terminology

This paper includes the following terminology:

TERM	DEFINITION
Oracle Single Instance	Oracle Single-Instance database consists of a set of memory structures, background processes, and physical database files, which serves the database users.
Oracle Automatic Storage Management (Oracle ASM)	Oracle ASM is a volume manager and a file system for Oracle database files that support Single-Instance Oracle Database and Oracle Real Application Cluster (RAC) configurations.
Oracle ASMLIB and Oracle ASMFD	Oracle ASMLIB maintains permissions and disk labels that are persistent on the storage device, so that the label is available even after an operating system upgrade. Oracle ASMFD helps prevent corruption in Oracle ASM disks and files within the disk group.

TABLE 1. Terminology

Technology Overview

This section provides an overview of the technologies used in this solution:

- VMware vSphere
- VMware vSAN
- VMware vSAN Storage Policy
- VMware Virtual Disk Provisioning Policies
- Storage Policy-Based Management
- VMware vSAN Stretched Cluster
- VMware SDDC
- Hybrid and Multi-Cloud as the VMware Cloud
- VMware Cloud on AWS
- Stretched Clusters for VMware Cloud on AWS
- VMware Cloud on Dell EMC
- Google Cloud VMware Engine
- Azure VMware Solution
- Oracle Cloud VMware Solution
- VMware Hybrid Cloud Extension
- Oracle Database Architecture
- Oracle ASM, ASMLIB and ASMFD

VMware vSphere

VMware vSphere, the industry-leading virtualization and cloud platform, is the efficient and secure platform for hybrid clouds, accelerating digital transformation by delivering simple and efficient management at scale, comprehensive built-in security, a universal application platform, and a seamless hybrid cloud experience. The result is a scalable, secure infrastructure that provides enhanced application performance and can be the foundation of any cloud.

As the next-generation infrastructure for next-generation applications, vSphere 7.0 has been rearchitected with native Kubernetes, enabling IT admins to use VMware vCenter Server® to operate Kubernetes clusters through namespaces. VMware vSphere with Tanzu allows IT admins to leverage their existing skillset to deliver self-service infrastructure access to their DevOps teams, while providing observability and troubleshooting of Kubernetes workloads. vSphere 7 provides an enterprise platform for both traditional and modern applications, enabling customers and partners to deliver a developer-ready infrastructure, scale without compromise, and simplify operations.

Learn more about *VMware vSphere 7.0*.

VMware vSAN

VMware vSAN is a software-defined storage solution, built from the ground up, for vSphere VMs.

It abstracts and aggregates locally attached disks in a vSphere cluster to create a storage solution that can be provisioned and managed from vCenter and the vSphere client. vSAN is embedded within the hypervisor, hence storage and compute for VMs are delivered from the same x86 server platform running the hypervisor.

Hyperconverged infrastructure (HCI) backed by VMware vSAN provides a wide array of deployment options, from a two-node setup to a standard cluster supporting up to 64 hosts. Also, vSAN accommodates a stretched cluster topology to serve as an active-active disaster recovery solution. vSAN includes HCI Mesh, which allows customers to remotely mount a vSAN datastore to other vSAN clusters, disaggregating storage and compute. This allows greater flexibility to scale storage and compute independently.

Learn more about *VMware vSAN*.

VMware vSAN Storage Policy

vSAN requires VMs deployed on vSAN datastores be assigned at least one storage policy. When provisioning a VM, if you do not explicitly assign a storage policy to the VM, the vSAN default storage policy is assigned.

The default policy contains vSAN rule sets and a range of basic storage capabilities typically used for the placement of VMs deployed on vSAN datastores.

vSAN Default Storage Policy Specifications

Specification	Setting
Primary level of failures to tolerate	1
Number of disk stripes per object	1
Flash read cache reservation, or flash capacity used for the read cache	0
Object space reservation	0 **Note:** Setting the Object space reservation to zero means that the virtual disk is thin provisioned, by default.
Force provisioning	No

FIGURE 1. Default vSAN Storage Policy

Key storage policy rules:

STORAGE POLICY	DESCRIPTION
Number of Failures to tolerate	Defines the number of host, disk, or network failures a VM object can tolerate. For n failures tolerated, n+1 copies of the VM object are created and 2n+1 hosts with storage are required. The settings applied to the VMs on the Virtual SAN datastore determines the datastore's usable capacity.
Object Space Reservation (OSR)	Percentage of the object logical size that should be reserved during the object creation. The default value is 0 percent and the maximum value is 100 percent.
Number of disk stripes per object	This policy defines how many physical disks across each copy of a storage object are striped. The default value is 1 and the maximum value is 12.
Flash read cache reservation	Flash capacity reserved as read cache for the VM object. Specified as a percentage of the logical size of the VMDK object. It is set to 0 percent by default and Virtual SAN dynamically allocates read cache to storage objects on demand.

TABLE 2. Key Storage Policy Rules

Object Space Reservation (OSR) – an administrator should always be aware of over-committing storage on vSAN, just as one needs to monitor over-commitment on a traditional SAN or NAS array.

By default, VM storage objects deployed on vSAN are **thinly provisioned**. This capability, *ObjectSpaceReservation*, specifies the percentage of the logical size of the storage object that should be reserved (thick provisioned) when the VM is being provisioned. The rest of the storage object will remain thin provisioned. The default value is 0%, implying the object is deployed as thin. The maximum value is 100%, meaning the space for the object is fully reserved, which can be thought of as full, thick provisioned. Since the default is 0%, all VMs deployed on vSAN are provisioned as thin disks unless one explicitly states a requirement for *ObjectSpaceReservation* in the policy. If *ObjectSpaceReservation* is specified, a portion of the storage object associated with that policy is reserved.

There is no eager-zeroed thick format on vSAN. OSR, when used, behaves similarly to lazy-zeroed thick.

More information on vSAN Object Space Reservation (OSR) can be found in the *VMware vSAN Design Guide*.

Learn more about *vSAN Default Storage Policy*.

VMware Virtual Disk Provisioning Policies

When performing certain VM management operations, it's possible to specify a provisioning policy for the virtual disk file. The operations include creating a virtual disk, cloning a VM to a template, or migrating a VM with VMware vSphere® Storage vMotion®.

You can also use VMware vSphere Storage vMotion or cross-host vSphere Storage vMotion to transform virtual disks from one format to another.

OPTION	DESCRIPTION
Thick Provision Lazy Zeroed	Creates a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation but is zeroed out on demand later on first write from the VM. VMs do not read stale data from the physical device.

Thick Provision Eager Zeroed (EZT)	A type of thick virtual disk that supports clustering features such as the multi-writer attribute for Oracle shared disk in an oracle cluster. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. Creating virtual disks in this format may take longer than creation of other types of disks. Increasing the size of an eager zeroed thick virtual disk causes a significant stun time for the VM.
Thin Provision	Use this format to save storage space. For the thin disk, provision as much datastore space as the disk would require based on the value entered for the virtual disk size. The thin disk starts small and, at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it. Thin provisioning is the fastest method to create a virtual disk because it creates a disk with only the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed.

TABLE 3. Virtual Disk Formats Available in vSphere Storage vMotion

VMDK modes are shown in the table below:

OPTION	DESCRIPTION
Dependent	Dependent disks are included in snapshots.
Independent-persistent	Disks in persistent mode behave like conventional disks on a physical computer. All data written to a disk in persistent mode is written permanently to the disk.
Independent– non-persistent	Changes to disks in non-persistent mode are discarded when the VM is turned off or reset. Non-persistent mode enables restarting of the VM with a virtual disk in the same state every time. Changes to the disk are written to and read from a redo log file that is deleted when the VM is turned off or reset.

TABLE 4. VMDK Modes

Learn more about *VMware virtual disk provisioning policies*.

Storage Policy-Based Management (SPBM)

Within a software-defined data center (SDDC), storage policy based management (SPBM) plays a significant role, helping to align storage with the application demands of your VMs. SPBM provides a storage policy framework that serves as a single unified control panel across a broad range of data services and storage solutions.

As an abstraction layer, SPBM abstracts storage services delivered by VMware vSphere® Virtual Volumes™, vSAN, I/O filters, or other storage entities.

Rather than integrating with each individual type of storage and data services, SPBM provides a universal framework for different types of storage.

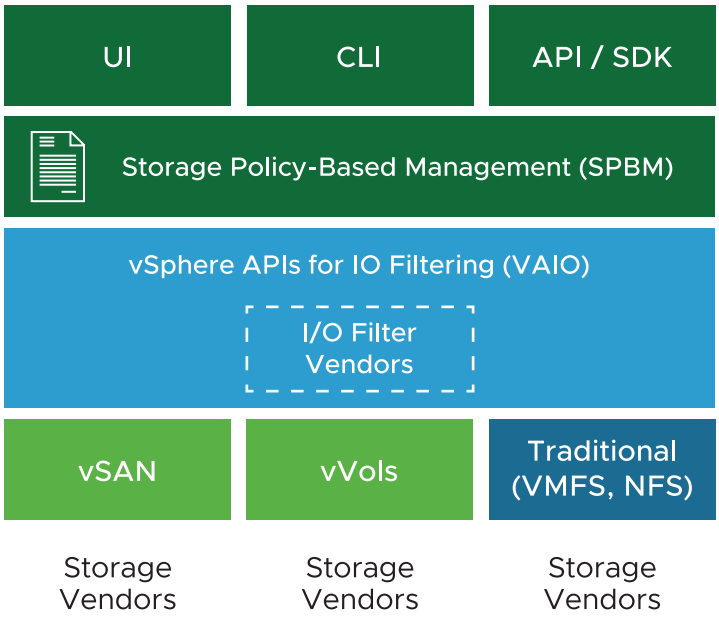


FIGURE 2. Storage Policy-Based Management (SPBM)

SPBM offers the following mechanisms:

- Promotion of storage capabilities and data services that storage arrays and other entities, such as I/O filters, offer
- Bidirectional communications between ESXi and vCenter Server on one side with storage arrays and entities on the other
- VM provisioning based on VM storage policies

Learn more about *Storage Policy-Based Management*.

VMware vSAN Stretched Cluster

Stretched clusters extend the vSAN cluster from a single data site to two sites for a faster level of availability and intersite load balancing. Stretched clusters are typically deployed in environments where the distance between data centers is limited, such as metropolitan or campus environments.

You can use stretched clusters to manage planned maintenance and avoid disaster scenarios, because maintenance or loss of one site does not affect the overall operation of the cluster. In a stretched cluster configuration, both data sites are active sites. If either site fails, vSAN uses the storage on the other site. vSphere HA restarts any VM that must be restarted on the remaining active site.

You must designate one site as the preferred site. The other site becomes a secondary or nonpreferred site. If the network connection between the two active sites is lost, vSAN continues operation with the preferred site. The site designated as preferred typically is the one that remains in operation unless it is resyncing or has another issue. The site that leads to maximum data availability is the one that remains in operation.

A vSAN stretched cluster can tolerate one link failure at a time without data becoming unavailable. A link failure is a loss of network connection between the two sites or between one site and the witness host. During a site failure or loss of network connection, vSAN automatically switches to fully functional sites.

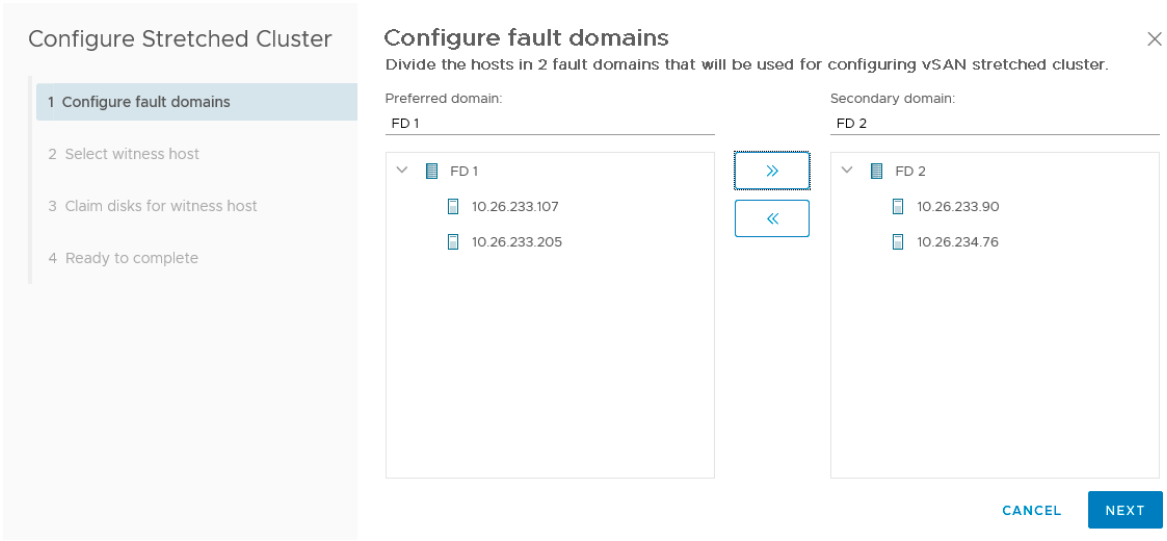


FIGURE 3. vSAN Stretched Cluster

Each stretched cluster consists of two data sites and one witness host. The witness host resides at a third site and contains the witness components of VM objects. It contains only metadata and does not participate in storage operations.

The witness host serves as a tiebreaker when a decision must be made regarding availability of datastore components and the network connection between the two sites is lost. In this case, the witness host typically forms a vSAN cluster with the preferred site. But if the preferred site becomes isolated from the secondary site and the witness, the witness host forms a cluster using the secondary site. When the preferred site is online again, data is resynchronized to ensure that both sites have the latest copies of all data.

More information on vSAN Stretched Cluster can be found *here* and *here*.

VMware SDDC

The mobile cloud era is changing line-of-business expectations of IT. For IT organizations to securely deliver the anticipated improvements in service quality and speed, a software-defined data center (SDDC) approach is required. The VMware approach to the SDDC delivers a unified platform that supports any application and provides flexible control.

The VMware architecture for the SDDC empowers companies to run hybrid clouds and to leverage unique capabilities to deliver key outcomes that enable efficiency, agility, and security. Enterprises using VMware technology have three ways to establish an SDDC and transition at their own pace: build their own using reference architectures, use a converged infrastructure, or use a hyper-converged infrastructure for which the full SDDC is delivered already implemented on the customer's hardware of choice.

Learn more about *VMware SDDC*.

Hybrid and Multi-Cloud as the VMware Cloud

The term *hybrid cloud* describes the use of both private and public cloud platforms, working in conjunction. It can refer to any combination of cloud solutions that work together on-premises and offsite to provide cloud computing services to a company. A hybrid cloud environment allows organizations to benefit from the advantages of both types of cloud platforms and choose which cloud to use based on specific data needs.

A multi-cloud environment is as its name suggests, reflecting multiple and disparate cloud offerings and forms, all of which are part of the ubiquitous VMware Cloud™.

VMware's *hybrid cloud* portfolio offers a combination of solutions that enable organizations to easily extend, protect, or replace on-premises infrastructure. These hybrid cloud offerings are built on an SDDC architecture, leveraging VMware's industry-leading compute, networking, and storage virtualization technologies.

Any combination of clouds powered by VMware creates a common operating environment across VMware-based on-premises private clouds and VMware-based public clouds. Cloud solutions from VMware Cloud Provider Partners (VCPP) including IBM, Oracle, Microsoft, Google, Amazon Web Services (AWS) and others. Native public clouds such as AWS, Azure, Oracle and Google Cloud Platform using VMware technologies including VMware Cloud Foundation, VMware vRealize® and VMware Cloud Services, along with on-premises managed cloud services such as VMware Cloud on Dell EMC, form the core of VMware Cloud offerings.

This approach enables a diverse set of use cases, including regional capacity expansion, disaster recovery, application migration, data center consolidation, new application development and burst capacity.

Learn more about *VMware Hybrid Cloud*.

VMware Cloud on AWS

VMware Cloud on AWS is an on-demand service that enables customers to run applications across vSphere-based cloud environments with access to a broad range of AWS services. Powered by VMware Cloud Foundation, this service integrates vSphere, vSAN and VMware NSX along with VMware vCenter management, and is optimized to run on dedicated, elastic, bare-metal AWS infrastructure.

With VMware Hybrid Cloud Extension™, customers can easily and rapidly perform large-scale bi-directional migrations between on-premises and VMware Cloud on AWS environments.

With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant business value from use of the AWS and VMware hybrid cloud experience. VMware Cloud on AWS is ideal for enterprise IT infrastructure and operations organizations looking to migrate on-premises vSphere-based workloads to the public cloud, consolidate and extend data center capacities, and optimize, simplify, and modernize their disaster recovery solutions.

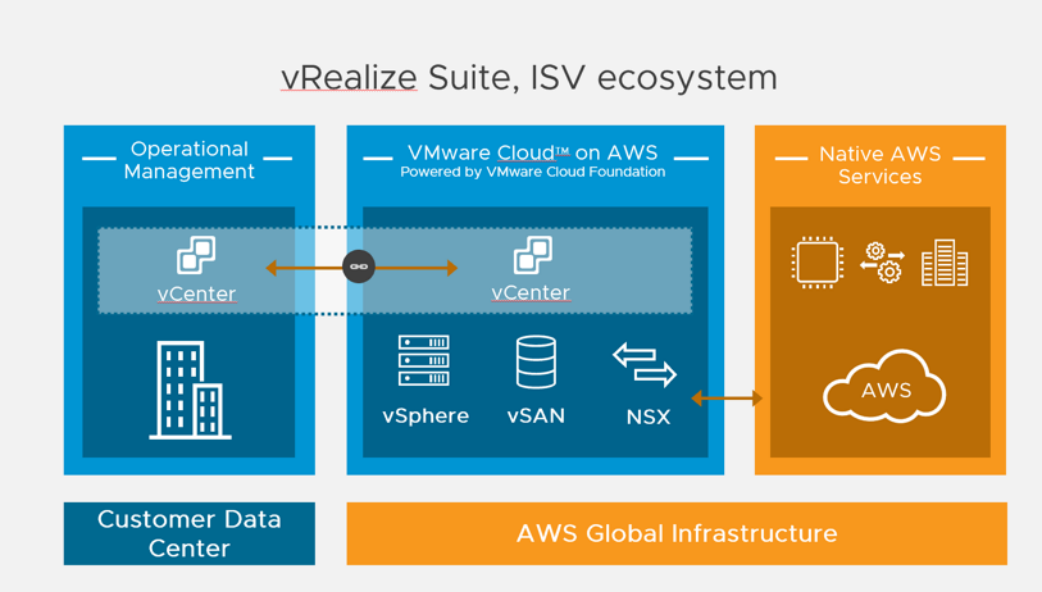


FIGURE 4. VMware Cloud on AWS

Learn more about *VMware Cloud on AWS*.

Stretched Clusters for VMware Cloud on AWS

Amazon's global infrastructure is broken up into regions. Each region supports the services for a given geography. Within each region, Amazon builds isolated and redundant islands of infrastructure called availability zones (AZ). When VMware deploys a vSphere cluster as part of the VMware Cloud on AWS managed service, all hosts for a given cluster are placed into a single AZ.

To protect against AZ failure, customers have the option to deploy a stretched cluster. When selected, a vSAN stretched cluster is created across three AZs, creating a vSphere cluster that can survive the loss of an entire availability zone. To protect against split-brain scenarios and help measure site health, a managed vSAN witness is also created in a third AZ. The third AZ is picked at random from the remaining AZs.

With a copy of the data in each AZ, vSphere HA is empowered to recover from any failure using a simple restart. In summary, stretched clusters simplify the cloud by providing the same trusted controls and capabilities in addition to the scale and flexibility of the AWS infrastructure.

Now applications can span multiple AWS availability zones within a VMware Cloud on AWS cluster. vSAN fault domains are configured to inform vSphere and vCenter which hosts reside in which AZs. Each fault domain is named after the AZ it resides within to increase clarity.

Some of the advantages are:

- Zero RPO high availability for enterprise applications virtualized on vSphere across AWS AZs, leveraging multi-AZ stretched clustering.
- Stretched clusters enable developers to focus on core application requirements and capabilities, instead of infrastructure availability.
- Significantly improve your application's availability without needing to architect it into your application.
- VMware Cloud on AWS infrastructure delivers protection against failures of AWS AZs at an infrastructure level. Stretching an SDDC cluster across two AWS AZs within a region means if an AZ goes down, it is simply treated as a vSphere HA event and the VM is restarted in the other AZ.

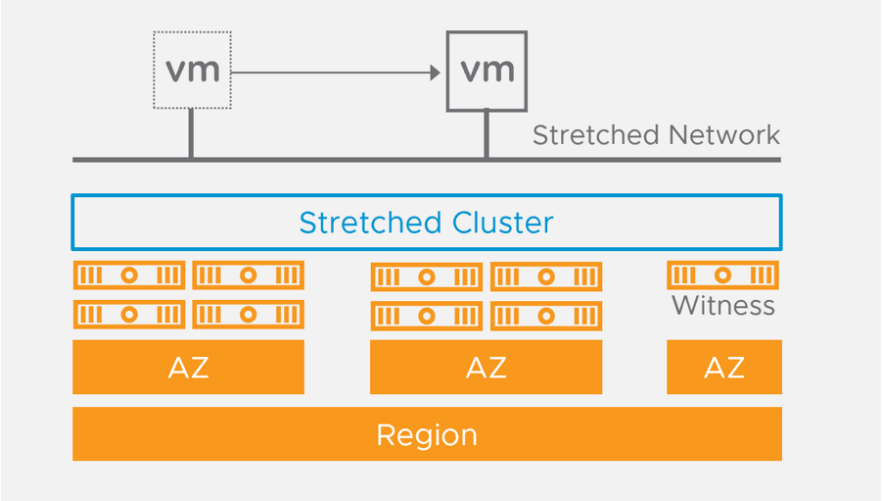


FIGURE 5. Stretched Clusters for VMware Cloud on AWS

More information on Stretched Clusters for VMware Cloud on AWS can be found *here* and *here*.

VMware Cloud on Dell EMC

VMware Cloud on Dell EMC combines the simplicity and agility of the public cloud with the enhanced security and control of on-premises infrastructure, delivered as-a-service to data center and edge locations. This fully managed VMware Cloud service provides a simple, secure, and scalable infrastructure for customer's on-premises datacenter and edge locations. VMware's industry leading compute, storage, and networking software is integrated with enterprise-class Dell EMC VxRail hardware, empowering you to drive any enterprise workload. The unique approach of this service empowers customers to focus on business innovation and differentiation, while VMware operates the entire infrastructure end-to-end.

VMware Cloud on Dell EMC is a fully managed VMware Cloud Service which includes a physical Dell VxRail hyper-converged infrastructure built to a customer's capacity needs and is delivered onsite preloaded with vSphere, NSX, and vSAN software. Included with this service is full management of the hardware infrastructure, including monitoring, software patching and upgrades, security updates, lifecycle management and break-fix service in the event of a hard failure. This service is backed by an enterprise-grade SLA.

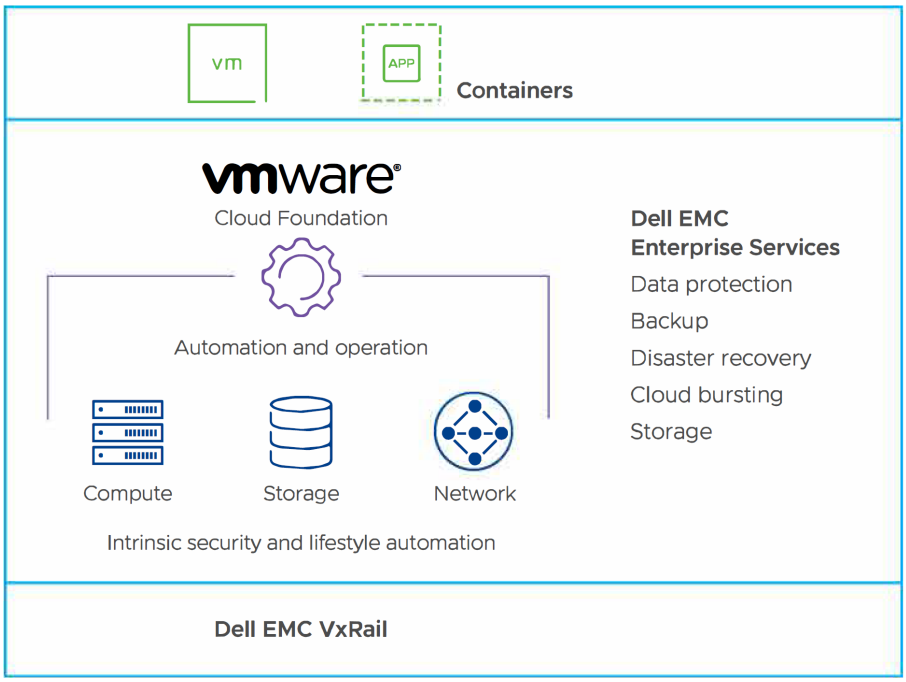


FIGURE 6. VMware Cloud on Dell EMC

Learn more about *VMware Cloud on Dell EMC*.

Google Cloud VMware Engine (GCVE)

Google Cloud VMware Engine allows organizations to seamlessly migrate their VMware workloads to the cloud. This solution offers flexible on-demand capacity and full operational consistency with your existing on-premises environments, allowing you to harness the power of the Google Cloud Platform to modernize your infrastructure, operations, and processes.

By integrating VMware's flagship compute, storage, network virtualization, and management technologies with dedicated, elastic, bare-metal infrastructure, GCVE allows customers to access the agility, scale, and innovative services of the cloud while maintaining operational consistency and leveraging existing tools and investments.

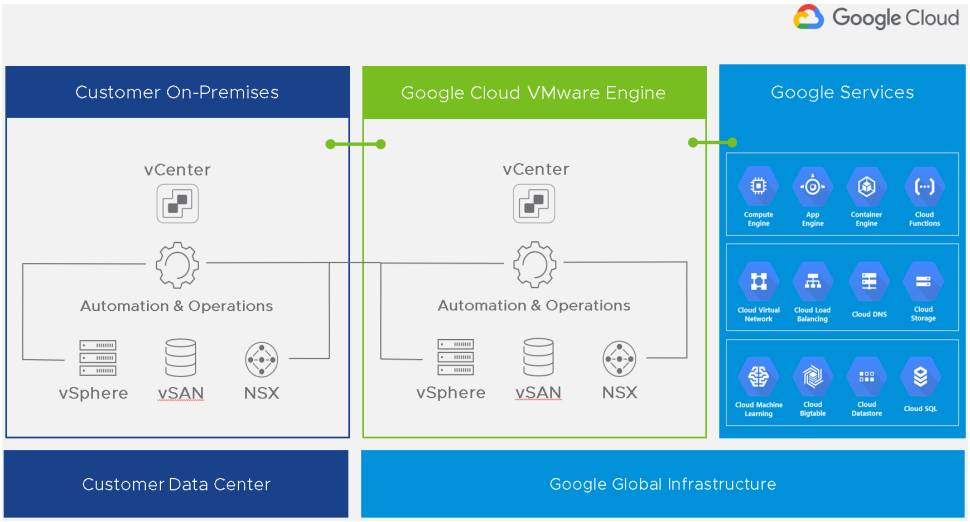


FIGURE 7. Google Cloud VMware Engine

Learn more about *Google Cloud VMware Engine*.

Azure VMware Solution (AVS)

Azure VMware Solution (AVS) is a first-party Microsoft service that delivers the VMware SDDC stack as a managed service—sold, operated, and supported by Microsoft—running natively on bare-metal infrastructure in the Microsoft Azure Cloud. Azure VMware Solution is a VMware Cloud-verified platform that offers vSphere, vSAN, NSX-T, and more, while being seamlessly integrated into Microsoft Azure infrastructure and management tools.

With Azure VMware Solution, you can modernize your infrastructure by seamlessly moving vSphere-based workloads directly to Microsoft Azure without application changes. Because Azure VMware Solution uses the same VMware SDDC components you use on-premises, you can leverage the same skills and tools you use every day to build an elastic, hybrid, and scalable platform for your existing or new vSphere applications.

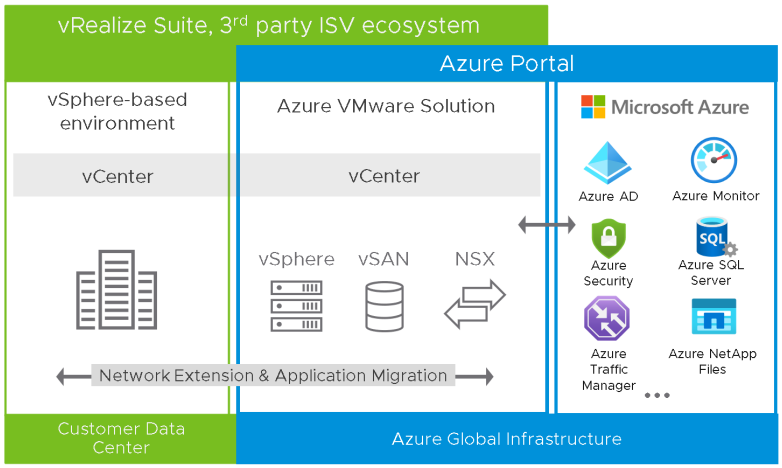


FIGURE 8. Azure VMware Solution

Learn more about *Azure VMware Solution*.

Oracle Cloud VMware Solution (OCVS)

Oracle Cloud VMware Solution integrates VMware on-premises tools, skillsets, and processes with public Oracle Cloud services. The solution is a customer-managed, native VMware cloud environment based on VMware Validated Design for use with the public Oracle Cloud. It allows enterprises to access the scale and agility of the Oracle Cloud while extending VMware-based workloads and applications across the Oracle Cloud. It also empowers enterprises to reduce operational costs and complexity, while mitigating operational risk.

Oracle Cloud VMware Solution leverages VMware Cloud Foundation compute, network virtualization, and storage functions deployed to Oracle bare-metal hosts in the Oracle Cloud. This consistent, unified cloud infrastructure and operations platform will enable your enterprise to migrate and modernize applications faster while seamlessly moving workloads between on-premises environments and Oracle Cloud at scale.

Enterprises can now move or extend VMware-based workloads without rearchitecting applications or retooling operations. Your IT teams can also easily leverage Oracle services, such as Oracle Autonomous Database, Exadata Cloud, and Database Cloud, from the same cloud data centers, on the same networks, with consistent portal access and modernized APIs.

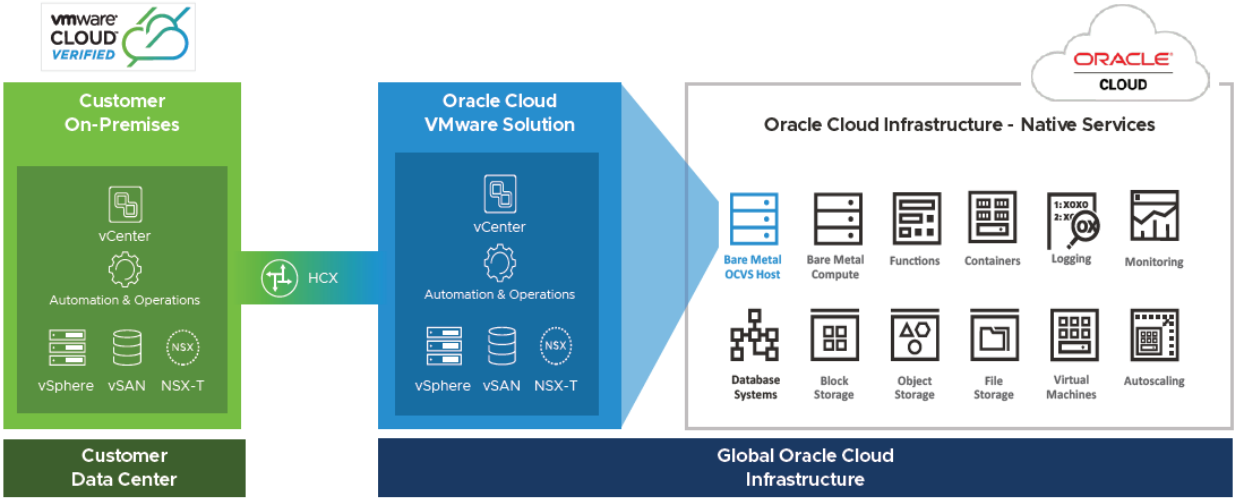


FIGURE 9. Oracle Cloud VMware Solution

Learn more about *Oracle Cloud VMware Solution*.

VMware Hybrid Cloud Extension

VMware Hybrid Cloud Extension is an application mobility platform designed to simplify application migration, workload rebalancing, and business continuity across data centers and clouds.

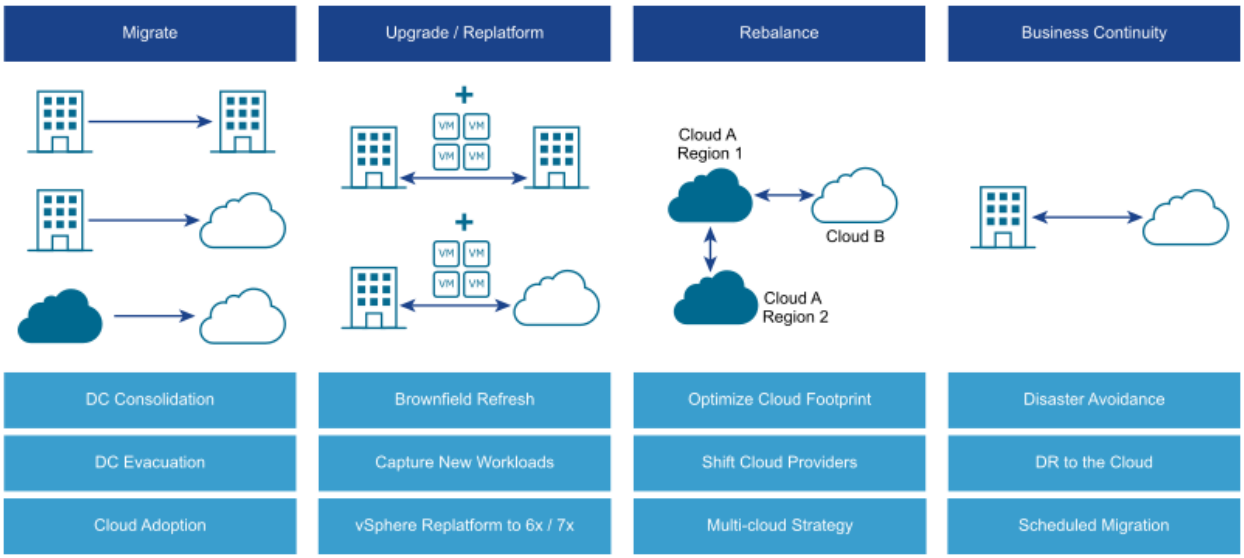


FIGURE 10. VMware Hybrid Cloud Extension

VMware Hybrid Cloud Extension enables:

- **Application migration** – schedule and migrate thousands of vSphere VMs within and across data centers without requiring a reboot.
- **Change platforms or upgrade vSphere versions** – migrate workloads from vSphere and from non-vSphere (KVM and Hyper-V) environments within and across data centers or clouds to current vSphere versions without requiring an upgrade.
- **Workload rebalancing** – provides a mobility platform across cloud regions and cloud providers to allow customers to move applications and workloads at any time to meet scale, cost management, compliance, and vendor neutrality goals.
- **Business continuity and protection** – with Hybrid Cloud Extension, administrators can protect workloads by replicating them to other Hybrid Cloud Extension-enabled sites. Workload migration is available on-demand, or it can be scheduled for business or for maintenance planning.

Learn more about *VMware Hybrid Cloud Extension*.

VMware Hybrid Cloud Extension Migration Types

VMs can be moved to and from VMware Hybrid Cloud Extension-activated data centers using multiple migration technologies.

VMware Hybrid Cloud Extension Bulk Migration

This migration method uses the VMware vSphere replication protocols to move the VMs to a destination site.

- The bulk migration option is designed for moving VMs in parallel.
- This migration type can set to complete on a pre-defined schedule.
- The VM runs at the source site until the failover begins. The service interruption with the bulk migration is equivalent to a reboot.

VMware Hybrid Cloud Extension vMotion

This migration method uses the VMware vMotion protocol to move a VM to a remote site.

- The vMotion migration option is designed for moving single VM at a time.
- VM state is migrated. There is no service interruption during the VMware Hybrid Cloud Extension vMotion migration.

VMware Hybrid Cloud Extension Cold Migration

This migration method uses the VMware NFC protocol. It is automatically selected when the source VM is powered off.

VMware Hybrid Cloud Extension Replication Assisted vMotion

VMware Hybrid Cloud Extension Replication-Assisted vMotion (RAV) combines advantages from VMware Hybrid Cloud Extension Bulk Migration (parallel operations, resiliency, and scheduling) with VMware Hybrid Cloud Extension vMotion (zero downtime VM state migration).

VMware Hybrid Cloud Extension OS Assisted Migration

This migration method provides for the bulk migration of guest (non-vSphere) VMs using OS-assisted migration to VMware vSphere on-premises or cloud-based data centers. Activating this service requires additional Hybrid Cloud Extension licensing.

Learn more about *VMware Hybrid Cloud Extension Migration Types*.

Oracle Database Architecture

Oracle Database 19c, the latest generation of the world's most popular database, provides businesses of all sizes with access to the world's fastest, most scalable, and reliable database technology. These capabilities enable secure and cost-effective deployment of transactional and analytical workloads in the cloud, on-premises, and in hybrid cloud configurations.

An Oracle database server consists of a database and at least one database instance. In a clustered Oracle configuration, an Oracle database will have more than one instance accessing the database.

- A database is a set of files, located on disk, that store data. These files can exist independently of a database instance.
- An instance is a set of memory structures that manage database files. The instance consists of a shared memory area, called the system global area (SGA), and a set of background processes. An instance can exist independently of database files.

The physical database structures that comprise a database are:

- **Data files** – Every Oracle database has one or more physical data files, which contain all database data. The data of logical database structures, such as tables and indexes, is physically stored in the data files.
- **Control files** – Every Oracle database has a control file. A control file contains metadata specifying the physical structure of the database, including the database name, along with the names and locations of the database files.
- **Online redo log files** – Every Oracle database has an online redo log, representing a set of two or more online redo log files. An online redo log is made up of redo entries (also called redo log records), which record all changes made to data.
- Many other files, including parameter files, archived redo files, backup files and networking files, are important to any oracle database operation.

Learn more about *Oracle database architecture*.

Oracle ASM, ASMLIB and ASMFD

ASM

Oracle Automatic Storage Management (ASM) is a volume manager and a file system for Oracle database files that supports single-instance and clustered Oracle Database configurations.

Oracle ASM is Oracle's recommended storage-management solution that can be used for both single-instance and clustered Oracle databases, providing an alternative to conventional volume managers, file systems, and raw devices.

Oracle ASM uses disk groups to store data files. An Oracle ASM disk group is a collection of disks that Oracle ASM manages as a unit. Users can add or remove disks from a disk group while a database continues to access files from the disk group.

Learn more about *Oracle Automatic Storage management (ASM)*.

ASMLIB

Oracle ASMLIB maintains permissions and disk labels that are persistent on the storage device so that the label is available even after an operating system upgrade.

The Oracle ASMLIB driver simplifies the configuration and management of block disk devices by eliminating the need to rebind block disk devices used with Oracle ASM each time the system is restarted.

Learn more about *Oracle ASMLIB*.

ASMFD

Oracle ASMFD helps prevent corruption in Oracle ASM disks and files within the disk group. Oracle ASMFD simplifies the configuration and management of disk devices by eliminating the need to rebind disk devices used with Oracle ASM each time the system is restarted.

Learn more about *Oracle ASMFD*.

Linux Device Persistence and udev Rules

Device names in Linux are not guaranteed persistent across reboots. A device (e.g., /dev/sdb) can be renamed on the next reboot (e.g., /dev/sdc).

Linux udev rules may be used to guarantee device persistence across reboot.

Learn more about *configuring device persistence for Oracle storage*.

Architectural Guidelines and Operational Considerations for Moving Oracle Workloads to VMware Cloud on AWS Solution Configuration

VMware Cloud on AWS allows users to create vSphere-based data centers (SDDCs) on AWS. Each deployed SDDC includes VMware ESXi hosts, VMware vCenter Server, VMware vSAN, VMware NSX components and other software. The same HTML5-based vSphere client is used to manage an SDDC once deployed.

One can rapidly and easily migrate application workloads from on-premises data centers running VMware SDDC to VMware Cloud on AWS using VMware Hybrid Cloud Extension and back with:

- No VM conversions
- No application refactoring and, therefore, no application downtime
- No networking changes with L2VPN capability between on-premises SDDC and VMware Cloud on AWS provided by Hybrid Cloud Extension Network Extension appliance

This is key, as some cloud providers require some level of refactoring to achieve the above. In this case, refactoring is not necessary, resulting in significantly reduced time, effort, and man hours in planning migrations between on-premises infrastructure and the cloud.

The planning and design phase is very important in ensuring that migrations of mission-critical application workloads to VMware Cloud on AWS are completed without negatively impacting application SLAs or affecting the performance, availability, manageability and scalability of the workloads themselves. This document provides architectural guidelines to help enterprises in migration planning.

Architecture Guidelines

This section provides a summary of the guidelines and approaches to consider when planning a migration of Oracle workloads to VMware Cloud on AWS, including use cases to aid requirements gathering and technical prerequisites to facilitate migration.

Use Case Definition

The following uses cases reflect those most frequently employed for Oracle workloads on VMware Cloud on AWS:

- Data center extension
  - Footprint expansion or on-demand capacity within few hours (no over-provisioning or complex demand forecasting with reduction in cost)
  - Run test/development workloads and stream database backups to the cloud
  - Run Oracle workloads in the cloud

- Disaster recovery
  - Oracle DR workloads can be scaled in storage and compute
  - Use VMware site recovery service for replication and orchestration
  - Use traditional methods as well, such as Oracle Data Guard, Oracle GoldenGate, or other third-party solution
  - Complement existing DR with existing solutions based on VMware Site Recovery Manager™ or vSphere replication

- Cloud migrations
  - Simple, low-risk, seamless migration of Oracle workloads to VMware Cloud on AWS using known tools (e.g., VMware Hybrid Cloud Extension, VMware vMotion, Oracle Data Guard, Oracle RMAN backup/restore)
  - Connect Oracle workloads on VMware Cloud on AWS workloads to on-premises or AWS environments – EC2, RDS
  - Data center wide evacuations - mass migrations
  - Hardware/software refresh cycle or Oracle re-implementation

- Application modernization
  - Leverage native AWS services (e.g., AWS Simple Storage Service (S3) for Oracle backups)
  - Update existing investments (e.g., extract data out of Oracle workloads and leverage analytics services)

Each particular use case, or combination of use cases, influences the general solution design and necessitates appropriate requirements gathering. This document focuses on the first three use cases, namely data center extension, disaster recovery and cloud migrations.

Rightsizing

Before considering where to place Oracle workloads on a cloud platform, ensure your VM container is rightsized. A workload's performance profile should be collected over a sufficient period of time to reflect application spikes in resource utilization. While defining the required time range to collect time series data, consult with DBAs and application owners to understand the workload profile. At least a full month of *non-rolled up* time series data is recommended prior to executing the performance analysis.

Utilizing *VMware vRealize True Visibility Suite™* is proven to be very helpful in this preparation phase. While analyzing captured data, make sure your rightsizing approach has been agreed upon by administrators, application owners and business owners, and that it comprehends both spikes (high performance) and average utilization (higher density).

The following should be considered while sizing Oracle workloads:

- For CPU and memory resources allocation, check the *host configuration* for VMware Cloud on AWS to verify the workload will fit and not overcommit host resources.
- Account for differences in physical CPU architectures between your current environment and the *host instances* used in VMware Cloud on AWS.
- Always size the CPU resource based on the actual workload.
- The storage layer in VMware Cloud on AWS is provided by VMware vSAN – or hyperconverged infrastructure solution, if using an Amazon EC2 I3.metal instance. Adding storage will require the addition of compute resources (hosts) as well. As an alternative, for workloads with the primary capacity requirements, use Amazon i3en.metal hosts. An I3 instance should remain your primary choice for a performance OLTP workloads.

Requirements

A crucial part of a successful migration is collecting business and technical requirements, allowing you to properly design a cloud platform. For guidance, review *Preparing for VMware Cloud on AWS* before beginning your requirements gathering.

Business requirements are an important part of the requirements gathering process. Input examples include:

- RTO/RPO targets
- Business SLAs
- *Licensing considerations*
- Security and data-management considerations

Technical requirements will directly influence logical design and should be collected and validated with care. Pay special attention to the following bullet points:

- Performance requirements of the workload (e.g., transactions-per-second, number of user connections, expected future workloads changes)
- Capacity requirements (e.g., future growth, other projects to be served)
- Manageability requirements (e.g., providing access to a SDDC to appropriate user groups, reconfiguring monitoring tools, backup solution in use, modifying scripting, vRealize Operations workflows)

- Scalability requirements (e.g., method for increasing capacity of a SDDC, scale-out versus scale-in approach)
- Availability requirements (e.g., Oracle high-availability solutions in use, DRS groups, host-isolation response, number of availability zones required)
- Application requirements (e.g., type of workloads [e.g., OLTP/data warehouse], dependencies between on-premises components and network flow between them)

Risks and Constraints

Ensure that risks and constraints are identified and documented and that the risk-mitigation plan has been agreed by all groups involved.

- An example of a constraint: available network bandwidth between on-premises and SDDC (e.g., is DirectAccess available?)
- An example of a risk: different CPU generations between on-premises ESXi hosts and hosts in an SDDC

High Level Architecture

A high-level solution architecture should include enough information to capture the on-premises environment hosting the Oracle workloads and planned SDDC(s) with multiple AZs, while also providing enough details to work on logical design.

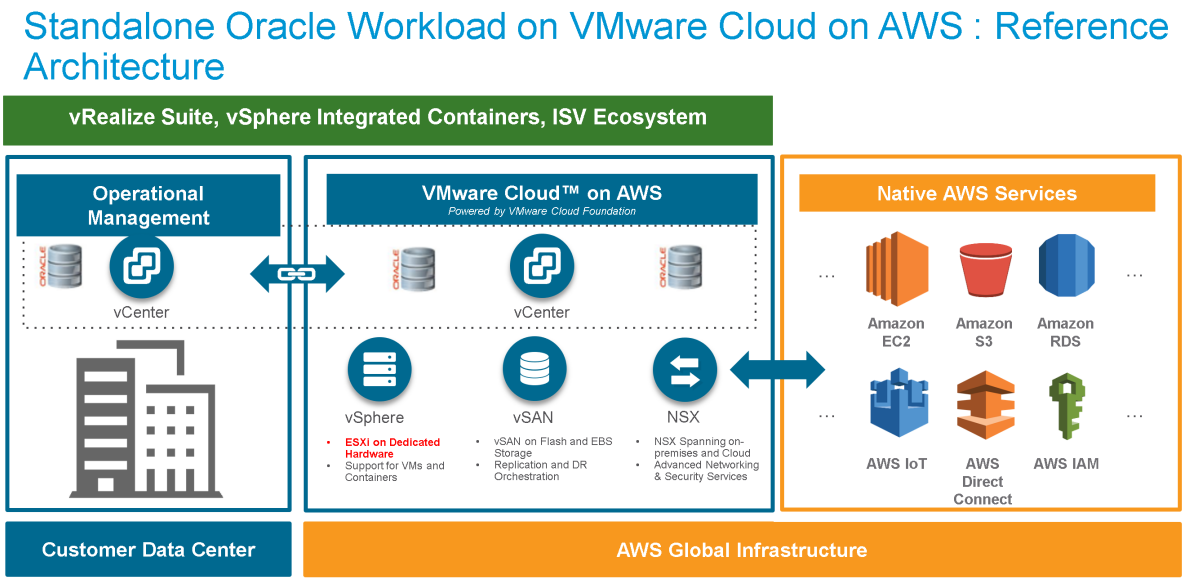


FIGURE 11. VMware Cloud on AWS

High Availability Options

VMware Cloud on AWS provides infrastructure level vSphere HA for Oracle workloads across non-stretched VMware Cloud on AWS which is turned on by default on all clusters in an SDDC on VMware Cloud on AWS.

With Stretched Clusters for VMware Cloud on AWS, in addition to the infrastructure-level high availability provided by vSphere HA, site-level high availability is provided by stretching across multiple AZs.

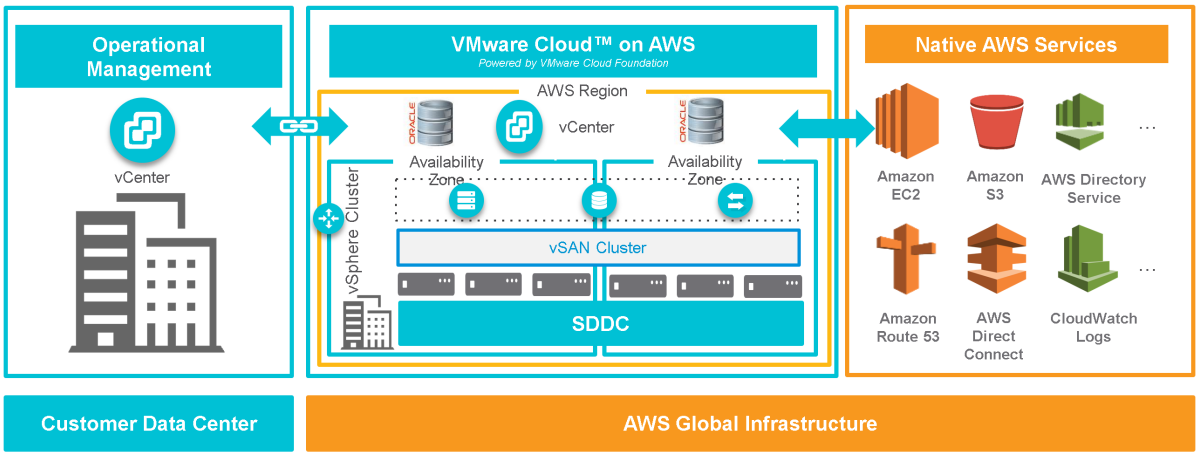


FIGURE 12. Stretched Clusters for VMware Cloud on AWS

Logical Design

A logical design describes all technical decisions made and addresses identified technical requirements while minimizing risk. The level of detail included should be sufficient to create an implementation guide for the solution. While specifics of each logical design are unique, it's important to ensure all technical prerequisites are met. The following prerequisites have been identified as crucial to the successful migration of Oracle workloads to VMware Cloud on AWS:

- For on-premises-located VMs, ESXi hosts, or vSphere clusters hosting Oracle workloads, check and document all advanced settings configured. Ensure corresponding options are available in VMware Cloud on AWS. For example, DRS anti-affinity groups and rules must be re-created in an SDDC as they cannot be migrated.
- Check the *Hybrid Migration with vMotion Checklist* and ensure all requirements are met.
- If a Hybrid Cloud Extension appliance will be used to migrate the workload, review *Hybrid Cloud Extension in the VMware Cloud on AWS* and ensure all requirements are met.
- Hybrid Cloud Extensions Network Extension (NE) provides a Layer 2 VPN (L2VPN) to extend a broadcast domain from a customer site into an AWS based SDDC. NE functionality is provided by a dedicated virtual appliance at both sites.
- It's recommended to ensure that *Hybrid Linked Mode* will be configured to allow managing both on-premises and public SDDCs within a single vSphere client interface. Verify that all required user accounts are added to the cloud administration group.

Operational Considerations

Post-implementation maintenance and operation guidelines are a key component of any well-prepared infrastructure architecture. While incorporating VMware Cloud on AWS SDDCs in an existing infrastructure, it's critical that Day 2 operational routines are updated accordingly, including:

- Backup configurations
- Monitoring configurations
- Operational documentations

If vRealize Operations Manager is used to monitor the environment, confirm that all SDDCs are added to vRealize Operations-managed resources and configured using vCenter adapter with the public cloud option.

Solution Configuration

This section introduces the resources and configurations for the solution:

- Architecture diagram
- Hardware resources
- Software resources
- Network configuration
- Storage configuration
- VMware and Oracle configuration
- VMware Hybrid Cloud Extension Configuration

Architecture Diagram

This solution architecture relies on a three-site scenario:

- On-premises vSphere cluster on Site A (Santa Clara)
- On-premises vSphere cluster on Site B (Wenatchee)
- Stretched Clusters for VMware Cloud on AWS

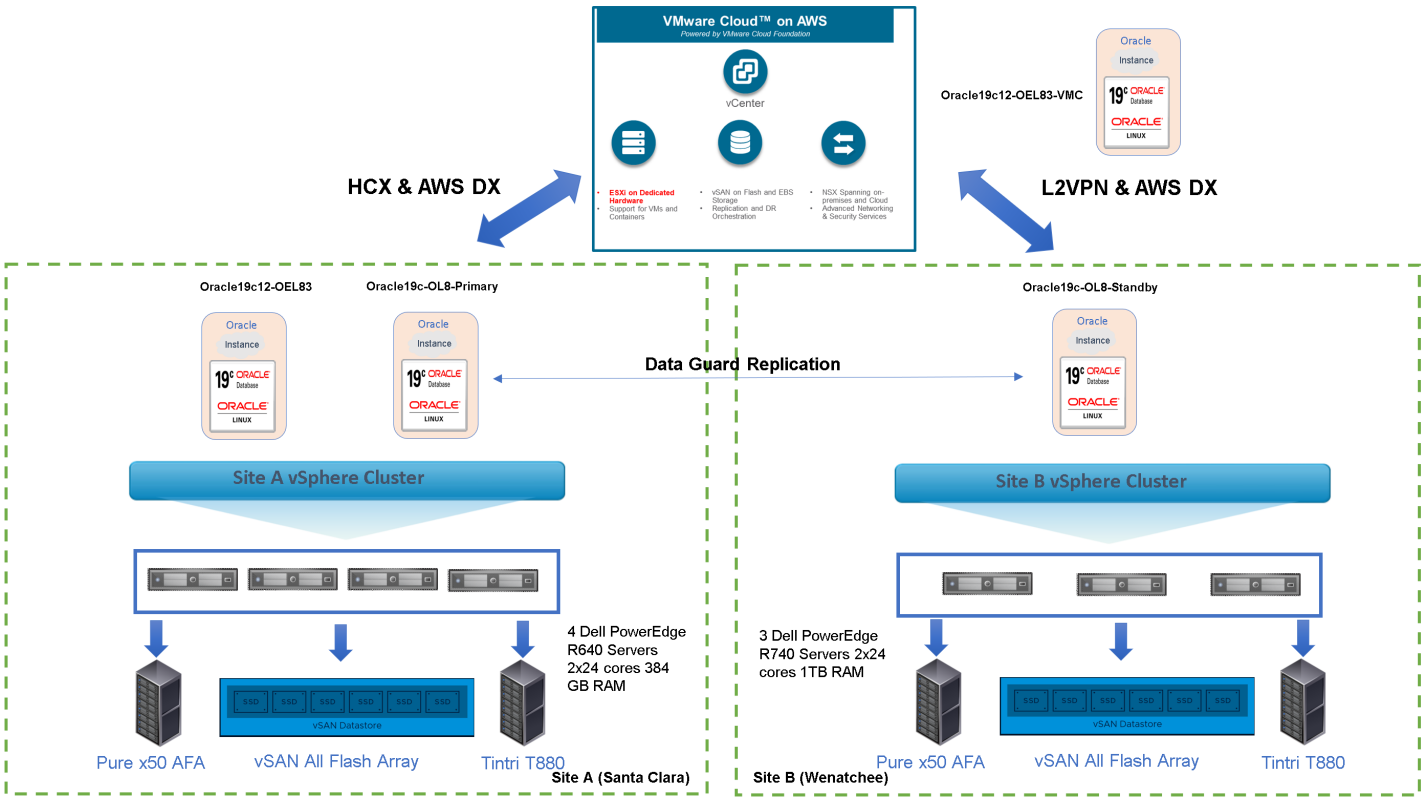


FIGURE 13. On-Premises Sites A and B with Connectivity to Stretched Clusters for VMware Cloud On AWS

The on-premises setup features two separate and dedicated vSphere cluster configurations: Site A and Site B.

- Site A is hosting production single-instance workloads.
- Site B is hosting disaster recovery (DR) single-instance workloads
- Both Site A and Site B are in hybrid linked mode.
- Both sites are connected to Stretched Clusters for VMware Cloud on AWS.

Site A infrastructure details are as follows:

- Virtual Center **sc2wvc03.vslab.**local version 7.0.2 Build 17694817
- vSphere Cluster **BCA-SiteC** with 4-nodes running ESXi version 7.0.2 Build 17867351
- Each ESXi server is a Dell PowerEdge R640 Server with Intel® Xeon® Platinum 8168 CPU @ 2.70GHz with 2x24 cores, and 384GB RAM with hyperthreading
- Each ESXi server has access to a Pure Storage FlashArray//x50 (Purity/FA 6.1.6) for both block FC storage and vVols
- Each ESXi server features:
  - 2 x QLogic ISP2812-based 64/32G Fibre Channel to PCIe Controller for FC storage
  - 2 x Intel® Ethernet Controller X710 for 10GbE SFP+ for network connection

Site B infrastructure details are as follows:

- Virtual Center **az2wvc01.vslab.local** version 7.0.2 Build 17694817
- vSphere Cluster **AZ2-DC** with 3-nodes running ESXi version 7.0.2 Build 17867351
- Each ESXi server is a Dell PowerEdge R740 Server with Intel® Xeon® Platinum 8168 CPU @ 2.70GHz with 2x24 cores, and 1TB RAM with hyperthreading
- Each ESXi server has access to a Pure Storage FlashArray//x50 (Purity/FA 6.1.6) for both block FC storage and vVols
- Each ESXi server features:
  - 2 x Emulex LightPulse LPe32000 Gen 6 16/32G PCIe Fibre Channel Adapter for FC storage
  - 2 x Intel® Ethernet Controller X710 for 10GbE SFP+ for network connection

The Stretched Clusters for VMware Cloud on AWS setup has the following configuration:

- Virtual Center vcenter.sddc-44-232-220-144.vmwarevmc.com Version 7.0.2 Build 18231847
- A 6-node stretched cluster for VMware Cloud on AWS is setup across two AZs, with three servers in AZ **us-west-2b** and three servers in AZ **us-west-2c**, with each ESXI server version 7.0.2 Build 18226209
- Each ESXi server is an Amazon EC2 i3.metal with two sockets, 18 cores each with Intel Xeon processor E5-2686 v4 at 2.30GHz without hyperthreading and 512GB RAM memory
- Storage is provided by the HCI vSAN instance

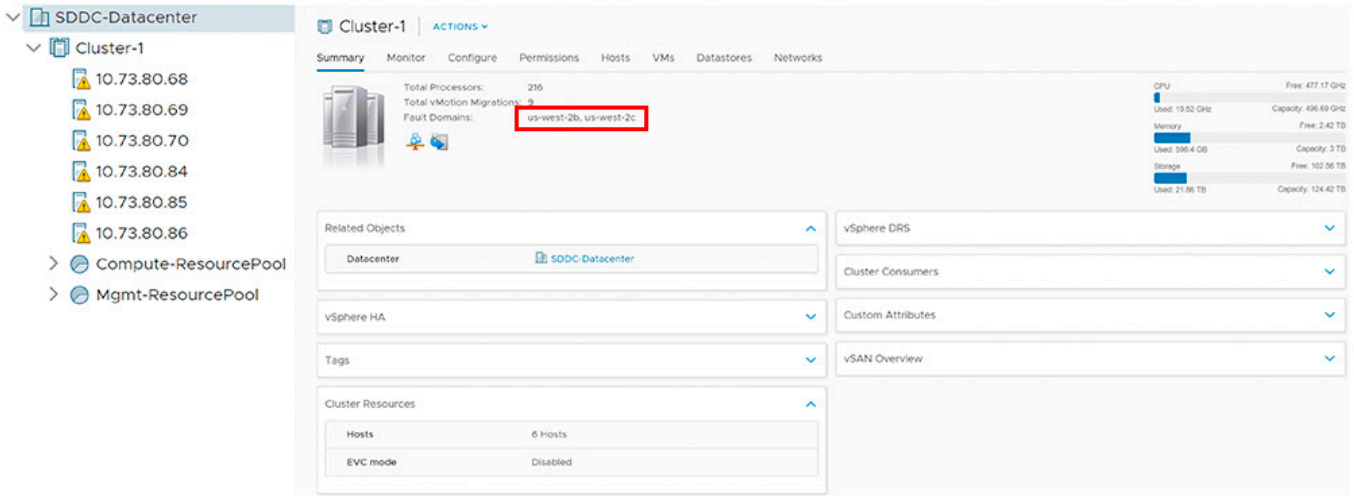


FIGURE 14. 6-Node Stretched Clusters for VMware Cloud on AWS

An L2VPN is used to extend the on-premises data center on Site A to VMware Cloud on AWS and to migrate application workloads rapidly and easily from on-premises to the VMware Cloud on AWS and back. This offers the following advantages:

- No VM conversions
- No application refactoring and, therefore, no application downtime
- No networking changes with L2VPN capability between the on-premises SDDC and VMware Cloud on AWS

Hardware Resources

Below are the hardware resources for the vSphere cluster on Site A):

DESCRIPTION	SPECIFICATION
Server	4 x ESXi Server
Server Model	Dell Inc. PowerEdge R640
CPU	2 sockets with 24 cores each, Intel® Xeon® Platinum 8168 CPU @ 2.70GHz with hyperthreading enabled
RAM	384GB RAM
Storage controller	2 x QLogic ISP2812-based 64/32G Fibre Channel to PCIe Controller for FC storage
Storage Array	Pure x50 AFA (Purity/FA 6.1.6)
Network	2 x Intel® Ethernet Controller X710 for 10GbE SFP+ for network connection
Internal Disk Controller	Dell HBA330 Mini
Internal Disks	Cache—1 x 372.61GB SSD ATA Capacity—2 x 894.25GB SSD ATA
vSAN Disk Group	1 vSAN Disk Group per ESXi Server

TABLE 5. Site A Hardware Resources

The following summarizes the virtual center **sc2wvc03.vslab.local**, vSphere cluster (**BCA-SiteC**), and one of the ESXi servers in the vSphere cluster on Site A:

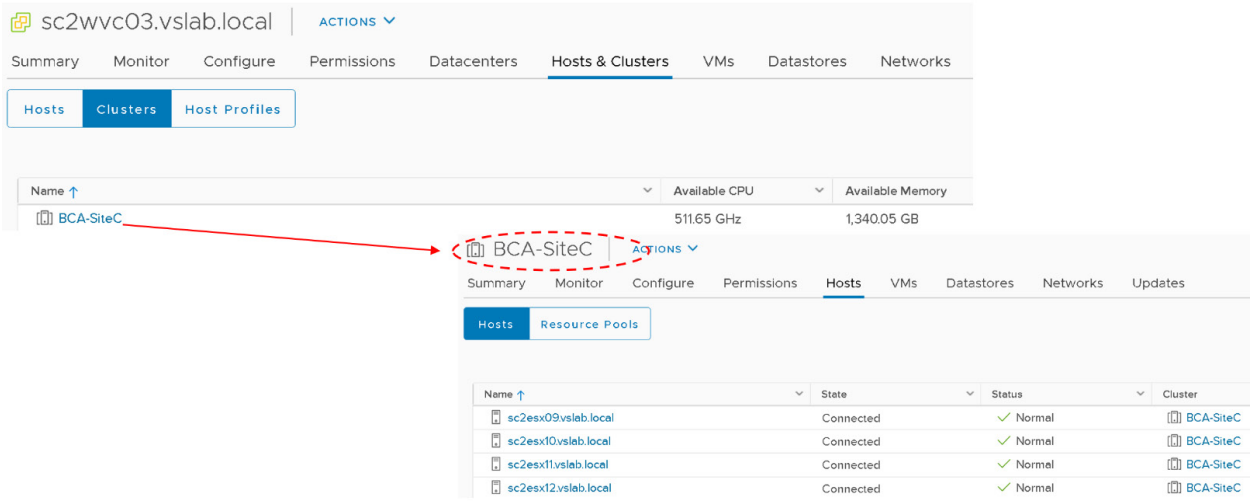


FIGURE 15. Site A vCenter and vSphere Cluster

FIGURE 16. Site A VMware ESXI Server Summary

Below are the hardware resources for the vSphere cluster on Site B:

DESCRIPTION	SPECIFICATION
Server	3 x ESXi Server
Server Model	Dell Inc. PowerEdge R740
CPU	2 sockets with 24 cores each, Intel® Xeon® Platinum 8168 CPU @ 2.70GHz with Hyperthreading enabled
RAM	1TB RAM
Storage controller	2 x Emulex LightPulse LPe32000 Gen 6 16/32G PCIe Fibre Channel Adapter for FC storage
Storage Array	Pure x50 AFA (Purity/FA 5.3.10)
Network	2 x Intel® Ethernet Controller X710 for 10GbE SFP+ for network connection
Internal Disk Controller	Dell HBA330 Mini
Internal Disks	Cache—1 x 372.61GB Samsung SSD ATA Capacity—3 x 894.25GB SSD ATA
vSAN Disk Group	1 vSAN Disk Group per ESXi Server

TABLE 6. Site B Hardware Resources

The following summarizes the Virtual Center **az2wvc01.vslab.local**, vSphere Cluster (**AZ2-DC**), and one of the ESXi servers in the vSphere cluster on Site B:

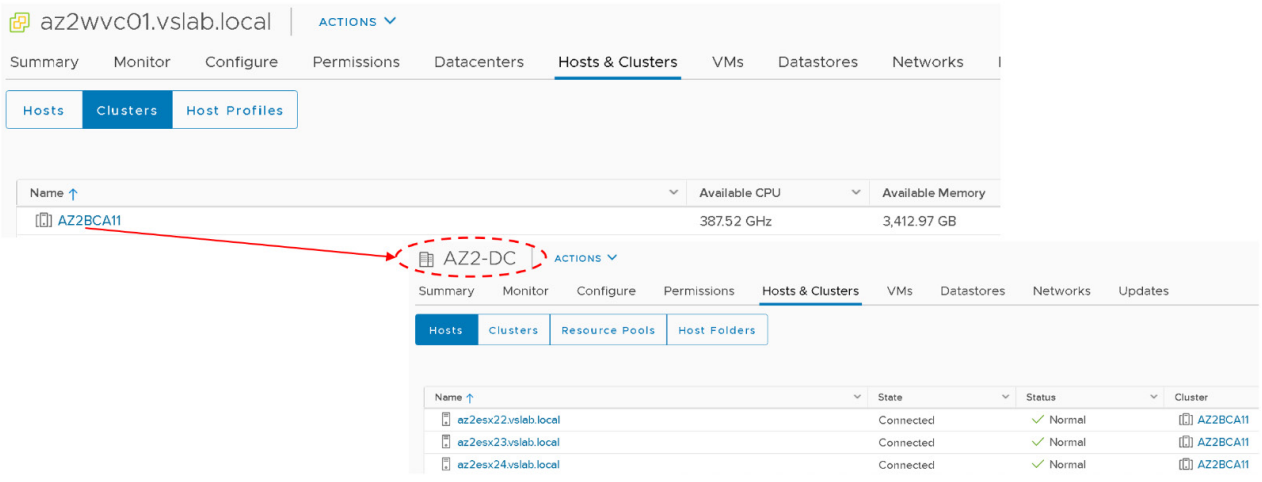


FIGURE 17. Site B vCenter and vSphere Cluster

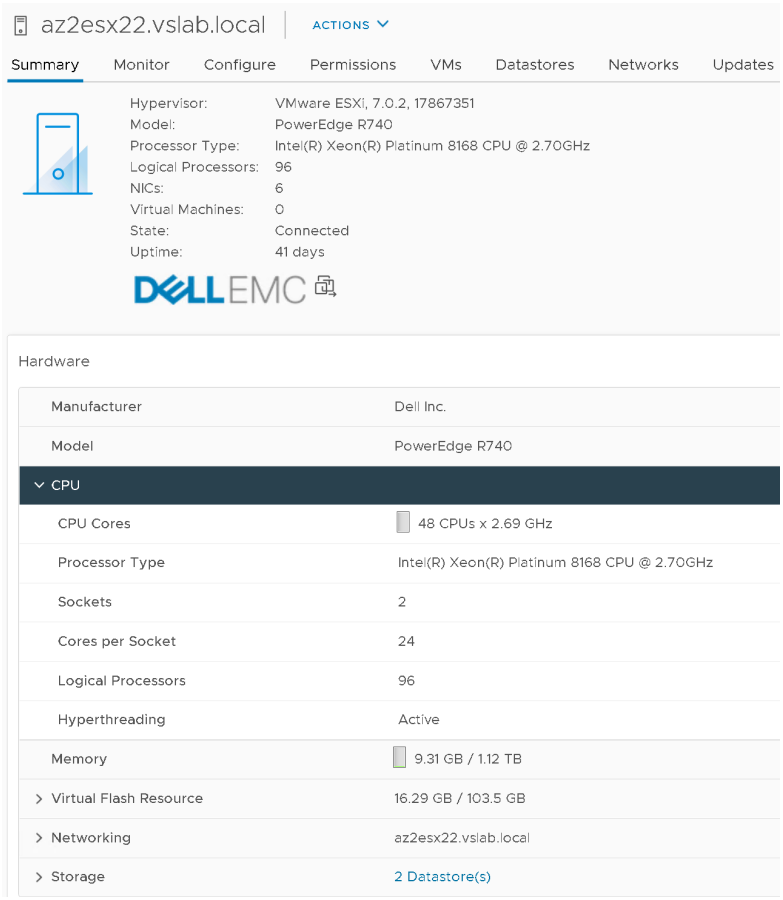


FIGURE 18. Site B VMware ESXI Server Summary

The following hardware resources are utilized for VMware Cloud on AWS:

DESCRIPTION	SPECIFICATION
Server	6 ESXi servers
Server model	Amazon EC2 i3.metal
CPU	2 sockets, 18 cores each, Intel Xeon Processor E5-2686 v4 at 2.30GHz without hyperthreading
RAM	512GB
Disks	8 NVMe drives, each drive 1.73TB across 2 vSAN disk groups
vSAN disk groups	2 disk groups, each disk group with 1 NVMe for cache and 3 NVMe for capacity
Network	One 25G Amazon Elastic network adapter

TABLE 7. VMware Cloud on AWS Hardware Resources

The Stretched Clusters for VMware Cloud on AWS features 6 ESXi servers across two fault domains (FD) or AZs for site-level HA, with three ESXi servers in each AZ.

vSAN fault domains are configured to inform vSphere and vCenter which hosts reside in which AZs. Each fault domain is named after the AZ it resides within to increase clarity.

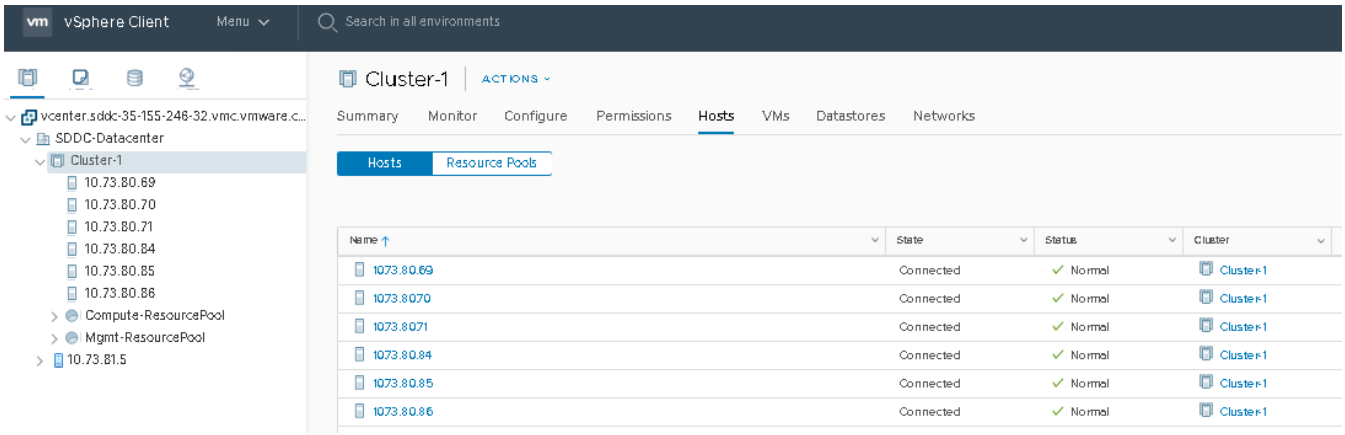


FIGURE 19. Stretched Clusters for VMware Cloud on AWS ESXi Servers

The two fault domains or AZs are **us-west-2b** and **us-west-2c** with three ESXi servers in each AZ.

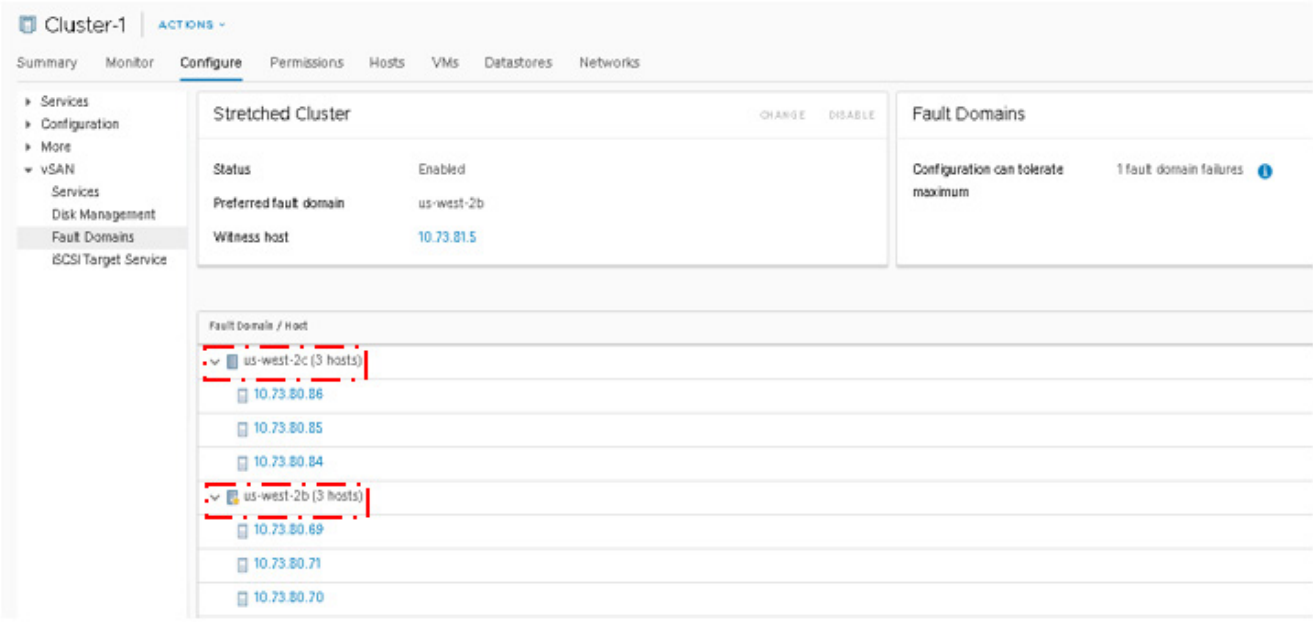


FIGURE 20. Fault Domains in Stretched Clusters for VMware Cloud on AWS

To protect against split-brain scenarios and help measure site health, a managed vSAN witness is also created in a third AZ. The third AZ is picked at random from the remaining AZs. The witness has been engineered to run on an EC2 m5.xlarge AMI to reduce the cost to the customer.

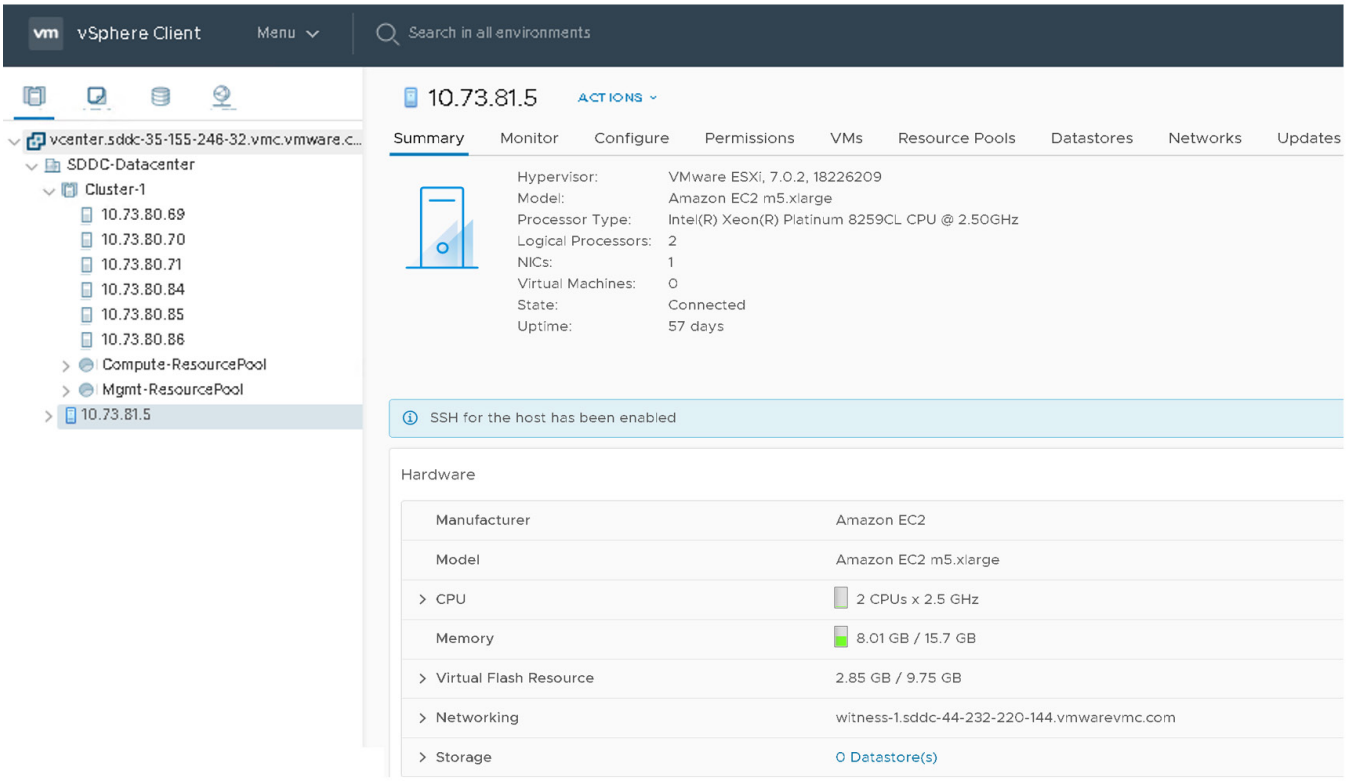


FIGURE 21. Witness in Stretched Clusters for VMware Cloud on AWS

The graphic below captures one of the ESXi servers in the Stretched Clusters for VMware Cloud on AWS environment:

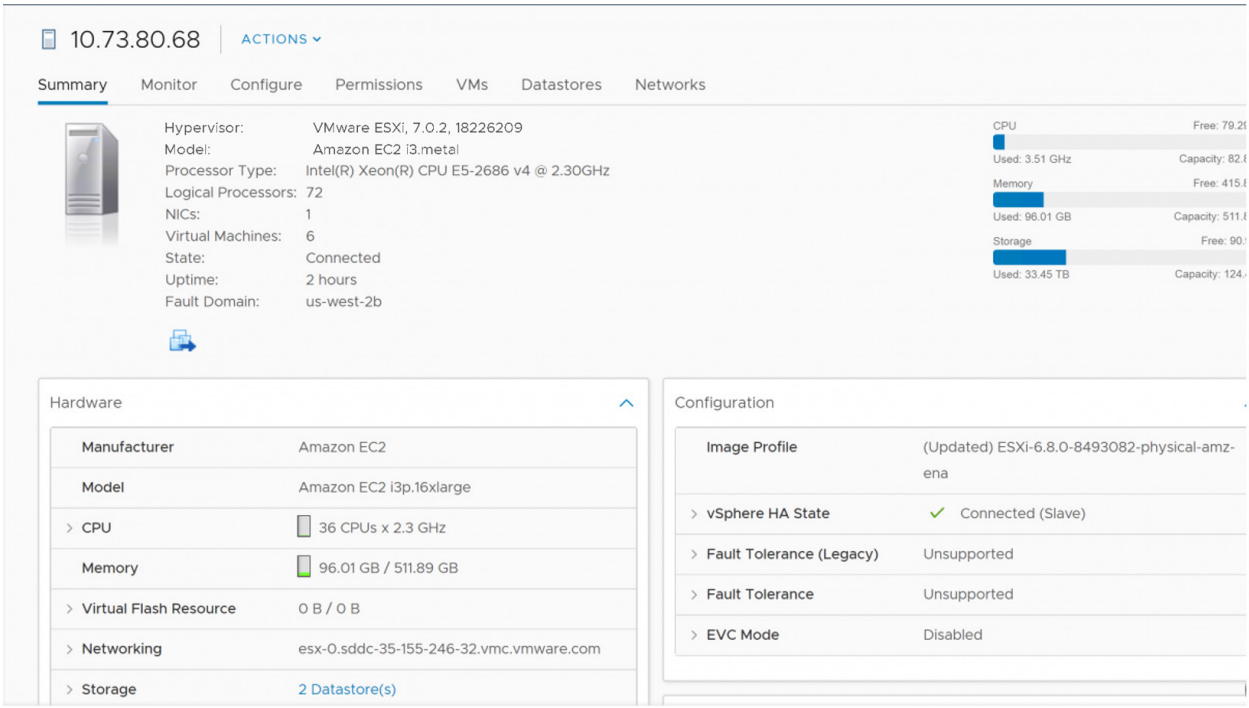


FIGURE 22. ESXi Server in Stretched Clusters for VMware Cloud on AWS

Software Resources

The following is a summary of the software resources used:

SOFTWARE	VERSION	PURPOSE
VMware vCenter Server	7.0.2 Build 17694817	VMware vCenter Server provides a centralized platform for managing VMware vSphere environments
VMware ESXi Server	7.0.2 Build 17867351	ESXi servers to host VMs
ESXi Datastores	Purity//FA 6.1.6	Pure AFA provides both VMFS and vVol datastores
Oracle Linux	8.3 UEK	Oracle database server nodes
Oracle Database 19c	19.12.0.0.0	Grid Infrastructure and Oracle database

TABLE 8. Software Resources

Network Configuration

A VMware vSphere® Distributed Switch™ acts as a single virtual switch across all associated hosts in the datacenter. This setup enables VMs to maintain a consistent network configuration as they migrate across multiple hosts.

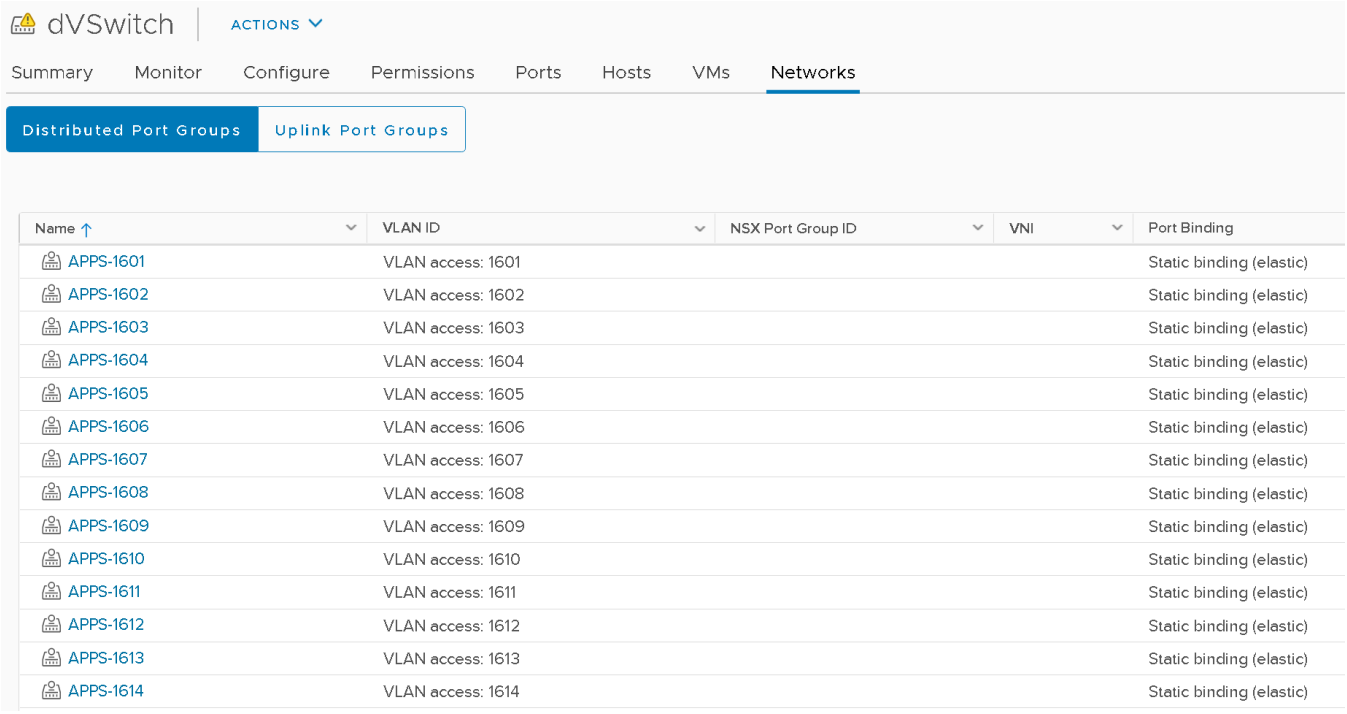
A port group defines properties regarding security, traffic-shaping, and network adapter-teaming. Jumbo frames (MTU=9000 bytes) are enabled on the VMware vSphere vMotion interface, and the default port group setting is used.

For Site A, VDS **dVSwitch** uses 2 x 10GbE adapter per host:

- 2 x 10GbE uplinks for VM traffic and VMkernel non-VM traffic

The following distributed switch-port groups were created for Oracle VM traffic to balance traffic across the available uplinks:

- Port group **APPS-1614** with VLAN ID 1614 (Subnet 172.16.14.1/24) is for VM user traffic
- Port group **APPS-1605** with VLAN ID 1605 (Subnet 172.16.05.1/24) and **APPS-1606** with VLAN ID 1606 (Subnet 172.16.06.1/24) for Oracle Private traffic with two active/active uplinks set to **Route based on originating virtual port**.
- Port group **APPS-1631** with VLAN ID 1631 for Management traffic
- Port group **APPS-1632** with VLAN ID 1632 for vMotion traffic
- Port group **APPS-1635** with VLAN ID 1635 for vSAN traffic



Name	VLAN ID	NSX Port Group ID	VNI	Port Binding
APPS-1601	VLAN access: 1601			Static binding (elastic)
APPS-1602	VLAN access: 1602			Static binding (elastic)
APPS-1603	VLAN access: 1603			Static binding (elastic)
APPS-1604	VLAN access: 1604			Static binding (elastic)
APPS-1605	VLAN access: 1605			Static binding (elastic)
APPS-1606	VLAN access: 1606			Static binding (elastic)
APPS-1607	VLAN access: 1607			Static binding (elastic)
APPS-1608	VLAN access: 1608			Static binding (elastic)
APPS-1609	VLAN access: 1609			Static binding (elastic)
APPS-1610	VLAN access: 1610			Static binding (elastic)
APPS-1611	VLAN access: 1611			Static binding (elastic)
APPS-1612	VLAN access: 1612			Static binding (elastic)
APPS-1613	VLAN access: 1613			Static binding (elastic)
APPS-1614	VLAN access: 1614			Static binding (elastic)

FIGURE 23. Site A vSphere Distributed Switch Port Group Configuration

For Site B, VDS **az2-dvSwitch** uses 2x 10GbE adapters per host:

- 2 x 10GbE uplinks for VM traffic and VMkernel non-VM traffic

The following distributed switch-port groups were created for Oracle VM traffic to balance traffic across the available uplinks:

- Port group **APPS-1810** with VLAN ID 1810 (Subnet 172.18.10.1/24) is for VM user traffic
- Port group **APPS-1805** with VLAN ID 1805 (Subnet 172.18.05.1/24) and **APPS-1806** with VLAN ID 1806 (Subnet 172.18.06.1/24) for Oracle Private traffic with two active/active uplinks set to **Route based on originating virtual port**.
- Port group **APPS-1809** with VLAN ID 1809 (Subnet 172.18.09.1/24) is for SRM Test Network
- Port group **AZ2-COMP-MGMT** with VLAN ID 1631 for Management traffic
- Port group **AZ2-COMP-VMOTION** with VLAN ID 1632 for vMotion traffic
- Port group **AZ2-COMP-NFS** with VLAN ID 1635 for NFS and vSAN traffic

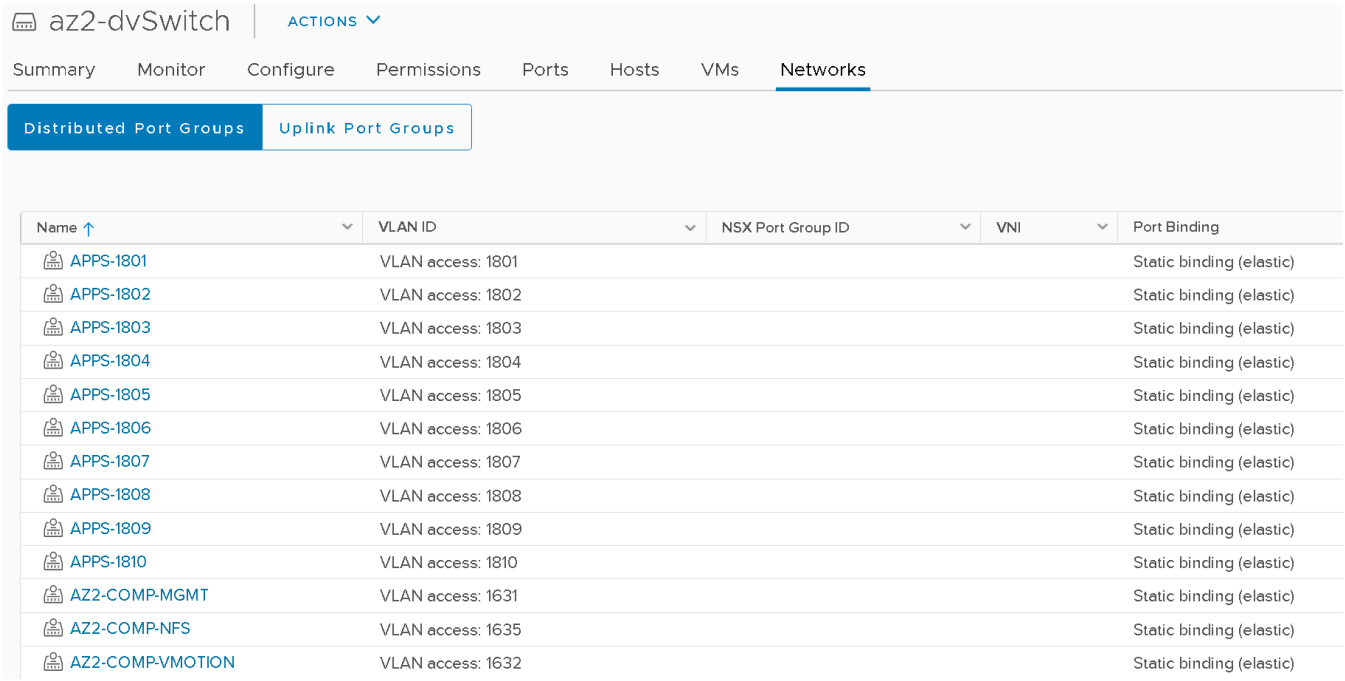


FIGURE 24. Site B vSphere Distributed Switch Port Group Configuration

For VMware Cloud on AWS, each ESXi server contains (1) 25GbE adapter per host.

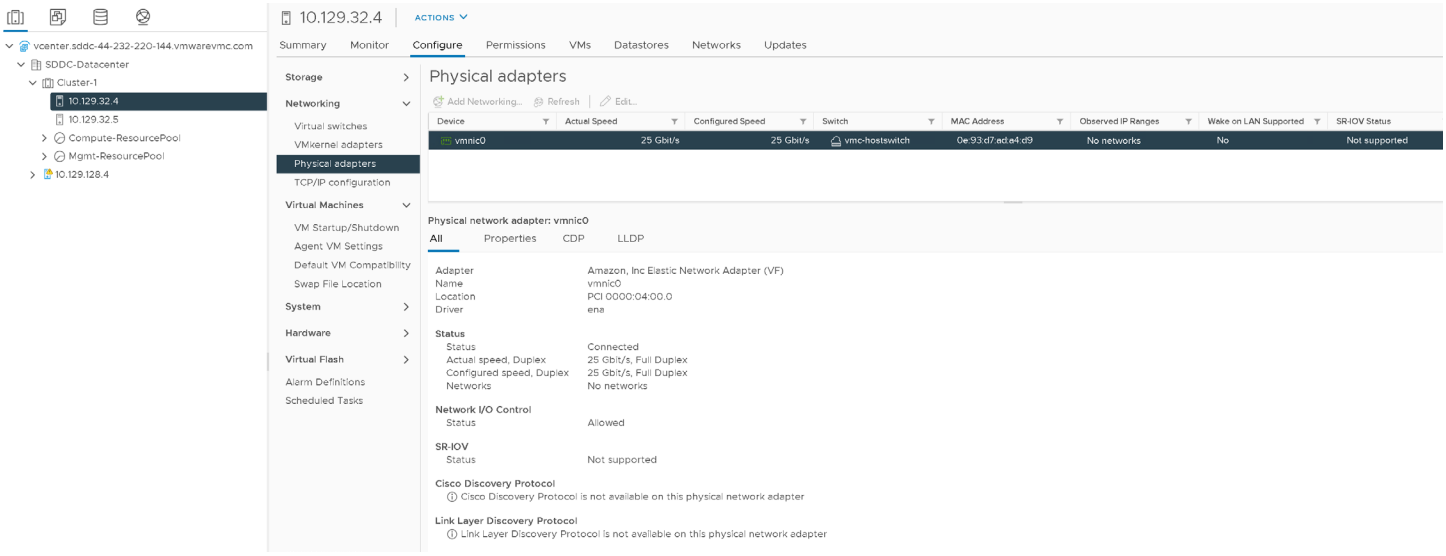


FIGURE 25. VMware Cloud on AWS ESXi Server Networking Details

To create a logical segment, navigate to the VMware Cloud on AWS portal and click **Networking & Security**. Click **Segments**, then Add **Segments**. The illustration below provides an example:

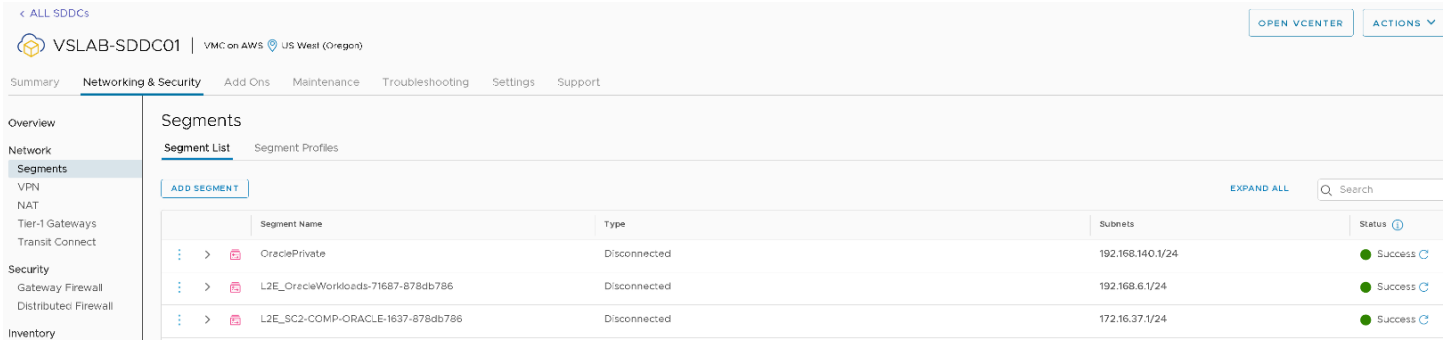


FIGURE 26. Logical Network Details

Fill in the required details as shown above. Select the Disconnected option and specify the CIDR block of the segment in the Gateway/ Prefix Length field. Click Save when done.

As mentioned before, a disconnected network segment has no uplink and provides an isolated network accessible only to the VMs connected to it.

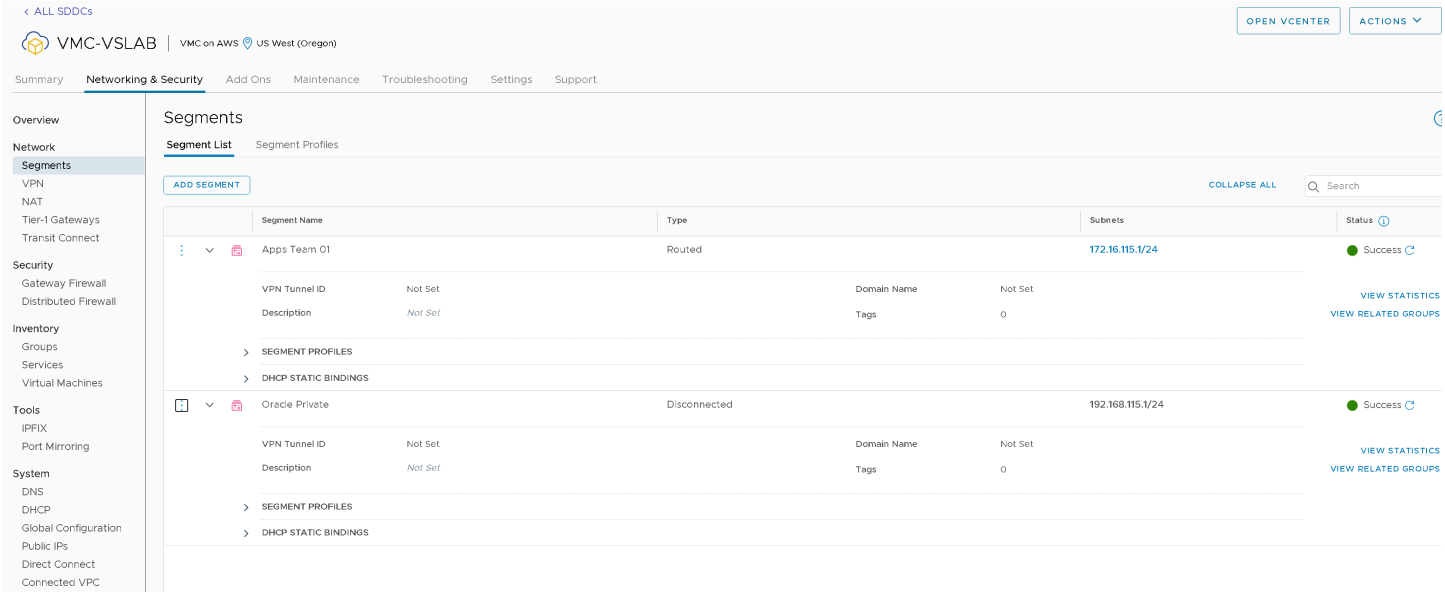


FIGURE 27. Logical Segments for Public and Private Network

Learn more about *VMware Cloud on AWS logical networks*.

The following are logical segments for Oracle VM traffic on VMware Cloud on AWS:

- Logical Segment **Apps Team 01** (Subnet 172.16.115.1/24) for VM user traffic
- Logical Segment **Oracle Private** (Subnet 192.168.115.1/24) for VM private traffic

The following extended segments were created for Oracle VM traffic between on-premises Site A and VMware Cloud on AWS:

- Port group **BCA-L2VPN** for **L2VPN for VM user traffic** (non-Hybrid Cloud Extension traffic) enables VMs to keep the same subnet when migrating from on-premises data centers to the cloud and back.
- Port group **BCA-VPN-Network** for routed VM: traffic enables VMs to communicate—or ping each other—without being on the same subnet.

vSphere vMotion enables live migration of running (i.e., powered on) VMs from an on-premises host to a host in VMware Cloud on AWS, with zero downtime for the application (less than one second switchover time), continuous service availability, and complete transaction integrity. Furthermore, by enabling certain advanced configurations, vMotion migration between on-premises VMs and VMware Cloud on AWS can be enabled across various VDS versions.

VMware Cloud on AWS provides multiple ways to establish network connectivity from on-premises environments, including different types of VPNs and AWS Direct Connect (DX). AWS DX is a service provided by AWS that allows creation of a high-speed, low-latency connection between an on-premises data center and AWS services, including VMware Cloud on AWS.

Learn more about *AWS Direct Connect*.

Learn more about *live vSphere vMotion migration between on-premises data centers and VMware Cloud on AWS*.

If a custom MTU size has been configured for on-premises port groups, it's important to recheck the MTU size and packet defragmentation after migrating to VMware Cloud on AWS.

For now, the default MTU size for inter-SDDC networks is 8950 and is configurable on direct access-based connections (should be set equally on all VIFs). For VPN-based connections, the MTU will be 1500. After changing the MTU size (switching to jumbo frames), always test the final configuration to ensure that no defragmentation is happening along the path. Defragmentation may have higher negative impact on the performance compared to gains from using jumbo frames.

Learn more about *VMware Cloud on AWS MTU*.

Storage Configuration

On Site A, each of the 4 ESXi servers contains 2 x QLogic ISP2812-based 64/32G Fibre Channel to PCIe Controllers for FC storage.

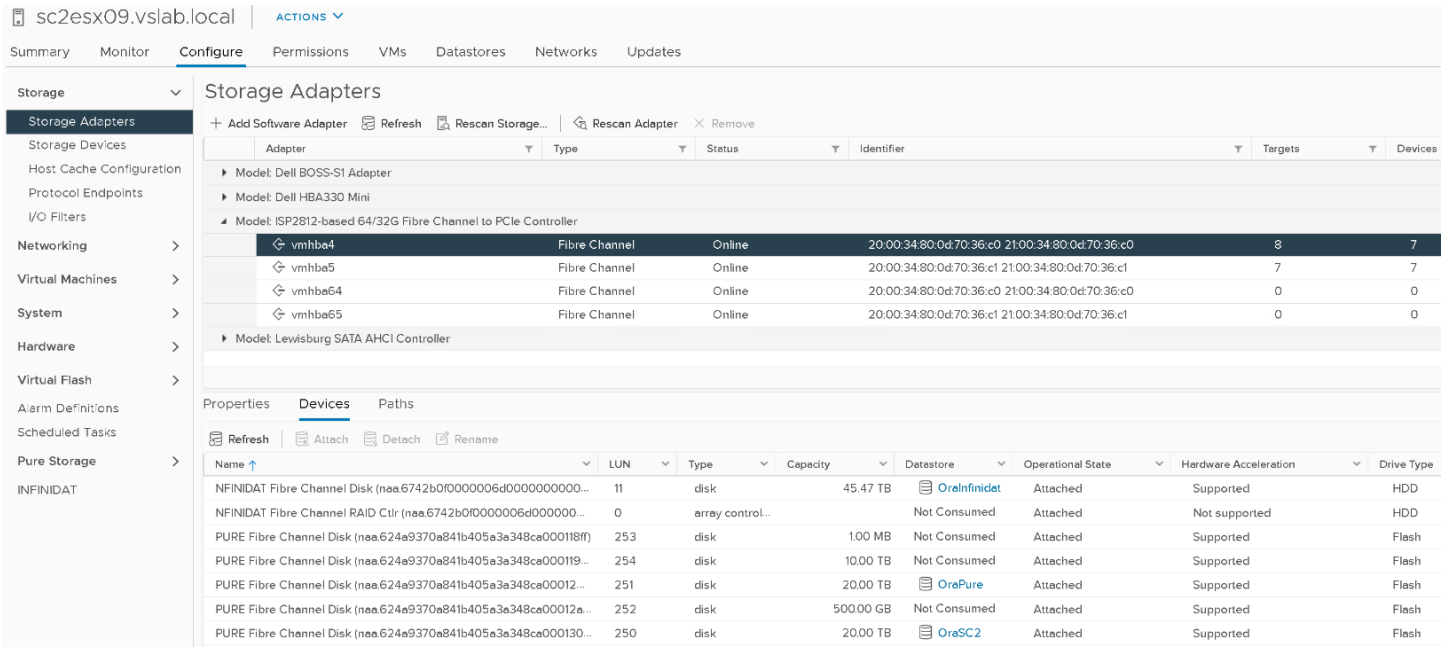


FIGURE 28. Site A ESXi Server Storage Adapter

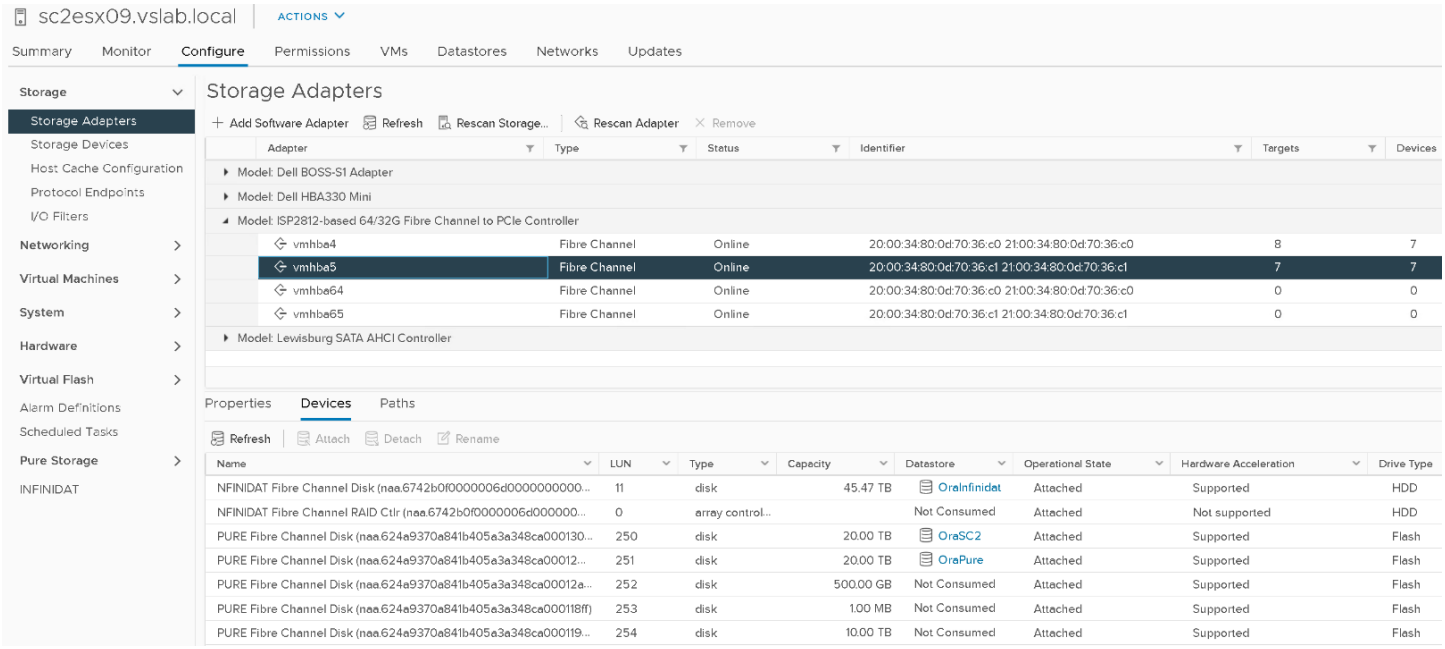


FIGURE 29. Site A ESXi Server FC Storage Connections

Site A contains the following VMFS, vVOL, NFS and vSAN datastores as shown below:

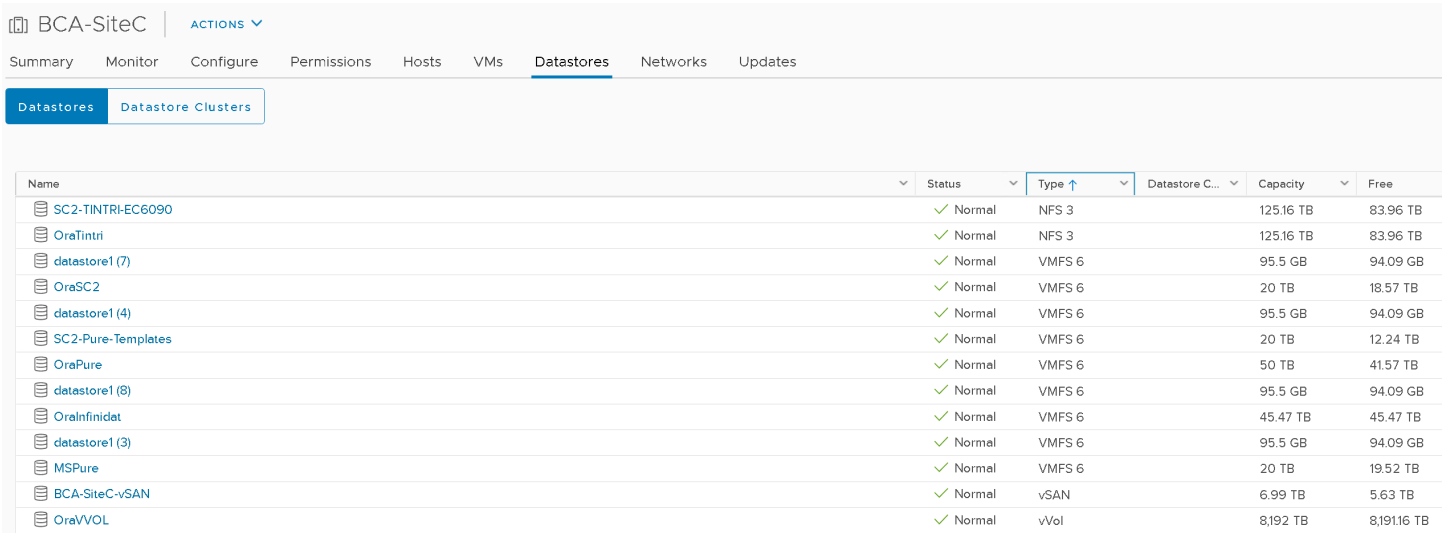


FIGURE 30. Site A Datastores

On Site B, each of the 4 ESXi servers contains 2 x Emulex LightPulse LPe32000 Gen 6 16/32G PCIe Fibre Channel Adapters for FC storage.

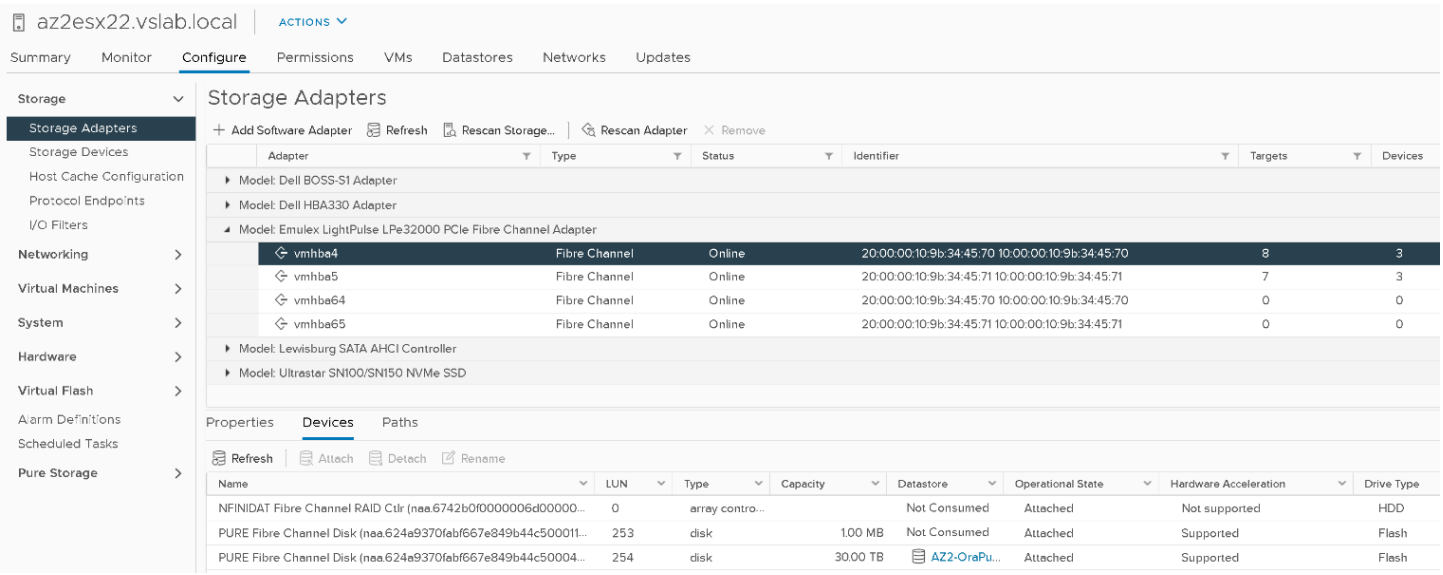


FIGURE 31. Site B ESXi Server Storage Adapter

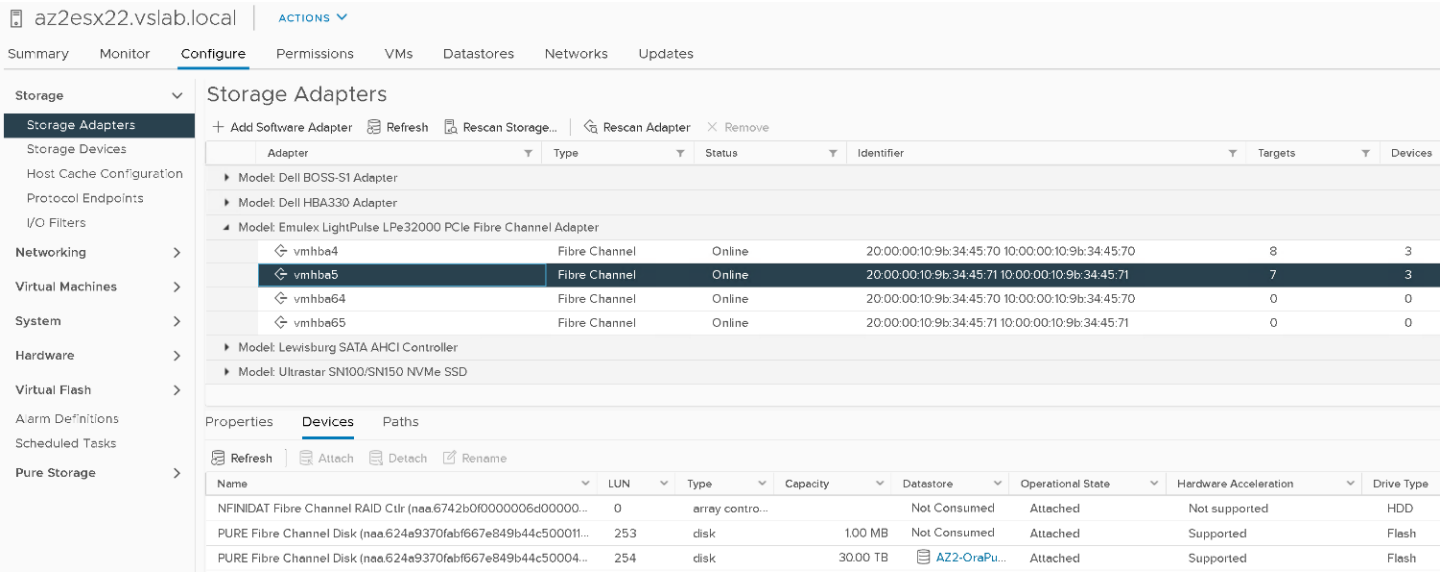


FIGURE 32. Site B ESXi Server FC Storage Connections

Site B contains the following VMFS, vVOL, NFS and vSAN datastores as shown below:

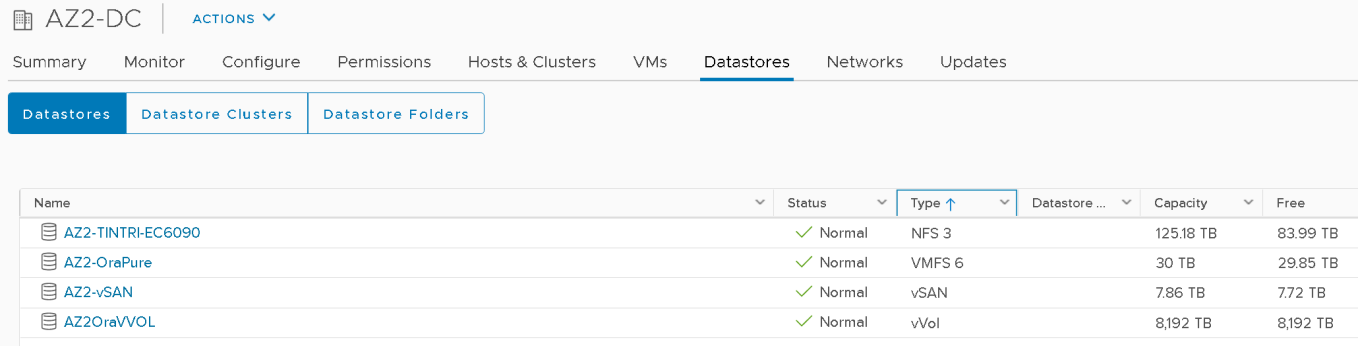


FIGURE 33. Site B Datastores

As indicated earlier, VMware vSAN can set availability, capacity, and performance policies per VM.

In the case of VMware Cloud on AWS, which uses vSAN storage internally, 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, **vsanDatastore**, is used to store the management VMs; the other datastore, **WorkloadDatastore**, is used for the customer VMs.

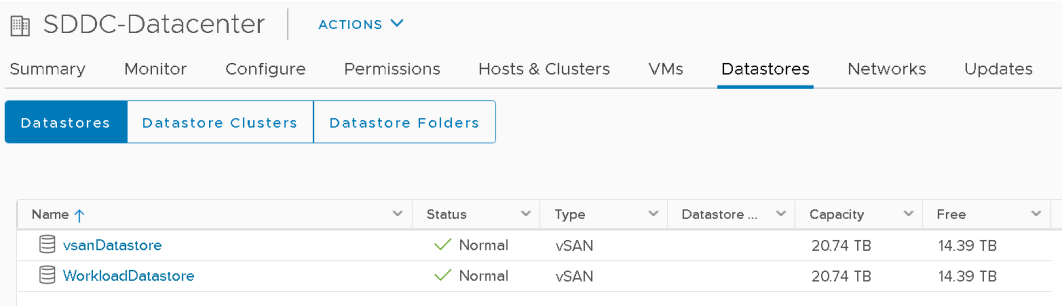


FIGURE 34. VMware Cloud on AWS vSAN Datastore

VMware creates and operates a separate resource pool to manage customer workloads. Customers have the option of creating child resource pools but cannot configure compute policies at initial availability.

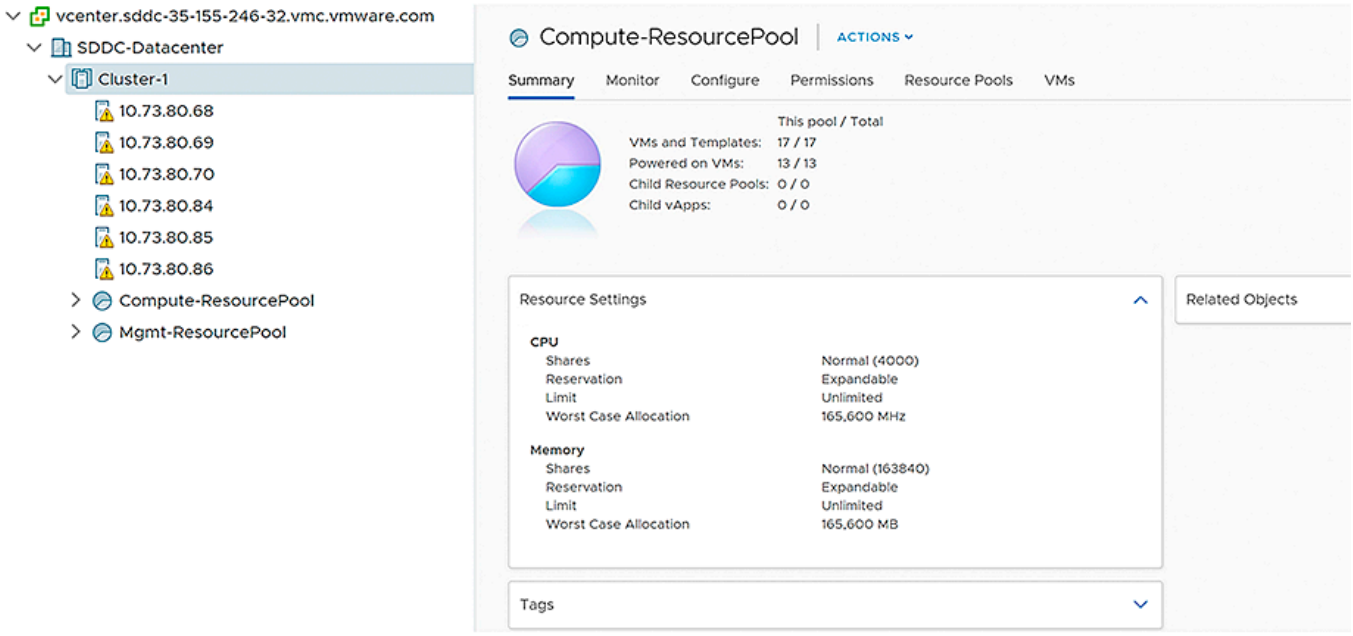


FIGURE 35. VMware Cloud on AWS Compute Resource Pool

The default vSAN storage policy, **vSAN Default Storage Policy**, on VMware Cloud on AWS is shown below:

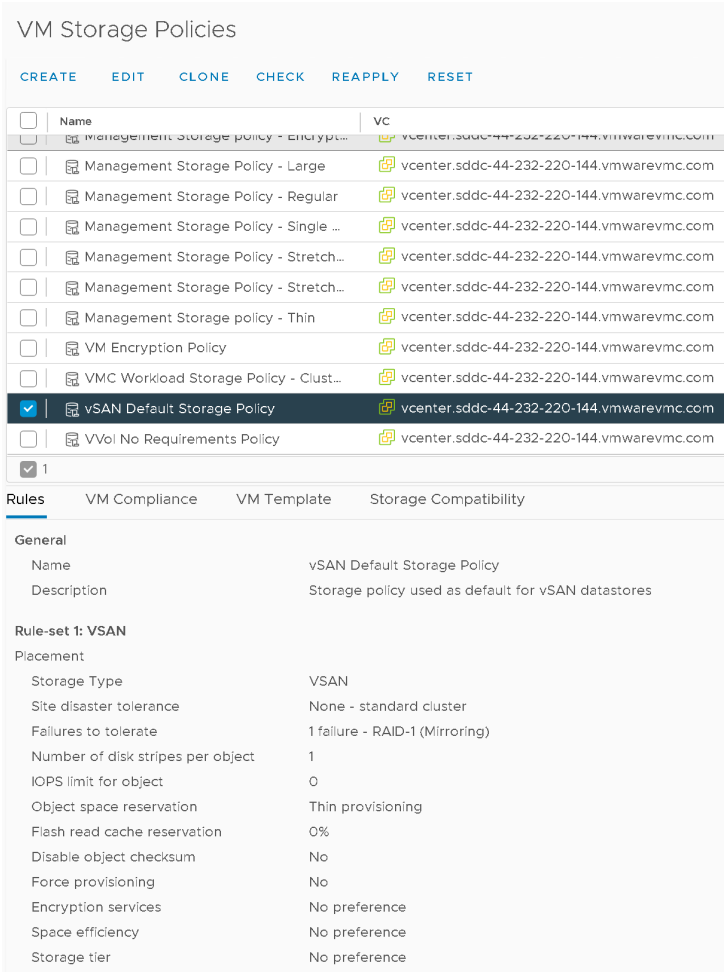


FIGURE 36. VMware Cloud on AWS Default vSAN Storage Policy

Learn more about *vSAN Storage Policies and RAID configuration options on VMware Cloud on AWS*.

VMware and Oracle Configuration

For on-premises Site A, two VMs were configured:

- One VM for production single-instance Oracle VM **Oracle19c12-OEL83**
- One VM for production single-instance Oracle VM **Oracle19c-OL8-Primary**

For on-premises Site B, one VM was configured:

- One VM for DR single-instance physical standby Oracle VM **Oracle19c-OL8-Standby** for the primary database Oracle VM **Oracle19c-OL8-Primary** on Site A

Storage for the three on-premises VMs was provisioned as indicated below:

- Production single-instance Oracle VMs **Oracle19c12-OEL83** and **Oracle19c-OL8-Primary** are provisioned on Pure Storage X50 All-Flash FC Block VMFS6 datastore.
- DR single-instance physical standby Oracle VM **Oracle19c-OL8-Standby** is provisioned on Tintri T880 All-Flash NFS Storage with support for vSphere APIs for array integration (VAAI).

The on-premises Site A and Site B single-instance and physical standby VMs were created with the following components and settings:

- 8 vCPUs and 32GB memory
- Oracle Enterprise Linux 8.3 OS
- Oracle 19.12 Grid infrastructure and RDBMS binaries installed on all VMs
- Oracle SGA set to 16GB, and PGA set to 6GB for all database instances
- Oracle ASM and Oracle ASMLib
- All ASM disk groups disks are presented on different PVSCSI controllers for purposes of performance and queue depth.
- All database-related VMDKs are partitioned using Linux utilities, with proper alignment offset and labeled Oracle ASMLib.
- For sake of simplicity and illustration, one ASM Disk Group was created (**DATA_DG**), housing all datafiles, control files, redo log files and archive log files. Separate ASM diskgroups for these components are recommended per best practice.
- All VMs host both Oracle Grid and RDBMS 19.12 multi-tenant production database **ora19c** with a pluggable database **pdb1**.

Network details for VM **Oracle19c-OL8-Primary** are as follows:

- VM network adapter is connected to port group **APPS-1614** and assigned an IP address 172.16.14.50

Network details for VM **Oracle19c-OL8-Standby** are as follows:

- VM network adapter is connected to port group **APPS-1810** and assigned an IP address 172.18.10.51

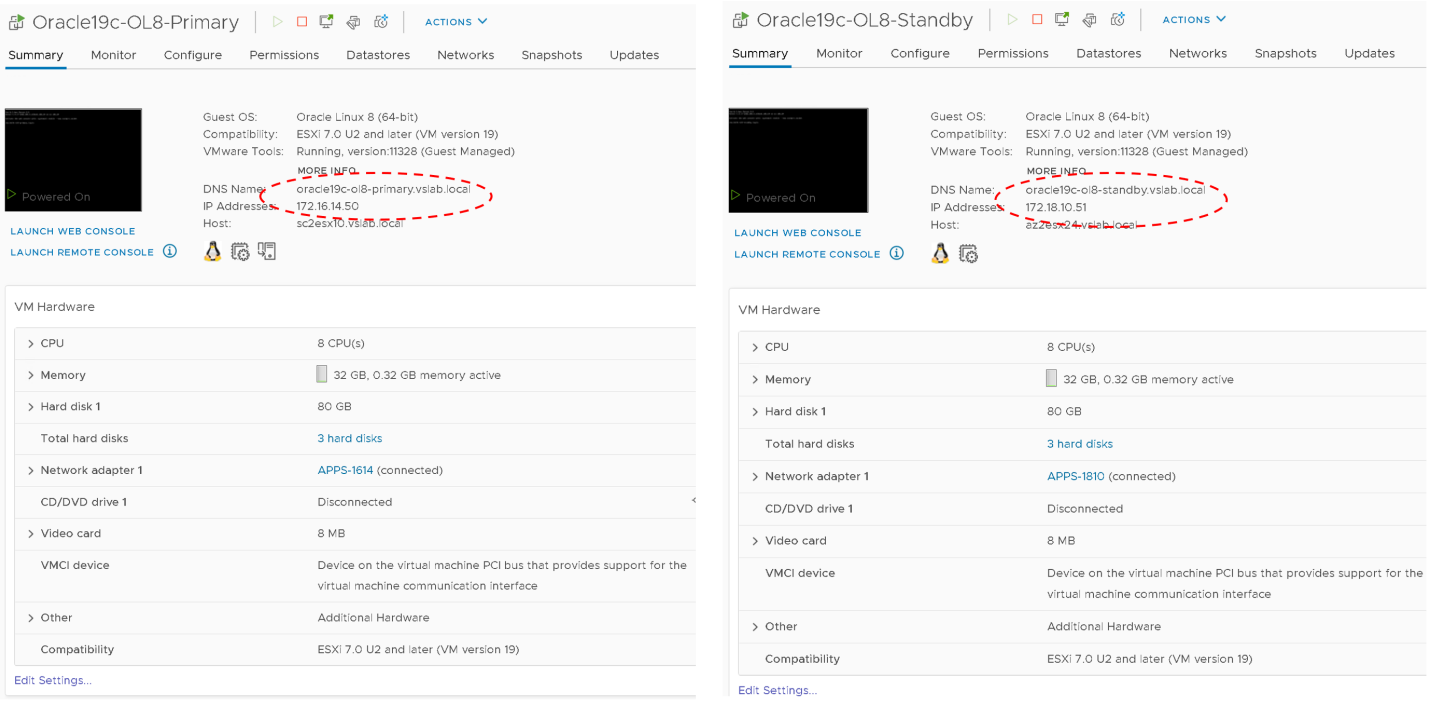


FIGURE 37. Single-Instance Oracle19c-OL8-Primary and Physical Standby Oracle19c-OL8-Standby VM Details

Details for VM **Oracle19c12-OEL83** are as follows:

– VM network adapter is connected to port group **APPS-1614** and assigned an IP address 172.16.14.45

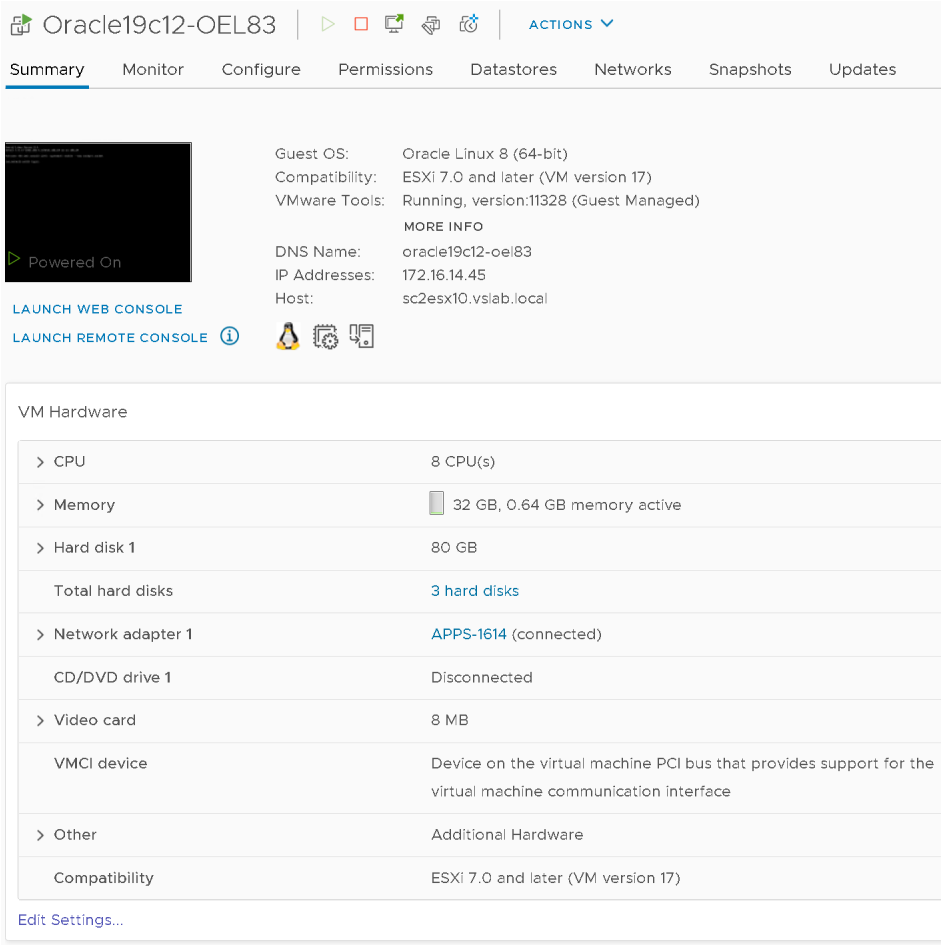


FIGURE 38. Single-Instance Oracle19c12-OEL83 VM Details

The table below details the Oracle VM **Oracle19c12-OEL83**, **Oracle19c-OL8-Primary** and **Oracle19c-OL8-Standby** disk layout and ASM disk group configuration:

NAME	SCSI TYPE	SCSI ID (CONTROLLER, LUN)	SIZE	TYPE	HARD DISK	DISK NAME
Operating System (OS) /	Paravirtual	SCSI (0:0)	80 GB	ext4 file system	1	/dev/sda1
Oracle binary disk /u01	Paravirtual	SCSI (0:1)	80 GB	ext4 file system	2	/dev/sdb1
DATA Disk 1	Paravirtual	SCSI (1:0)	500 GB	DATA_DG	3	DATA_DISK01

TABLE 9. VMs Oracle19c12-OEL83, Oracle19c-OL8-Primary and Oracle19c-OL8-Standby Disk Layout

The table below summarizes the network details:

- Production single-instance Oracle VM **Oracle19c12-OEL83**
- Production single-instance Oracle primary VM **Oracle19c-OL8-Primary** with production single-instance Oracle physical standby **Oracle19c-OL8-Standby**

NETWORK	SITE A VM	SINGLE-INSTANCE PRIMARY	SINGLE-INSTANCE STANDBY
VM Name	Oracle19c12-OEL83	Oracle19c-OL8-Primary	Oracle19c-OL8-Standby
Public FDQN	oracle19c12-oel83.vslab.local	oracle19c-ol8-primary.vslab.local	oracle19c-ol8-standby.vslab.local
Public IP	172.16.14.45	172.16.14.50	172.18.10.51

For VMware Cloud on AWS, one single-instance Oracle VM **Oracle19c12-OEL83-VMC** was configured.

Storage for the VMware Cloud on AWS VM was provisioned on HCI vSAN storage.

The VMware Cloud on AWS single instance was created with the following components and settings:

- 8 vCPUs and 32GB memory
- Oracle Enterprise Linux 8.3 OS
- Oracle 19.12 Grid infrastructure and RDBMS binaries installed on all VMs
- Oracle SGA set to 16GB, and PGA set to 6GB for all database instances
- Oracle ASM and Oracle ASMLib
- All ASM disk groups disks are presented on different PVSCSI controllers for purposes of performance and queue depth.
- All database-related VMDKs are partitioned using Linux utilities, with proper alignment offset and labeled Oracle ASMLib.
- For sake of simplicity and illustration, one ASM disk group was created (**DATA_DG**) housing all datafiles, control files, redo log files and archive log files. Separate ASM diskgroups are recommended for these components per best practice.
- VM hosts both Oracle Grid and RDBMS 19.12 multi-tenant standby production database **ora19c** with a pluggable database **pdb1**.

Network details for VM **Oracle19c12-OEL83-VMC** are as follows:

  – VM network adapter is connected to port group **Apps Team 01** and assigned an IP address 172.16.115.45

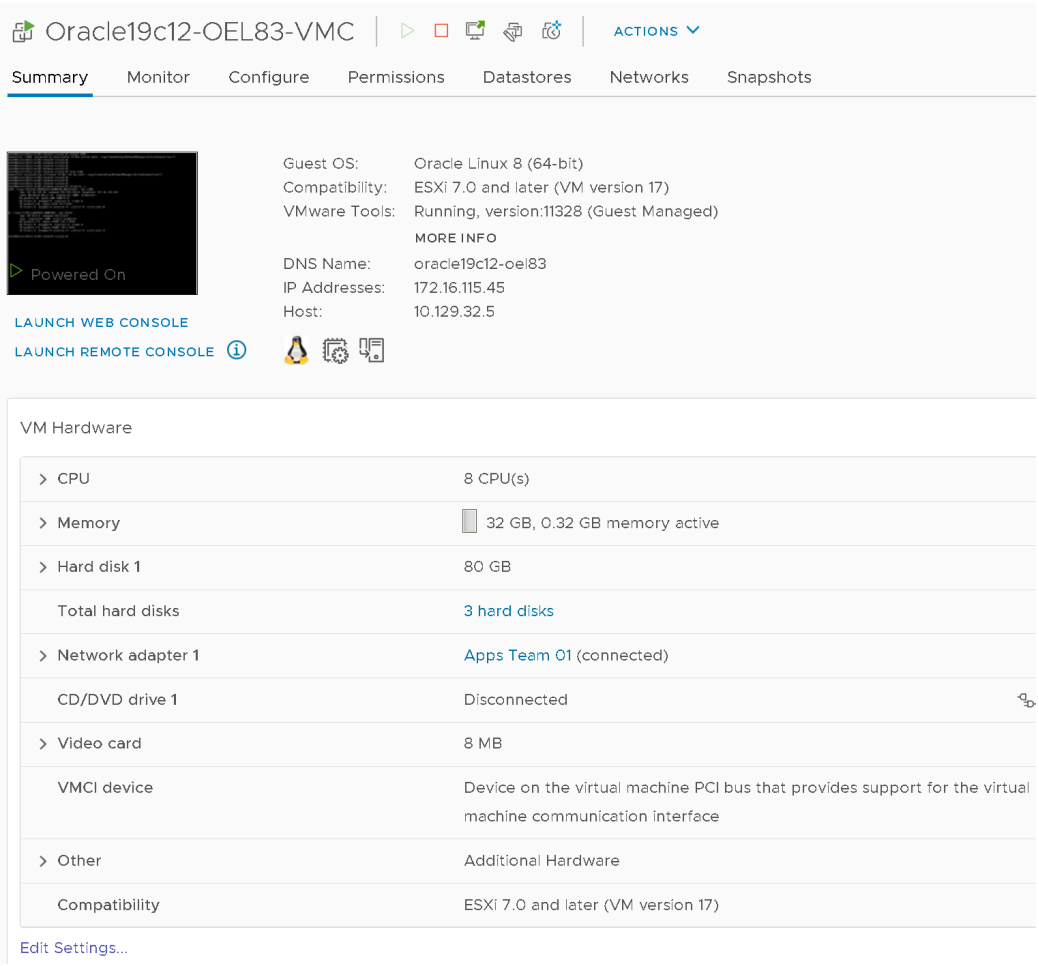


FIGURE 39. Single-Instance Oracle19c12-OEL83-VMC VM Details

The table below details the Oracle VM **Oracle19c12-OEL83-VMC** disk layout and ASM disk group configuration:

NAME	SCSI TYPE	SCSI ID (CONTROLLER, LUN)	SIZE	TYPE	HARD DISK	DISK NAME
Operating System (OS) /	Paravirtual	SCSI (0:0)	80 GB	ext4 file system	1	/dev/sda1
Oracle binary disk /u01	Paravirtual	SCSI (0:1)	80 GB	ext4 file system	2	/dev/sdb1
DATA Disk 1	Paravirtual	SCSI (1:0)	500 GB	DATA_DG	3	DATA_DISK01

TABLE 10. VMs Oracle19c12-OEL83-VMC Disk Layout

The table below summarizes the network details for cloud single-instance Oracle VM **Oracle19c12-OEL83-VMC**:

NETWORK	VMWARE CLOUD ON AWS VM
VM Name	Oracle19c12-OEL83-VMC
Public FDQN	oracle19c12-oel83-vmc.vslab.local
Public IP	172.16.115.45

TABLE 11. VMs Oracle19c12-OEL83-VMC Network Details

See *Appendix A* for the complete list of Oracle initialization parameters for the RAC **vmcrac** database.

All best practices for Oracle workloads on a VMware SDDC were followed in accordance with the *Oracle Databases on VMware Best Practices Guide*.

VMware Hybrid Cloud Extension Configuration

VMware Hybrid Cloud Extension was used for migrating Oracle workloads from Site A to VMware Cloud on AWS.

The hybrid cloud extension connector at Site A (VSLAB) initiates site pairing and the service mesh appliances initiate the interconnect tunnels. The Hybrid Cloud Extension Cloud Manager and the service mesh appliances at the public cloud (VMware Cloud on AWS – **VMC-VSLAB**) are the receivers.

Learn more about *VMware Hybrid Cloud Extension Deployment types*.

Refer to *Hybrid Cloud Extension Installation Workflow for Hybrid Cloud Extension Public Clouds* for activating Hybrid Cloud Extension on VMware Cloud on AWS.

Download, deploy and activate the Hybrid Cloud Extension Manager in the source environment using the Hybrid Cloud Extension Connector OVA as per *Hybrid Cloud Extension Installation Workflow for Hybrid Cloud Extension Public Clouds*.

Pair Hybrid Cloud Extension Connector with Hybrid Cloud Extension Cloud as outlined in *Adding a Site Pair*.

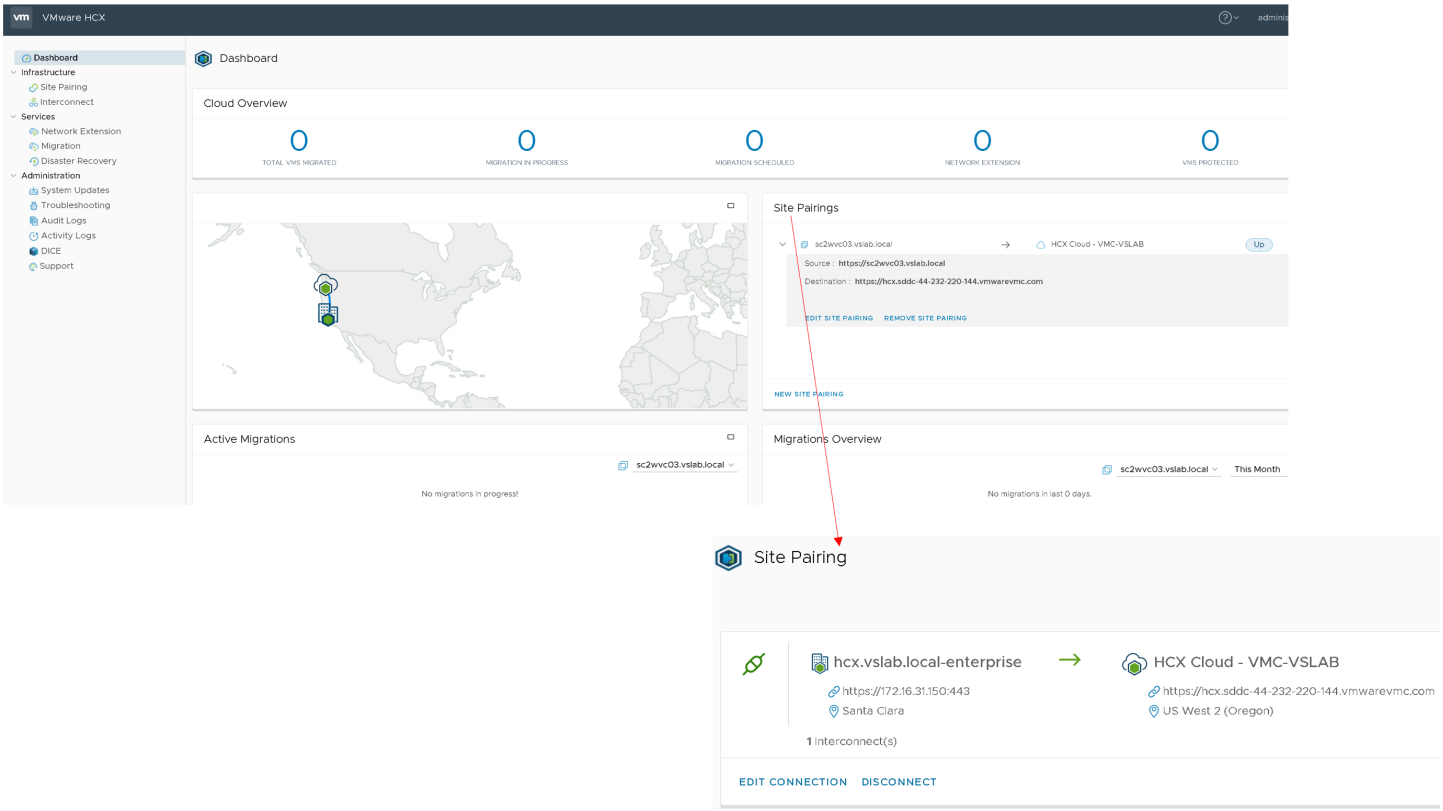


FIGURE 40. Hybrid Cloud Extension Site Pairing Between Site A (VSLAB) and VMware Cloud on AWS (VMC-VSLAB)

The Hybrid Cloud Extension Manager (connector) on Site A and Hybrid Cloud Extension Cloud Manager on VMware Cloud on AWS are as shown below:

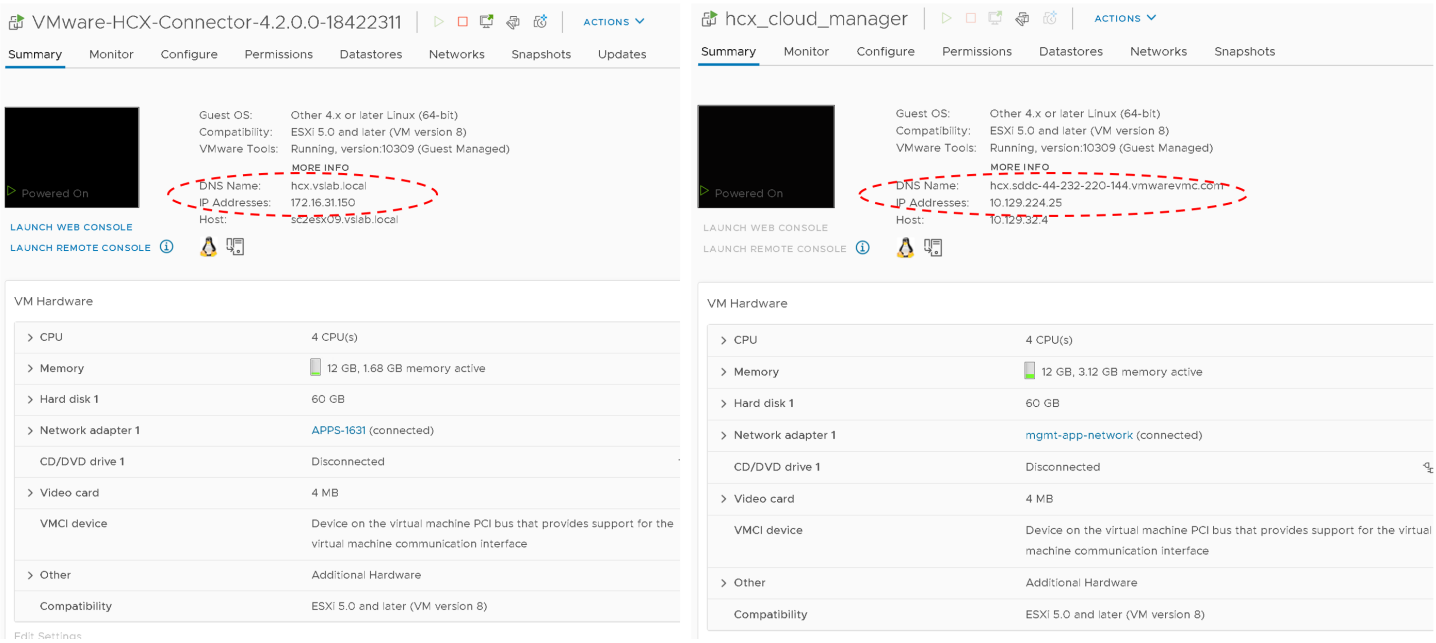


FIGURE 41. Hybrid Cloud Extension Manager (Connector) on Site A and Hybrid Cloud Extension Cloud Manager on VMware Cloud on AWS

Hybrid Cloud Extension Network profiles for Site A are as shown below:

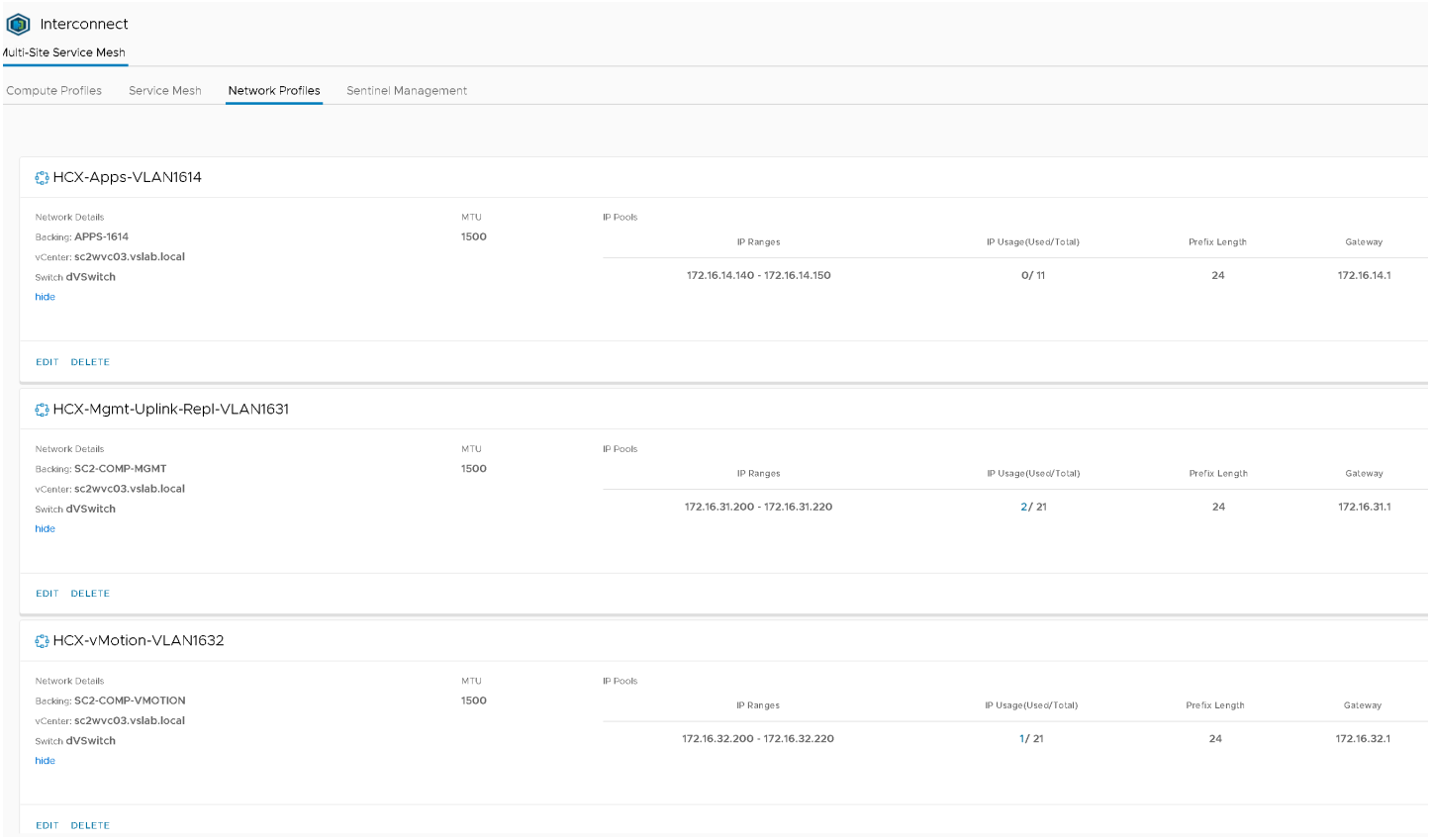


FIGURE 42. Hybrid Cloud Extension Network Profiles for Site A

Hybrid Cloud Extension Network profiles for VMware Cloud on AWS are as shown below:

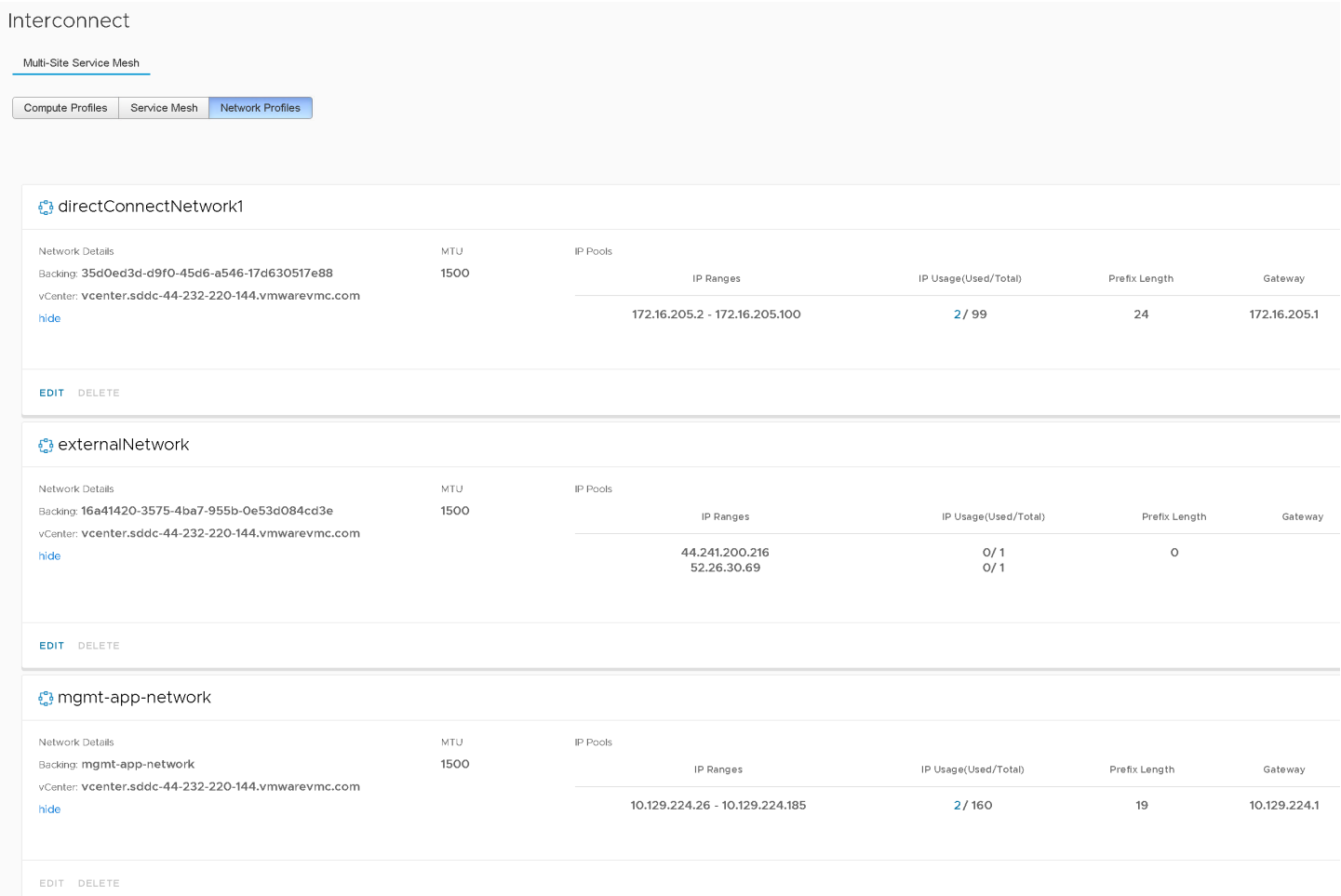


FIGURE 43. Hybrid Cloud Extension Network Profiles for VMware Cloud on AWS

Hybrid Cloud Extension network mapping for Site A and VMware Cloud on AWS is as shown below:

NETWORK	SOURCE SITE	NETWORK PROFILE	DESTINATION SITE	DESTINATION NETWORK
VM Network	Site A	Hybrid Cloud Extension-Apps-VLAN1614	VMware Cloud on AWS	Apps Team 01
Management, Replication	Site A	Hybrid Cloud Extension-Mgmt-Uplink-Repl-VLAN1631	VMware Cloud on AWS	directConnectNetwork1
vMotion	Site A	Hybrid Cloud Extension-vMotion-VLAN1632	VMware Cloud on AWS	Part of the Service Mesh

TABLE 12. Hybrid Cloud Extension Network Details Between Site A and VMware Cloud on AWS

The compute profile for Site A is as shown below:

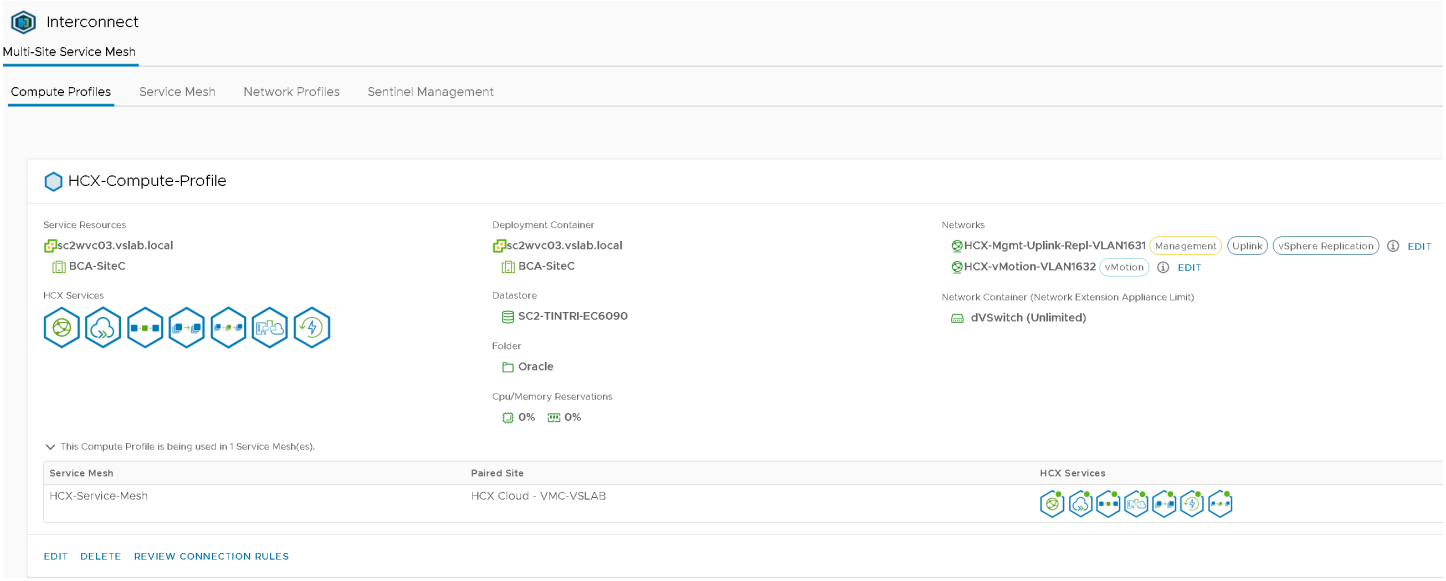


FIGURE 44. Site A Compute Profile

The summary of **HCX-Compute-Profile** is shown below:

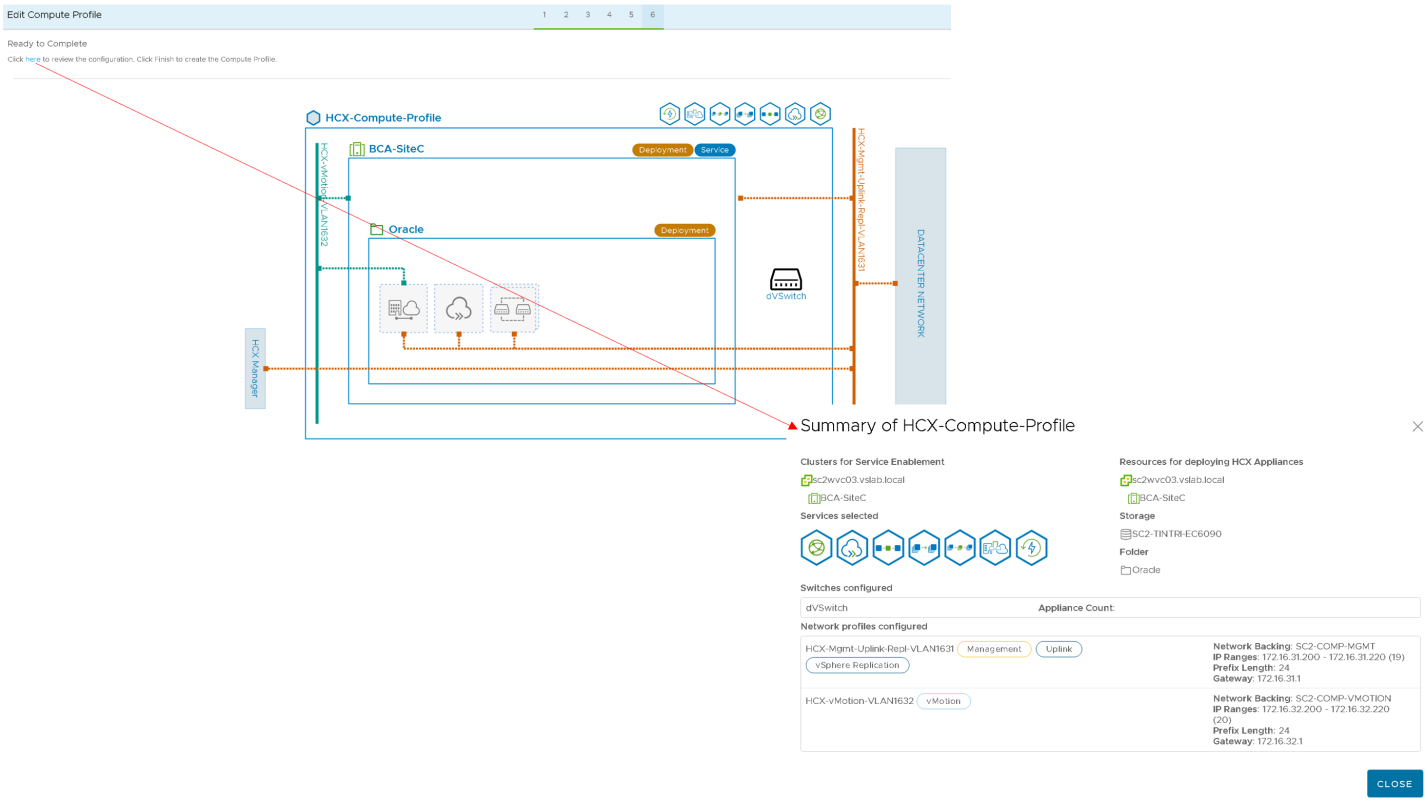


FIGURE 45. Summary of HCX-Compute-Profile

The compute profile for VMware Cloud on AWS is as shown below:

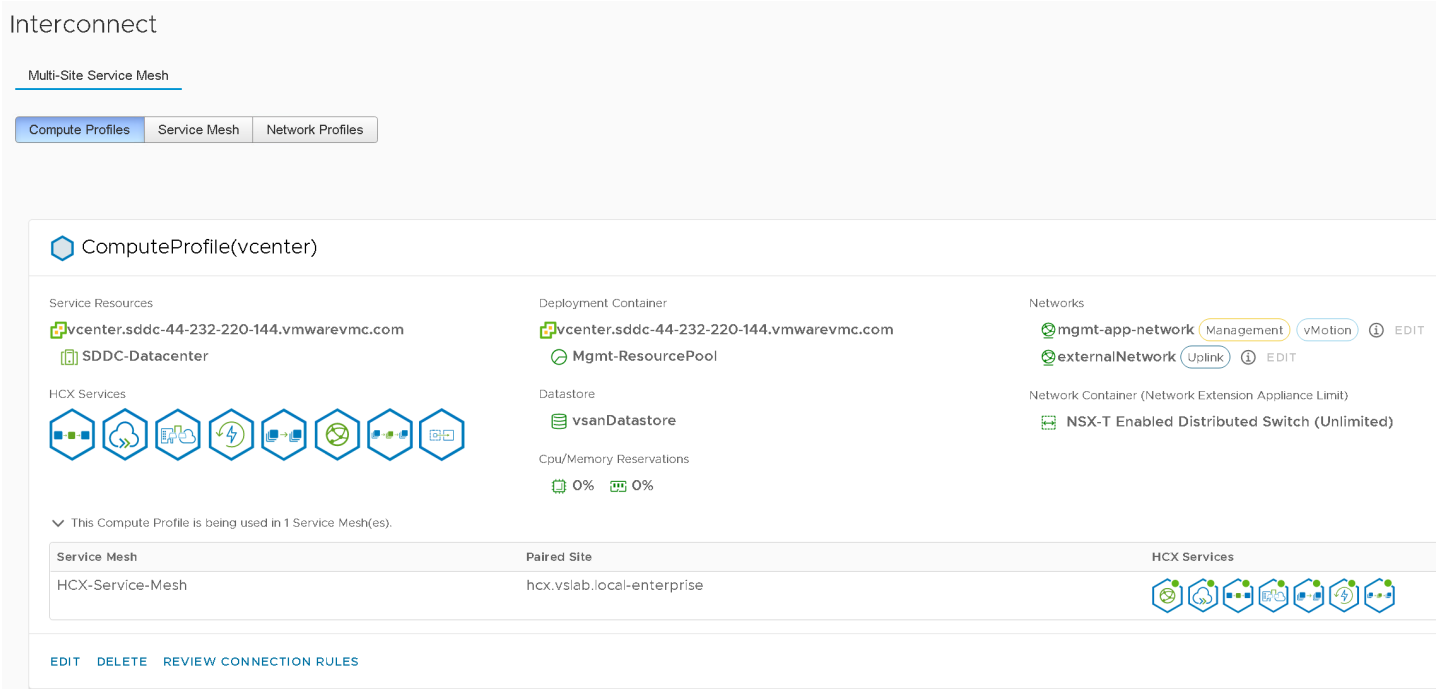


FIGURE 46. VMware Cloud on AWS Compute Profile

The summary of VMware Cloud on AWS **HCX-Compute-Profile** is shown below:

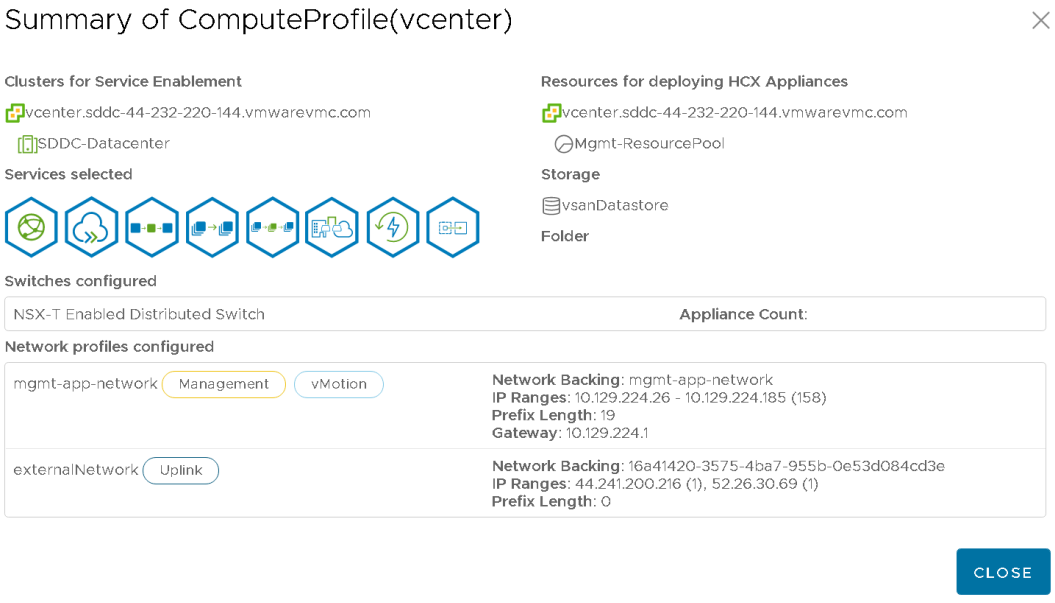


FIGURE 47. Summary of HCX-Compute-Profile

The service mesh topology on Site A is as shown below:

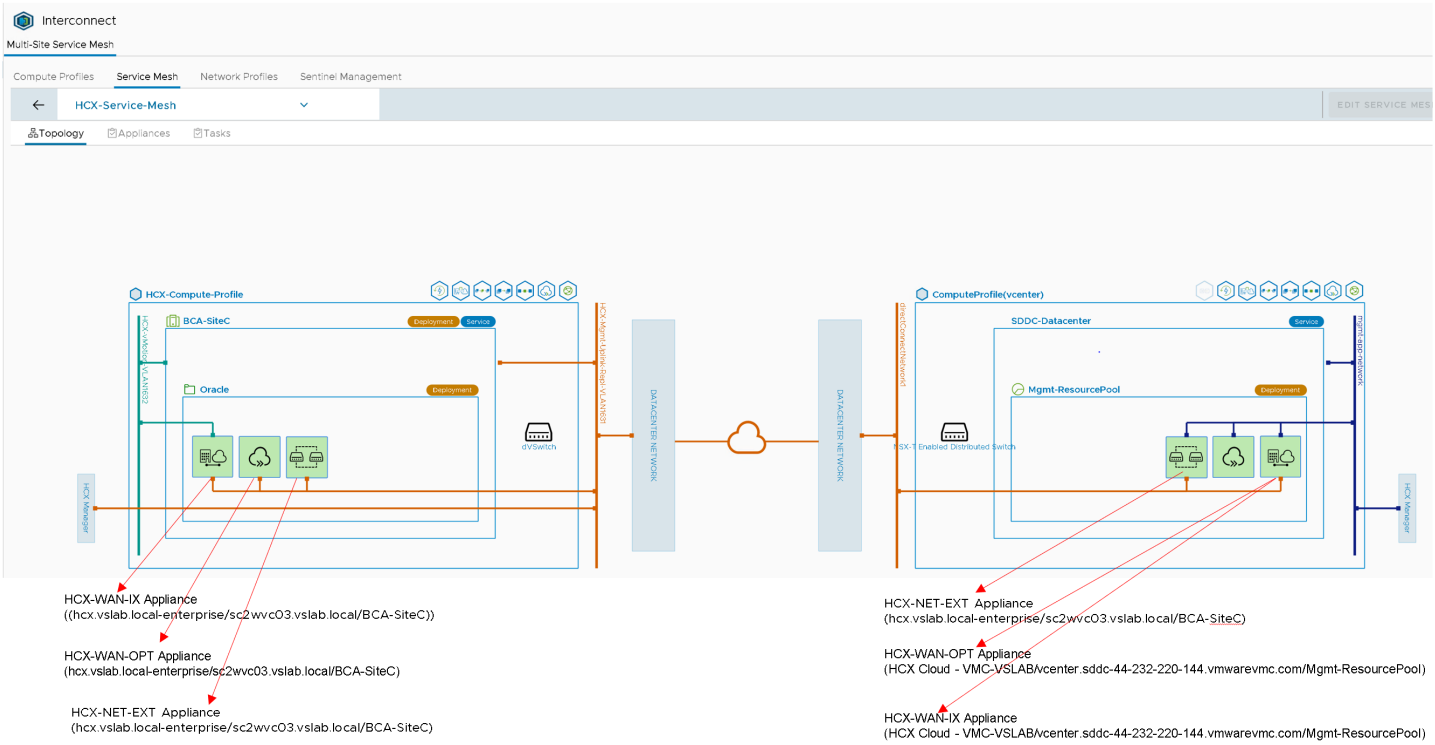


FIGURE 48. Site A Service Mesh Topology

The service mesh appliances view on Site A is as shown below:

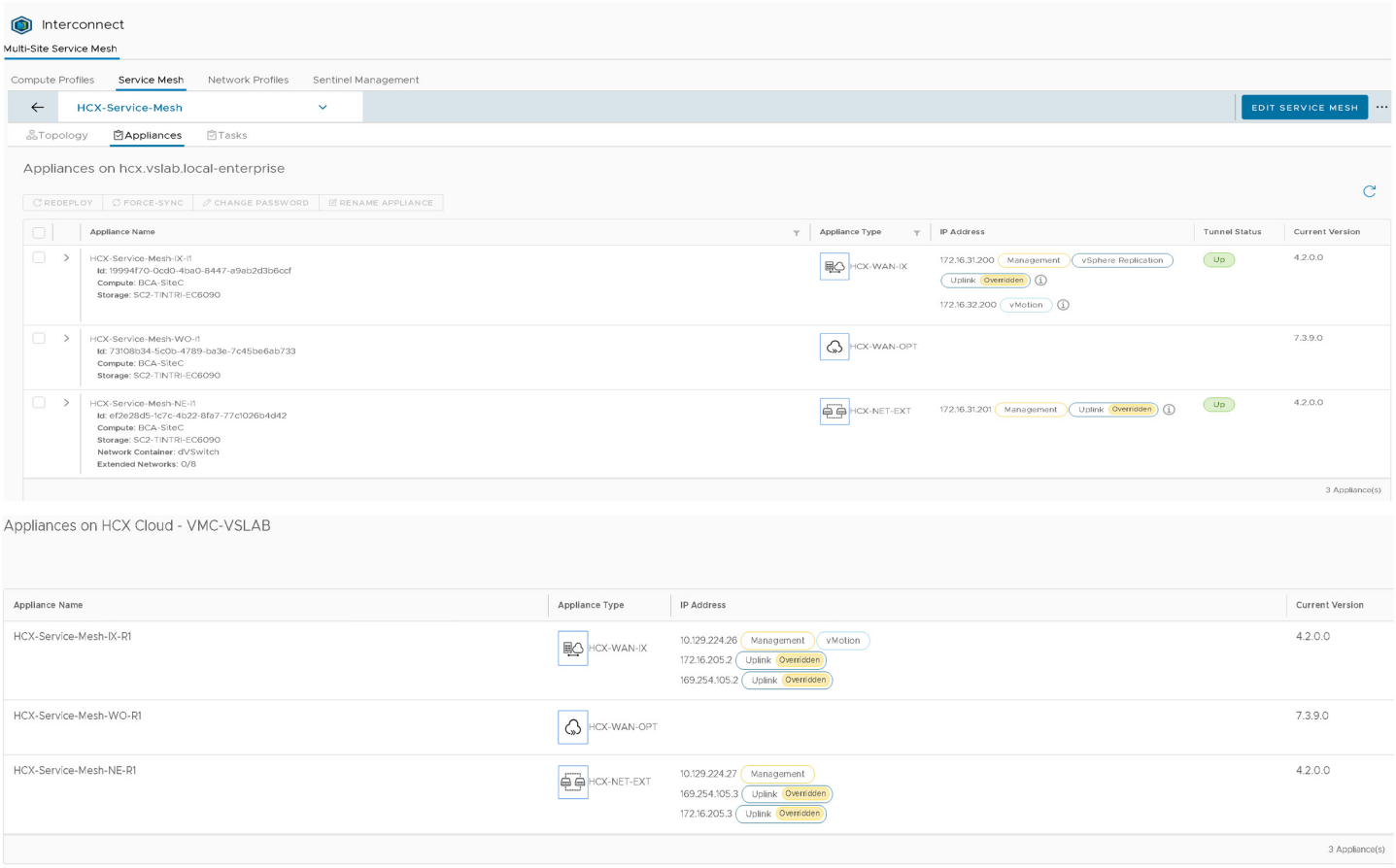


FIGURE 49. Site A Service Mesh Appliances

The service mesh on VMware Cloud on AWS is as shown below:

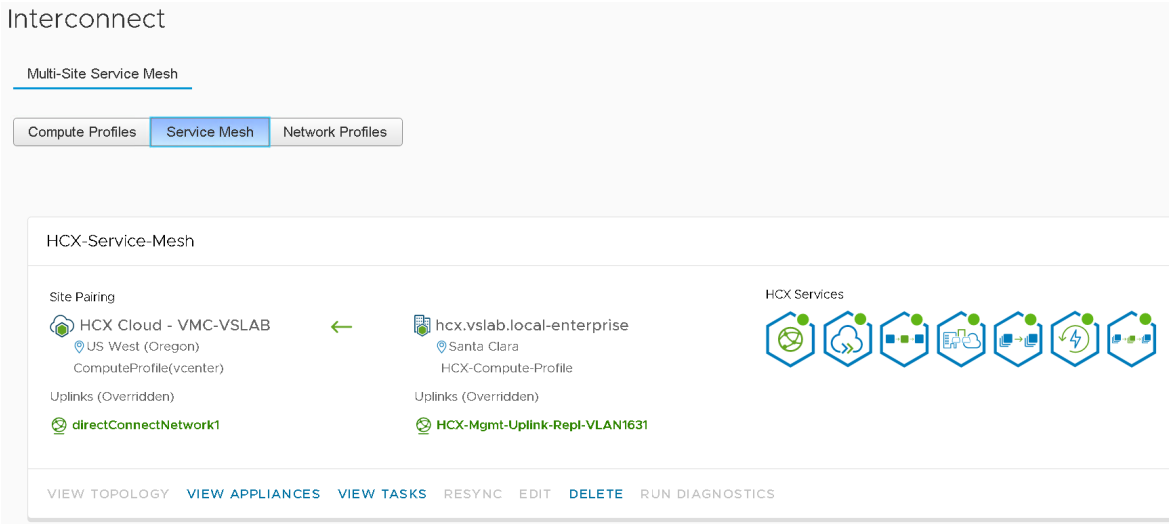


FIGURE 50. VMware Cloud on AWS Service Mesh

The service mesh appliances on VMware Cloud on AWS are as shown below:

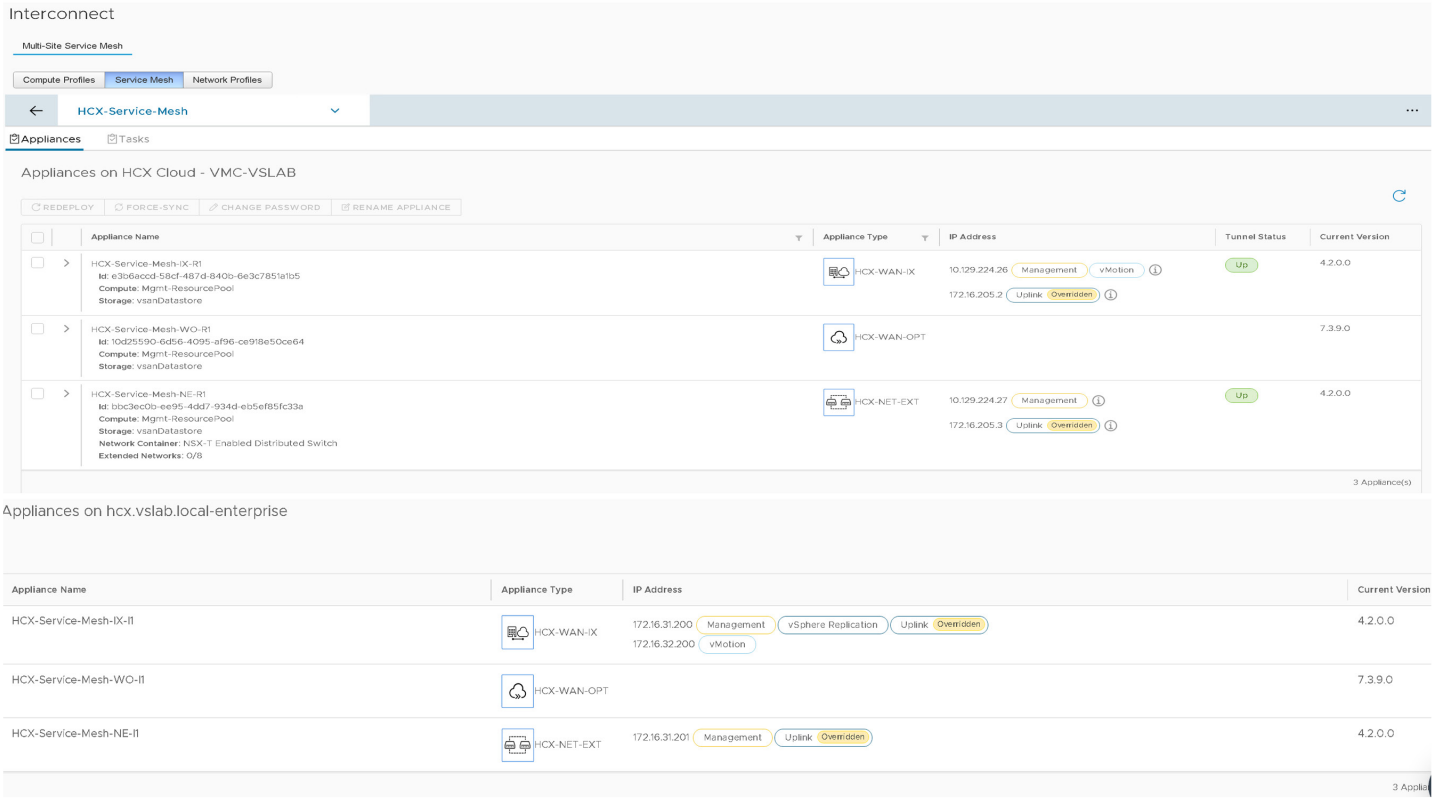


FIGURE 51. VMware Cloud on AWS Service Mesh Appliances

Solution Validation

This solution is designed and deployed three separate environments:

For on-premises Site A, one VM was configured:

- One VM for production single-instance Oracle VM **Oracle19c12-OEL83**

For on-premises Site A and Site B, one primary-standby VM pair was configured:

- One VM for production single-instance Oracle primary VM **Oracle19c-OL8-Primary** on Site A
- One VM for DR single-instance Oracle physical standby VM **Oracle19c-OL8-Standby** on Site B

For VMware Cloud on AWS, one single-instance Oracle VM **Oracle19c12-OEL83-VMC** was configured.

In this section, we present the test methodologies and processes used in this reference architecture.

Solution Test Overview

The solution validated the following:

- Deployment of a:
  - Production single-instance Oracle VM **Oracle19c12-OEL83** on Site A
  - Production single-instance Oracle VM **Oracle19c-OL8-Primary** on Site A and single-instance physical standby Oracle VM **Oracle19c-OL8-Standby** on Site B
  - Production single-instance Oracle VM **Oracle19c12-OEL83-VMC** in VMware Cloud on AWS
- Understanding VMware Hybrid Cloud Extension and Oracle migration methods to migrate Oracle workloads from on-premises to VMware Cloud on AWS
- Migration of a:
  - Production single-instance Oracle VM **Oracle19c12-OEL83** from on-premises Site A to VMware Cloud on AWS
  - Production single-instance physical standby Oracle VM **Oracle19c-OL8-Standby** from on-premises Site B to VMware Cloud on AWS

Test and Performance Metrics Data Collection Tools

The test and performance metrics data collection tools are as indicated below:

Test Tools and Configuration

SLOB Workload

SLOB is an Oracle workload generator designed to stress test storage I/O capability, specifically for Oracle Database using OLTP workload. SLOB is not a traditional transactional benchmark tool. It is used to validate performance of the storage subsystem without application contention.

SLOB Configuration

- Database VM with a 16GB SLOB schema
- SLOB parameter UPDATE_PCT set to 100 to reflect very heavy I/O workload
- Think Time was set 0 to hit database with maximum requests concurrently to generate extremely intensive batch workload
- SLOB parameter SCALE for the workload set to 16GB with Oracle SGA set to 16GB
- SLOB parameter REDO_STRESS for the workload set to HEAVY
- SLOB parameter RUN_TIME set to 30 minutes

The detailed SLOB configuration is included in *Appendix C: SLOB Configuration*.

Key Metrics Data Collection Tools

The following monitoring tools are used in this solution:

- Oracle Automatic Workload Repository
  - (AWR) reports with Automatic Database Diagnostic Monitor (ADDM). AWR collects, processes, and maintains performance statistics for problem-detection and self-tuning purposes for Oracle Database. This tool can generate reports for analyzing Oracle performance. ADDM analyzes data in AWR to identify potential performance bottlenecks. For each of the identified issues, it locates the root cause and provides recommendations for correcting the problem. Learn more about *Oracle AWR*.
- Oracle dynamic performance (V$) views and Oracle Alert log to check for errors
- Linux system activity report (SAR)
  - Linux SAR helps collect and evaluate a variety of information regarding system activity. With performance problems, SAR also permits retroactive analysis of the load values for various subsystems (e.g., CPUs, memory, disks, interrupts, network interfaces). Learn more about *Linux SAR*.

Deploying Oracle Workloads on On-premises

Successful deployment of Oracle workloads on VMware vSphere platform using VMDKs, regardless of the underlying storage (VMFS, iSCSI, NFS, vSAN, vVOL) is not significantly different from deploying Oracle on physical servers. Oracle DBAs can fully leverage their current skill set while also delivering the benefits associated with virtualization.

A VM template **Template-OL8-ORA19C** with all of the required OS patches was used to provision the below VMs. Oracle ASM with Oracle ASMLib was used to provision the database storage.

The steps to deploy a production single-instance Oracle database **ora19c** on VM **Oracle19c12-OEL83** Oracle database on Site A are no different than deploying a single-instance Oracle database on any physical architecture.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Aug 20 20:46:52 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 52. Oracle Database ora19c in VM Oracle19c12-OEL83 on Site A

The steps to deploy a production single-instance Oracle database **ora19c** on VM **Oracle19c-OL8-Primary** on Site A and single-instance physical standby database **ora19c** on VM **Oracle19c-OL8-Standby** on Site B are no different than deploying the same on any physical architecture.

Two VMs are utilized for this use case:

- Primary Oracle database VM **Oracle19c-OL8-Primary** with IP address 172.16.14.50 on Site A
- Physical standby database VM **Oracle19c-OL8-Standby** with IP address 172.18.10.51 on Site B

```
oracle@oracle19c-ol8-primary:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.50  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:a0:7d:17  txqueuelen 1000  (Ethernet)
        RX packets 126861  bytes 110854760 (105.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 43915  bytes 34882819 (33.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16328  bytes 1434738 (1.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16328  bytes 1434738 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c-ol8-primary:ora19c:/home/oracle>
oracle@oracle19c-ol8-primary:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Sat Aug 21 20:21:15 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name,database_role,open_mode from v$database;

NAME      DATABASE_ROLE    OPEN_MODE
--------- ---------------- --------------------
ORA19C    PRIMARY          READ WRITE

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c-ol8-primary:ora19c:/home/oracle>
```

```
oracle@oracle19c-ol8-standby:ora19csb:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.10.51  netmask 255.255.255.0  broadcast 172.18.10.255
        ether 00:50:56:a0:75:a1  txqueuelen 1000  (Ethernet)
        RX packets 128251  bytes 142822193 (136.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44949  bytes 3317519 (3.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16232  bytes 1416535 (1.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16232  bytes 1416535 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c-ol8-standby:ora19csb:/home/oracle>
oracle@oracle19c-ol8-standby:ora19csb:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Sat Aug 21 20:21:35 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name,database_role,open_mode from v$database;

NAME      DATABASE_ROLE    OPEN_MODE
--------- ---------------- --------------------
ORA19C    PHYSICAL STANDBY MOUNTED

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c-ol8-standby:ora19csb:/home/oracle>
```

FIGURE 53. Primary and Standby Oracle Database Details

Setup of Oracle Data Guard and Oracle GoldenGate are beyond the scope of this paper. Learn more about *Oracle Data Guard*.

The primary and standby database statuses are as shown below. There is no archive log gap on the standby database.

Primary Oracle Database VM Oracle19C-OL8-Primary	Standby Oracle Database VM Oracle19C-OL8-Standby
SQL> SELECT sequence#, first_time, next_time, applied FROM v$archived_log ORDER BY sequence#; SEQUENCE# FIRST_TIM NEXT_TIME APPLIED ---------- --------- --------- --------- 10 28-JUL-21 29-JUL-21 NO 11 29-JUL-21 29-JUL-21 NO 12 29-JUL-21 31-JUL-21 NO 13 31-JUL-21 31-JUL-21 NO 14 31-JUL-21 01-AUG-21 NO 15 01-AUG-21 02-AUG-21 NO 16 02-AUG-21 02-AUG-21 NO 17 02-AUG-21 03-AUG-21 NO 18 03-AUG-21 03-AUG-21 NO 19 03-AUG-21 03-AUG-21 NO 20 03-AUG-21 03-AUG-21 NO 20 03-AUG-21 03-AUG-21 YES 21 03-AUG-21 03-AUG-21 NO ... 48 04-AUG-21 04-AUG-21 NO 48 04-AUG-21 04-AUG-21 YES 49 04-AUG-21 04-AUG-21 YES 49 04-AUG-21 04-AUG-21 NO 70 rows selected. SQL>	SQL> SELECT ARCH.THREAD# "Thread", ARCH.SEQUENCE# "Last Sequence Received", APPL.SEQUENCE# "Last Sequence Applied", ARCH.SEQUENCE# - APPL.SEQUENCE# "Difference" FROM (SELECT THREAD#,SEQUENCE# FROM V$ARCHIVED_LOG WHERE (THREAD#,FIRST_TIME) IN (SELECT THREAD#,MAX(FIRST_TIME) FROM V$ARCHIVED_LOG GROUP BY THREAD#)) ARCH, (SELECT THREAD#,SEQUENCE# FROM V$LOG_HISTORY WHERE (THREAD#,FIRST_TIME) IN (SELECT THREAD#,MAX(FIRST_TIME) FROM V$LOG_HISTORY GROUP BY THREAD#)) APPL WHERE ARCH.THREAD# = APPL.THREAD# ORDER BY 1; Thread Last Sequence Received Last Sequence Applied Difference ---------- ------------------------- ------------------------ ---------- 1 49 49 0 SQL> SQL> SELECT * FROM V$ARCHIVE_GAP; no rows selected SQL>

FIGURE 54. Primary and Standby Oracle Database Status

The standby Oracle VM **Oracle19c-OL8-Standby** alert log for the database **ora19c** on Site B shows no errors and shows redo log application as they are generated on primary database on Site A.

```
ARC6 started with pid=50, OS id=3599
Starting background process ARC7
2021-08-04T12:37:59.207328-07:00
ARC7 started with pid=37, OS id=3603
Starting background process ARC8
2021-08-04T12:37:59.219953-07:00
ARC8 started with pid=51, OS id=3607
Starting background process ARC9
2021-08-04T12:37:59.233571-07:00
ARC9 started with pid=53, OS id=3610
2021-08-04T12:37:59.233589-07:00
TMON (PID:3546): ARC1: Archival started
TMON (PID:3546): ARC2: Archival started
TMON (PID:3546): ARC3: Archival started
TMON (PID:3546): ARC4: Archival started
TMON (PID:3546): ARC5: Archival started
TMON (PID:3546): ARC6: Archival started
TMON (PID:3546): ARC7: Archival started
TMON (PID:3546): ARC8: Archival started
TMON (PID:3546): ARC9: Archival started
TMON (PID:3546): STARTING ARCH PROCESSES COMPLETE
2021-08-04T12:38:03.477307-07:00
 rfs (PID:3628): krsr_rfs_atc: Identified database type as 'PHYSICAL STANDBY': Client is Foreground (PID:3584)
2021-08-04T12:38:03.477329-07:00
 rfs (PID:3631): krsr_rfs_atc: Identified database type as 'PHYSICAL STANDBY': Client is ASYNC (PID:3632)
 rfs (PID:3631): Primary database is in MAXIMUM PERFORMANCE mode
2021-08-04T12:38:03.540775-07:00
 rfs (PID:3631): Selected LNO:5 for T-1.S-50 dbid 1132297011 branch 1079108979
2021-08-04T12:38:03.629148-07:00
 rfs (PID:3634): krsr_rfs_atc: Identified database type as 'PHYSICAL STANDBY': Client is FAL (PID:3599)
2021-08-04T12:38:03.691470-07:00
 rfs (PID:3634): Selected LNO:6 for T-1.S-49 dbid 1132297011 branch 1079108979
2021-08-04T12:38:03.790533-07:00
ARC0 (PID:3572): Archived Log entry 32 added for T-1.S-49 ID 0x437cbe33 LAD:1
2021-08-04T12:38:06.387418-07:00
alter database recover managed standby database disconnect from session nodelay
2021-08-04T12:38:06.396206-07:00
Attempt to start background Managed Standby Recovery process (ora19csb)
Starting background process MRP0
2021-08-04T12:38:06.409855-07:00
MRP0 started with pid=57, OS id=3643
2021-08-04T12:38:06.411115-07:00
Background Managed Standby Recovery process started (ora19csb)
2021-08-04T12:38:11.432045-07:00
 Started logmerger process
2021-08-04T12:38:11.445963-07:00
PR00 (PID:3646): Managed Standby Recovery starting Real Time Apply
max_pdb is 3
2021-08-04T12:38:11.640630-07:00
Parallel Media Recovery started with 8 slaves
2021-08-04T12:38:11.683899-07:00
Stopping change tracking
2021-08-04T12:38:11.746157-07:00
PR00 (PID:3646): Media Recovery Log +DATA_DG/ORA19CSB/ARCHIVELOG/2021_08_04/thread_1_seq_49.318.1079699883
PR00 (PID:3646): Media Recovery Waiting for T-1.S-50 (in transit)
2021-08-04T12:38:11.881635-07:00
Recovery of Online Redo Log: Thread 1 Group 5 Seq 50 Reading mem 0
  Mem# 0: +DATA_DG/ORA19CSB/stdby_group05_redo01.log
  Mem# 1: +DATA_DG/ORA19CSB/stdby_group05_redo02.log
2021-08-04T12:38:12.416178-07:00
Completed: alter database recover managed standby database disconnect from session nodelay
2021-08-04T12:46:28.424144-07:00
```

FIGURE 55. Alert log for Standby Oracle Database on Site B

Primary-standby log shipping can be tested by switching log files on the primary database on Site A and observing the same log sequence being applied on the standby database on Site B.

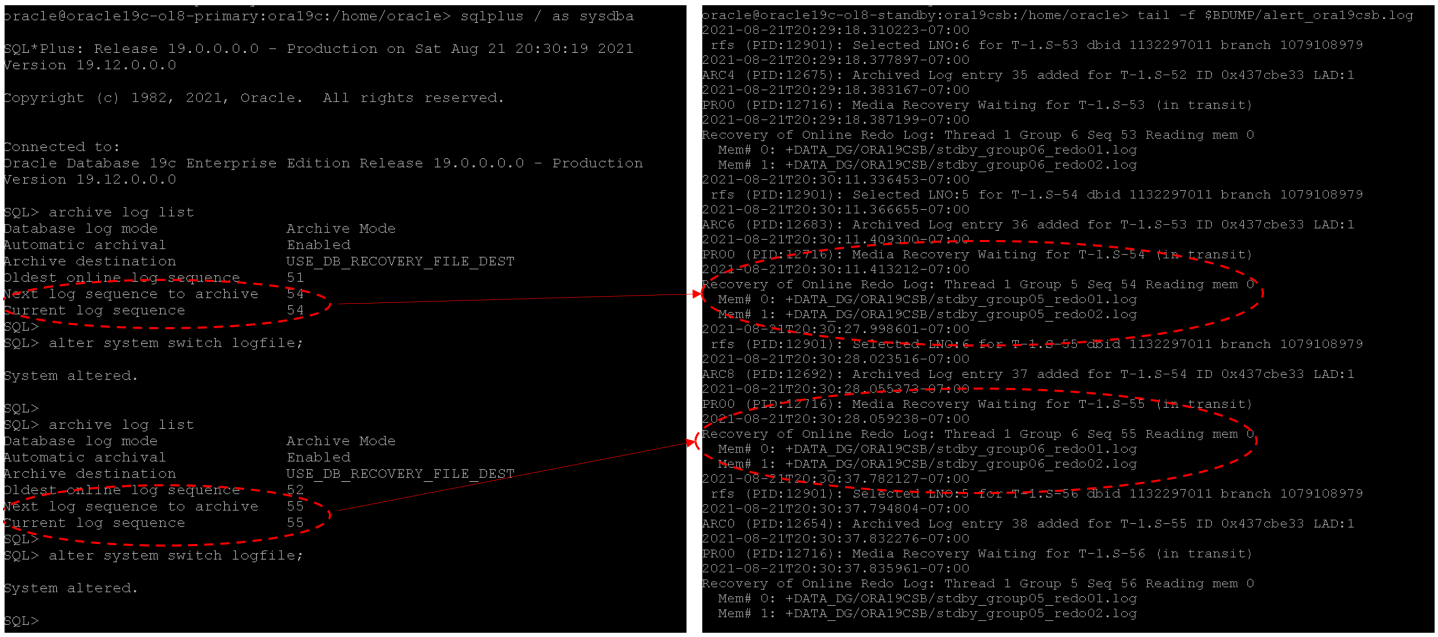


FIGURE 56. Log Switch on Primary Database Results in Changes Applied on Standby Database

Oracle Data Guard role transitions switchover and failover are the same as those for any physical architecture. Learn more about *role transitions*.

The Oracle Databases on VMware Best Practices Guide provides best practice guidelines for deploying Oracle workloads on a VMware SDDC.

In addition to this guide, VMware has created separate best practice documents for storage, networking, and performance. They can be found for the versions specific to vSphere *here*.

Deploying Oracle Workloads on VMware Cloud on AWS

The steps to deploy production single-instance Oracle database **ora19c** on VM **Oracle19c12-OEL83-VMC** Oracle database on VMware Cloud on AWS are no different than those required to deploy a single-instance Oracle database on any VMware vSphere platform.

A VM template **Template-OL8-ORA19C** with all of the required OS patches is used to provision the below VM. Oracle ASM with Oracle ASMLib was used to provision the database storage.

```
oracle@oracle19c12-oel83-vmc:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.115.45  netmask 255.255.255.0  broadcast 172.16.115.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 4044  bytes 719944 (703.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3291  bytes 618096 (603.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 15735  bytes 1556182 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15735  bytes 1556182 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83-vmc:ora19c:/home/oracle>
oracle@oracle19c12-oel83-vmc:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Sat Aug 21 19:59:46 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83-vmc:ora19c:/home/oracle>
oracle@oracle19c12-oel83-vmc:ora19c:/home/oracle>
oracle@oracle19c12-oel83-vmc:ora19c:/home/oracle>
```

FIGURE 57. Oracle Database ora19c in VM Oracle19c12-OEL83-VMC on VMware Cloud on AWS

The steps to deploy a production single-instance physical standby database ora19c on VM Oracle19c-OL8-Standby on VMware Cloud on AWS are no different than those required to deploy the same physical standby architecture on Site B, with the primary instance on VM Oracle19c-OL8-Primary on Site A.

Two VMs are utilized for this use case:

– Primary Oracle database VM **Oracle19c-OL8-Primary** with IP address 172.16.14.50 on Site A

– Physical standby database VM **Oracle19c-OL8-Standby** with IP address 172.16.115.51 on VMware Cloud on AWS

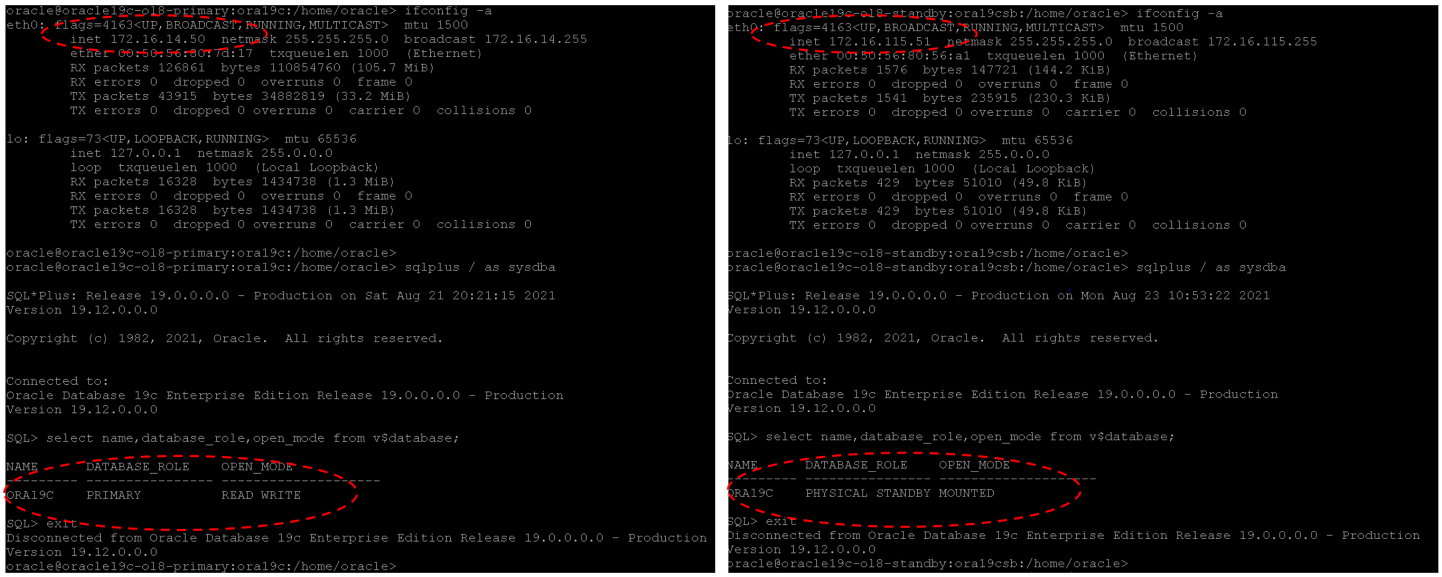


FIGURE 58. Primary and Standby Oracle Database Details

Setup of Oracle Data Guard and Oracle GoldenGate are beyond the scope of this paper. Learn more about *Oracle Data Guard*.

The standby Oracle VM **Oracle19c-OL8-Standby** alert log for the database **ora19c** on VMware Cloud on AWS shows no errors and shows redo log application as generated on the primary database on Site A.

```
2021-08-23T10:51:08.198720-07:00
ARC2 started with pid=46, OS id=4533
Starting background process ARC3
2021-08-23T10:51:08.213059-07:00
ARC3 started with pid=47, OS id=4536
Starting background process ARC4
2021-08-23T10:51:08.232016-07:00
ARC4 started with pid=48, OS id=4539
Starting background process ARC5
2021-08-23T10:51:08.244937-07:00
ARC5 started with pid=49, OS id=4542
Starting background process ARC6
2021-08-23T10:51:08.263833-07:00
ARC6 started with pid=50, OS id=4545
Starting background process ARC7
Completed: ALTER DATABASE   MOUNT
2021-08-23T10:51:08.279167-07:00
ARC7 started with pid=51, OS id=4548
Starting background process ARC8
2021-08-23T10:51:08.302581-07:00
alter database recover managed standby database disconnect from session nodelay
Starting background process ARC9
2021-08-23T10:51:08.308159-07:00
ARC8 started with pid=38, OS id=4552
2021-08-23T10:51:08.309609-07:00
Attempt to start background Managed Standby Recovery process (ora19csb)
2021-08-23T10:51:08.322101-07:00
ARC9 started with pid=53, OS id=4556
2021-08-23T10:51:08.323701-07:00
TMON (PID:4492): ARC1: Archival started
Starting background process MRP0
TMON (PID:4492): ARC2: Archival started
TMON (PID:4492): ARC3: Archival started
TMON (PID:4492): ARC4: Archival started
TMON (PID:4492): ARC5: Archival started
TMON (PID:4492): ARC6: Archival started
TMON (PID:4492): ARC7: Archival started
TMON (PID:4492): ARC8: Archival started
TMON (PID:4492): ARC9: Archival started
TMON (PID:4492): STARTING ARCH PROCESSES COMPLETE
2021-08-23T10:51:08.338364-07:00
MRP0 started with pid=54, OS id=4559
2021-08-23T10:51:08.339725-07:00
Background Managed Standby Recovery process started (ora19csb)
2021-08-23T10:51:13.361132-07:00
 Started logmerger process
2021-08-23T10:51:13.400193-07:00
PR00 (PID:4562): Managed Standby Recovery starting Real Time Apply
max_pdb is 3
2021-08-23T10:51:13.617769-07:00
Parallel Media Recovery started with 8 slaves
2021-08-23T10:51:13.654057-07:00
Stopping change tracking
2021-08-23T10:51:13.817537-07:00
Recovery of Online Redo Log: Thread 1 Group 5 Seq 56 Reading mem 0
  Mem# 0: +DATA_DG/ORA19CSB/stdby_group05_redo01.log
  Mem# 1: +DATA_DG/ORA19CSB/stdby_group05_redo02.log
2021-08-23T10:51:14.345055-07:00
Completed: alter database recover managed standby database disconnect from session nodelay
2021-08-23T10:58:47.187555-07:00
db_recovery_file_dest_size of 10240 MB is 2.09% used. This is a
user-specified limit on the amount of space that will be used by this
database for recovery-related files, and does not reflect the amount of
space available in the underlying filesystem or ASM diskgroup.
oracle@oracle19c-ol8-standby:ora19csb:/home/oracle>
```

FIGURE 59. Alert Log for Standby Oracle Database on VMware Cloud on AWS

Primary-standby log shipping can be tested by switching log files on the Site A primary database and observing the same log sequence being applied on the VMware Cloud on AWS standby database.

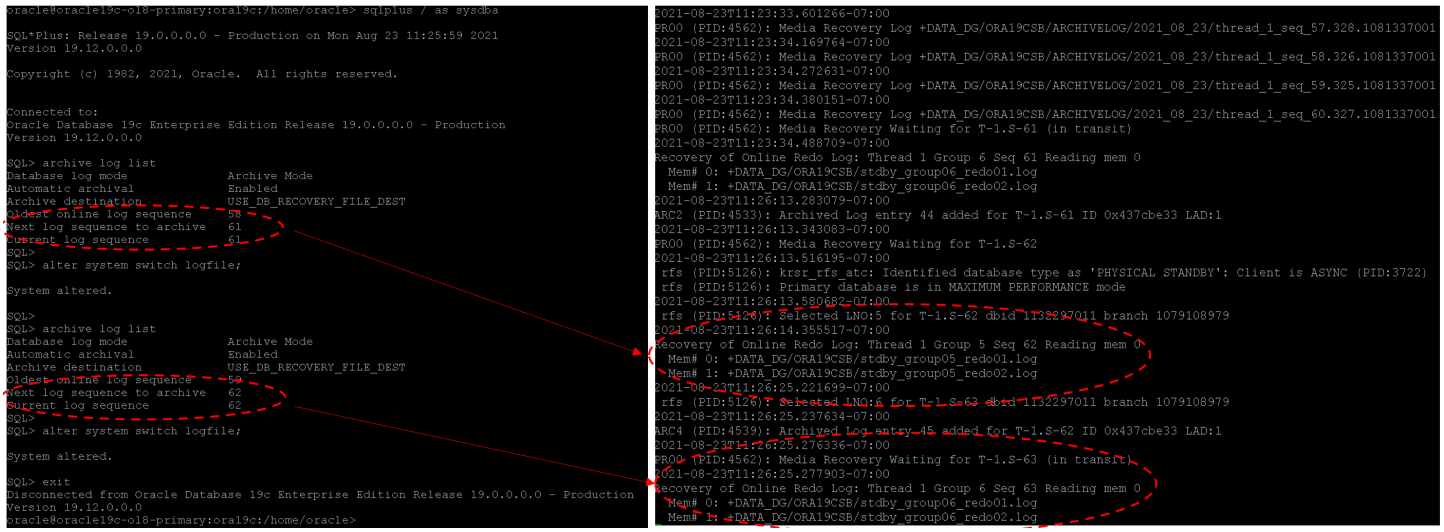


FIGURE 60. Log Switch on Primary Database Results in Changes Applied on Standby Database

Oracle Data Guard role transitions switchover and failover are the same when working with any physical architecture. Learn more about *role transitions*.

The *Oracle Databases on VMware Best Practices Guide* provides best practice guidelines for deploying Oracle workloads on a VMware SDDC.

In addition to this guide, VMware has created separate best practice documents for storage, networking, and performance. They can be found for the versions specific to vSphere *here*.

Migration methodology for Oracle Workloads to VMware Cloud on AWS

Existing single-instance Oracle workloads can be migrated transparently and seamlessly, without any application refactoring, from on-premises Site A or Site B to VMware Cloud on AWS.

There are broadly two ways existing Oracle workloads can be migrated from on-premises to VMware Cloud on AWS, depending on certain restrictions:

- Using VMware and Oracle native tools
- Using VMware Hybrid Cloud Extension

Using VMware and Oracle Native Tools

The section below describes the methods for migrating Oracle single-instance workloads to VMware Cloud on AWS using a mix of VMware vSphere and Oracle native tools.

Using Oracle Native Tools

Migrating Oracle single-instance workloads to VMware Cloud on AWS using Oracle native tools can be achieved by using any of the below tools:

- Oracle Data Guard to set up replication between the two sites and failover to VMware Cloud on AWS after replication is complete
- Oracle GoldenGate
- Backup and recovery of on-premises Oracle databases using Oracle RMAN to VMware Cloud on AWS

All of these Oracle utilities operate at an Oracle application level and are therefore completely transparent to the underlying physical infrastructure.

Oracle Data Guard role transitions switchover and failover are the same when working with any physical architecture. Learn more about *role transitions*.

Set up of Oracle Data Guard and Oracle GoldenGate are beyond the scope of this paper. Learn more about *Oracle Data Guard*.

Using VMware vSphere Native Tools

Migrating Oracle single-instance workloads to VMware Cloud on AWS using VMware vSphere native tools can be achieved by using regular Cross vCenter vMotion.

Click **Edit Settings** on VM **Oracle19c12-OEL83** and select **Cross vCenter Server export**,

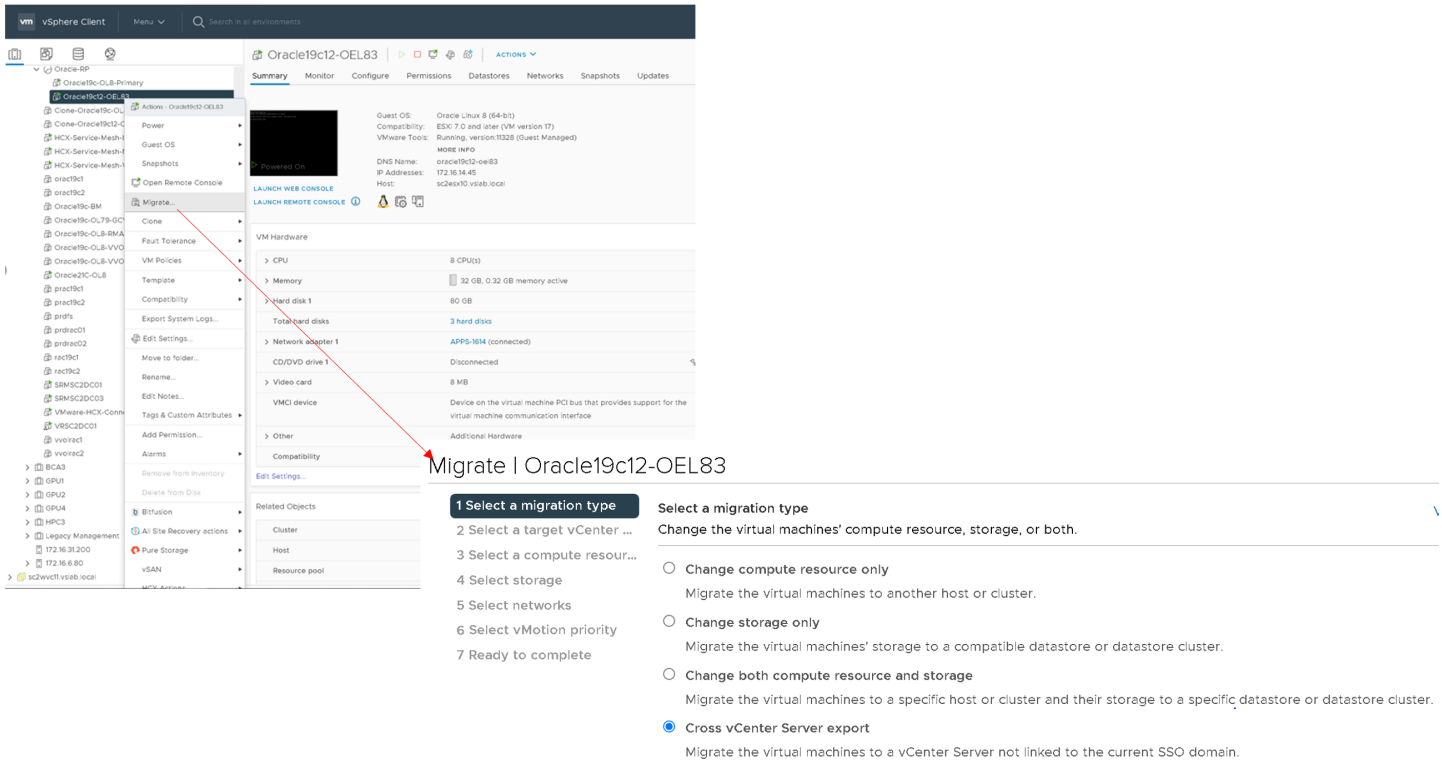


FIGURE 61. Cross vCenter vMotion for VM Oracle19c12-OEL83

Select a target vCenter, compare resource and storage.

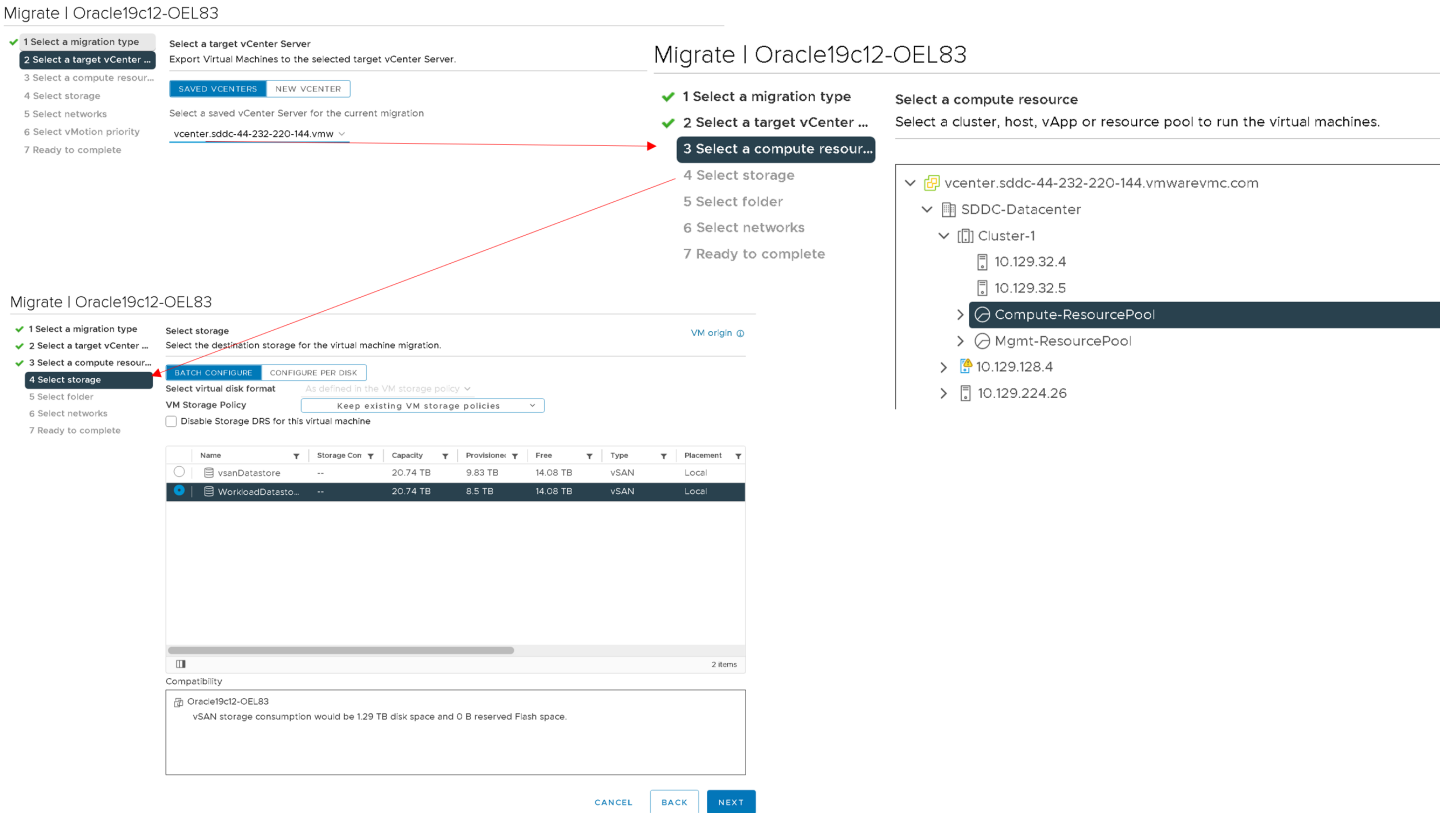


FIGURE 62. Target vCenter, Compare Resource and Storage for VM Oracle19c12-OEL83

Select target network details for VM **Oracle19c12-OEL83**.

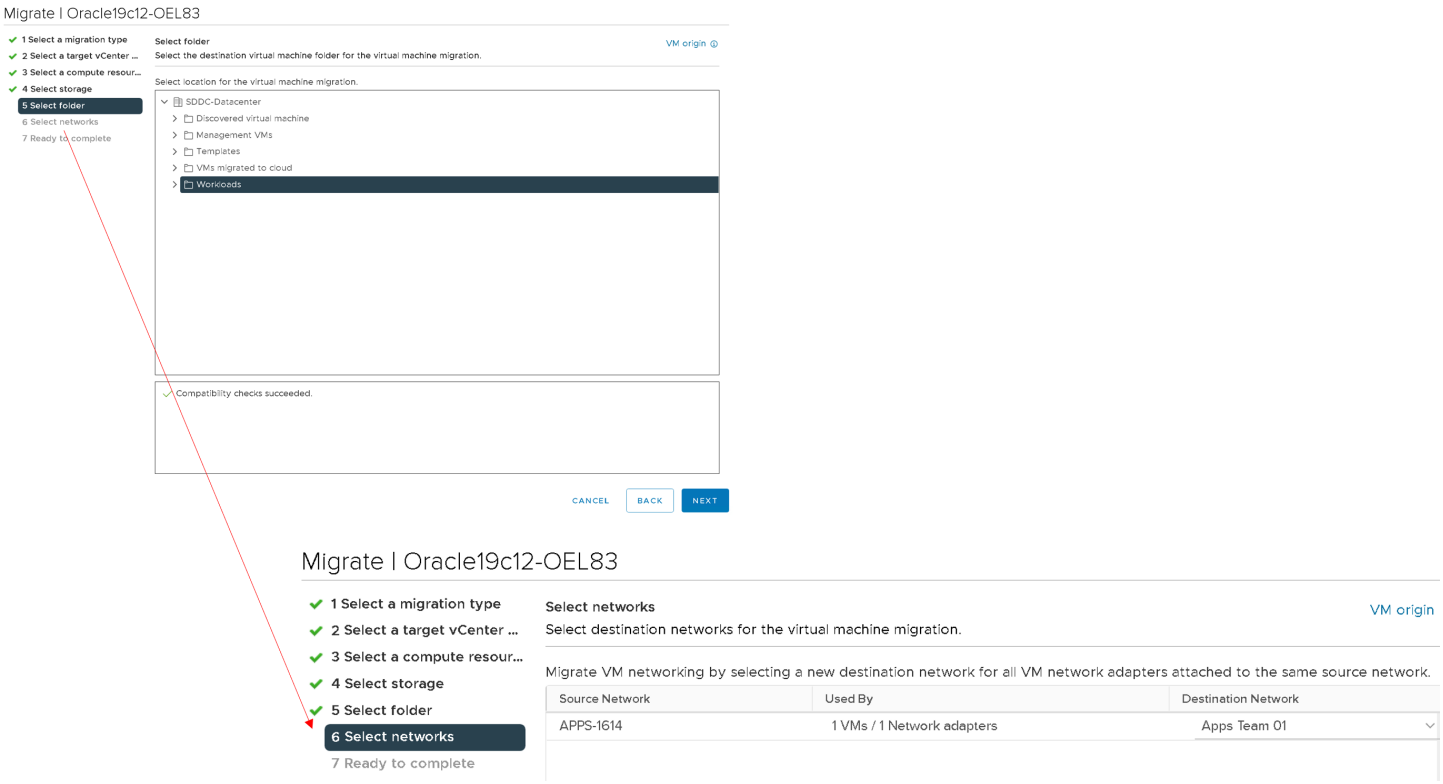


FIGURE 63. Target Network Details for VM Oracle19c12-OEL83

The migration summary for VM **Oracle19c12-OEL83** is as shown below:

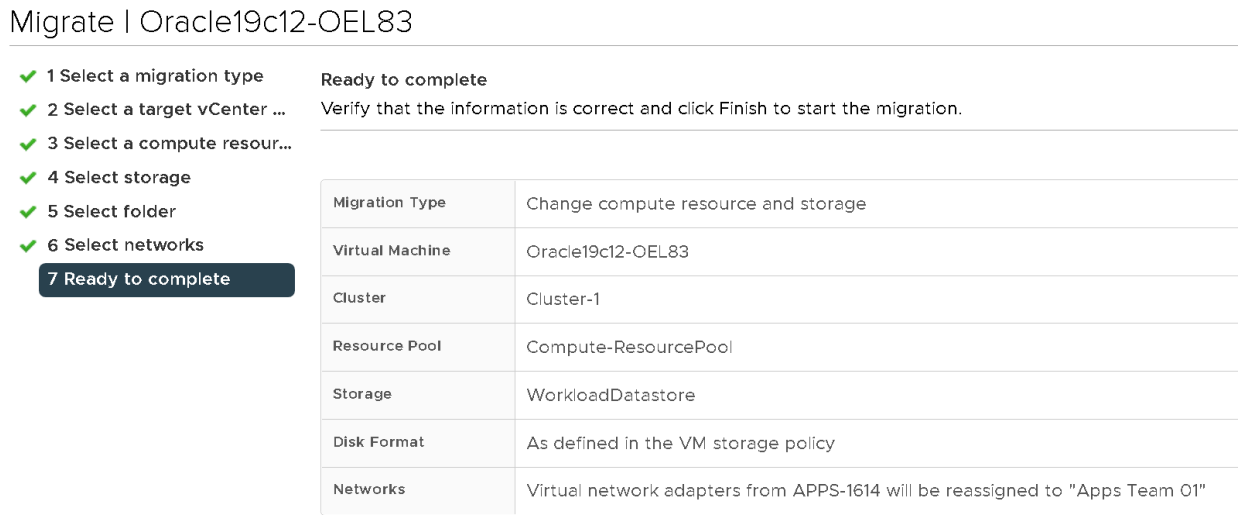


FIGURE 64. Migration Summary for VM Oracle19c12-OEL83

The VM **Oracle19c12-OEL83** has been successfully migrated to VMware Cloud on AWS.

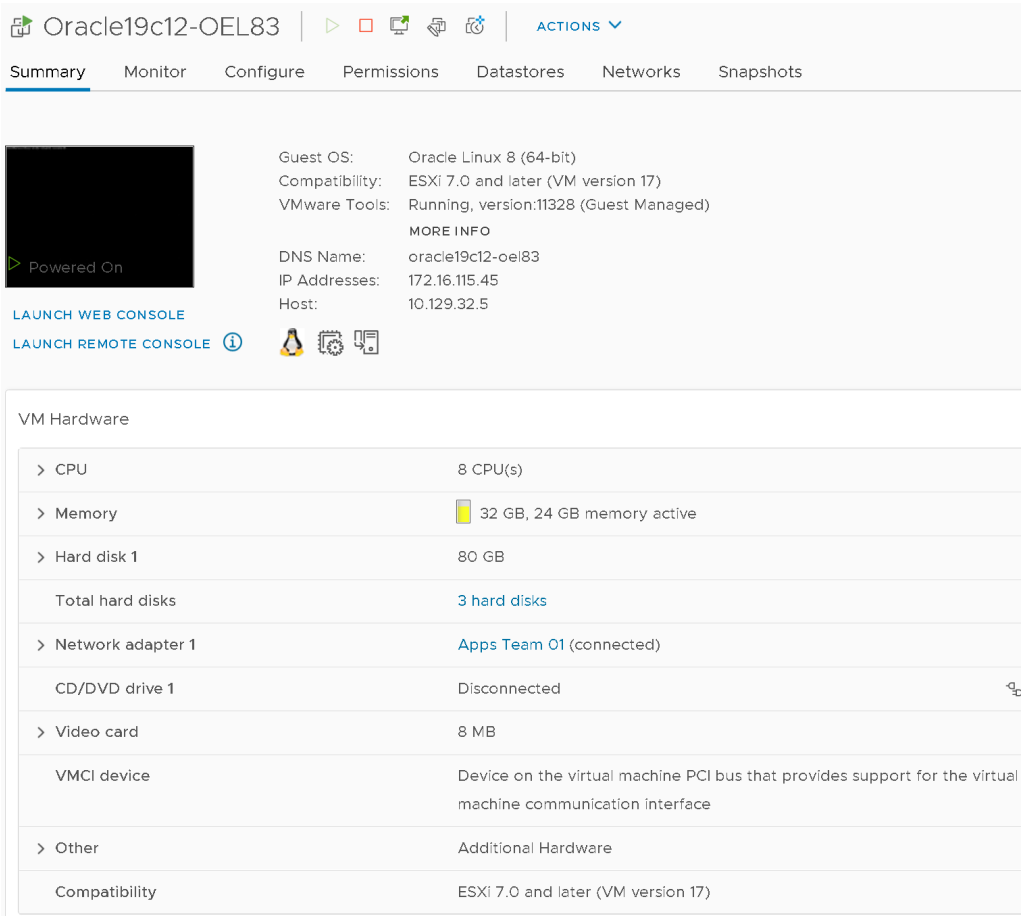


FIGURE 65. VM Oracle19c12-OEL83 on VMware Cloud on AWS

Migration of production single-instance physical standby Oracle VM **Oracle19c-OL8-Standby** from on-premises Site B to VMware Cloud on AWS is no different than the above scenario in which VM **Oracle19c12-OEL83** is migrated from Site A to VMware Cloud on AWS.

Using VMware Hybrid Cloud Extension

VMware Hybrid Cloud Extension abstracts on-premises versus cloud notions and presents capabilities to VMs as a continuous hybrid cloud. VMs can be moved to and from VMware Hybrid Cloud Extension-activated data centers using multiple migration technologies.

Currently, the five different Hybrid Cloud Extension methods are:

- VMware Hybrid Cloud Extension Bulk Migration
- VMware Hybrid Cloud Extension Cold Migration
- VMware Hybrid Cloud Extension vMotion
- VMware Hybrid Cloud Extension Replication Assisted vMotion
- VMware Hybrid Cloud Extension OS Assisted Migration

Learn more about *VMware Hybrid Cloud Extension migration types*.

The methods mentioned above (except Hybrid Cloud Extension OS Assisted Migration) can be used to migrate standalone Oracle workloads as SLA requirements dictate.

The migration of Oracle VMs using Hybrid Cloud Extension OS Assisted Migration is outside the scope of this paper.

VMs with shared disks using multi-writer attribute are NOT supported because of the shared disk restriction (i.e., VMs with shared .vmdk files) using VMware Hybrid Cloud Extension migration methods. More information on this restriction can be found in *Hybrid Migration with VMware Hybrid Cloud Extension Checklist*. In any event, if VMs with multi-writer attribute can be migrated, the resulting multi-writer configuration is no longer functional, as outlines in the restrictions section of *Understanding VMware Hybrid Cloud Extension Bulk Migration*.

The production single-instance Oracle VM **Oracle19c12-OEL83** on Site A was used for all Hybrid Cloud Extension deployments.

Some caveats that one may encounter during Hybrid Cloud Extension migration:

- Migration of VMs between ESXi hosts with different CPU models may create an issue because vMotion requires the same family of CPUs among the ESXi hosts to ensure the same CPU feature set is presented to all VMs. Refer to *KB 1003212* "The target host does not support the VM's current hardware requirements" error during vMotion migration of a VM (1003212). One can enable per-VM EVC as shown below:

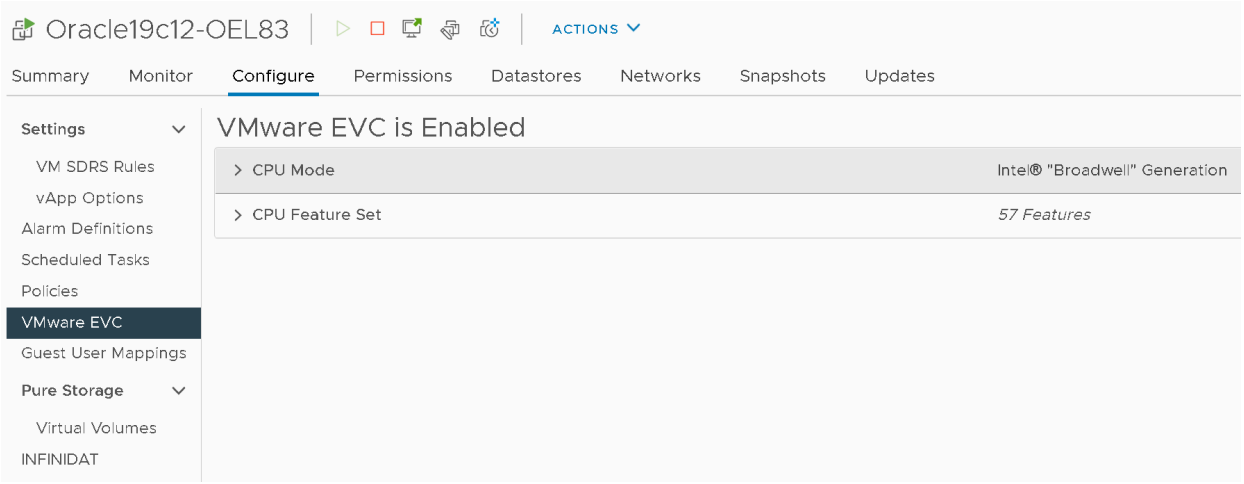


FIGURE 66. VMware EVC CPU Mode

- Occasionally, an issue may arise using bulk migration at the time of cutover because a guest OS may not reach a fully powered off state within 100 seconds of the initial **Shutdown Guest OS** call (as part of bulk migration cutover). If the 100 second period elapses and the VM does not reflect a powered off status, the migration will fail. If VMware Tools is not detected on the guest OS, pre-migration validation will prompt a user to select **Force Power Off**.
- With **Force Power Off** selected, VMware Hybrid Cloud Extension Bulk Migration still utilizes VMware Tools (if present) to gracefully shutdown a guest OS. After 100 seconds has elapsed since the initial **Shutdown Guest OS** call, an immediate power off will be performed (if necessary) on the VM to move forward with the migration.

  Refer to *KB 82269 Unable to Power Off Guest OS during Switchover Using Hybrid Cloud Extension Bulk Migration (82269)*.
- Using the on-premises vSphere client (Hybrid Cloud Extension plug-in), one may occasionally encounter a message during bulk migration validation check: "Non-VMware or out of date tools detected on [VM name]. Hybrid Cloud Extension will attempt a graceful shutdown" is displayed during the bulk migration validation check.

  Refer to *KB 74740* for more details.

Migrating Oracle Single-Instance Workloads Using Hybrid Cloud Extension Bulk Migration

Bulk migration uses the host-based replication to move a VM between Hybrid Cloud Extension data centers. To reduce the downtime, the source VM remains online during the replication and is bootstrapped on the destination ESX host after replication completes.

Learn more about *Hybrid Cloud Extension Bulk Migration*.

The production single-instance Oracle VM **Oracle19c12-OEL83** on Site A was used for the Hybrid Cloud Extension bulk migration deployment use case.

Oracle VM **Oracle19c12-OEL83** was powered up with IP Address 172.16.14.45 with database ora19c **online**. Click **Migrate** and add VM **Oracle19c12-OEL83** to the migration process.

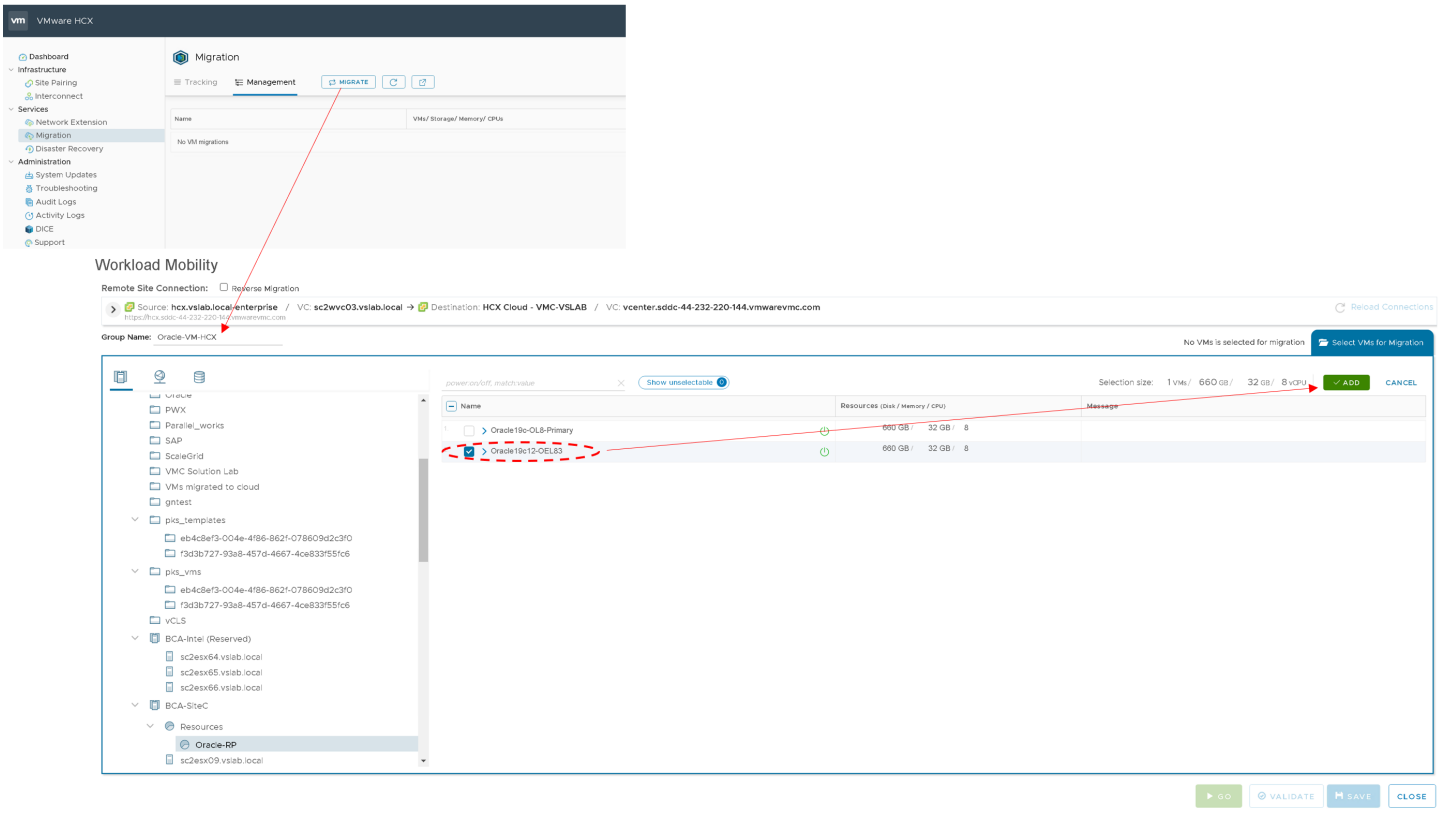


FIGURE 67. Add VM Oracle19c12-OEL83 to Migration Process

Select the target Compute-Resource Pool.

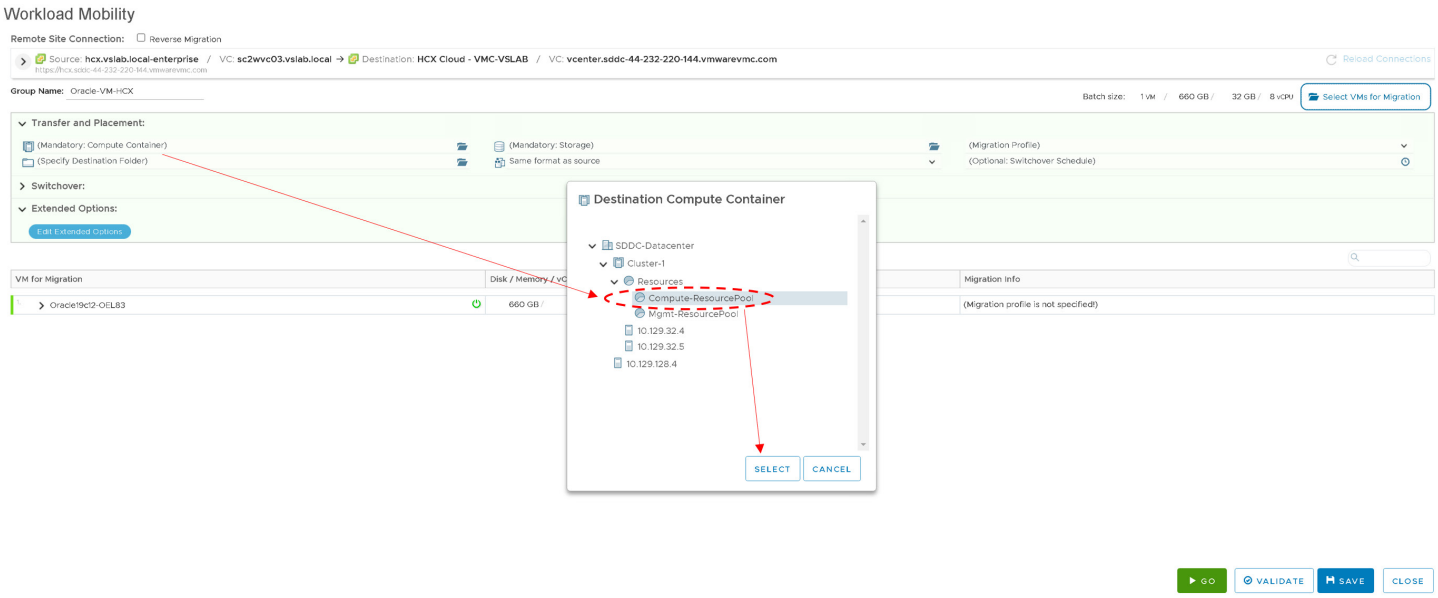


FIGURE 68. Select Target Compute-Resource Pool

Select the target Destination Folder.

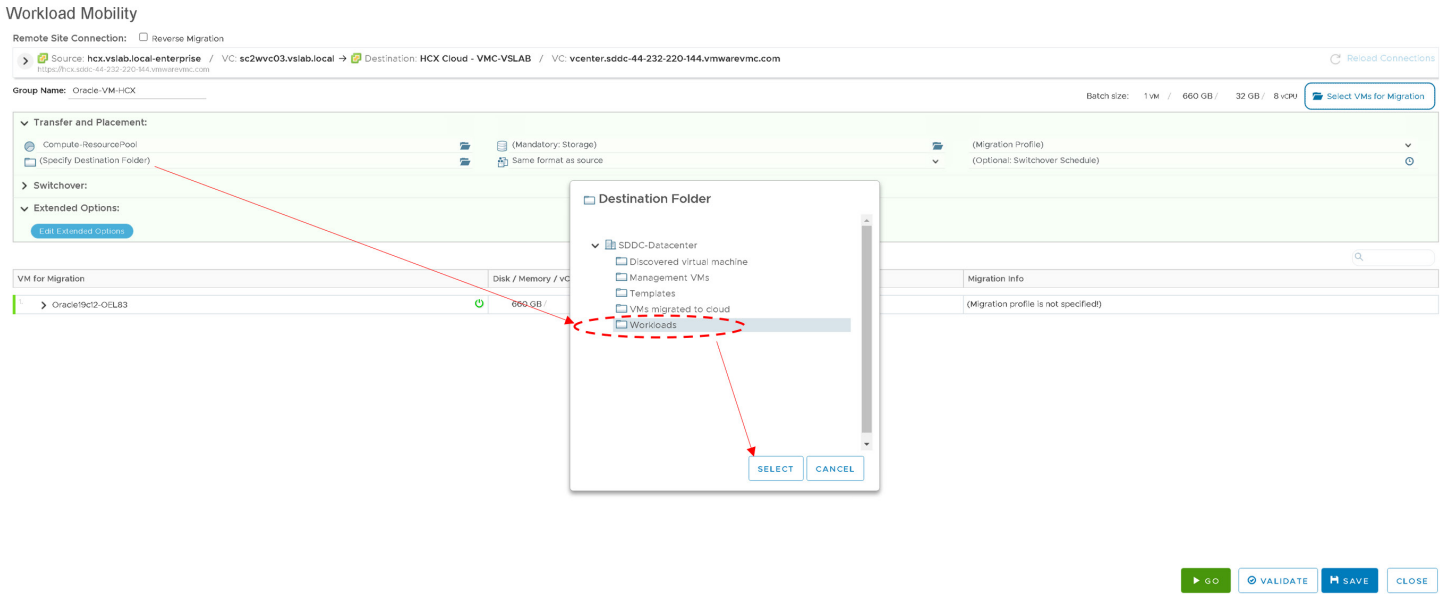


FIGURE 69. Select Destination Folder

Select the target datastore **WorkloadDatastore**.

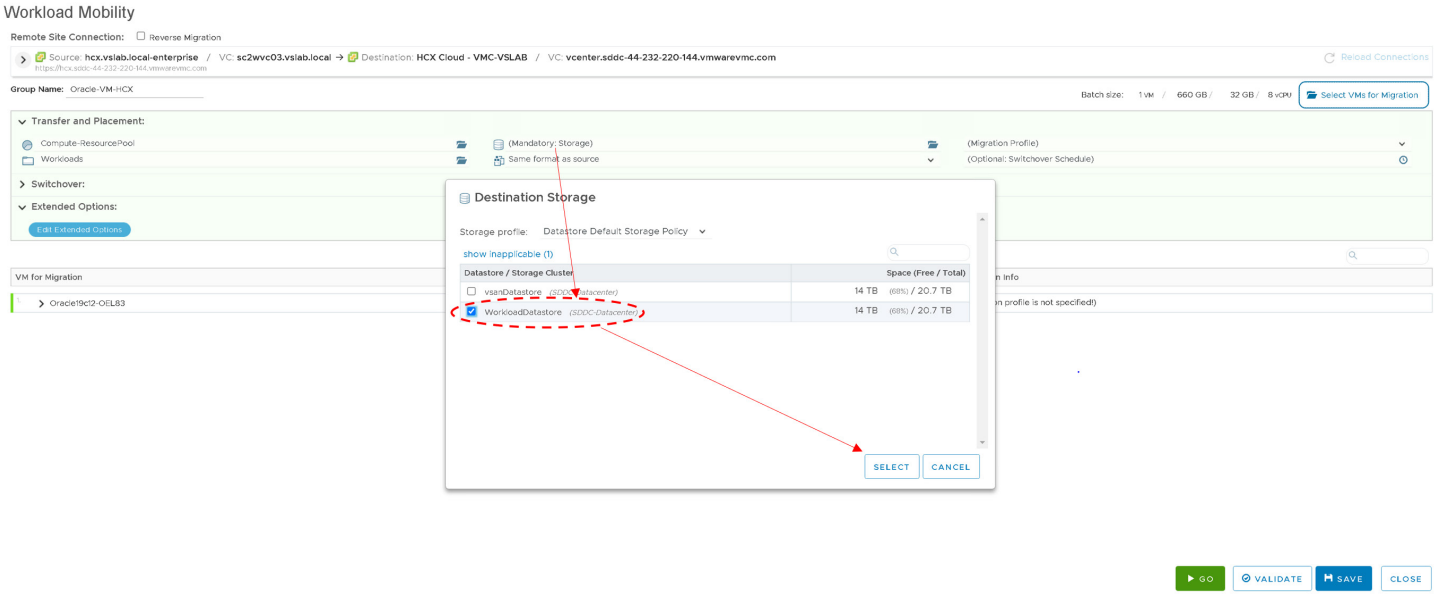


FIGURE 70. Select Target Datastore

Select the migration profile **Bulk Migration**.

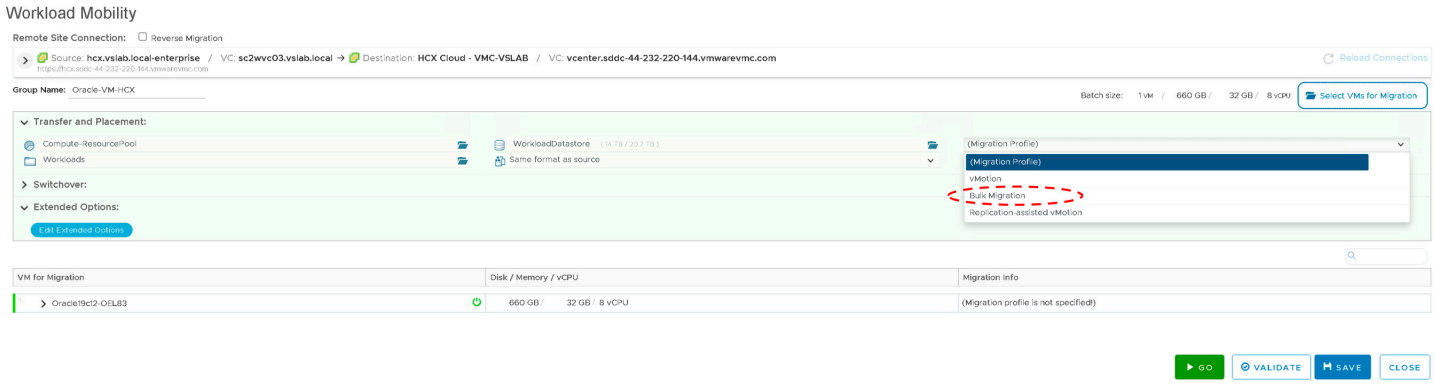


FIGURE 71. Select Migration Profile

Select target network port group **Apps Team 01**. The **Force Power-off** VM is optional (refer to *KB 82269*).

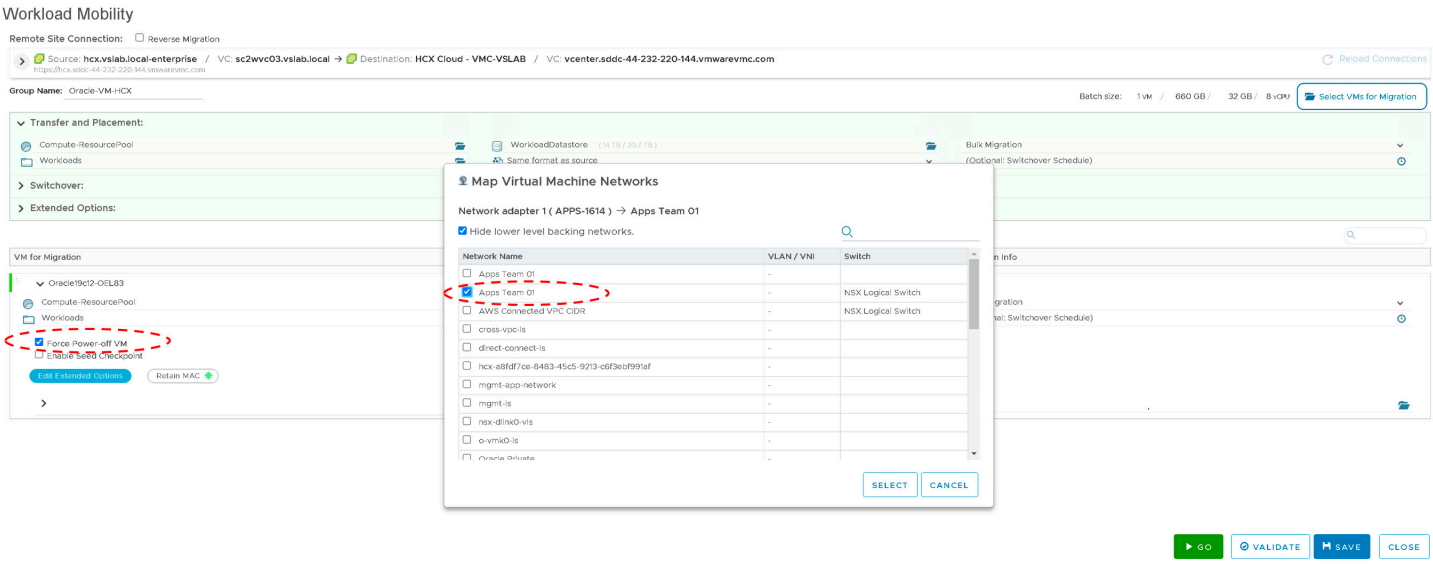


FIGURE 72. Select Target Network Port Groups

Assign target IP address 172.16.115.45 with gateway and netmask information to the VM as shown below:

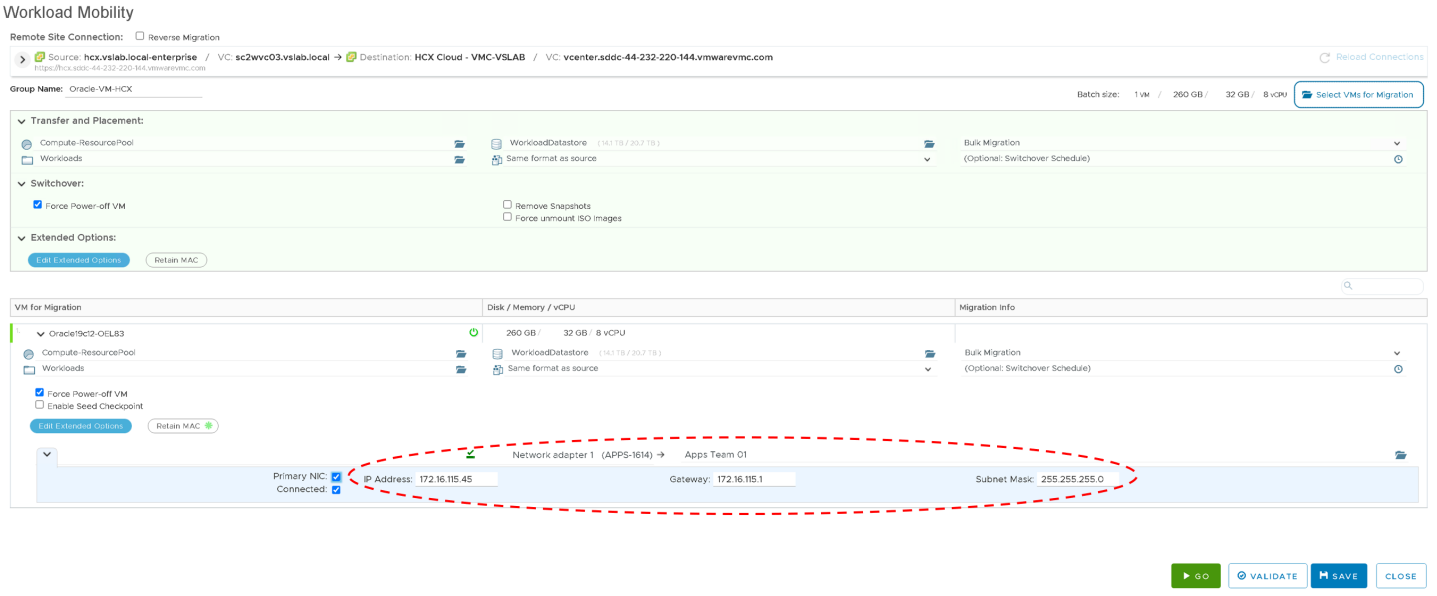


FIGURE 73. Assign Target IP address 172.16.115.45

Assign DNS information to the workflow.

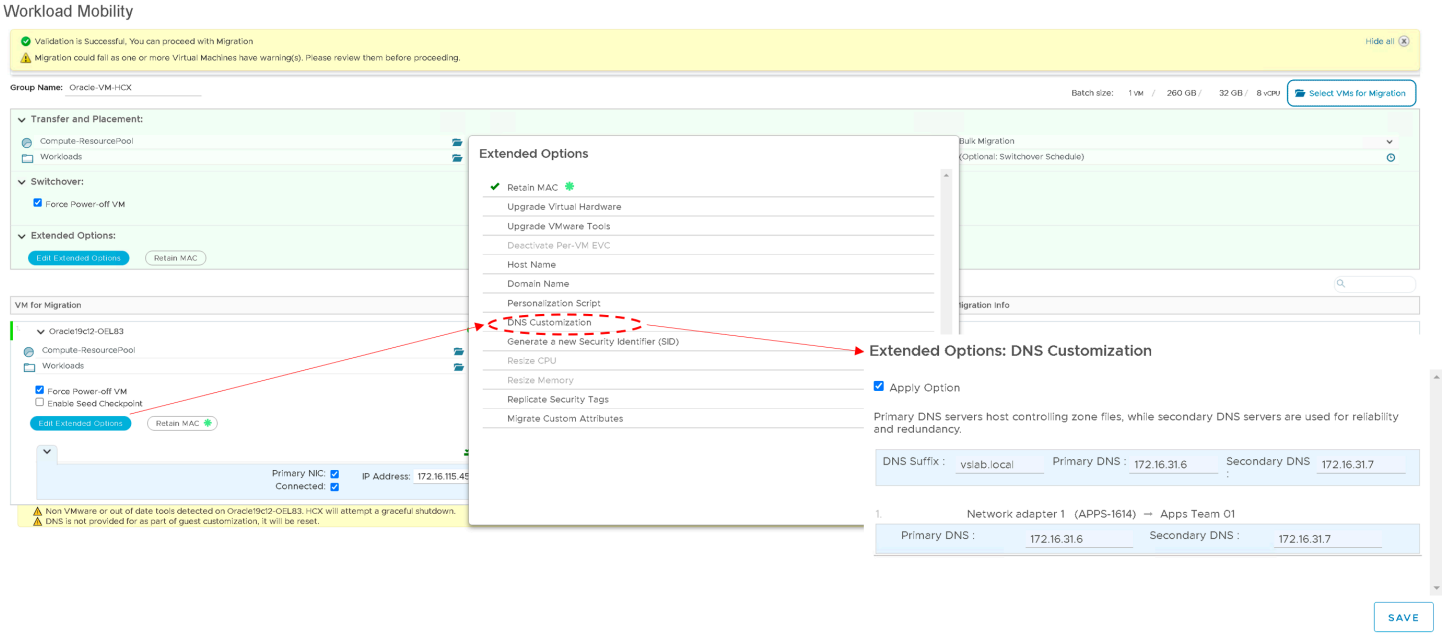


FIGURE 74. Assign DNS Information

Click **Validate** to validate the configuration.

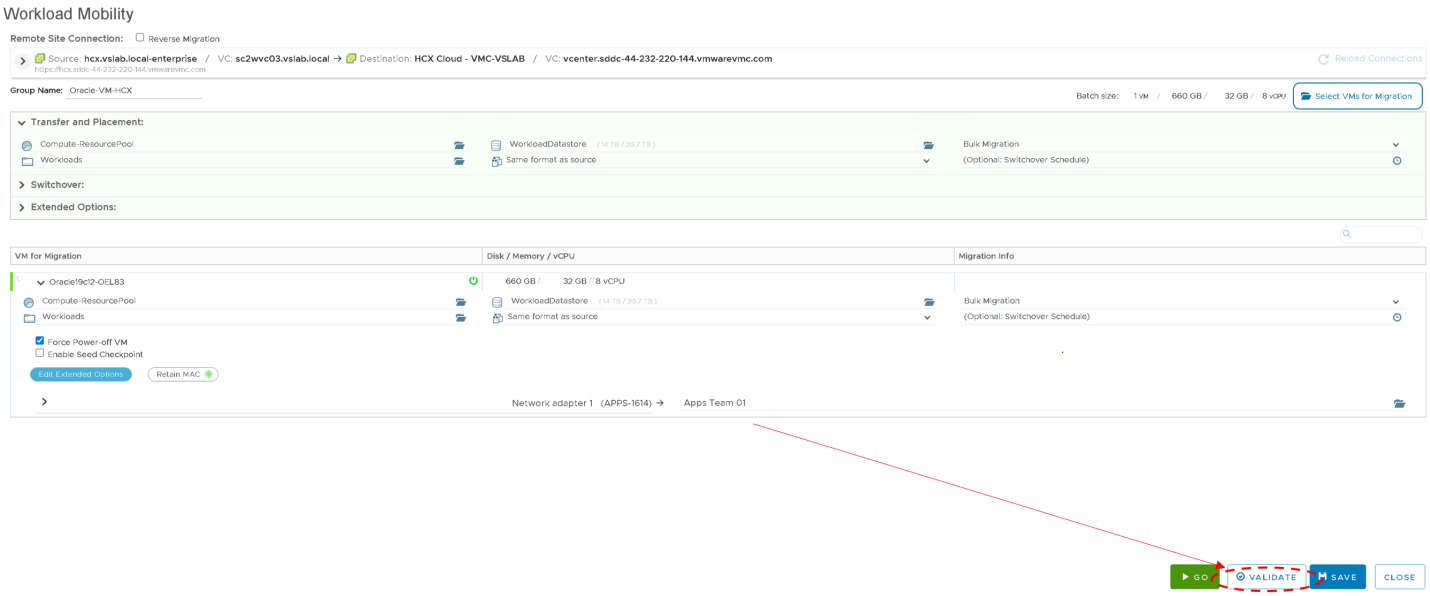


FIGURE 75. Validate the Configuration

Refer to *KB 74740* for more details regarding the VMware Tools message shown below:

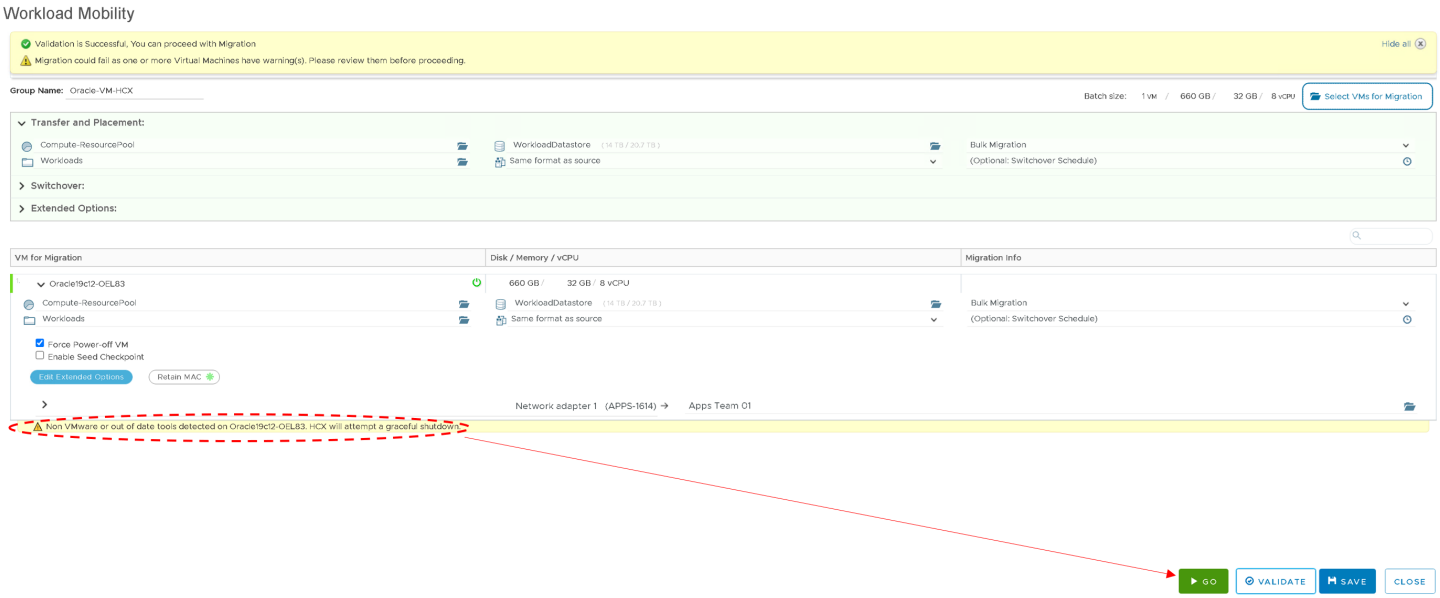


FIGURE 76. VMware Tools Message

Click **Go** to start the migration.

Steps for the migration start are as shown below:

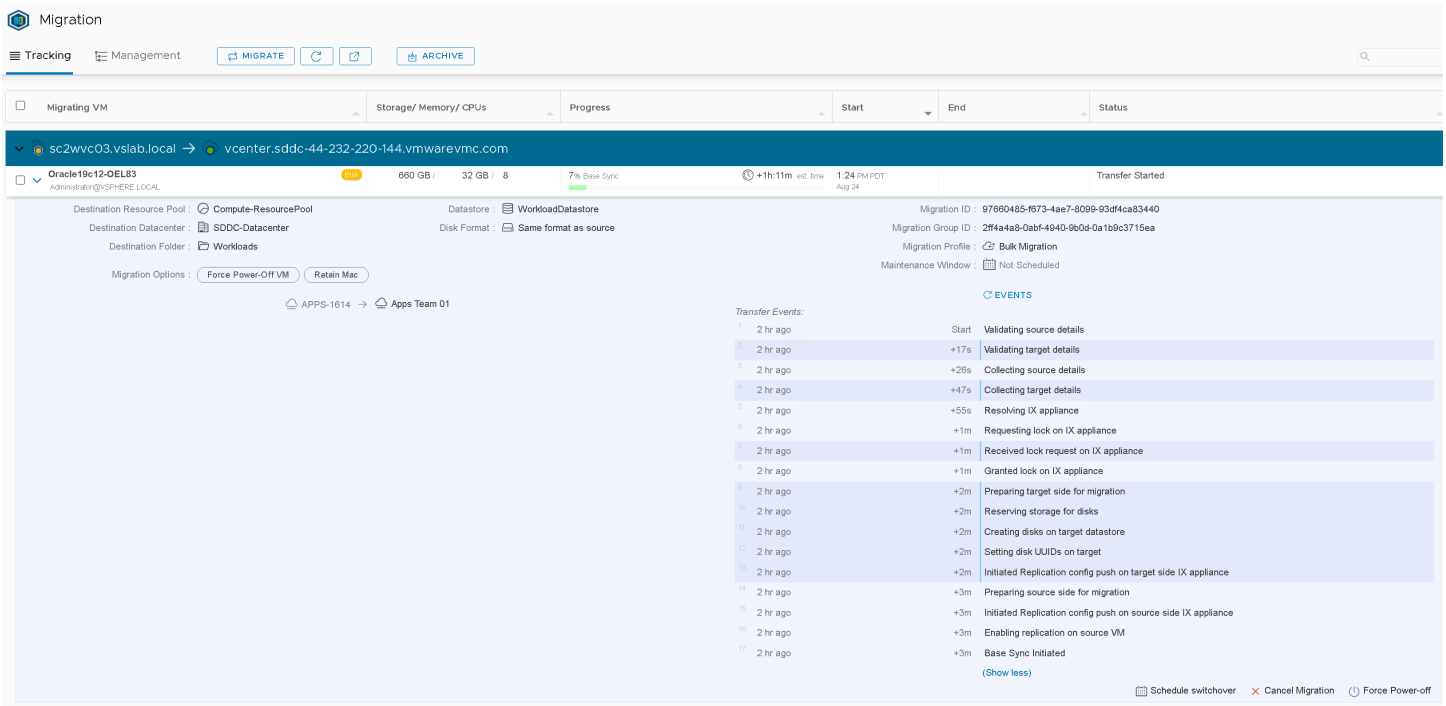


FIGURE 77. Migration Start

The migration completes successfully.

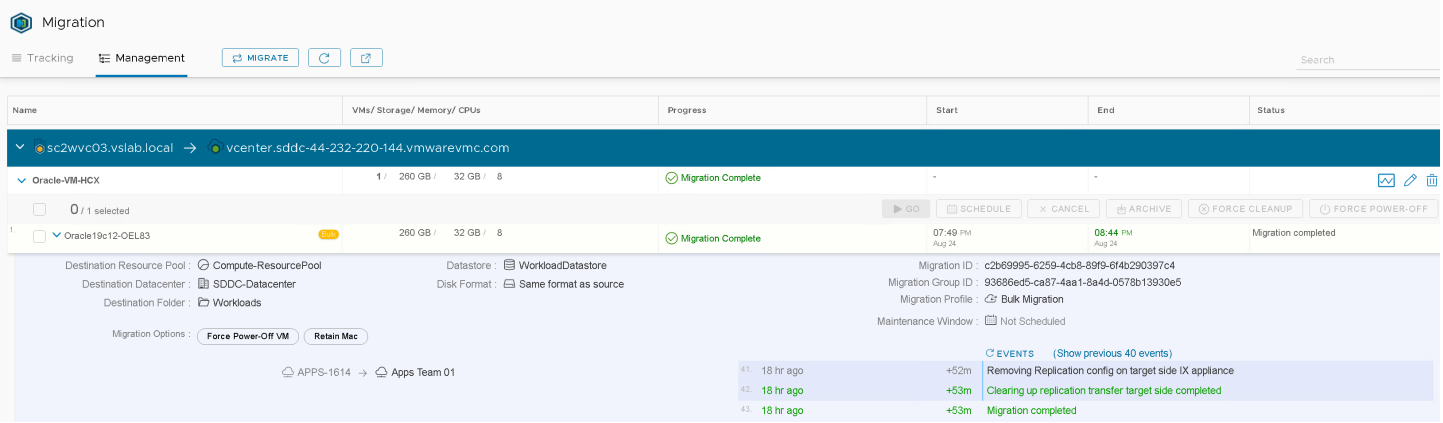


FIGURE 78. Migration Complete

Oracle VM **Oracle19c12-OEL83** is now on VMware Cloud on AWS with IP address 172.16.115.45.

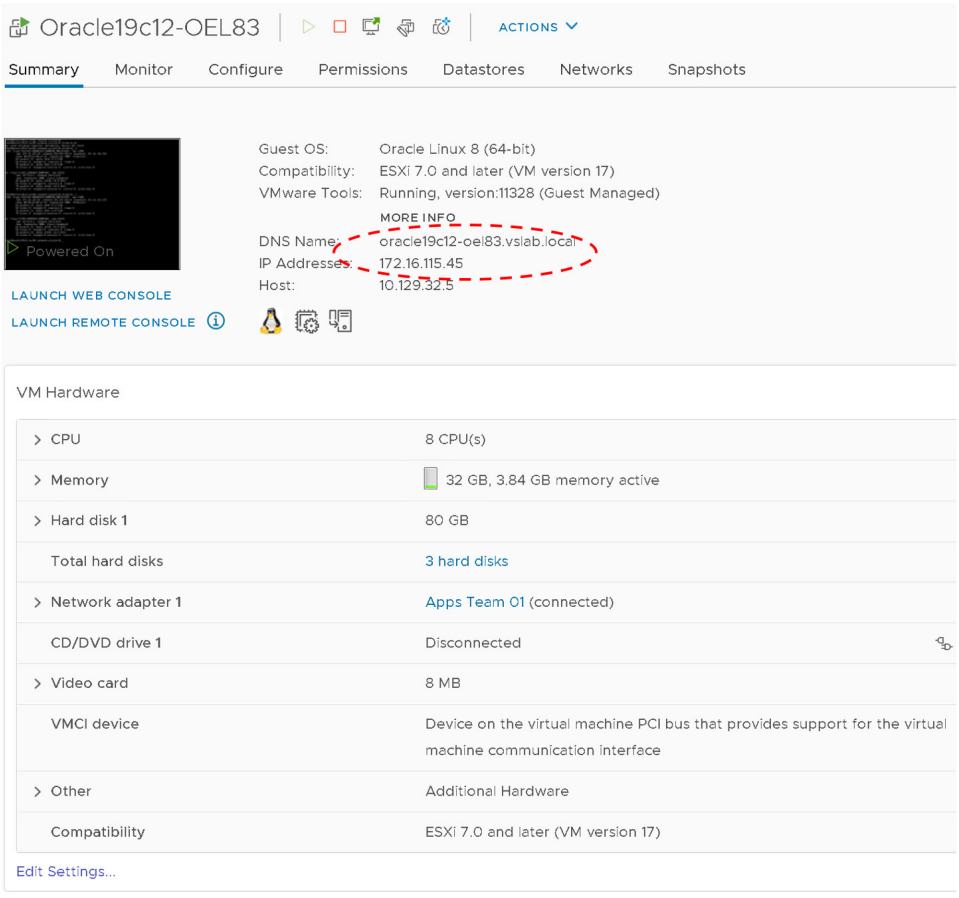


FIGURE 79. Oracle VM Oracle19c12-OEL83 Migration Summary

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.115.45  netmask 255.255.255.0  broadcast 172.16.115.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 455  bytes 41633 (40.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 367  bytes 47761 (46.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 237  bytes 37517 (36.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 237  bytes 37517 (36.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Aug 25 15:45:41 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 80. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1050 alert_ora19c.log
Starting background process TMON
2021-08-25T15:43:55.739190-07:00
NOTE: ASMB (index:0) registering with ASM instance as Standard client 0xffffffffffffffff (reg:626979542) (startid:1081525433) (new connection)
2021-08-25T15:43:55.748101-07:00
TMON started with pid=36, OS id=3590
2021-08-25T15:43:55.754935-07:00
NOTE: Loaded library: /opt/oracle/extapi/64/asm/orcl/1/libasm.so
2021-08-25T15:43:55.758930-07:00
Setting CPU count to 8
ORACLE_BASE from environment = /u01/app/oracle
2021-08-25T15:43:55.816419-07:00
NOTE: ASMB (index:0) (3571) connected to ASM instance +ASM, osid: 3583 (Standard mode; client id 0xffffffffffffffff)
NOTE: initiating MARK startup
Starting background process MARK
2021-08-25T15:43:55.840130-07:00
ALTER DATABASE   MOUNT
2021-08-25T15:43:55.840833-07:00
MARK started with pid=38, OS id=3595
2021-08-25T15:43:55.843397-07:00
NOTE: MARK has subscribed
2021-08-25T15:43:59.036350-07:00
NOTE: ASMB mounting group 1 (DATA_DG)
NOTE: Assigning number (1,1) to disk (ORCL:DATA_DISK02)
SUCCESS: mounted group 1 (DATA_DG)
NOTE: grp 1 disk 1: DATA_DISK02 path:ORCL:DATA_DISK02
2021-08-25T15:43:59.218575-07:00
ERROR: failed to establish dependency between database ORA19C and diskgroup resource ora.DATA_DG.dg
2021-08-25T15:44:03.287143-07:00
.... (PID:3592): Redo network throttle feature is disabled at mount time
2021-08-25T15:44:03.339159-07:00
Successful mount of redo thread 1, with mount id 1134691451
2021-08-25T15:44:03.341098-07:00
Database mounted in Exclusive Mode
Lost write protection disabled
.... (PID:3592): Using STANDBY_ARCHIVE_DEST parameter default value as USE_DB_RECOVERY_FILE_DEST [krsd.c:18222]
Completed: ALTER DATABASE   MOUNT
2021-08-25T15:44:03.475764-07:00
ALTER DATABASE OPEN
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-08-25T15:44:03.576891-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-25T15:44:03.581420-07:00
Beginning crash recovery of 1 threads
 parallel recovery started with 7 processes
 Thread 1: Recovery starting at checkpoint rba (logseq 19 block 49614), scn 0
2021-08-25T15:44:03.655124-07:00
Started redo scan
2021-08-25T15:44:03.681490-07:00
Completed redo scan
 read 29 KB redo, 15 data blocks need recovery
2021-08-25T15:44:03.688408-07:00
Started redo application at
 Thread 1: logseq 19, block 49614, offset 0
2021-08-25T15:44:03.692536-07:00
Recovery of Online Redo Log: Thread 1 Group 3 Seq 19 Reading mem 0
  Mem# 0: +DATA_DG/ORA19C/group03_redo01.log
  Mem# 1: +DATA_DG/ORA19C/group03_redo02.log
2021-08-25T15:44:03.694071-07:00
Completed redo application of 0.01MB
2021-08-25T15:44:03.725623-07:00
Completed crash recovery at
 Thread 1: RBA 19.49672.16, nab 49672, scn 0x0000000000189c1d
 15 data blocks read, 15 data blocks written, 29 redo k-bytes read
Endian type of dictionary set to little
2021-08-25T15:44:03.794030-07:00
LGWR (PID:3525): STARTING ARCH PROCESSES
2021-08-25T15:44:03.810338-07:00
TT00 (PID:3646): Gap Manager starting
```

FIGURE 81. Database ora19c Alert Log

As stated earlier, VMware Hybrid Cloud Extension copies the original VM to the migrated VMs folder in **vSphere Templates** view.

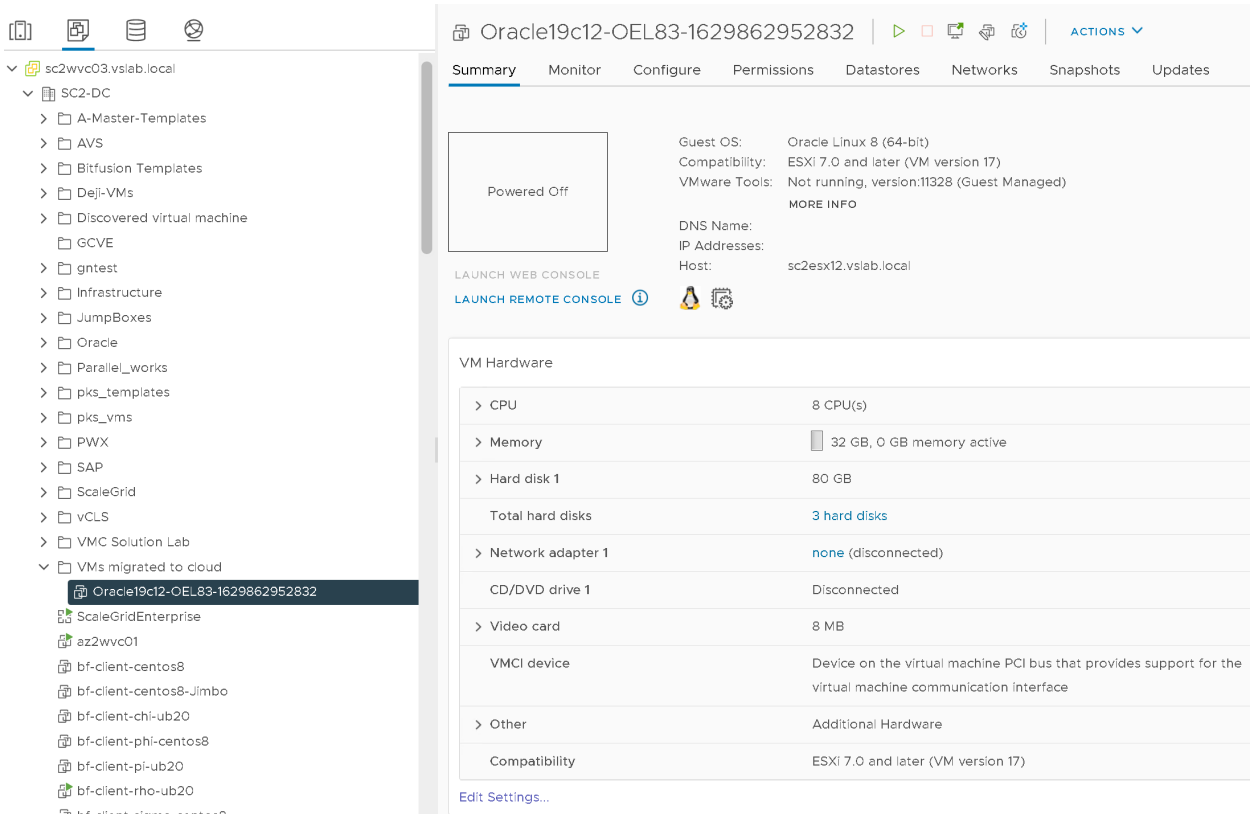


FIGURE 82. VMware vSphere Templates View

The steps to perform the reverse migration from VMware Cloud on AWS to Site A are the same as those required for migration from Site A to VMware Cloud on AWS.

Select the **Reverse Migration** checkbox and select the Oracle VM **Oracle19c12-OEL83**. The remaining steps are the same as those previously outlined.

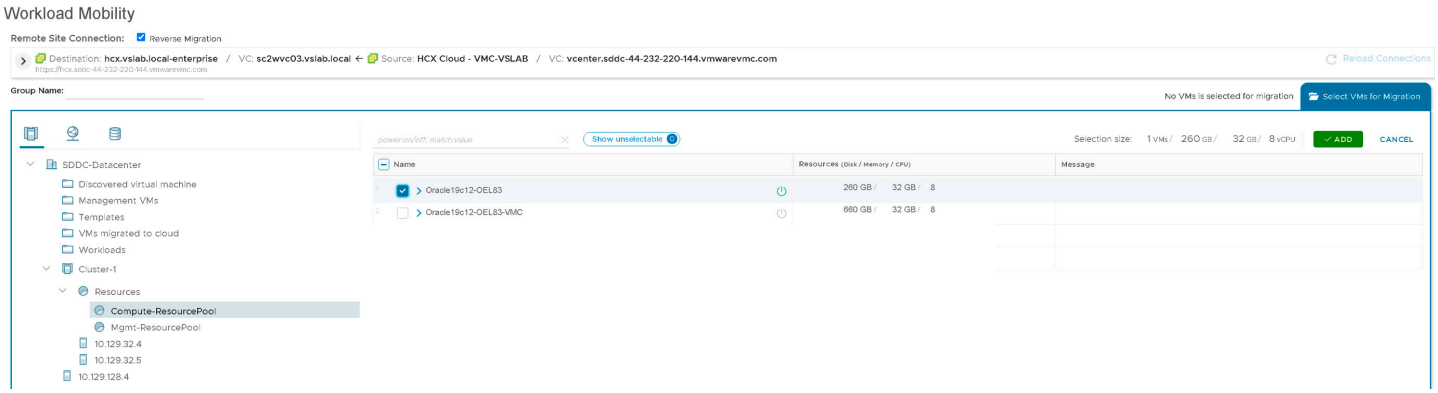


FIGURE 83. Reverse Migration of Oracle VM Oracle19c12-OEL83

The summary of the reverse migration is as shown below:

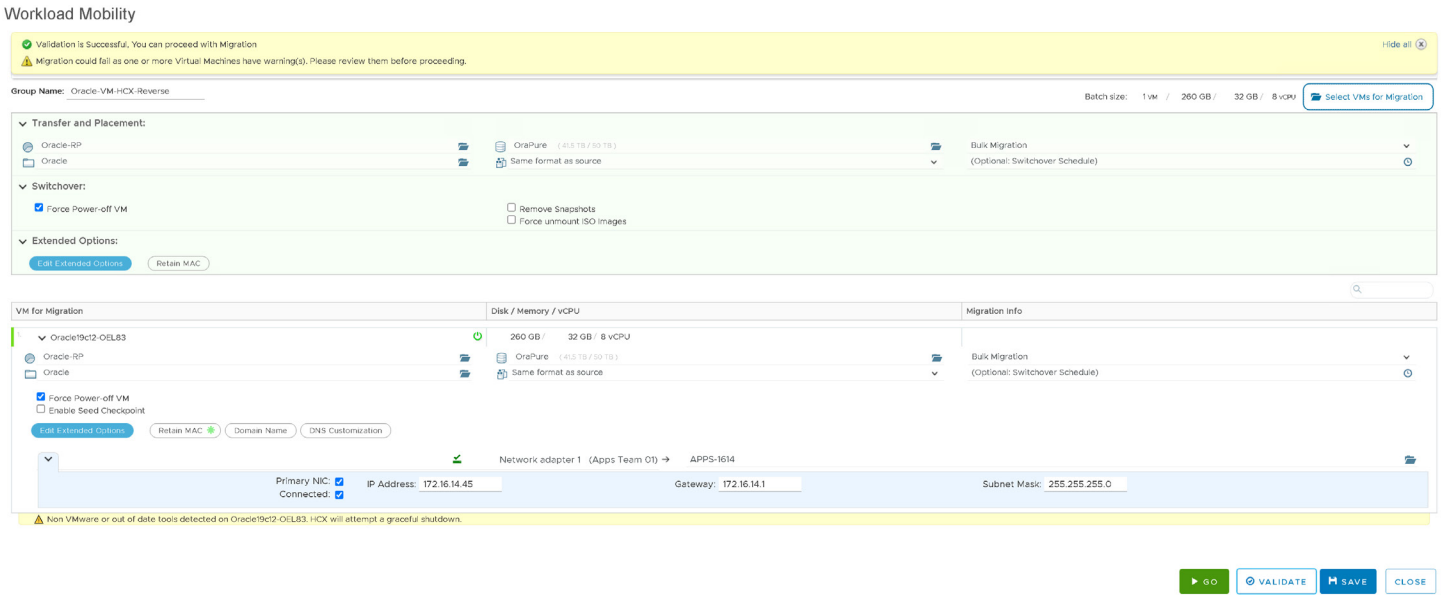


FIGURE 84. Oracle VM Oracle19c12-OEL83 Reverse Migration Summary

The reverse migration is successful.

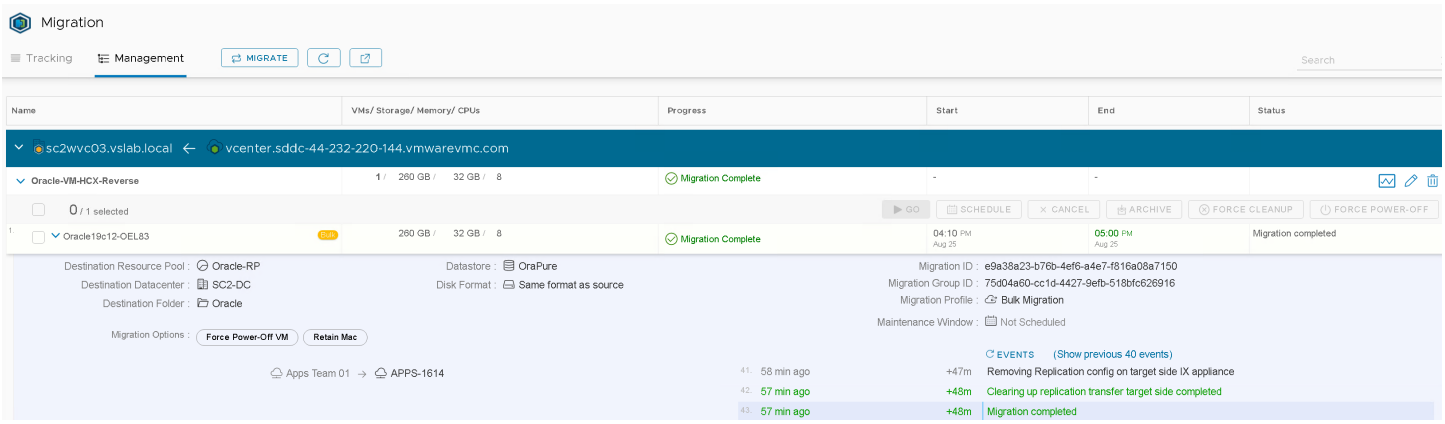


FIGURE 85. Migration Complete

The Oracle VM **Oracle19c12-OEL83** is now back on Site A with the IP address 172.16.14.45.

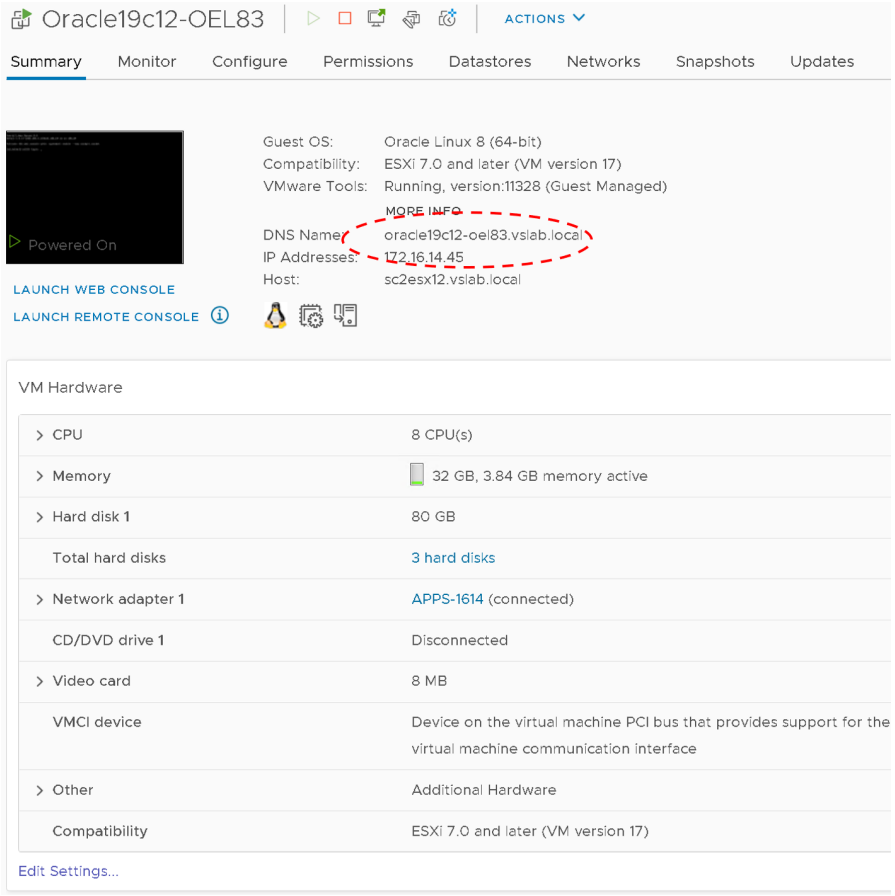


FIGURE 86. Site A VM Oracle19c12-OEL83

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.45  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 1355  bytes 101289 (98.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 814  bytes 954313 (931.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 331  bytes 47477 (46.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 331  bytes 47477 (46.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Aug 25 18:00:54 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 87. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1050 alert_ora19c.log
Starting background process MMON
2021-08-25T17:49:56.255138-07:00
MMON started with pid=34, OS id=3494
Starting background process MMNL
2021-08-25T17:49:56.267207-07:00
MMNL started with pid=35, OS id=3499
Starting background process TMON
2021-08-25T17:49:56.273563-07:00
NOTE: ASMB (index:0) registering with ASM instance as Standard client 0xffffffffffffffff (reg:1913977987) (startid:1081532994) (new connection)
2021-08-25T17:49:56.279844-07:00
TMON started with pid=36, OS id=3503
2021-08-25T17:49:56.283444-07:00
NOTE: Loaded library: /opt/oracle/extapi/64/asm/orcl/1/libasm.so
2021-08-25T17:49:56.284914-07:00
Setting CPU count to 8
ORACLE_BASE from environment = /u01/app/oracle
2021-08-25T17:49:56.337336-07:00
ALTER DATABASE   MOUNT
2021-08-25T17:49:56.341020-07:00
NOTE: ASMB (index:0) (3484) connected to ASM instance +ASM, osid: 3497 (Standard mode; client id 0xffffffffffffffff)
NOTE: initiating MARK startup
Starting background process MARK
2021-08-25T17:49:56.354782-07:00
MARK started with pid=38, OS id=3508
2021-08-25T17:49:56.357185-07:00
NOTE: MARK has subscribed
2021-08-25T17:49:59.470145-07:00
NOTE: ASMB mounting group 1 (DATA_DG)
NOTE: Assigning number (1,1) to disk (ORCL:DATA_DISK02)
SUCCESS: mounted group 1 (DATA_DG)
NOTE: grp 1 disk 1: DATA_DISK02 path:ORCL:DATA_DISK02
2021-08-25T17:49:59.580407-07:00
ERROR: failed to establish dependency between database ORA19C and diskgroup resource ora.DATA_DG.dg
2021-08-25T17:50:03.662468-07:00
.... (PID:3505): Redo network throttle feature is disabled at mount time
2021-08-25T17:50:03.692240-07:00
Successful mount of redo thread 1, with mount id 1134664452
2021-08-25T17:50:03.694359-07:00
Database mounted in Exclusive Mode
Lost write protection disabled
.... (PID:3505): Using STANDBY_ARCHIVE_DEST parameter default value as USE_DB_RECOVERY_FILE_DEST [krsd.c:18222]
Completed: ALTER DATABASE   MOUNT
2021-08-25T17:50:03.796170-07:00
ALTER DATABASE OPEN
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-08-25T17:50:03.877906-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-25T17:50:03.881331-07:00
Beginning crash recovery of 1 threads
 parallel recovery started with 7 processes
 Thread 1: Recovery starting at checkpoint rba (logseq 20 block 49851), scn 0
2021-08-25T17:50:03.944333-07:00
Started redo scan
2021-08-25T17:50:03.967743-07:00
Completed redo scan
 read 39 KB redo, 25 data blocks need recovery
2021-08-25T17:50:03.971574-07:00
Started redo application at
 Thread 1: logseq 20, block 49851, offset 0
2021-08-25T17:50:03.975588-07:00
Recovery of Online Redo Log: Thread 1 Group 4 Seq 20 Reading mem 0
  Mem# 0: +DATA_DG/ORA19C/group04_redo01.log
  Mem# 1: +DATA_DG/ORA19C/group04_redo02.log
2021-08-25T17:50:03.976963-07:00
Completed redo application of 0.02MB
2021-08-25T17:50:04.001480-07:00
Completed crash recovery at
 Thread 1: RBA 20.49930.16, nab 49930, scn 0x000000000018ff2a
 25 data blocks read, 25 data blocks written, 39 redo k-bytes read
Endian type of dictionary set to little
2021-08-25T17:50:04.063555-07:00
LGWR (PID:3438): STARTING ARCH PROCESSES
2021-08-25T17:50:04.075820-07:00
TT00 (PID:3566): Gap Manager starting
Starting background process ARC0
```

FIGURE 88. Database ora19c Alert Log

As stated earlier, VMware Hybrid Cloud Extension copies the original VM to the migrated VMs folder in the **vSphere Templates** view.

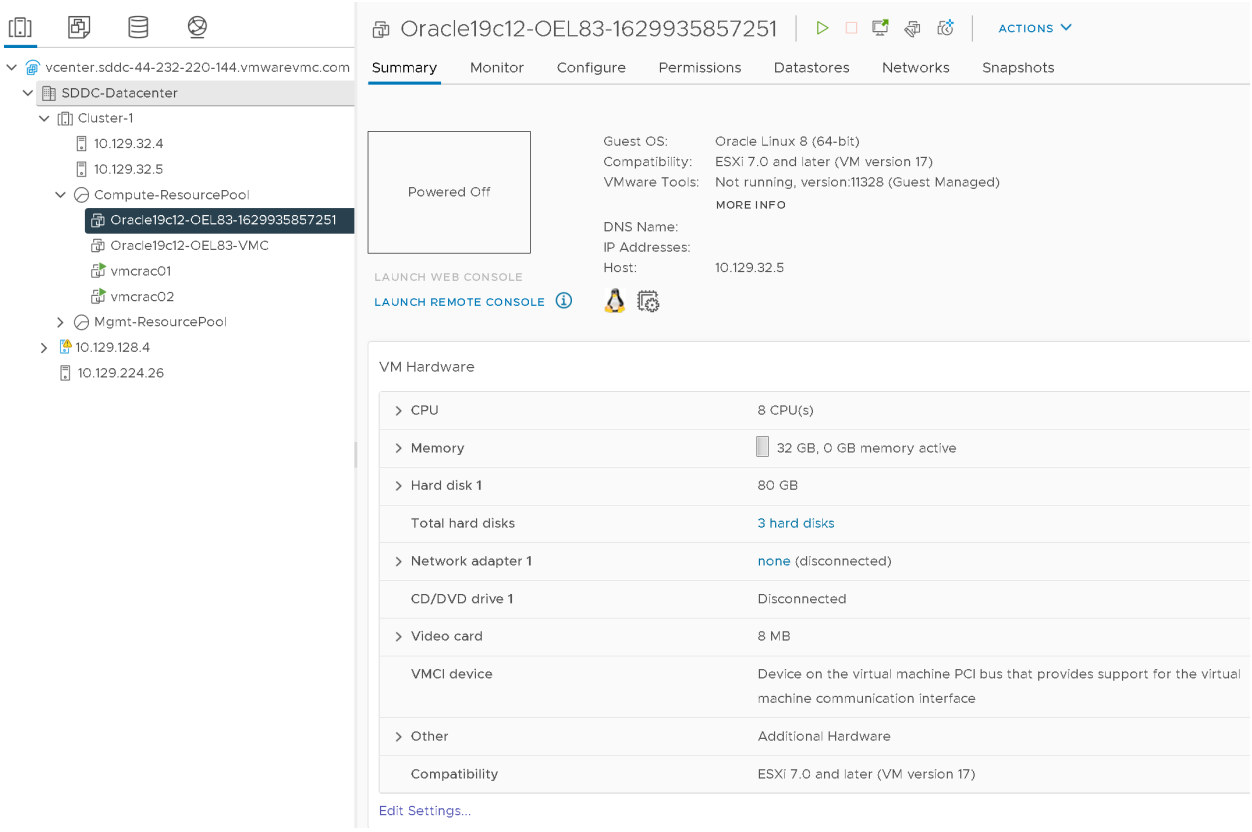


FIGURE 89. VM Oracle19c12-OEL83 Summary

Migrating Oracle Single-Instance Workloads Using Hybrid Cloud Extension Cold Migration

Cold migration uses the same network path as VMware Hybrid Cloud Extension vMotion to transfer a powered-off VM. During a cold migration, the VM IP address and MAC address are preserved. Cold migrations must satisfy the vMotion requirements.

Learn more about *Hybrid Cloud Extension Cold Migration*.

The production single-instance Oracle VM **Oracle19c12-OEL83** on Site A was used for the Hybrid Cloud Extension Cold Migration deployment use case.

Oracle VM **Oracle19c12-OEL83** was powered down with database ora19c **offline**. Click **Migrate** and add VM **Oracle19c12-OEL83** to the migration process.

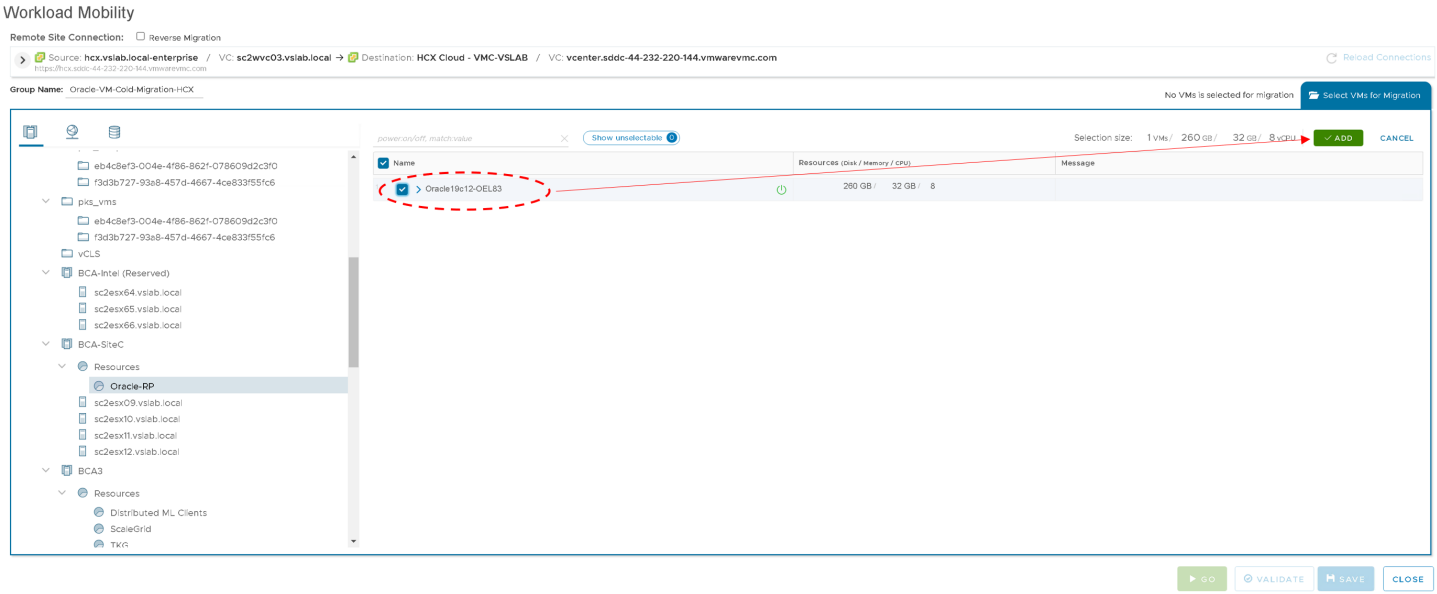


FIGURE 90. VM Oracle19c12-OEL83 Migration Start

Follow the same steps when selecting the target resource pool, datastore, folder, extended options, and network options. Click **Go** to start the migration process.

Note that adding the target IP address 172.16.115.45 with gateway and netmask information is not a supported option and target networking information will not be applied.

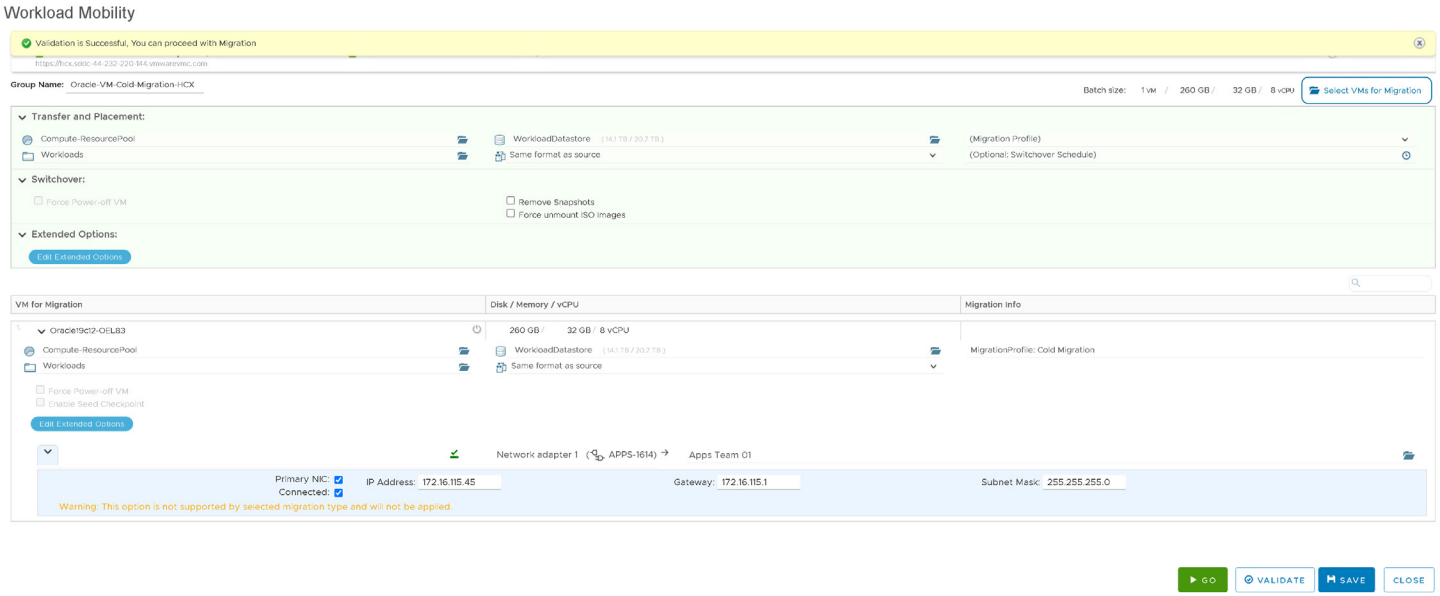


FIGURE 91. Targeting IP Address 172.16.115.45 with Gateway and Netmask Not Supported

The steps for the migration start are as shown below:

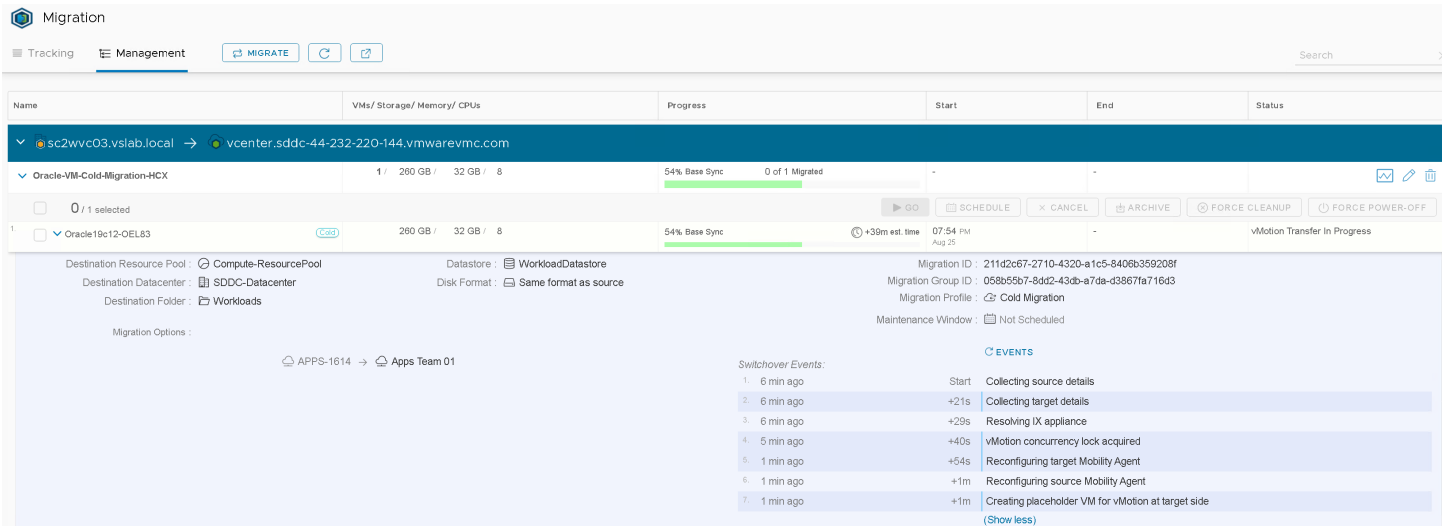


FIGURE 92. VM Oracle19c12-OEL83 Migration Start

The migration completes successfully.

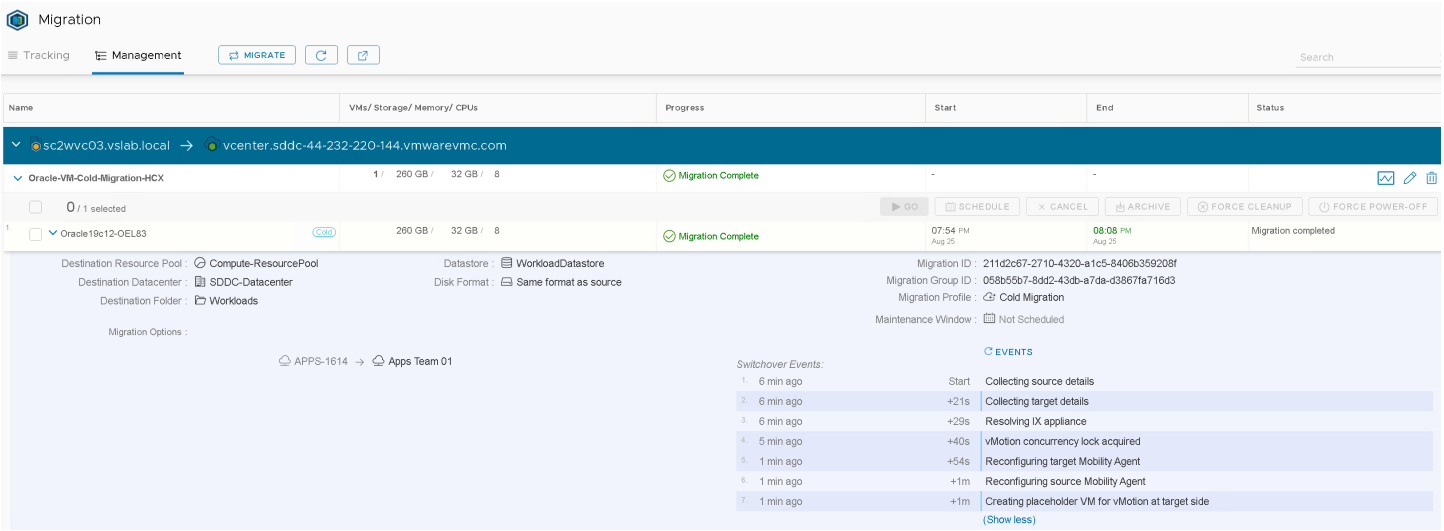


FIGURE 93. VM Oracle19c12-OEL83 Migration Successful

The Oracle VM **Oracle19c12-OEL83** is now on VMware Cloud on AWS and powered off as Hybrid Cloud Extension Cold Migration was performed. Power on the VM and assign IP address 172.16.115.45.

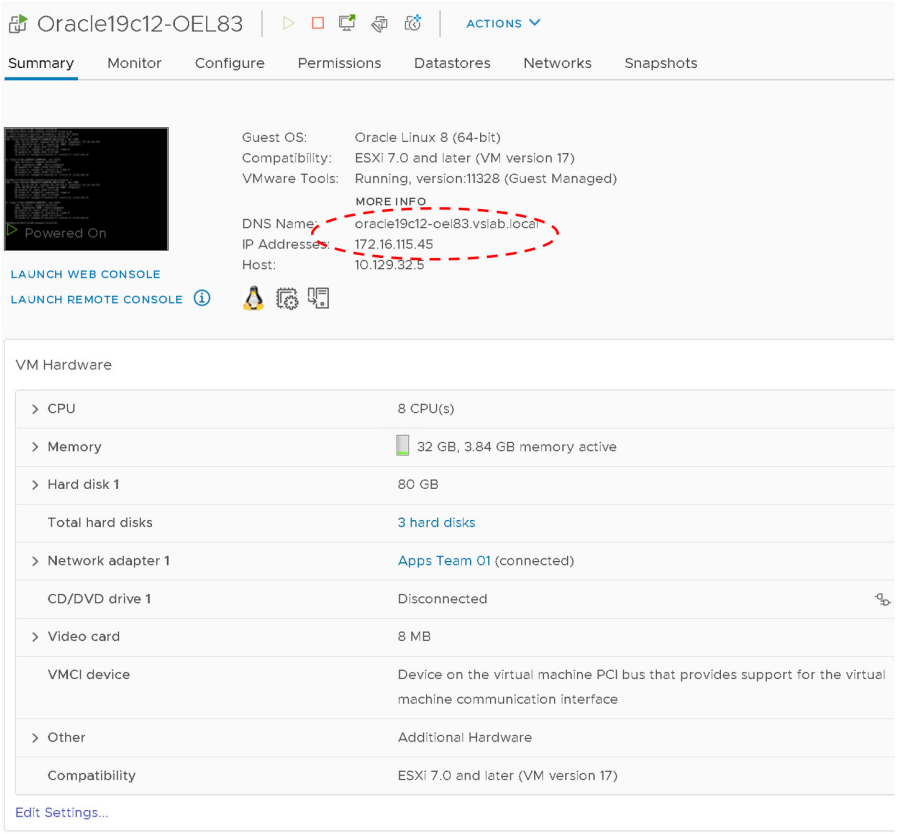


FIGURE 94. VM Oracle19c12-OEL83 Summary

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.115.45  netmask 255.255.255.0  broadcast 172.16.115.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 740  bytes 66603 (65.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 714  bytes 111302 (108.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 228  bytes 28133 (27.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 228  bytes 28133 (27.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Aug 25 20:15:29 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 95. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle database is started normally when the database starts up, which is normal and expected.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1050 alert_ora19c.log
SMON started with pid=23, OS id=4679
LGWR slave LG01 created with pid=24, OS pid=4684
Starting background process SMCO
2021-08-25T20:17:23.953799-07:00
SMCO started with pid=25, OS id=4687
Starting background process RECO
2021-08-25T20:17:23.972059-07:00
RECO started with pid=26, OS id=4690
Starting background process LREG
2021-08-25T20:17:24.001016-07:00
LREG started with pid=28, OS id=4696
Starting background process PXMN
2021-08-25T20:17:24.041841-07:00
PXMN started with pid=30, OS id=4704
Starting background process RBAL
2021-08-25T20:17:24.065947-07:00
RBAL started with pid=31, OS id=4707
Starting background process ASMB
2021-08-25T20:17:24.090432-07:00
ASMB started with pid=32, OS id=4712
Starting background process FENC
2021-08-25T20:17:24.113478-07:00
FENC started with pid=33, OS id=4717
Starting background process MMON
2021-08-25T20:17:24.128013-07:00
MMON started with pid=34, OS id=4724
Starting background process MMNL
2021-08-25T20:17:24.138428-07:00
NOTE: ASMB (index:0) registering with ASM instance as Standard client 0xffffffffffffffff (reg:1360179684) (startid:1081541842) (new connection)
2021-08-25T20:17:24.146124-07:00
NOTE: Loaded library: /opt/oracle/extapi/64/asm/orcl/1/libasm.so
2021-08-25T20:17:24.146678-07:00
MMNL started with pid=35, OS id=4728
Starting background process TMON
2021-08-25T20:17:24.162763-07:00
TMON started with pid=36, OS id=4731
2021-08-25T20:17:24.168653-07:00
Setting CPU count to 8
ORACLE_BASE from environment = /u01/app/oracle
2021-08-25T20:17:24.175286-07:00
NOTE: ASMB (index:0) (4712) connected to ASM instance +ASM, osid: 4722 (Standard mode; client id 0xffffffffffffffff)
NOTE: initiating MARK startup
Starting background process MARK
2021-08-25T20:17:24.196135-07:00
MARK started with pid=37, OS id=4734
2021-08-25T20:17:24.198543-07:00
NOTE: MARK has subscribed
2021-08-25T20:17:24.221678-07:00
ALTER DATABASE   MOUNT
2021-08-25T20:17:27.351502-07:00
NOTE: ASMB mounting group 1 (DATA_DG)
NOTE: Assigning number (1,1) to disk (ORCL:DATA_DISK02)
SUCCESS: mounted group 1 (DATA_DG)
NOTE: grp 1 disk 1: DATA_DISK02 path:ORCL:DATA_DISK02
2021-08-25T20:17:27.511210-07:00
ERROR: failed to establish dependency between database ORA19C and diskgroup resource ora.DATA_DG.dg
2021-08-25T20:17:31.591366-07:00
.... (PID:4735): Redo network throttle feature is disabled at mount time
2021-08-25T20:17:31.633581-07:00
Successful mount of redo thread 1, with mount id 1134771860
2021-08-25T20:17:31.635451-07:00
Database mounted in Exclusive Mode
Lost write protection disabled
.... (PID:4735): Using STANDBY_ARCHIVE_DEST parameter default value as USE_DB_RECOVERY_FILE_DEST [krsd.c:18222]
Completed: ALTER DATABASE   MOUNT
2021-08-25T20:17:31.763348-07:00
ALTER DATABASE OPEN
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-08-25T20:17:31.830980-07:00
```

FIGURE 96. Database ora19c Alert Log

In the case of cold migration, we do not see Hybrid Cloud Extension copying the original VM to the migrated VMs folder in the **vSphere Templates** view.

The steps to perform the reverse migration from VMware Cloud on AWS to Site A are the same as those required to migrate from Site A to VMware Cloud on AWS.

Select the **Reverse Migration** checkbox and select the Oracle VM **Oracle19c12-OEL83**. The remaining steps are the same as those previously outlined.

The summary of the reverse migration is as shown below:

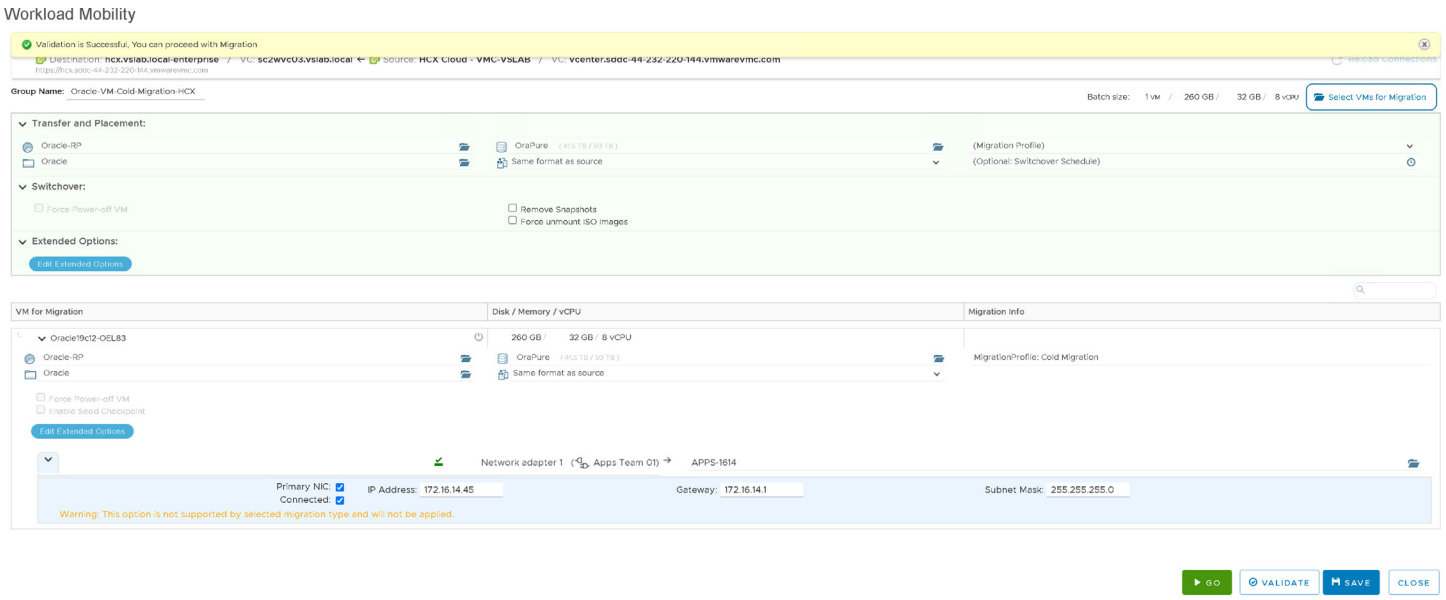


FIGURE 97. VM Oracle19c12-OEL83 Summary

The reverse migration is successful.

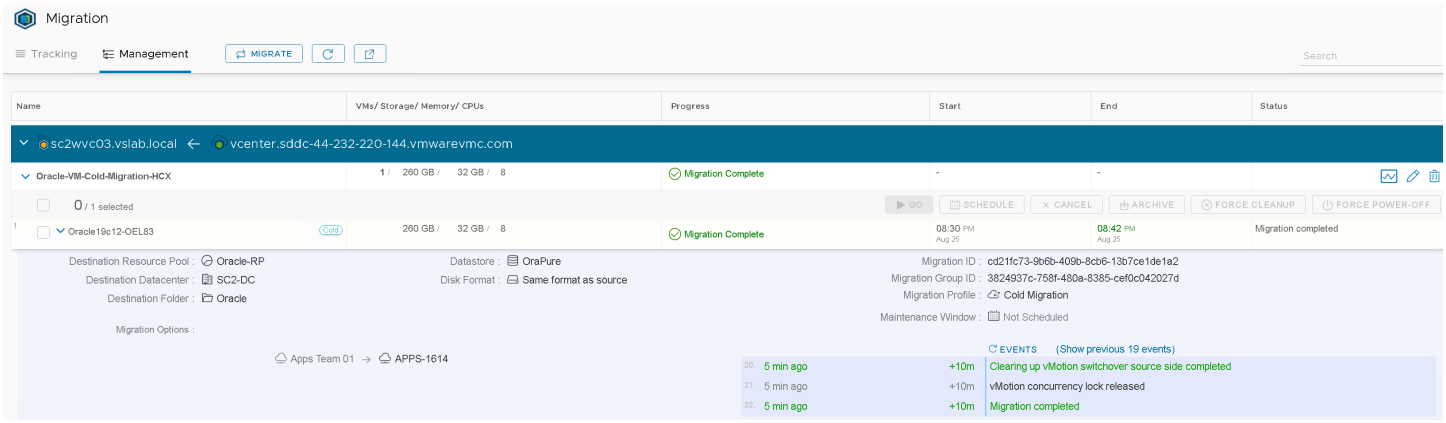


FIGURE 98. VM Oracle19c12-OEL83 Reverse Migration Successful

The Oracle VM **Oracle19c12-OEL83** is now back on Site A and powered off. Power on the VM and assign it IP address 172.16.14.45.

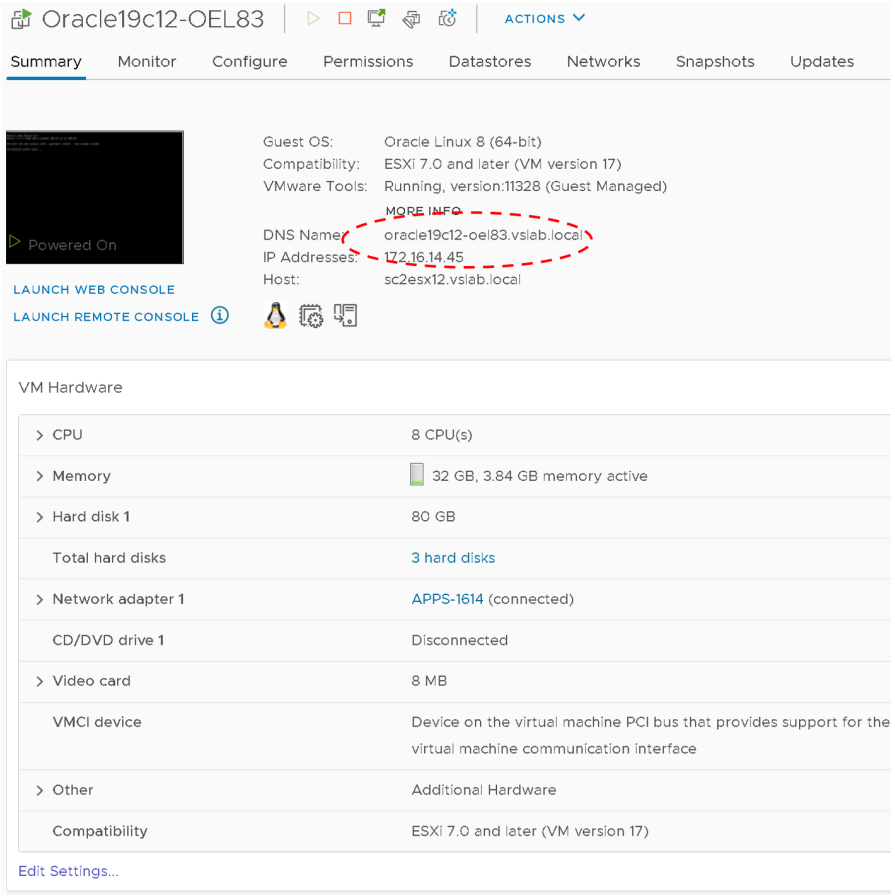


FIGURE 99. VM Oracle19c12-OEL83 Summary

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.45  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 806  bytes 67438 (65.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 657  bytes 121092 (118.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 343  bytes 48505 (47.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 343  bytes 48505 (47.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Aug 25 20:54:09 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 100. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1050 alert_ora19c.log
2021-08-25T20:53:28.838694-07:00
SMCO started with pid=25, OS id=3823
Starting background process RECO
2021-08-25T20:53:28.849838-07:00
RECO started with pid=26, OS id=3826
Starting background process LREG
2021-08-25T20:53:28.875154-07:00
LREG started with pid=28, OS id=3832
Starting background process PXMN
2021-08-25T20:53:28.899499-07:00
PXMN started with pid=30, OS id=3840
Starting background process RBAL
2021-08-25T20:53:28.912440-07:00
RBAL started with pid=31, OS id=3843
Starting background process ASMB
2021-08-25T20:53:28.924760-07:00
ASMB started with pid=32, OS id=3848
Starting background process FENC
2021-08-25T20:53:28.938619-07:00
FENC started with pid=33, OS id=3853
Starting background process MMON
2021-08-25T20:53:28.951441-07:00
MMON started with pid=34, OS id=3858
Starting background process MMNL
2021-08-25T20:53:28.962519-07:00
MMNL started with pid=35, OS id=3863
Starting background process TMON
2021-08-25T20:53:28.968160-07:00
NOTE: ASMB (index:0) registering with ASM instance as Standard client 0xffffffffffffffff (reg:3182390355) (startid:1081544007) (new connection)
2021-08-25T20:53:28.974179-07:00
TMON started with pid=36, OS id=3867
2021-08-25T20:53:28.980738-07:00
Setting CPU count to 8
ORACLE_BASE from environment = /u01/app/oracle
2021-08-25T20:53:28.982090-07:00
NOTE: Loaded library: /opt/oracle/extapi/64/asm/orcl/1/libasm.so
2021-08-25T20:53:29.012322-07:00
NOTE: ASMB (index:0) (3848) connected to ASM instance +ASM, osid: 3861 (Standard mode; client id 0xffffffffffffffff)
NOTE: initiating MARK startup
Starting background process MARK
2021-08-25T20:53:29.033376-07:00
MARK started with pid=38, OS id=3872
2021-08-25T20:53:29.036083-07:00
NOTE: MARK has subscribed
2021-08-25T20:53:29.040320-07:00
ALTER DATABASE   MOUNT
2021-08-25T20:53:32.158394-07:00
NOTE: ASMB mounting group 1 (DATA_DG)
NOTE: Assigning number (1,1) to disk (ORCL:DATA_DISK02)
SUCCESS: mounted group 1 (DATA_DG)
NOTE: grp 1 disk 1: DATA_DISK02 path:ORCL:DATA_DISK02
2021-08-25T20:53:32.263426-07:00
ERROR: failed to establish dependency between database ORA19C and diskgroup resource ora.DATA_DG.dg
2021-08-25T20:53:36.293427-07:00
.... (PID:3869): Redo network throttle feature is disabled at mount time
2021-08-25T20:53:36.325658-07:00
Successful mount of redo thread 1, with mount id 1134750729
2021-08-25T20:53:36.328502-07:00
Database mounted in Exclusive Mode
Lost write protection disabled
.... (PID:3869): Using STANDBY_ARCHIVE_DEST parameter default value as USE_DB_RECOVERY_FILE_DEST [krsd.c:18222]
Completed: ALTER DATABASE   MOUNT
2021-08-25T20:53:36.433733-07:00
ALTER DATABASE OPEN
```

FIGURE 101. Database ora19c Alert Log

Migrating Oracle Single-Instance Workloads Using Hybrid Cloud Extension vMotion

VMware Hybrid Cloud Extension vMotion can transfer a live VM from a VMware Hybrid Cloud Extension-activated vCenter server to a VMware Hybrid Cloud Extension-activated destination site (or from the VMware Hybrid Cloud Extension destination site towards the local site). The vMotion transfer captures the VM's active memory, its execution state, its IP address, and its MAC address. Migration duration depends on the connectivity, including both the bandwidth available and the latency between the two sites.

Learn more about *Hybrid Cloud Extension vMotion Migration*.

The production single-instance Oracle VM **Oracle19c12-OEL83** on Site A was used for the Hybrid Cloud Extension vMotion Migration deployment use case.

Oracle VM **Oracle19c12-OEL83** was powered up with IP Address 172.16.14.45 with database ora19c **online**. Click **Migrate** and add VM **Oracle19c12-OEL83** to the migration process:

As mentioned earlier, Hybrid Cloud Extension Network Extension (NE) provides a Layer 2 VPN (L2VPN) to extend a broadcast domain from a customer site into an AWS based SDDC. NE functionality is provided by a dedicated virtual appliance at both sites.

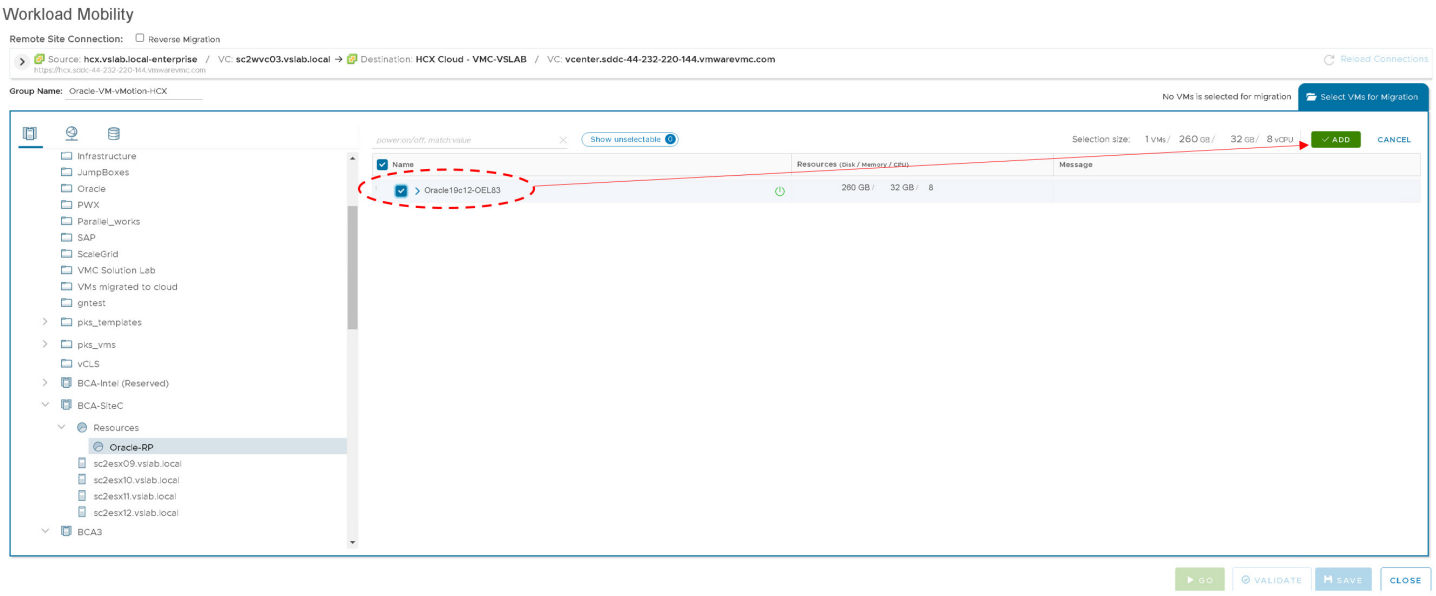


FIGURE 102. Add VM Oracle19c12-OEL83 for Migration

Follow the same steps when selecting the target resource pool, datastore, folder, extended options, and network options. Click **Go** to start the migration process.

Note that adding the target IP address 172.16.115.45 with gateway and netmask information is not a supported option and target networking information will not be applied.

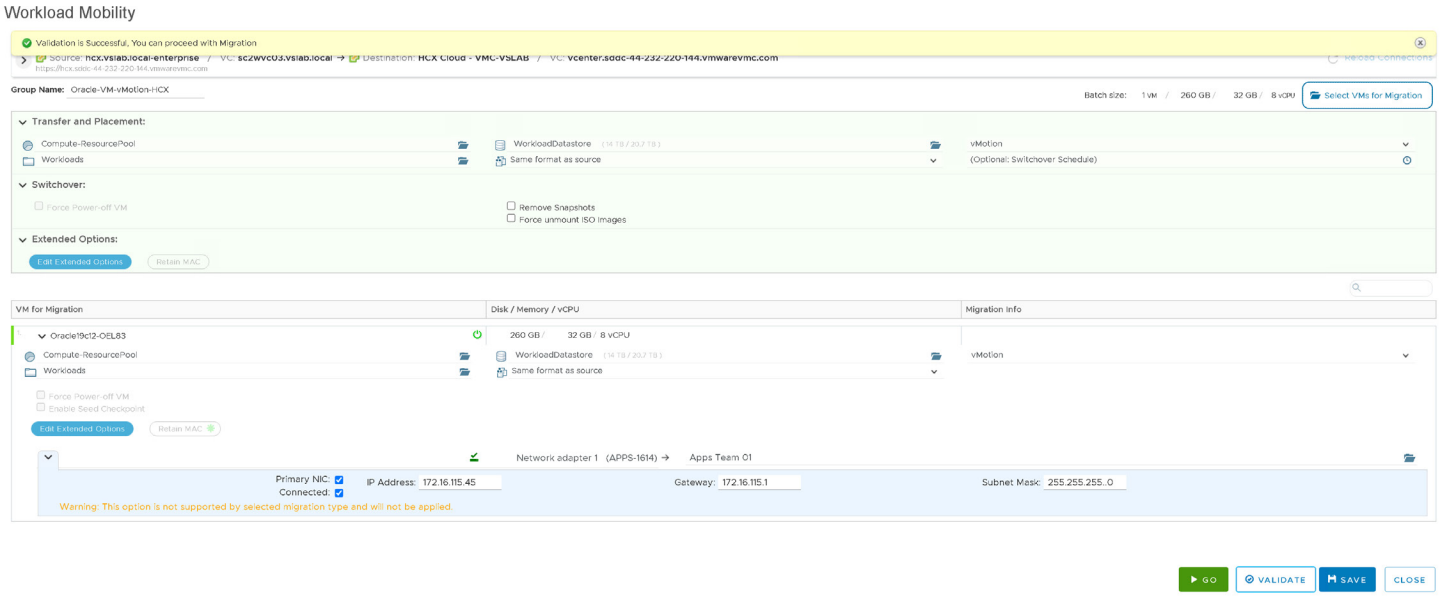


FIGURE 103. Targeting IP Address 172.16.115.45 with Gateway and Netmask Not Supported

The steps for the migration start are as shown below:

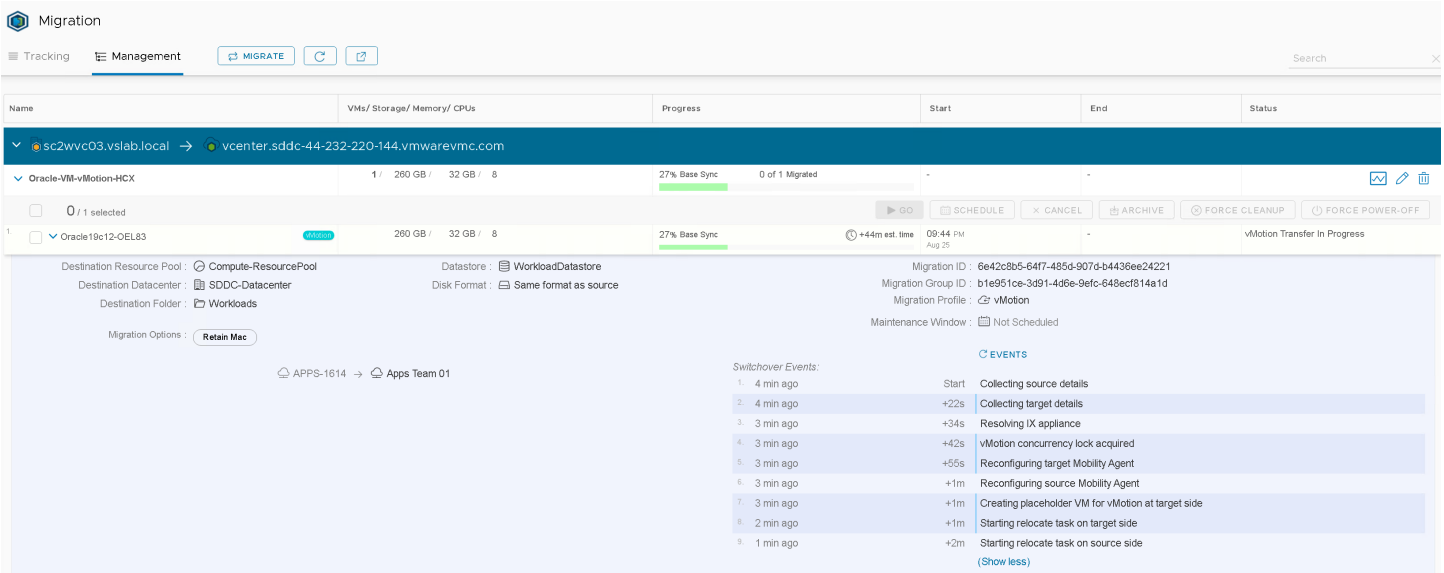


FIGURE 104. VM Oracle19c12-OEL83 Migration Start

The migration completes successfully.

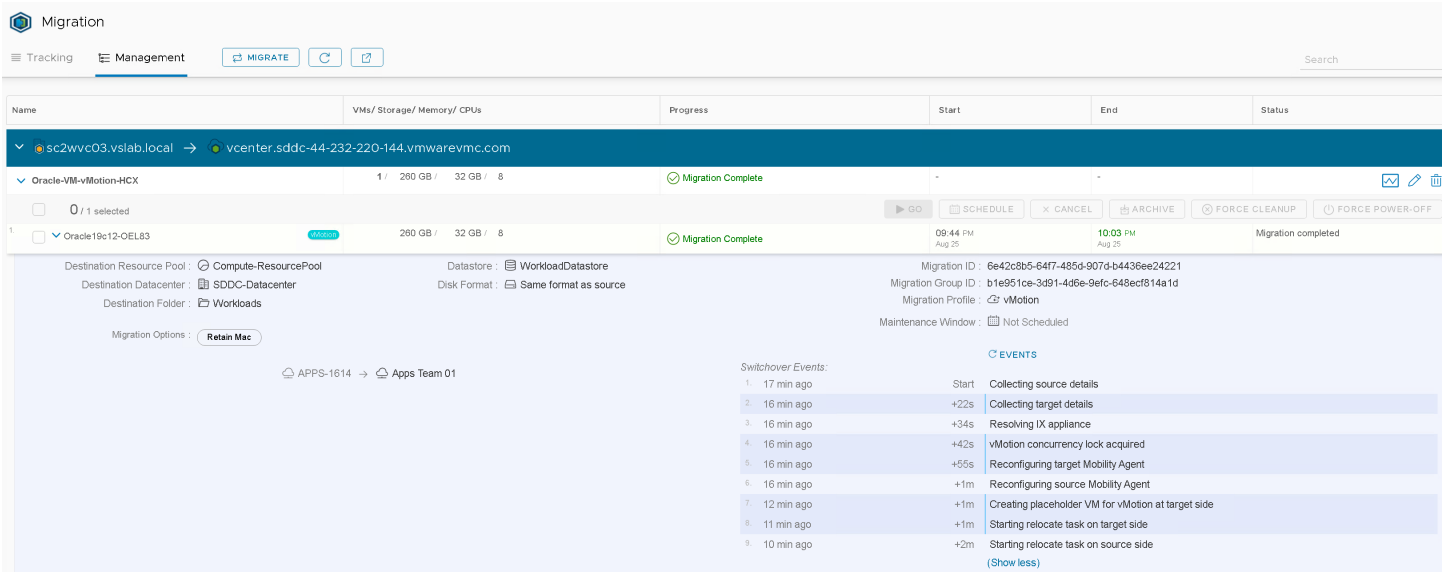


FIGURE 105. VM Oracle19c12-OEL83 Migration Successful

The Oracle VM **Oracle19c12-OEL83** is now on VMware Cloud on AWS with IP address 172.16.14.45. Change the IP address to 172.16.115.45 as adding the target IP address with gateway and netmask information is not a supported option and target networking information will not be applied (as noted in the migration process above).

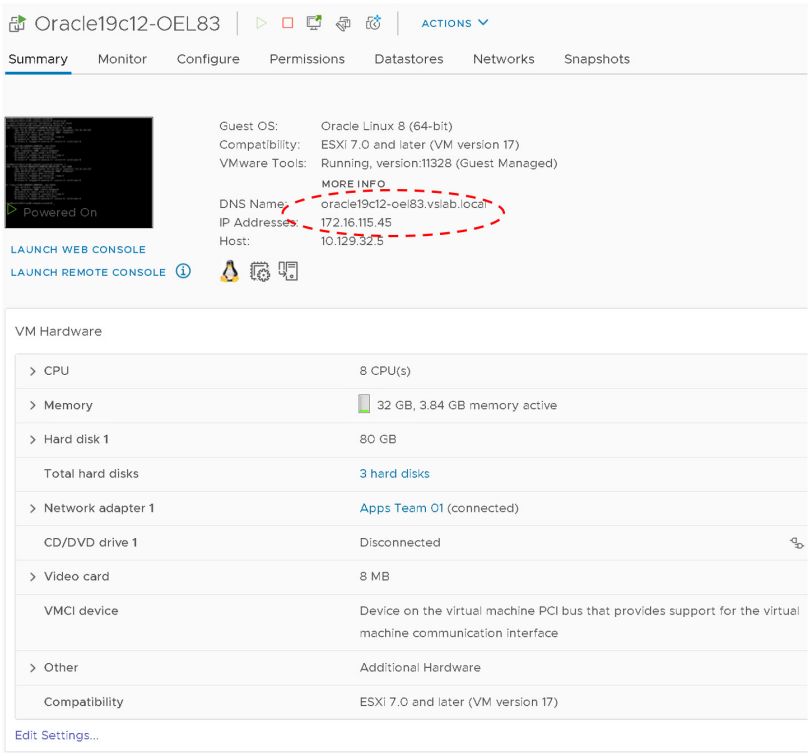


FIGURE 106. VM Oracle19c12-OEL83 Summary

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.115.45  netmask 255.255.255.0  broadcast 172.16.115.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 3671  bytes 321764 (314.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1415  bytes 271283 (264.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3700  bytes 378238 (369.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3700  bytes 378238 (369.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Aug 25 22:07:35 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 107. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle database has been online during the entire migration process.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1000 alert_ora19c.log
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-08-25T20:53:36.512208-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-25T20:53:36.512345-07:00
Crash Recovery excluding pdb 3 which was cleanly closed.
Endian type of dictionary set to little
2021-08-25T20:53:36.533229-07:00
LGWR (PID:3802): STARTING ARCH PROCESSES
2021-08-25T20:53:36.544031-07:00
TT00 (PID:3901): Gap Manager starting
Starting background process ARC0
2021-08-25T20:53:36.556863-07:00
ARC0 started with pid=44, OS id=3904
2021-08-25T20:53:36.566983-07:00
LGWR (PID:3802): ARC0: Archival started
LGWR (PID:3802): STARTING ARCH PROCESSES COMPLETE
2021-08-25T20:53:36.567113-07:00
ARC0 (PID:3904): Becoming a 'no FAL' ARCH
ARC0 (PID:3904): Becoming the 'no SRL' ARCH
2021-08-25T20:53:36.570097-07:00
TMON (PID:3867): STARTING ARCH PROCESSES
Starting background process ARC1
2021-08-25T20:53:36.581339-07:00
ARC1 started with pid=46, OS id=3910
Starting background process ARC2
Starting background process ARC3
2021-08-25T20:53:36.592261-07:00
ARC2 started with pid=47, OS id=3913
2021-08-25T20:53:36.593678-07:00
Redo log for group 2, sequence 22 is not located on DAX storage
2021-08-25T20:53:36.605182-07:00
TMON (PID:3867): ARC1: Archival started
TMON (PID:3867): ARC2: Archival started
2021-08-25T20:53:36.605419-07:00
ARC3 started with pid=48, OS id=3916
2021-08-25T20:53:36.615379-07:00
Thread 1 opened at log sequence 22
2021-08-25T20:53:36.615401-07:00
TMON (PID:3867): ARC3: Archival started
2021-08-25T20:53:36.615424-07:00
  Current log# 2 seq# 22 mem# 0: +DATA_DG/ORA19C/group02_redo01.log
2021-08-25T20:53:36.615456-07:00
TMON (PID:3867): STARTING ARCH PROCESSES COMPLETE
2021-08-25T20:53:36.615464-07:00
  Current log# 2 seq# 22 mem# 1: +DATA_DG/ORA19C/group02_redo02.log
Successful open of redo thread 1
2021-08-25T20:53:36.615666-07:00
MTTR advisory is disabled because FAST_START_MTTR_TARGET is not set
Stopping change tracking
Undo initialization recovery: Parallel FPTR complete: start:292791 end:292794 diff:3 ms (0.0 seconds)
Undo initialization recovery: err:0 start: 292790 end: 292794 diff: 4 ms (0.0 seconds)
[3898] Successfully onlined Undo Tablespace 2.
Undo initialization online undo segments: err:0 start: 292794 end: 292920 diff: 126 ms (0.1 seconds)
Undo initialization finished serial:0 start:292790 end:292926 diff:136 ms (0.1 seconds)
Database Characterset is AL32UTF8
No Resource Manager plan active
2021-08-25T20:53:37.568214-07:00
joxcsys_required_dirobj_exists: directory object exists with required path /u01/app/oracle/product/19.0.0/dbhome_1/javavm/admin/, pid 3898 cid 1
replication_dependency_tracking turned off (no async multimaster replication found)
Starting background process AQPC
2021-08-25T20:53:37.880142-07:00
AQPC started with pid=50, OS id=3925
2021-08-25T20:53:37.963698-07:00
PDB$SEED(2):Pluggable database PDB$SEED opening in read only
PDB$SEED(2):Endian type of dictionary set to little
```

FIGURE 108. Database ora19c Alert Log

The steps to perform the reverse migration from VMware Cloud on AWS to Site A are the same as those required for migration from Site A to VMware Cloud on AWS.

Select the **Reverse Migration** checkbox and select the Oracle VM **Oracle19c12-OEL83**. The remaining steps are the same as previously outlined.

The summary of the reverse migration is as shown below:

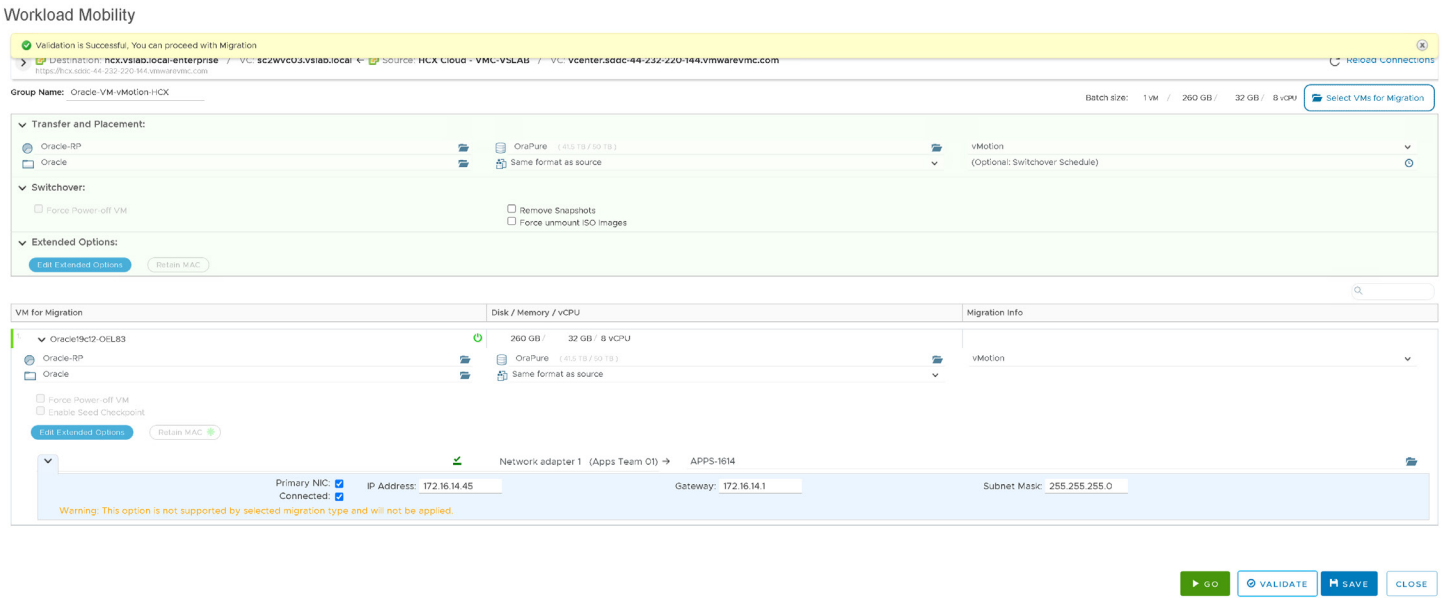


FIGURE 109. VM Oracle19c12-OEL83 Reverse Migration Summary

The reverse migration is successful.

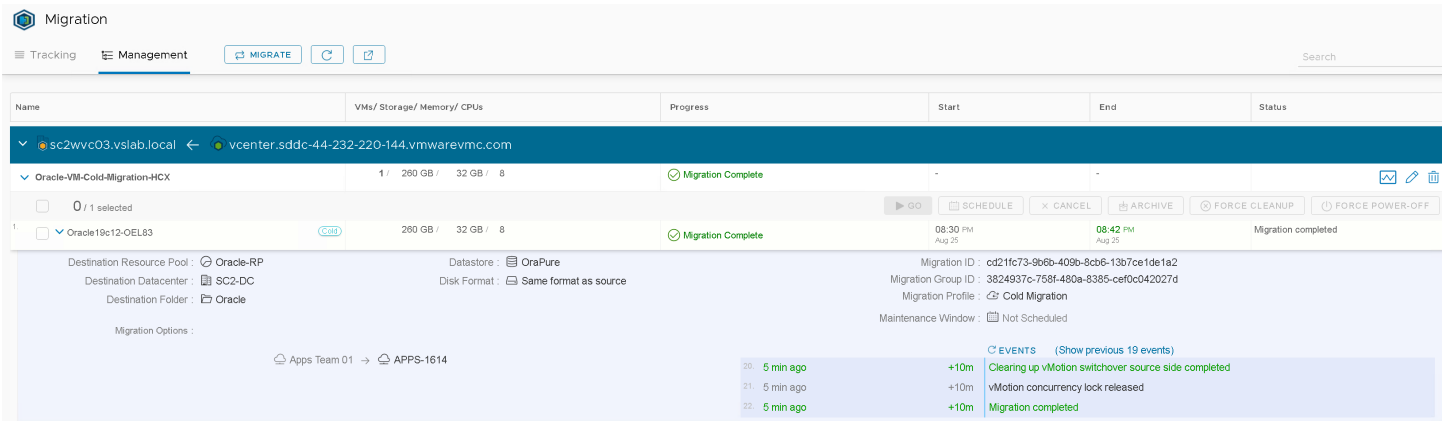


FIGURE 110. VM Oracle19c12-OEL83 Reverse Migration Successful

The Oracle VM **Oracle19c12-OEL83** is now back on Site A with IP address 172.16.115.45. Change the IP address to 172.16.14.45.

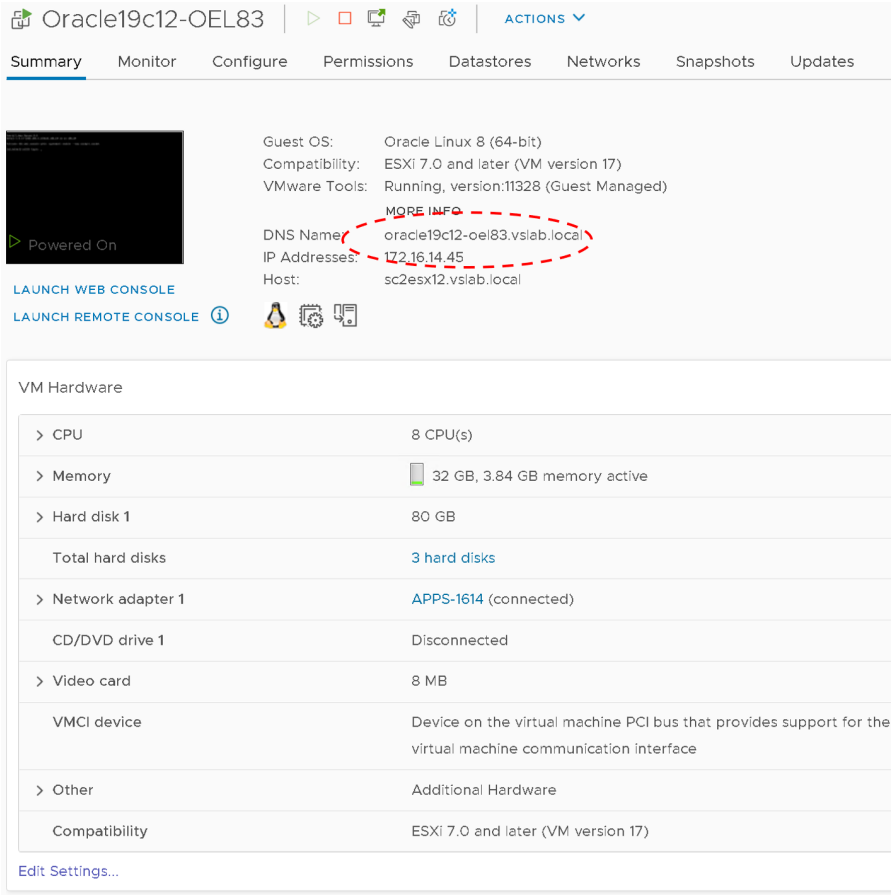


FIGURE 111. VM Oracle19c12-OEL83 Summary

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.45  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 4526  bytes 391344 (382.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2208  bytes 651222 (635.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 3763  bytes 387972 (378.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3763  bytes 387972 (378.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Aug 25 22:29:47 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 112. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle database has been online during the entire migration process.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1000 alert_ora19c.log
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-08-25T20:53:36.512208-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-25T20:53:36.512345-07:00
Crash Recovery excluding pdb 3 which was cleanly closed.
Endian type of dictionary set to little
2021-08-25T20:53:36.533229-07:00
LGWR (PID:3802): STARTING ARCH PROCESSES
2021-08-25T20:53:36.544031-07:00
TT00 (PID:3901): Gap Manager starting
Starting background process ARC0
2021-08-25T20:53:36.556863-07:00
ARC0 started with pid=44, OS id=3904
2021-08-25T20:53:36.566983-07:00
LGWR (PID:3802): ARC0: Archival started
LGWR (PID:3802): STARTING ARCH PROCESSES COMPLETE
2021-08-25T20:53:36.567113-07:00
ARC0 (PID:3904): Becoming a 'no FAL' ARCH
ARC0 (PID:3904): Becoming the 'no SRL' ARCH
2021-08-25T20:53:36.570097-07:00
TMON (PID:3867): STARTING ARCH PROCESSES
Starting background process ARC1
2021-08-25T20:53:36.581339-07:00
ARC1 started with pid=46, OS id=3910
Starting background process ARC2
Starting background process ARC3
2021-08-25T20:53:36.592261-07:00
ARC2 started with pid=47, OS id=3913
2021-08-25T20:53:36.593678-07:00
Redo log for group 2, sequence 22 is not located on DAX storage
2021-08-25T20:53:36.605182-07:00
TMON (PID:3867): ARC1: Archival started
TMON (PID:3867): ARC2: Archival started
2021-08-25T20:53:36.605419-07:00
ARC3 started with pid=48, OS id=3916
2021-08-25T20:53:36.615379-07:00
Thread 1 opened at log sequence 22
2021-08-25T20:53:36.615401-07:00
TMON (PID:3867): ARC3: Archival started
2021-08-25T20:53:36.615424-07:00
  Current log# 2 seq# 22 mem# 0: +DATA_DG/ORA19C/group02_redo01.log
2021-08-25T20:53:36.615456-07:00
TMON (PID:3867): STARTING ARCH PROCESSES COMPLETE
2021-08-25T20:53:36.615464-07:00
  Current log# 2 seq# 22 mem# 1: +DATA_DG/ORA19C/group02_redo02.log
Successful open of redo thread 1
2021-08-25T20:53:36.615666-07:00
MTTR advisory is disabled because FAST_START_MTTR_TARGET is not set
Stopping change tracking
Undo initialization recovery: Parallel FPTR complete: start:292791 end:292794 diff:3 ms (0.0 seconds)
Undo initialization recovery: err:0 start: 292790 end: 292794 diff: 4 ms (0.0 seconds)
[3898] Successfully onlined Undo Tablespace 2.
Undo initialization online undo segments: err:0 start: 292794 end: 292920 diff: 126 ms (0.1 seconds)
Undo initialization finished serial:0 start:292790 end:292926 diff:136 ms (0.1 seconds)
Database Characterset is AL32UTF8
No Resource Manager plan active
2021-08-25T20:53:37.568214-07:00
joxcsys_required_dirobj_exists: directory object exists with required path /u01/app/oracle/product/19.0.0/dbhome_1/javavm/admin/, pid 3898 cid 1
replication_dependency_tracking turned off (no async multimaster replication found)
Starting background process AQPC
2021-08-25T20:53:37.880142-07:00
AQPC started with pid=50, OS id=3925
2021-08-25T20:53:37.963698-07:00
PDB$SEED(2):Pluggable database PDB$SEED opening in read only
PDB$SEED(2):Endian type of dictionary set to little
```

FIGURE 113. Database ora19c Alert Log

Migrating Oracle Single-Instance Workloads Using Hybrid Cloud Extension Replication Assisted vMotion

VMware Hybrid Cloud Extension Replication Assisted vMotion (RAV) uses the Hybrid Cloud Extension interconnect appliance along with replication and vMotion technologies to provide large scale, parallel migrations with zero downtime.

Learn more about *Hybrid Cloud Extension Replication Assisted vMotion (RAV) Migration*.

The production single-instance Oracle VM **Oracle19c12-OEL83** on Site A was used for the Hybrid Cloud Extension Replication Assisted vMotion (RAV) migration deployment use case.

Oracle VM **Oracle19c12-OEL83** was powered up with IP Address 172.16.14.45 with database ora19c **online**. Click **Migrate** and add VM **Oracle19c12-OEL83** to the migration process.

As mentioned earlier, Hybrid Cloud Extension Network Extension (NE) provides a Layer 2 VPN (L2VPN) to extend a broadcast domain from a customer site into an AWS based SDDC. NE functionality is provided by a dedicated virtual appliance at both sites.

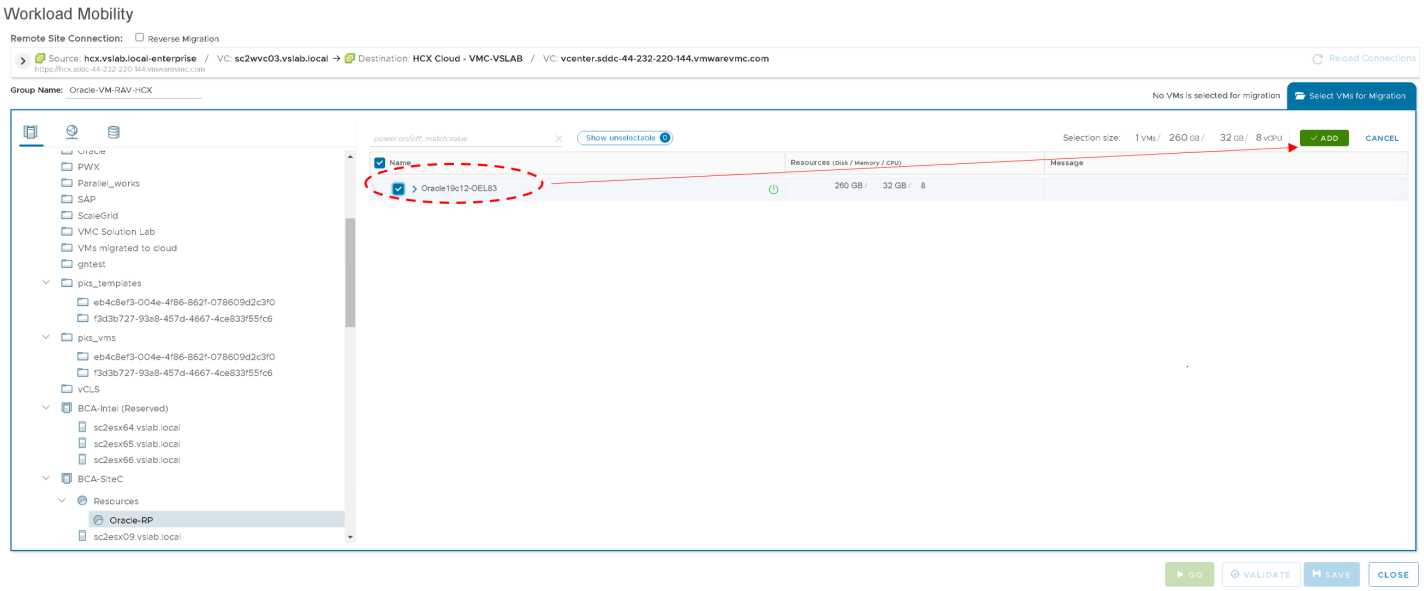


FIGURE 114. Add VM Oracle19c12-OEL83 for Migration

Follow the same steps when selecting the target resource pool, datastore, folder, extended options, and network options. Click **Go** to start the migration process.

Note that adding the target IP address 172.16.115.45 with gateway and netmask information is not a supported option and target networking information will not be applied.

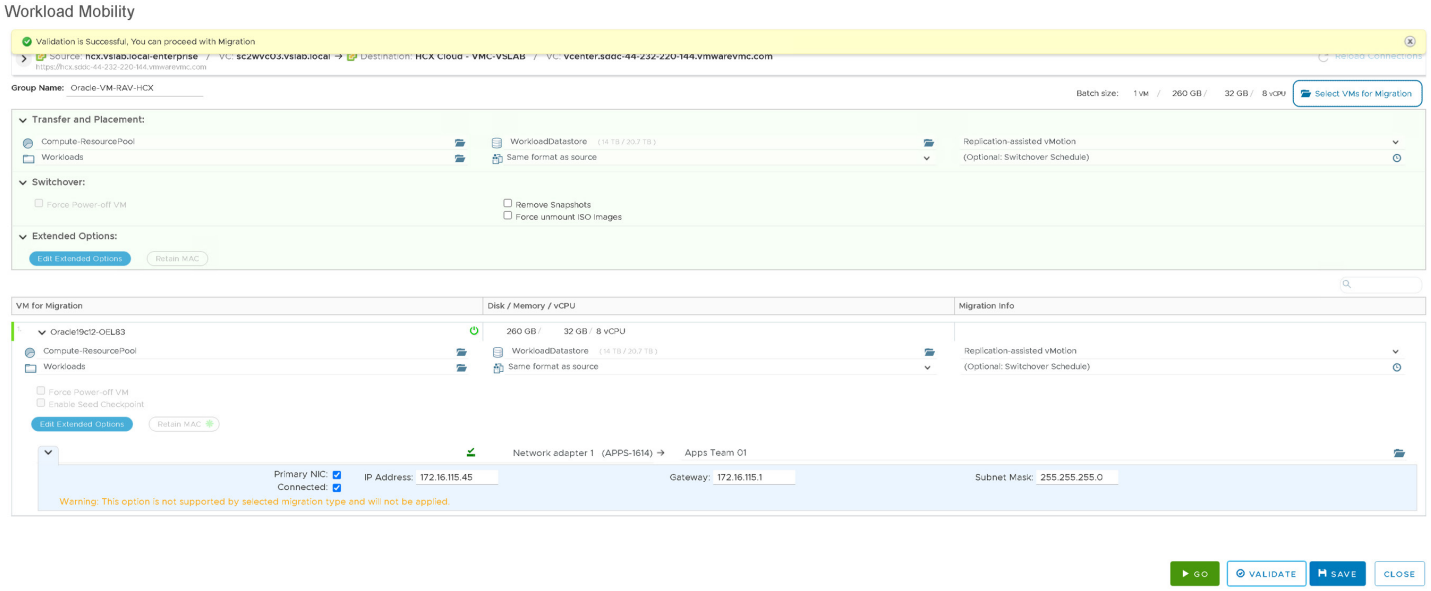


FIGURE 115. Targeting IP Address 172.16.115.45 with Gateway and Netmask Not Supported

The steps for the migration start are as shown below:

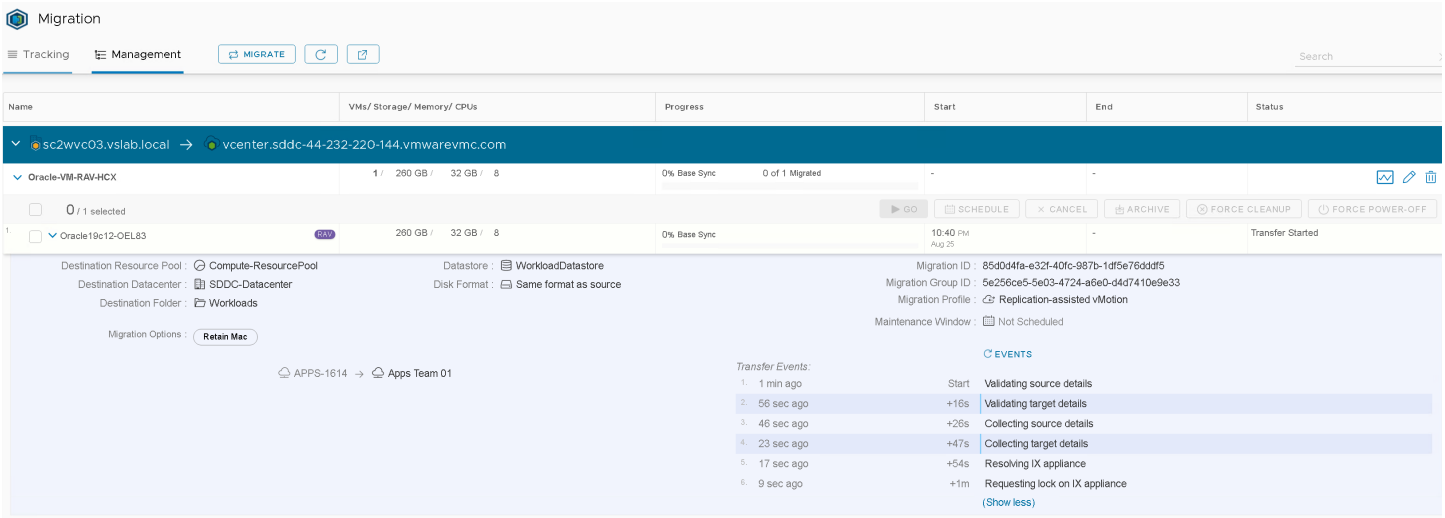


FIGURE 116. VM Oracle19c12-OEL83 Migration Start

The migration completes successfully.

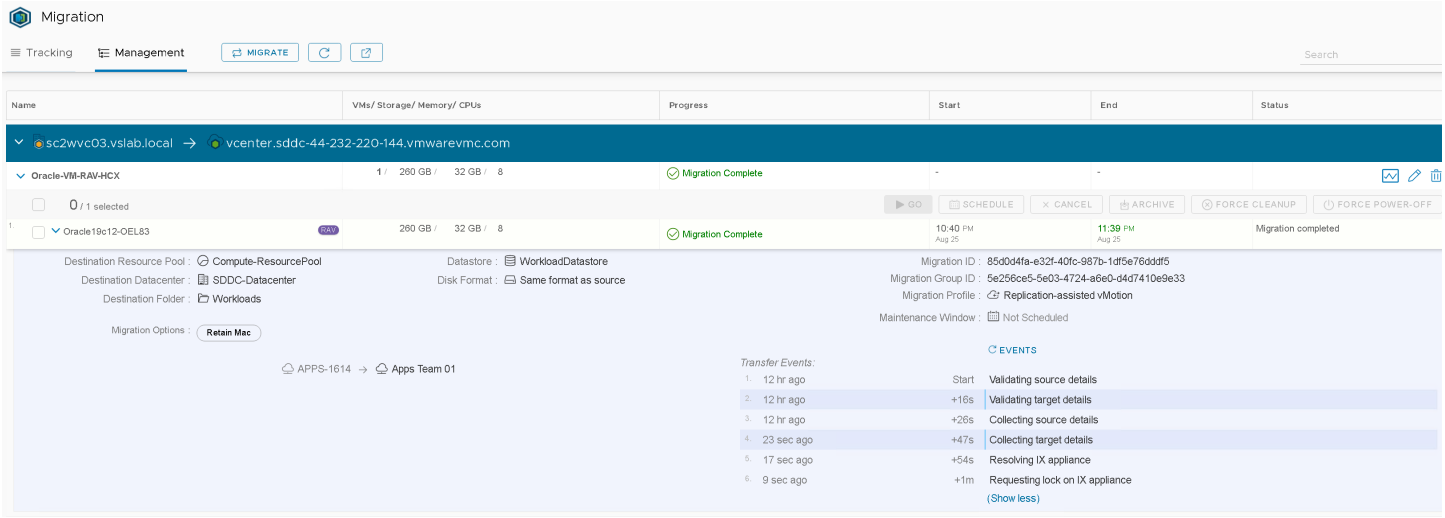


FIGURE 117. VM Oracle19c12-OEL83 Migration Successful

Oracle VM **Oracle19c12-OEL83** is now on VMware Cloud on AWS with IP address 172.16.14.45. Change the IP address to 172.16.115.45 as adding target IP address with gateway and netmask information is not a supported option and target networking information will not be applied (as noted in the migration process above).

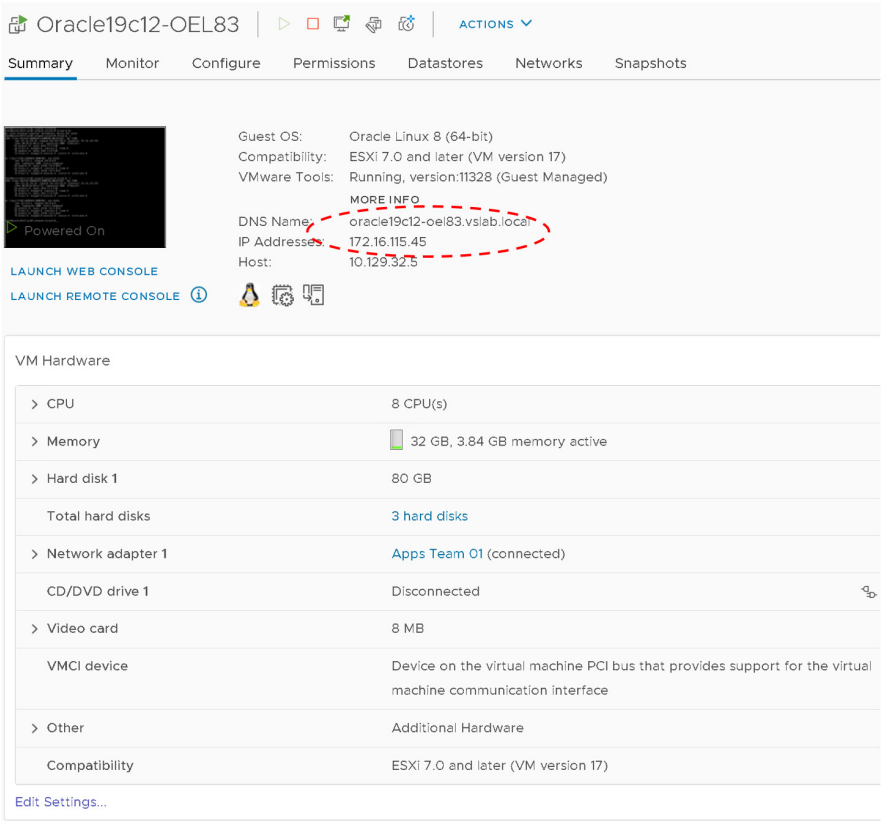


FIGURE 118. VM Oracle19c12-OEL83 Summary

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.115.45  netmask 255.255.255.0  broadcast 172.16.115.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 7529  bytes 589438 (575.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3723  bytes 924889 (903.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 13197  bytes 1307087 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13197  bytes 1307087 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Aug 26 11:19:19 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 119. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle database has been online during the entire migration process.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1050 alert_ora19c.log
NOTE: ASMB (index:0) registering with ASM instance as Standard client 0xffffffffffffffff (reg:3182390355) (startid:1081544007) (new connection)
2021-08-25T20:53:28.974179-07:00
TMON started with pid=36, OS id=3867
2021-08-25T20:53:28.980738-07:00
Setting CPU count to 8
ORACLE_BASE from environment = /u01/app/oracle
2021-08-25T20:53:28.982090-07:00
NOTE: Loaded library: /opt/oracle/extapi/64/asm/orcl/1/libasm.so
2021-08-25T20:53:29.012322-07:00
NOTE: ASMB (index:0) (3848) connected to ASM instance +ASM, osid: 3861 (Standard mode; client id 0xffffffffffffffff)
NOTE: initiating MARK startup
Starting background process MARK
2021-08-25T20:53:29.033376-07:00
MARK started with pid=38, OS id=3872
2021-08-25T20:53:29.036083-07:00
NOTE: MARK has subscribed
2021-08-25T20:53:29.040320-07:00
ALTER DATABASE   MOUNT
2021-08-25T20:53:32.158394-07:00
NOTE: ASMB mounting group 1 (DATA_DG)
NOTE: Assigning number (1,1) to disk (ORCL:DATA_DISK02)
SUCCESS: mounted group 1 (DATA_DG)
NOTE: grp 1 disk 1: DATA_DISK02 path:ORCL:DATA_DISK02
2021-08-25T20:53:32.263426-07:00
ERROR: failed to establish dependency between database ORA19C and diskgroup resource ora.DATA_DG.dg
2021-08-25T20:53:36.293427-07:00
.... (PID:3869): Redo network throttle feature is disabled at mount time
2021-08-25T20:53:36.325658-07:00
Successful mount of redo thread 1, with mount id 1134750729
2021-08-25T20:53:36.328502-07:00
Database mounted in Exclusive Mode
Lost write protection disabled
.... (PID:3869): Using STANDBY_ARCHIVE_DEST parameter default value as USE_DB_RECOVERY_FILE_DEST [krsd.c:18222]
Completed: ALTER DATABASE   MOUNT
2021-08-25T20:53:36.433733-07:00
ALTER DATABASE OPEN
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-08-25T20:53:36.512208-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-25T20:53:36.512345-07:00
Crash Recovery excluding pdb 3 which was cleanly closed.
Endian type of dictionary set to little
2021-08-25T20:53:36.533229-07:00
LGWR (PID:3802): STARTING ARCH PROCESSES
2021-08-25T20:53:36.544031-07:00
TT00 (PID:3901): Gap Manager starting
Starting background process ARC0
2021-08-25T20:53:36.556863-07:00
ARC0 started with pid=44, OS id=3904
2021-08-25T20:53:36.566983-07:00
LGWR (PID:3802): ARC0: Archival started
LGWR (PID:3802): STARTING ARCH PROCESSES COMPLETE
2021-08-25T20:53:36.567113-07:00
ARC0 (PID:3904): Becoming a 'no FAL' ARCH
ARC0 (PID:3904): Becoming the 'no SRL' ARCH
2021-08-25T20:53:36.570097-07:00
TMON (PID:3867): STARTING ARCH PROCESSES
Starting background process ARC1
2021-08-25T20:53:36.581339-07:00
ARC1 started with pid=46, OS id=3910
Starting background process ARC2
Starting background process ARC3
2021-08-25T20:53:36.592261-07:00
ARC2 started with pid=47, OS id=3913
2021-08-25T20:53:36.593678-07:00
Redo log for group 2, sequence 22 is not located on DAX storage
2021-08-25T20:53:36.605182-07:00
TMON (PID:3867): ARC1: Archival started
TMON (PID:3867): ARC2: Archival started
2021-08-25T20:53:36.605419-07:00
ARC3 started with pid=48, OS id=3916
```

FIGURE 120. Database ora19c Alert Log

The steps to perform the reverse migration from VMware Cloud on AWS to Site A are the same as those required to migrate from Site A to VMware Cloud on AWS.

Select the **Reverse Migration** checkbox and select the Oracle VM **Oracle19c12-OEL83**. The remaining steps are the same as previously outlined.

The summary of the reverse migration is as shown below:

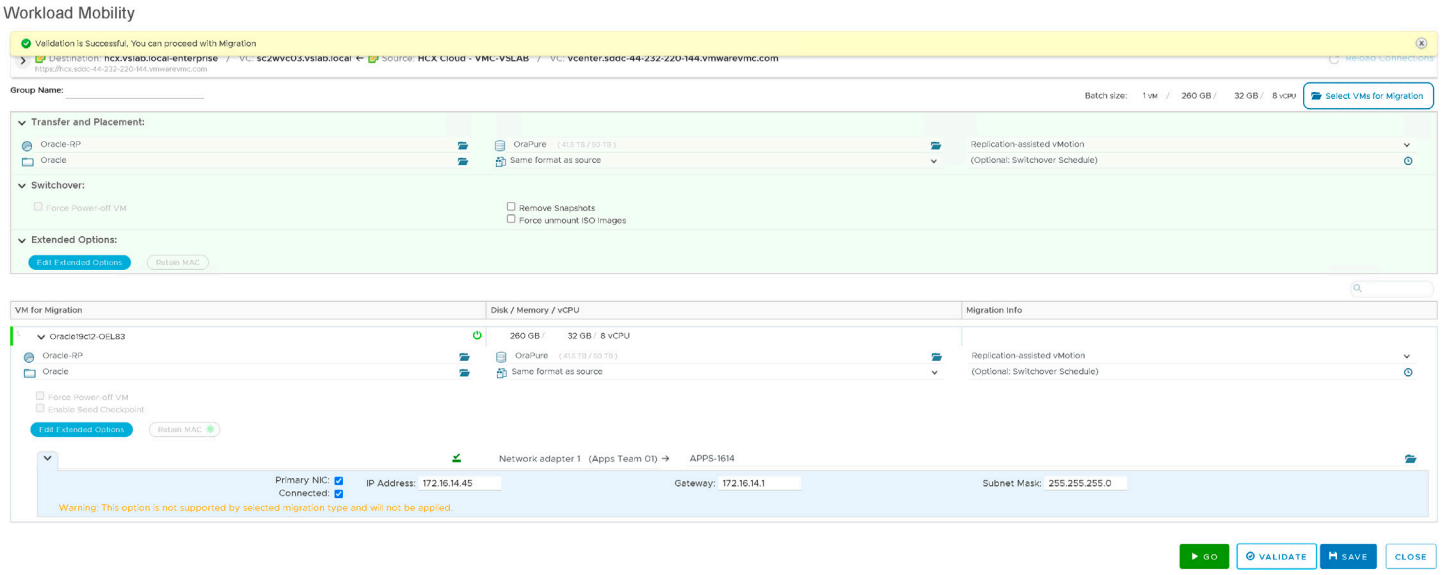


FIGURE 121. VM Oracle19c12-OEL83 Reverse Migration Summary

The reverse migration is successful:

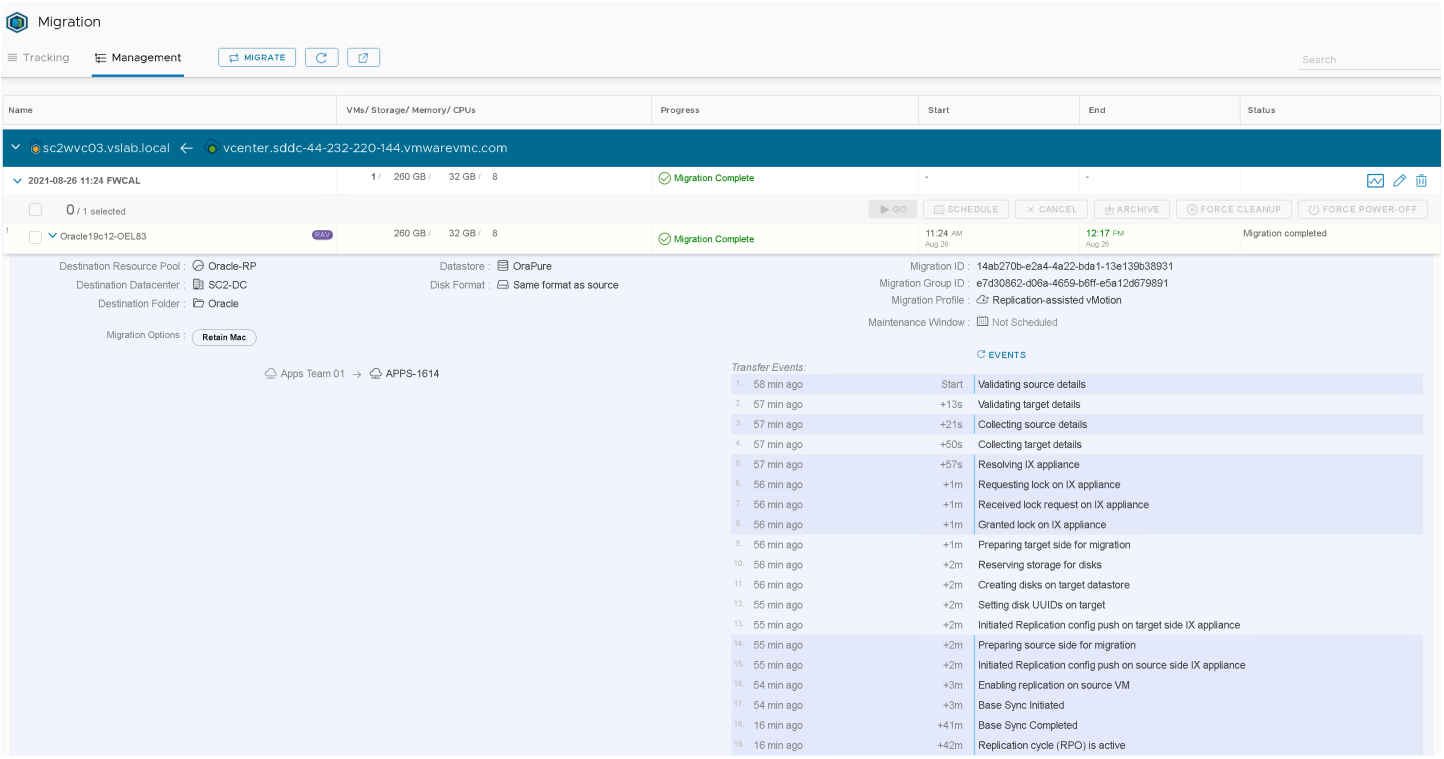


FIGURE 122. VM Oracle19c12-OEL83 Revers Migration Successful

The Oracle VM **Oracle19c12-OEL83** is now back on Site A with IP address 172.16.115.45. Change the IP address to 172.16.14.45.

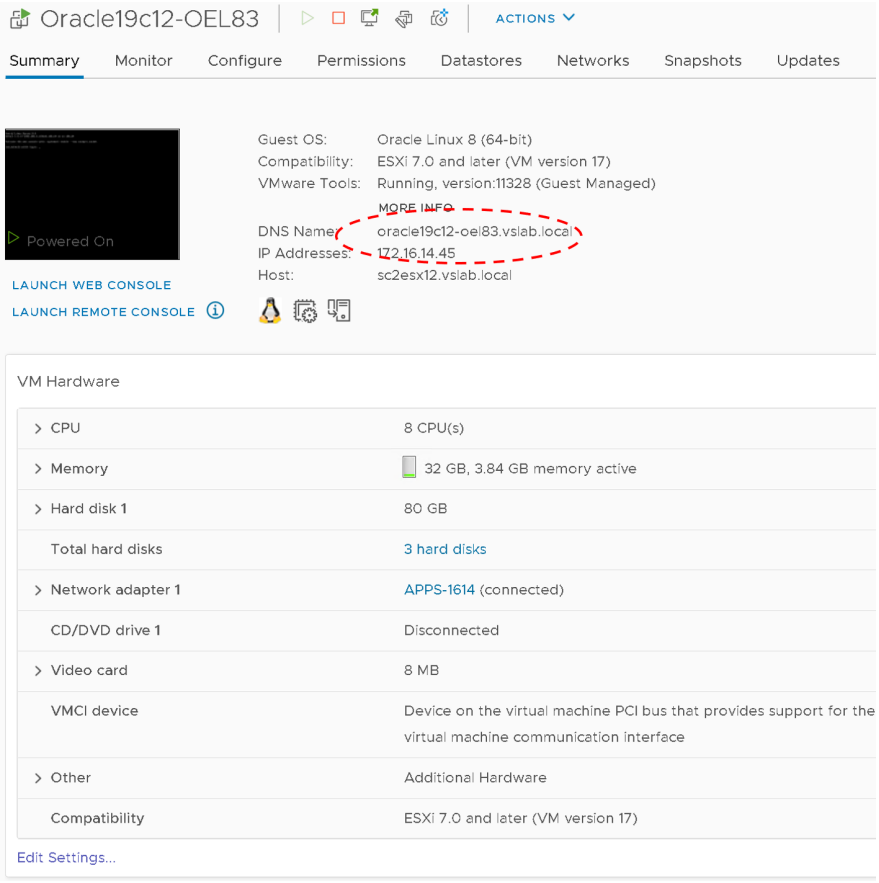


FIGURE 123. VM Oracle19c12-OEL83 Summary

The database **ora19c** is up.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.45  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:a2:f9  txqueuelen 1000  (Ethernet)
        RX packets 8501  bytes 663256 (647.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5010  bytes 1255944 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 13301  bytes 1325437 (1.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13301  bytes 1325437 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@oracle19c12-oel83:ora19c:/home/oracle>
oracle@oracle19c12-oel83:ora19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Aug 26 12:26:52 2021
Version 19.12.0.0.0

Copyright (c) 1982, 2021, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0

SQL> select name from v$database;

NAME
---------
ORA19C

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.12.0.0.0
oracle@oracle19c12-oel83:ora19c:/home/oracle>
```

FIGURE 124. Database ora19c Alert Log

The alert log for the database shows no errors. Oracle database has been online during the entire migration process.

```
oracle@oracle19c12-oel83:ora19c:/home/oracle> tail -1050 alert_ora19c.log
TMON started with pid=36, OS id=3867
2021-08-25T20:53:28.980738-07:00
Setting CPU count to 8
ORACLE_BASE from environment = /u01/app/oracle
2021-08-25T20:53:28.982090-07:00
NOTE: Loaded library: /opt/oracle/extapi/64/asm/orcl/1/libasm.so
2021-08-25T20:53:29.012322-07:00
NOTE: ASMB (index:0) (3848) connected to ASM instance +ASM, osid: 3861 (Standard mode; client id 0xffffffffffffffff)
NOTE: initiating MARK startup
Starting background process MARK
2021-08-25T20:53:29.033376-07:00
MARK started with pid=38, OS id=3872
2021-08-25T20:53:29.036083-07:00
NOTE: MARK has subscribed
2021-08-25T20:53:29.040320-07:00
ALTER DATABASE   MOUNT
2021-08-25T20:53:32.158394-07:00
NOTE: ASMB mounting group 1 (DATA_DG)
NOTE: Assigning number (1,1) to disk (ORCL:DATA_DISK02)
SUCCESS: mounted group 1 (DATA_DG)
NOTE: grp 1 disk 1: DATA_DISK02 path:ORCL:DATA_DISK02
2021-08-25T20:53:32.263426-07:00
ERROR: failed to establish dependency between database ORA19C and diskgroup resource ora.DATA_DG.dg
2021-08-25T20:53:36.293427-07:00
.... (PID:3869): Redo network throttle feature is disabled at mount time
2021-08-25T20:53:36.325658-07:00
Successful mount of redo thread 1, with mount id 1134750729
2021-08-25T20:53:36.328502-07:00
Database mounted in Exclusive Mode
Lost write protection disabled
.... (PID:3869): Using STANDBY_ARCHIVE_DEST parameter default value as USE_DB_RECOVERY_FILE_DEST [krsd.c:18222]
Completed: ALTER DATABASE   MOUNT
2021-08-25T20:53:36.433733-07:00
ALTER DATABASE OPEN
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-08-25T20:53:36.512208-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-25T20:53:36.512345-07:00
Crash Recovery excluding pdb 3 which was cleanly closed.
Endian type of dictionary set to little
2021-08-25T20:53:36.533229-07:00
LGWR (PID:3802): STARTING ARCH PROCESSES
2021-08-25T20:53:36.544031-07:00
TT00 (PID:3901): Gap Manager starting
Starting background process ARC0
2021-08-25T20:53:36.556863-07:00
ARC0 started with pid=44, OS id=3904
2021-08-25T20:53:36.566983-07:00
LGWR (PID:3802): ARC0: Archival started
LGWR (PID:3802): STARTING ARCH PROCESSES COMPLETE
2021-08-25T20:53:36.567113-07:00
ARC0 (PID:3904): Becoming a 'no FAL' ARCH
ARC0 (PID:3904): Becoming the 'no SRL' ARCH
2021-08-25T20:53:36.570097-07:00
TMON (PID:3867): STARTING ARCH PROCESSES
Starting background process ARC1
2021-08-25T20:53:36.581339-07:00
ARC1 started with pid=46, OS id=3910
Starting background process ARC2
Starting background process ARC3
2021-08-25T20:53:36.592261-07:00
ARC2 started with pid=47, OS id=3913
2021-08-25T20:53:36.593678-07:00
Redo log for group 2, sequence 22 is not located on DAX storage
2021-08-25T20:53:36.605182-07:00
TMON (PID:3867): ARC1: Archival started
TMON (PID:3867): ARC2: Archival started
```

FIGURE 125. Database ora19c Alert Log

Summary

Deploying Oracle Workloads on on-premises and VMware Cloud on AWS is different than deploying a single-instance Oracle database on any physical architecture.

Deploying a production single-instance primary database on Site A and single-instance physical standby database on Site B is no different than deploying the same on any physical architecture.

Deploying a production single-instance primary database or single-instance physical standby database on VMware Cloud on AWS is no different than deploying the same on any physical architecture.

Migrating Oracle workloads to VMware Cloud on AWS can be achieved using Oracle native tools (e.g., Data Guard, GoldenGate) OR with VMware-native tools using VMware Cross vCenter vMotion technology.

Migrating Oracle workloads to VMware Cloud on AWS using VMware Hybrid Cloud Extension can be achieved using:

- VMware Hybrid Cloud Extension Bulk Migration
- VMware Hybrid Cloud Extension Cold Migration
- VMware Hybrid Cloud Extension vMotion
- VMware Hybrid Cloud Extension Replication Assisted vMotion
- VMware Hybrid Cloud Extension OS Assisted Migration

The migration of Oracle VMs using Hybrid Cloud Extension OS-assisted migration is outside the scope of this paper.

Best Practices

VMware Cloud on AWS is an on-demand service that enables customers to run applications across vSphere-based cloud environments with access to a broad range of AWS services. Powered by VMware Cloud Foundation, this service integrates vSphere, vSAN and NSX along with VMware vCenter management, and is optimized to run on dedicated, elastic, bare-metal AWS infrastructure. ESXi hosts in VMware Cloud on AWS reside in an AWS availability Zone (AZ) and are protected by vSphere HA.

All best practices for running Oracle workloads on a VMware SDDC also apply to Oracle workloads on VMware Cloud on AWS and Stretched Clusters for VMware Cloud on AWS and can be found *here*, along with the *vSphere Performance Best Practices Guide*, for specific version of vSphere. Additional best practices for running Oracle workloads on VMware Cloud on AWS can be found in *Optimize Virtual Machine Configurations in VMware Cloud on AWS for Enterprise Applications Workload*.

In addition to the above best practices, with vSAN as the underlying storage component for VMware Cloud on AWS, a well-designed HCI cluster powered by vSAN is key to a successful implementation of mission-critical Oracle databases.

VMware vSAN Design Guide provides a comprehensive set of guidelines for designing vSAN and most of these guidelines apply to VMware Cloud on AWS with some subtle nuances.

Refer to the key guidelines relevant to Oracle Database in section 5.1 vSAN All-Flash Configuration Guidelines in the *Oracle Database on VMware vSAN 6.7 guide*.

Conclusion

Customers have successfully run business-critical Oracle workloads with high performance demands on VMware vSphere for many years.

VMware Cloud on AWS is an on-demand service that enables customers to run applications across VMware vSphere cloud environments with access to a broad range of AWS services. Powered by VMware Cloud Foundation™, this service integrates vSphere, vSAN and VMware NSX along with VMware vCenter management, and is optimized to run on dedicated, elastic, bare-metal AWS infrastructure. ESXi hosts in VMware Cloud on AWS reside in an AWS availability zone and are protected by vSphere high availability.

Stretched Clusters for VMware Cloud on AWS is designed to protect against an AWS AZ failure. With Stretched Clusters for VMware Cloud on AWS, business-critical Oracle workloads with exceptionally high SLA, performance, and application availability requirements can take advantage of cloud deployment while simultaneously achieving high availability across multiple AZs.

This reference architecture outlines the deployment and migration strategies and use cases involved in movement of Oracle workloads to VMware Cloud on AWS.

- Deploying Oracle workloads on VMware Cloud on AWS
- Migrating Oracle workloads from VMware on-premises to VMware Cloud on AWS
- Deploying Oracle workloads on Stretched Clusters for VMware Cloud on AWS

Appendix A: On-Premises Oracle Configuration

Production Oracle Oracle19c12-OEL83 Initialization Parameters

*.audit_file_dest='/u01/admin/ORA19C/adump'
*.audit_trail='db'
*.audit_sys_operations=TRUE
*.compatible=12.1.0.0.0
*.control_files='+DATA_DG/control01.ctl','+DATA_DG/control02.ctl','+DATA_DG/control03.ctl'
*.db_block_size=8192
*.db_domain=''
*.db_name='ORA19C'
*.db_create_file_dest='+DATA_DG'
*.db_recovery_file_dest='+DATA_DG'
*.db_recovery_file_dest_size=10G
*.diagnostic_dest='/u01/admin/ORA19C'
*.enable_pluggable_database=true
*.instance_number=1
*.instance_name='ORA19C'
*.log_archive_format='%t_%s_%r.dbf'
*.open_cursors=1000
*.processes=2000
*.parallel_instance_group='ORA19C'
*.parallel_max_servers=100
*.pga_aggregate_target=256M
*.pga_aggregate_limit=6G
*.remote_login_passwordfile='exclusive'
*.resource_manager_plan=''
*.result_cache_max_size=4M
*.sec_case_sensitive_logon=FALSE
*.sga_max_size=16G
*.sga_target=16G
*.shared_pool_size=0
*.thread=1
*.undo_tablespace='UNDOTBS01'
*.USE_LARGE_PAGES=only

Production Oracle Oracle19c-OL8-Primary Initialization Parameters

*.audit_file_dest='/u01/admin/ORA19C/adump'
*.audit_sys_operations=TRUE
*.audit_trail='db'
*.compatible='12.1.0.0.0'
*.control_files='+DATA_DG/control01.ctl','+DATA_DG/control02.ctl','+DATA_DG/control03.ctl'
*.db_block_size=8192
*.db_create_file_dest='+DATA_DG'
*.db_domain=''
*.db_file_name_convert='+DATA_DG/ORA19CSB','+DATA_DG/ORA19C'
*.log_file_name_convert='+DATA_DG/ORA19CSB','+DATA_DG/ORA19C'
*.db_name='ORA19C'
*.db_unique_name='ora19c'
*.db_recovery_file_dest='+DATA_DG'
*.db_recovery_file_dest_size=10G
*.diagnostic_dest='/u01/admin/ORA19C'
*.enable_pluggable_database=true
*.fal_client='ORA19C'
*.fal_server='ORA19CSB'
*.instance_name='ora19c'
*.instance_number=1
*.log_archive_config='dg_config=(ora19c,ora19csb)'
*.log_archive_dest_1='location=use_db_recovery_file_dest valid_for=(all_logfiles,all_roles) db_unique_name=ora19c'
*.log_archive_dest_2='service=ora19csb async valid_for=(online_logfiles,primary_role) db_unique_name=ora19csb'
*.log_archive_dest_state_2='ENABLE'
*.log_archive_format='%t_%s_%r.dbf'
*.log_archive_max_processes=10
*.job_queue_processes=0
*.open_cursors=1000
*.parallel_instance_group='ORA19C'
*.parallel_max_servers=100
*.pga_aggregate_limit=6G
*.pga_aggregate_target=256M
*.processes=2000
*.remote_login_passwordfile='exclusive'
*.resource_manager_plan=''
*.result_cache_max_size=4M
*.sga_max_size=16G

*.sga_target=16G
*.standby_file_management='AUTO'
*.thread=1
*.undo_tablespace='UNDOTBS01'

Production Oracle **Oracle19c-OL8-Standby** Initialization Parameters

*.audit_file_dest='/u01/admin/ORA19CSB/adump'
*.audit_sys_operations=TRUE
*.audit_trail='db'
*.compatible='12.1.0.0.0'
*.control_files='+DATA_DG/stdby_control01.ctl','+DATA_DG/stdby_control02.ctl','+DATA_DG/stdby_control03.ctl'
*.db_block_size=8192
*.db_create_file_dest='+DATA_DG'
*.db_domain=''
*.db_file_name_convert='+DATA_DG/ORA19C','+DATA_DG/ORA19CSB'
*.log_file_name_convert='+DATA_DG/ORA19C','+DATA_DG/ORA19CSB'
*.db_name='ORA19C'
*.db_unique_name='ora19csb'
*.db_recovery_file_dest='+DATA_DG'
*.db_recovery_file_dest_size=10G
*.diagnostic_dest='/u01/admin/ORA19CSB'
*.enable_pluggable_database=true
*.fal_client='ORA19CSB'
*.fal_server='ORA19C'
*.instance_name='ora19csb'
*.instance_number=1
*.log_archive_config='dg_config=(ora19c,ora19csb)'
*.log_archive_dest_1='location=use_db_recovery_file_dest valid_for=(all_logfiles,all_roles) db_unique_name=ora19csb'
*.log_archive_dest_2='service=ora19c async valid_for=(online_logfiles,primary_role) db_unique_name=ora19c'
*.log_archive_dest_state_2='ENABLE'
*.log_archive_format='%t_%s_%r.dbf'
*.log_archive_max_processes=10
*.job_queue_processes=0
*.open_cursors=1000
*.parallel_instance_group='ORA19C'
*.parallel_max_servers=100

*.pga_aggregate_limit=6G
*.pga_aggregate_target=256M
*.processes=2000
*.remote_login_passwordfile='exclusive'
*.resource_manager_plan=''
*.result_cache_max_size=4M
*.sga_max_size=16G
*.sga_target=16G
*.standby_file_management='AUTO'
*.thread=1
*.undo_tablespace='UNDOTBS01'

Appendix B: VMware Cloud on AWS Oracle Configuration

Production Oracle Oracle19c12-OEL83-VMC Initialization Parameters

*.audit_file_dest='/u01/admin/ORA19C/adump'
*.audit_trail='db'
*.audit_sys_operations=TRUE
*.compatible=12.1.0.0.0
*.control_files='+DATA_DG/control01.ctl','+DATA_DG/control02.ctl','+DATA_DG/control03.ctl'
*.db_block_size=8192
*.db_domain=''
*.db_name='ORA19C'
*.db_create_file_dest='+DATA_DG'
*.db_recovery_file_dest='+DATA_DG'
*.db_recovery_file_dest_size=10G
*.diagnostic_dest='/u01/admin/ORA19C'
*.enable_pluggable_database=true
*.instance_number=1
*.instance_name='ORA19C'
*.log_archive_format='%t_%s_%r.dbf'
*.open_cursors=1000
*.processes=2000
*.parallel_instance_group='ORA19C'
*.parallel_max_servers=100
*.pga_aggregate_target=256M
*.pga_aggregate_limit=6G

*.remote_login_passwordfile='exclusive'
*.resource_manager_plan=''
*.result_cache_max_size=4M
*.sec_case_sensitive_logon=FALSE
*.sga_max_size=16G
*.sga_target=16G
*.shared_pool_size=0
*.thread=1
*.undo_tablespace='UNDOTBS01'
*.USE_LARGE_PAGES=only

Appendix C: SLOB Configuration

SLOB Configuration

SLOB 2.4.0 slob.conf

UPDATE_PCT=100
SCAN_PCT=0
RUN_TIME=1800
WORK_LOOP=0
SCALE=16G
SCAN_TABLE_SZ=1M
WORK_UNIT=64
REDO_STRESS=HEAVY
LOAD_PARALLEL_DEGREE=5

THREADS_PER_SCHEMA=1

DATABASE_STATISTICS_TYPE=awr # Permitted values: [statspack|awr]

Settings for SQL*Net connectivity:
Uncomment the following if needed:
ADMIN_SQLNET_SERVICE=ora19c-pdb1
SQLNET_SERVICE_BASE=ora19c-pdb1
#SQLNET_SERVICE_MAX="if needed, replace with a non-zero integer"
#
Note: Admin connections to the instance are, by default, made as SYSTEM

```
# with the default password of “manager”. If you wish to use another
# privileged account (as would be the cause with most DBaaS), then
# change DBA_PRIV_USER and SYSDBA_PASSWD accordingly.
#### Uncomment the following if needed:
DBA_PRIV_USER=sys
SYSDBA_PASSWD=vmware123

#### The EXTERNAL_SCRIPT parameter is used by the external script calling feature of runit.sh.
#### Please see SLOB Documentation at https://kevinclosson.net/slob for more information

EXTERNAL_SCRIPT=''

##########################
#### Advanced settings:
#### The following are Hot Spot related parameters.
#### By default Hot Spot functionality is disabled (DO_HOTSPOT=FALSE).

DO_HOTSPOT=FALSE
HOTSPOT_MB=8
HOTSPOT_OFFSET_MB=16
HOTSPOT_FREQUENCY=3

#### The following controls operations on Hot Schema
#### Default Value: 0. Default setting disables Hot Schema

HOT_SCHEMA_FREQUENCY=0

#### The following parameters control think time between SLOB
#### operations (SQL Executions).
#### Setting the frequency to 0 disables think time.

THINK_TM_FREQUENCY=0
THINK_TM_MIN=.1
THINK_TM_MAX=.5
```

Reference

White Papers

For additional information, see the following white papers:

- *Oracle Databases on VMware Best Practices Guide*
- *Optimize Virtual Machine Configurations in VMware Cloud on AWS for Enterprise Applications Workload*
- *Oracle Database 12c on VMware vSAN 6.7 All-Flash*
- *Oracle Database 12c on VMware vSAN – Day 2 Operations and Management*

Product Documentation

For additional information, see the following product documentation:

- *Oracle Database Documentation*
- *VMware Cloud on AWS*

Other Documentation

For additional information, see the following document:

- *SLOB Resources*

Author Info and Acknowledgements

Author: Sudhir Balasubramanian, Senior Staff Solution Architect, works in the Cloud Business Unit (CSBU). Sudhir specializes in the virtualization of Oracle business-critical applications. Sudhir has more than 26 years' experience in IT infrastructure and database, working as the Principal Oracle DBA and Architect for large enterprises focusing on Oracle, EMC storage, and Unix/Linux technologies. Sudhir holds a Master's degree in Computer Science from San Diego State University. Sudhir is the Lead Author of the *Virtualize Oracle Business Critical Databases* book, which is a comprehensive authority for Oracle DBAs on the subject of Oracle and Linux on vSphere. Sudhir is a VMware vExpert, Alumni Member of the VMware CTO Ambassador Program and an Oracle ACE.

Acknowledgments

Thanks to the following for their reviews and input:

- **Oleg Ulyanov** – Senior Solution Architect

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