TECHNICAL WHITE PAPER – SEPTEMBER 2021

Oracle Business Continuity and Disaster Recovery on VMware Hybrid Multi-Clouds

REFERENCE ARCHITECTURE

vmware®

Table of contents

Executive Summary

Business Case

Customers have successfully run their business-critical Oracle workloads with high-performance demands on VMware vSphere® for many years. Virtualization of mission-critical databases adds layers of complexity to the infrastructure, however, making common operations like backup and recovery, cloning, disaster recovery and other day-to-day activities difficult. The most efficient storage operations for mission-critical databases are offloaded to the storage array.

Concerns that often delay virtualization of business-critical database workloads include:

- Rapid database growth and the need to reduce backup windows to meet performance and business SLAs
- The size of modern databases makes it harder to regularly clone and refresh data from production to QA and other environments
- Correct choice of business continuity plan to ensure rapid recovery from significant disruption to the operations
- Correct choice of disaster recovery technology to ensure business needs of RTO and RPO are met

A business continuity plan is a detailed strategy and set of systems for ensuring an organization's ability to prevent or rapidly recover from a significant disruption to its operations. The plan is essentially a playbook for how any type of organization will continue its day-to-day business during a disaster scenario or otherwise abnormal conditions.

Disaster recovery (DR) is an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or even business disruptions related to the COVID-19 pandemic. DR is one aspect of business continuity. Disaster recovery relies upon the replication of data and computer processing in an off-premises location not affected by the disaster.

On-Premises with VMware vSphere

VMware vSphere provides many tools for customers to successfully ensure business continuity and disaster recovery for their business-critical databases.

VMware snapshots preserve the state and data of a VM at the time the snapshot is taken. When a VM snapshot is captured, an image of the VM in a given state is copied and stored.

VMware Clone creates a VM that is a copy of the original VM. The new VM is configured with the same virtual hardware, installed software, and other properties that were configured for the original VM.

VMware Site Recovery Manager™ is a business continuity and disaster recovery solution that helps you plan, test, and run the recovery of virtual machines between a protected VMware vCenter Server® site and a recovery vCenter Server site. One can use Site Recovery Manager to implement different types of recovery from the protected site to the recovery site.

VMware vSphere® Replication™ is an extension to VMware vCenter Server that provides hypervisor-based virtual machine replication and recovery. vSphere Replication is an alternative to storage-based replication. It protects virtual machines from partial or complete site failures by replicating the virtual machines between sites.

Site Recovery Manager can also protect VMs in a datastore by using third-party disk replication mechanisms to configure array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads.

Migrating to VMware Cloud

Enterprise IT infrastructure and operations organizations are looking for ways to provide business continuity and disaster recovery for on-premises vSphere-based workloads to the public cloud, consolidate and extend data center capacities, and optimize, simplify and modernize their disaster recovery solutions.

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.

VMware Site Recovery brings VMware enterprise-class SDDC disaster recovery-as-a-service to the AWS Cloud. VMware Site Recovery works in conjunction with VMware Site Recovery Manager 8.0 and VMware vSphere Replication 8.0 to automate the process of recovering, testing, re-protecting, and failing-back virtual machine workloads.

VMware Cloud Disaster Recovery is an on-demand disaster recovery service that provides an easy-to-use software-as-a-service (SaaS) solution and offers cloud economics to keep your disaster recovery costs under control. You can use VMware Cloud Disaster Recovery to protect your vSphere virtual machines by replicating them to the cloud and recovering them as needed to a target VMware Cloud SDDC. You can create the target SDDC immediately prior to performing a recovery, and it does not need to be provisioned to support replications in the steady state.

Solution Overview

This paper describes the configuration and implementation of various business continuity and disaster recovery options across the application, VMware platform, and storage levels of Oracle single instance and Real Application Cluster (RAC) workloads on the VMware vSphere hybrid multi-cloud platform. This includes on-premises and VMware clouds, with an emphasis on VMware Cloud™ on AWS.

Key Results

The following highlights validate the capability of the VMware vSphere hybrid multi-cloud platform, including on-premises and VMware clouds with a special emphasis on VMware Cloud on AWS, to provide business continuity and disaster recovery to business-critical Oracle single-instance and RAC workloads across application, VMware platform, and storage levels using native Oracle tools and VMware vSphere products.

Introduction

Purpose

The following highlights validate the capability of the VMware vSphere hybrid multi-cloud platform, including on-premises and VMware clouds with a special emphasis on VMware Cloud on AWS, to provide business continuity and disaster recovery to business-critical Oracle single instance and RAC workloads across application, VMware platform, and storage levels using native Oracle tools and VMware vSphere products.

Audience

This reference architecture is intended for Oracle database administrators (DBAs) as well as virtualization and storage architects involved in planning, architecting, and administering business continuity and disaster recovery processes for business-critical Oracle environments on the VMware SDDC platform.

Terminology

The following terms are used throughout this paper:

TERM	DEFINITION
Oracle Single Instance	An Oracle single-instance database consists of a set of memory structures, background processes, and physical database files, which serves the database users.
Oracle Clusterware	Oracle Clusterware is a portable cluster software that allows clustering of independent servers so that they cooperate as a single system.
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 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

Overview

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

- VMware vSphere®
- VMware Datastores
- VMware vSAN™
- VMware vSphere® Virtual Volumes™
- VMware Virtual Disks
- VMware Virtual Machine Snapshots
- VMware Virtual Machine Clones
- VMware Multi-Writer Attribute for Shared VMDKs
- VMware Site Recovery Manager™
- VMware vSphere® Replication™
- Hybrid and Multi-Cloud as the VMware Cloud
- VMware Cloud™ on AWS
- VMware Cloud on Dell EMC
- Google Cloud VMware Engine
- Azure VMware Solution
- Oracle Cloud VMware Solution
- VMware Site Recovery
- VMware Cloud Disaster Recovery
- VMware Site Recovery Manager and vSphere Replication for other VMware Multi-Clouds
- Oracle Database Architecture
- Oracle ASM, ASMLIB and ASMFD
- Oracle Backup and Recovery
- Oracle User Managed Database Backup
- Oracle Crash-Consistent Backup
- Oracle RMAN
- Oracle Database Cloning
- Oracle Real Application Clusters on VMware vSphere
- Oracle Data Guard

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 Datastores

VMware datastores are logical containers, analogous to file systems, that hide specifics of physical storage and provide a uniform model for storing virtual machine files. Datastores can also be used for storing ISO images, virtual machine templates, and floppy images.

To store virtual disks, VMware ESXi™ uses datastores. The datastores are logical containers that hide specifics of physical storage from virtual machines (VM) and provide a uniform model for storing the VM files. The datastores that you deploy on block storage devices use the native vSphere virtual machine file system (VMFS) format. It is a special high-performance file system format that is optimized for storing VMs.

Depending on the storage you use, datastores can be of different types. VMware vCenter Server® and ESXi support the following types of datastores:

- VMFS (version 5 and 6)
- NFS (version 3 and 4.1)
- vSAN
- vVols

Learn more about *VMware Datastores*.

VMware vSAN

VMware vSAN™ is VMware's software-defined storage solution, built from the ground up for vSphere virtual machines.

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.

VMware vSAN-backed hyperconverged infrastructure (HCI) provides a wide array of deployment options, ranging from a two-node setup to a standard cluster with up to 64 hosts in a cluster. Also, vSAN accommodates a stretched cluster topology to serve as an active-active disaster recovery solution. vSAN incorporates HCI mesh, allowing 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 vSphere Virtual Volumes

Historically, vSphere storage management used a datastore-centric approach. The datastore then is the lowest granularity level at which data management occurs from a storage perspective. However, a single datastore contains multiple virtual machines, all of which may have differing requirements. Using a traditional approach, it is difficult to meet the storage requirements of an individual VM.

With VMware vSphere® Virtual Volumes™ (vVols), an individual VM, not the datastore, becomes a unit of storage management, while storage hardware gains complete control over virtual disk content, layout, and management.

vVols functionality helps to improve granularity. It helps to differentiate VM services on a per-application level by offering a new approach to storage management. Rather than arranging storage around features of a storage system, vVols arranges storage around the needs of individual virtual machines, making storage VM-centric.

More information on vVols datastores can be found on *VMware Docs* and *Core.vmware.com/vVols*.

VMware Virtual Disks

It's possible to add large-capacity virtual disks to virtual machines and add more space to existing disks, even when the VM is running. Most virtual disk parameters can be set during VM creation or after the guest operating system is installed.

VM data can be stored in a new virtual disk, an existing virtual disk, or a mapped SAN LUN. A virtual disk appears as a single hard disk to the guest operating system. The virtual disk is composed of one or more files on the host file system. You can copy or move virtual disks on the same hosts or between hosts.

Virtual disks (VMDKs) can be provisioned on the above VMware datastores types. The concept of VMDK remains the same regardless of the underlying datastore types, the difference being in the way the underlying storage for the datastore is provisioned.

Learn more about *VMware virtual disks*.

VMware Virtual Machine Snapshots

Snapshots preserve the state and data of a VM at the time the snapshot is taken. When a VM snapshot is captured, an image of the VM in a given state is copied and stored. Snapshots are useful when frequently reverting to a particular VM state and creating multiple VMs is undesirable.

VMware snapshots are point-in-time (PIT) snapshots and therefore write-order fidelity is guaranteed for all VMDKs of the VM.

Snapshots for Oracle databases on VMware vSphere can be performed in three ways:

- **Database** – using Oracle ACFS snapshots, for example, which is an online, read-only or read-write point-in-time copy of an Oracle ACFS file system. See *About Oracle ACFS Snapshots* for detailed information.
- **vSphere VM** – using VMware snapshots.
- **Storage** – using LUN-based snapshots available in a traditional storage array.

VMware vSphere, using VM snapshots, enables users to capture point-in-time state and data of a VM. This includes the VM's storage, memory, and other devices, such as virtual NICs.

Snapshots are useful for creating point-in-time state and data of a VM for backup or archival purposes and for creating test and rollback environments for applications.

For further information about using VM snapshots in a vSphere environment, see *Using Snapshots To Manage Virtual Machines*.

A VM snapshot can be taken through:

- Web Client GUI – see *Taking a Snapshot* for detailed information.
- PowerCLI commands – see *PowerCLI Reference: New Snapshot* for detailed information.

VMware Virtual Machine Clones

Cloning a VM creates a VM that is a copy of the original. The new VM is configured with the same virtual hardware, installed software, and other properties that were configured for the original VM.

Clones for Oracle databases on VMware vSphere can be performed in three ways:

- **Database** – using Oracle Enterprise Manager Cloud Control, for example, or classic cloning using RMAN backups. See *Cloning Oracle Databases and Pluggable Databases* for more information.
- **vSphere** – using VMware cloning technology.
- **Storage** – using traditional storage-array-based cloning.

There are two types of cloning operations performed in this guide:

- Cloning of an entire VM containing all VMDKs, including the operating system, Oracle binaries, and Oracle data VMDKs.
- Cloning the database VMDKs of a VM alone.

For further information about VM cloning in a vSphere environment, see *Clone a Virtual Machine*.

VMware Multi-Writer Attribute for Shared VMDKs

VMFS is a clustered file system that disables (by default) multiple VMs from opening and writing to the same virtual disk (.vmdk file). This prevents more than one VM from inadvertently accessing the same .vmdk file. The multi-writer option allows VMFS-backed disks to be shared by multiple VMs. An Oracle RAC cluster using shared storage is a common use case.

VMware vSphere on VMFS, VVols (beginning with ESXi 6.5), network files system (NFS) datastores and VMware vSAN prevents multiple VMs from opening the same virtual disk (VMDK) in read-write mode.

Current restrictions of the multi-writer attribute documented in *KB 1034165* include:

- VMware vSphere® Storage vMotion® is disallowed.
- Snapshots are not supported (snapshots of VMs with independent-persistent disks are supported, however).
- Changed-block tracking (CBT) is not supported.
- Cloning, hot-extend virtual disk are not supported.

Independent-persistent mode is **NOT** required for enabling multi-writer attribute.

For further information about multi-writer attribute for shared VMDKs, see *KB 1034165*.

VMware Site Recovery Manager

VMware Site Recovery Manager™ is a business continuity and disaster recovery solution that helps you plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.

You can use Site Recovery Manager to implement different types of recovery from the protected site to the recovery site.

Planned migration is the orderly migration of VMs from the protected site to the recovery site. Planned migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functional.

Disaster recovery does not require that both sites be up and running, and it can be initiated in the event of the protected site going offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site is reported, but otherwise ignored.

Site Recovery Manager orchestrates the recovery process with the replication mechanisms, to minimize data loss and system downtime.

See *VMware Site Recovery Manager* for more further details.

VMware vSphere Replication

VMware vSphere® Replication™ is an extension to VMware vCenter Server that provides a hypervisor-based virtual machine replication and recovery.

vSphere Replication is an alternative to storage-based replication. It protects virtual machines from partial or complete site failures by replicating the VMs between the following sites:

- From a source site to a target site
- Within a single site from one cluster to another
- From multiple source sites to a shared remote target site

vSphere Replication provides several benefits as compared to storage-based replication:

- Data protection at a lower cost per VM.
- A replication solution that allows flexibility in the storage vendor selection at the source and target sites.
- Lower overall cost per replication.

With vSphere Replication, you can configure the replication of a virtual machine from a source site to a target site, monitor and manage the status of the replication, and recover the VM at the target site.

When you configure a VM for replication, the vSphere Replication agent sends changed blocks in the VM disks from the source site to the target site. The changed blocks are applied to the copy of the VM. This process occurs independently of the storage layer. vSphere Replication performs an initial full synchronization of the source VM and its replica copy. You can use replication seeds to reduce the network traffic that data transfer generates during the initial full synchronization.

During replication configuration, you can set a recovery point objective (RPO) and enable retention of instances from multiple points-in-time (MPIT).

Write-order fidelity is guaranteed with vSphere Replication on the disks or VMDKs that comprise a VM. However, consistency cannot be guaranteed across multiple VMs.

vSphere Replication supports replicating VMs on local, attached, vSAN, FC, iSCSI, or NFS storage. vSphere Replication cannot replicate VMs that are part of an MSCS cluster. vSphere Replication cannot replicate disks in multi-writer mode.

Learn more about *Best Practices for Using and Configuring vSphere Replication*.

For further information about VMware vSphere Replication, see *VMware vSphere Replication and Array-Based Replication Versus vSphere Replication*.

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 off-site 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.

The VMware *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) include 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 DellEMC – 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.

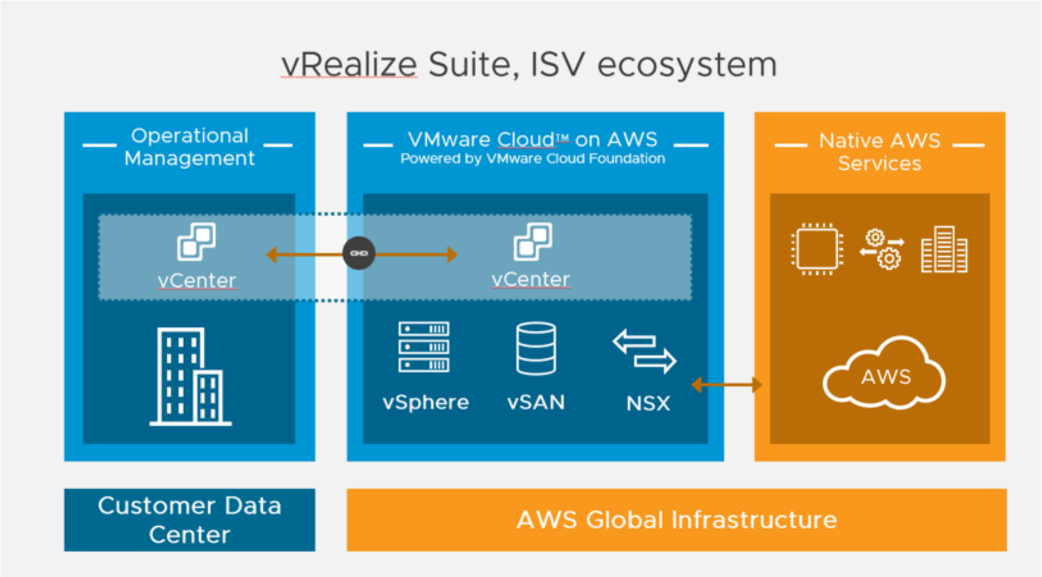


FIGURE 1. VMware Cloud on AWS

Learn more about *VMware Cloud on AWS*.

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. Industry-leading compute, storage, and networking software from VMware 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 hyperconverged 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 service-level agreement (SLA).

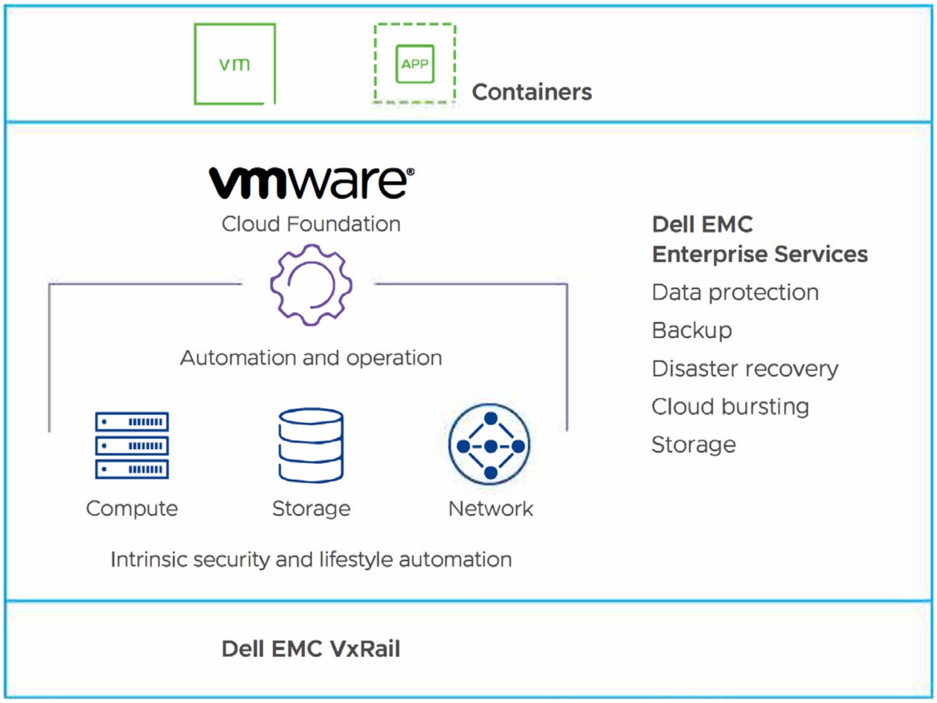


FIGURE 2. VMware Cloud on Dell EMC

Learn more about *VMware Cloud on Dell EMC*.

Google Cloud VMware Engine

Google Cloud VMware Engine (GCVE) allows organizations to seamlessly migrate and run 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 flagship compute, storage, network virtualization, and management technologies with dedicated, elastic, bare-metal infrastructure, Google Cloud VMware Engine allows customers to access the agility, scale, and innovative services of the cloud while maintaining operational consistency and leveraging existing tools and investments.

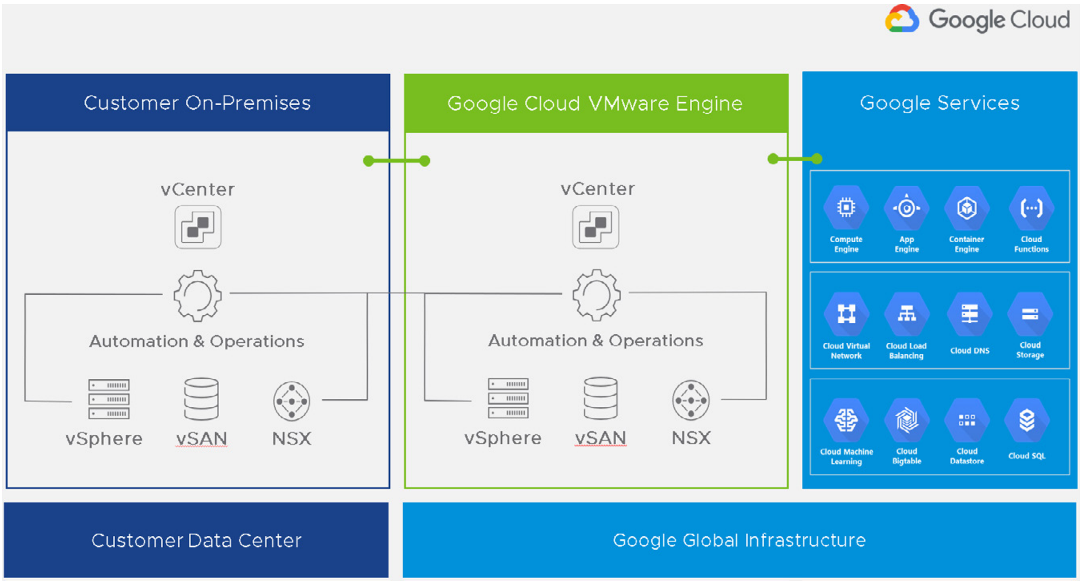


FIGURE 3. Google Cloud VMware Engine

Learn more about *Google Cloud VMware Engine*.

Azure VMware Solution

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.

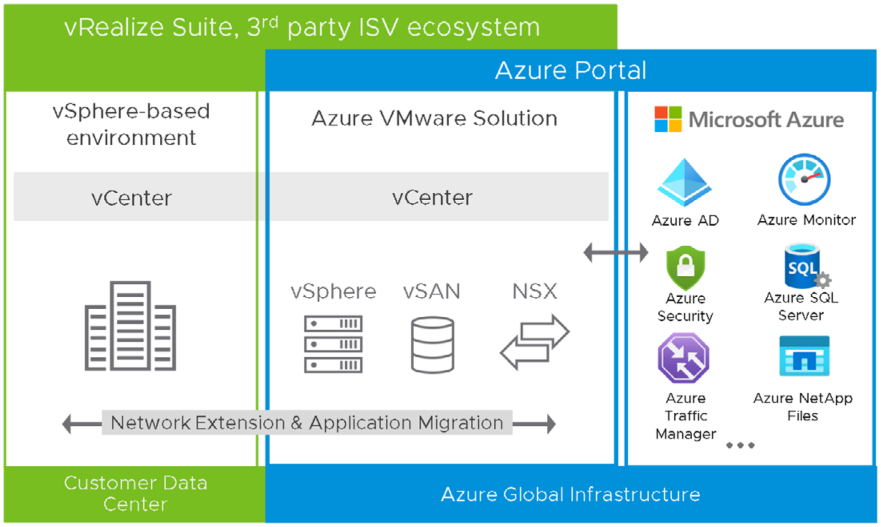


FIGURE 4. Azure VMware Solution

Learn more about *Azure VMware Solution*.

Oracle Cloud VMware Solution

Oracle Cloud VMware Solution (OCVS) 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.

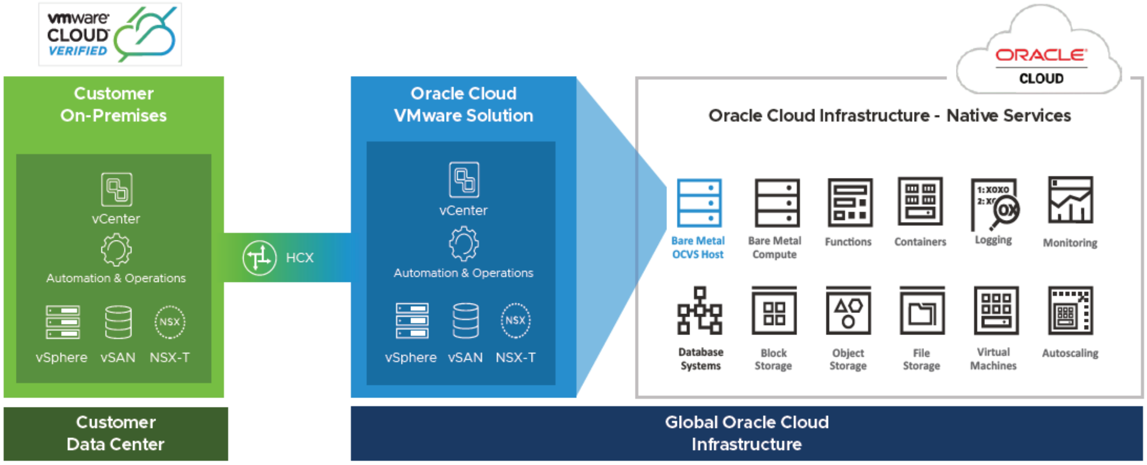


FIGURE 5. Oracle Cloud VMware Solution

Learn more about *Oracle Cloud VMware Solution*.

VMware Site Recovery

VMware Site Recovery brings VMware enterprise-class SDDC disaster recovery-as-a-service to the AWS Cloud. It enables customers to protect and recover applications without the requirement for a dedicated secondary site. It is delivered, sold, supported, maintained and managed by VMware as an on-demand service. IT teams manage their cloud-based resources with familiar VMware tools—without the difficulties of learning new abilities or utilizing new tools.

VMware Site Recovery is an add-on feature to VMware Cloud on AWS, powered by VMware Cloud Foundation. VMware Cloud on AWS integrates VMware flagship compute, storage, and network virtualization products—VMware vSphere, VMware vSAN, and VMware NSX—along with VMware vCenter Server management. It optimizes them to run on elastic, bare-metal AWS infrastructure. With the same architecture and operational experience on-premises and in the cloud, IT teams can now get instant business value via the AWS and VMware hybrid cloud experience.

VMware Site Recovery works in conjunction with VMware Site Recovery Manager and VMware vSphere Replication to automate the process of recovering, testing, re-protecting, and failing-back virtual machine workloads.

VMware Site Recovery utilizes VMware Site Recovery Manager servers to coordinate the operations of the VMware SDDC. This is so that as VMs at the protected site are shut down, copies of these VMs at the recovery site start up. By using the data replicated from the protected site, these VMs assume responsibility for providing the same services.

VMware Site Recovery can be used between a customer's datacenter and an SDDC deployed on VMware Cloud on AWS, or it can be used between two SDDCs deployed to different AWS availability zones or regions. The second option allows VMware Site Recovery to provide a fully VMware managed and maintained disaster recovery solution.

For further information about VMware Site Recovery, see *VMware Site Recovery Technical Overview*.

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery is an on-demand disaster recovery service that provides an easy-to-use software-as-a-service (SaaS) solution and offers cloud economics to keep your disaster recovery costs under control.

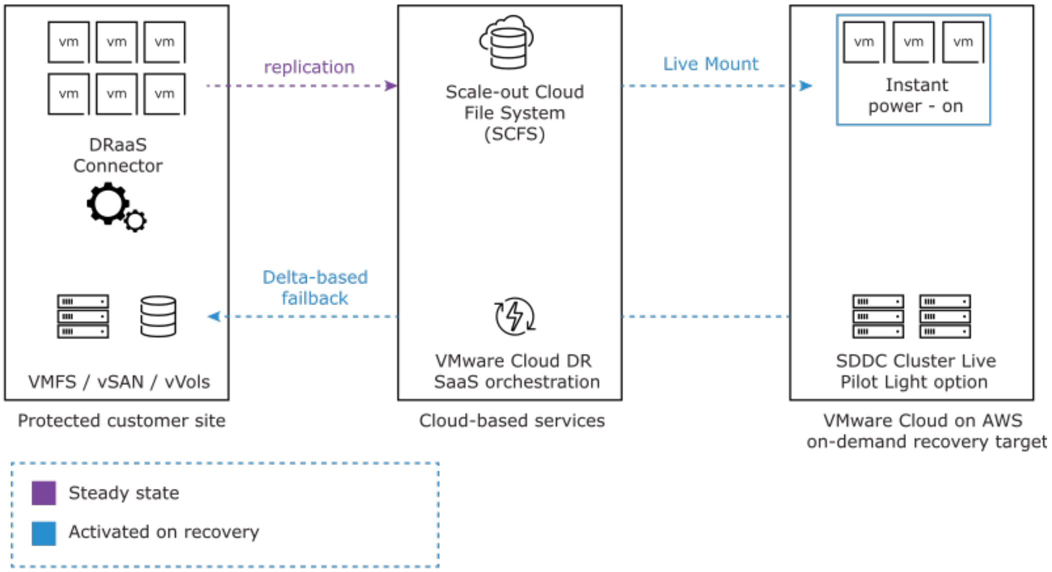


FIGURE 6. VMware Cloud Disaster Recovery

You can use VMware Cloud Disaster Recovery to protect your vSphere VMs by replicating them to the cloud and recovering them as needed to a target VMware Cloud SDDC. You can create the target SDDC immediately prior to performing a recovery, and it does not need to be provisioned to support replications in the steady state.

You can protect VMs in vSphere environments running on any storage with the *DRaaS Connector*. With the DRaaS Connector in a vSphere environment (on-premises or cloud), you can back up VMs using *protection groups* which are replicated to the scale-out cloud file System (SCFS) using regularly scheduled snapshots. You can define which snapshots to use if there is a disaster or planned recovery using *DR plans*. VMs captured in snapshots are then restarted on the recovery SDDC in VMware Cloud on AWS.

VMware Cloud Disaster Recovery lets you *deploy a recovery SDDC* in VMware Cloud on AWS to use for recovery and testing of your DR plans. You can add hosts, new networks, request public IP addresses, configure NAT rules, and also delete the recovery SDDC. In the event of a disaster or planned recovery operation, you can recover VMs from your protected site to your recovery SDDC.

VMware Cloud Disaster Recovery uses regularly scheduled snapshots to replicate to the SCFS. VMware snapshots are point-in-time (PIT) snapshots and are therefore crash-consistent.

VMware snapshots are not compatible with disks in multi-writer mode and VMware Cloud Disaster Recovery cannot replicate disks in multi-writer mode. Learn more about *VMware Cloud DR and shared disks*.

Both VMware Cloud Disaster Recovery and VMware Site Recovery are DRaaS solutions that can be used to protect mission-critical applications. Refer to VMware documentation for the RPO and RTO values for DRaaS solutions.

Learn more about *VMware Cloud DR Backup Considerations*. For further information about VMware Cloud Disaster Recovery, see VMware Cloud Disaster Recovery Documentation.

VMware Site Recovery Manager and vSphere Replication for other VMware Multi-Clouds

VMware Site Recovery Manager, along with VMware vSphere Replication, can be used to provide disaster recovery services from on-premises VMware environments to other VMware multi-clouds including VMware Cloud on Dell EMC, Google Cloud VMware Engine, Azure VMware Solutions, or Oracle Cloud VMware Solution.

Information on Site Recovery Manager and vSphere Replication for VMware Cloud on Dell EMC is the same as on-premises VMware environments.

Further information about Site Recovery Manager and vSphere Replication for Google Cloud VMware Engine (GCVE) can be found at *Configuring disaster recovery using VMware SRM*.

Further information about Site Recovery Manager and VMware vSphere Replication for Azure VMware Solution can be found at *Set up Private Cloud as a disaster recovery target with VMware Site Recovery Manager*.

Further information about Site Recovery Manager and vSphere Replication for Oracle Cloud VMware Solution can be found at Implement the VMware Site Recovery Manager.

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 for 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 Oracle RAC, 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 Oracle Database and Oracle RAC configurations.

Oracle ASM is Oracle's recommended storage-management solution that can be used for both Oracle RAC and single-instance Oracle databases and provides 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*.

Oracle Backup and Recovery

The purpose of backup and recovery is to protect the database against data loss and reconstruct the database after data loss. Oracle provides different options for database backup and recovery.

Oracle Recovery Manager (RMAN) is the most popular and preferred backup solution for Oracle Database.

Common Oracle backup and recovery options include:

- User-managed database backup (hot and cold backup)
- Crash-consistent backup using storage-based snapshots
- Oracle RMAN
- Oracle Data Pump export/import

Learn more about *Oracle Backup and Recovery Solutions*.

Oracle User Managed Database Backup

The user-managed backup and recovery mechanism includes performing backup and recovery with a mixture of host operating system commands and SQL*Plus recovery commands. This strategy does not depend on using Oracle RMAN.

A database-consistent backup is a whole database backup that can be opened with the RESETLOGS option without performing media recovery. It's not necessary to apply redo to this backup to make it consistent. Unless the redo generated is applied after the consistent backup is created, however, all transactions since the time of the consistent backup will be lost.

All datafiles in a consistent backup must:

- Have the same checkpoint system change number (SCN) in their headers, unless they are datafiles in tablespaces that are read-only or offline normal (in which case they will have a clean SCN that is earlier than the checkpoint SCN).
- Contain no changes past the checkpoint SCN (i.e., are not fuzzy).
- Match the data file checkpoint information stored in the control file.

See *Oracle Backup and Recovery User Guide* for more information.

Consistent backups can only be taken after a clean shutdown has been completed or by turning on hot backup mode of the database. This is the most trusted backup by DBAs but is also complex, as the admin will need to run scripts to put the database in hot-backup mode, take a snapshot, and then take the database out of the hot-backup mode.

Oracle data pump backups are *logical* database backups in that they extract logical definitions and data from the database to a file.

With a cold backup, it's possible to make a consistent whole database backup of all files in a database after the database is shut down with the **NORMAL**, **IMMEDIATE**, or **TRANSACTIONAL** options.

See *Making User-Managed Backups of the Whole Database* for more information.

With a hot backup, this would require:

- Putting the tablespace or database (depending on whether it is a tablespace level or database level backup) in a **BEGIN** backup mode by the **ALTER TABLESPACE/DATABASE BEGIN BACKUP** command.
- Taking an operating system-level backup of the tablespace or database data files.
- Taking the tablespace or database out of the backup mode with the **ALTER TABLESPACE/ DATABASE END BACKUP** command.

There is overhead involved in transitioning a database in and out of backup mode:

- Additional redo data is logged.
- Complete database checkpoint is required.
- More operational steps and complexity during the backup operation

Oracle Crash-Consistent Backup

A crash-consistent backup is the backup of a point-in-time image of an Oracle database that is equivalent to a database crash induced by a power outage, other failures, or a shutdown abort.

When the database is started up, instance recovery (i.e., the process of applying records in the online redo log to data files to reconstruct changes) is performed automatically to bring the database to a consistent state.

This is one of the most common backup methods used for storage-based backups and is fully supported by Oracle as long as the following conditions are met.

As noted in *Supported Backup, Restore and Recovery Operations using Third Party Snapshot Technologies* (Oracle Doc ID 604683.1), third-party vendor snapshots must conform to the following requirements:

- Integrated with Oracle's recommended restore and recovery operations above
- Database crash-consistent at the point of the snapshot
- Write-ordering is preserved for each file within a snapshot

See *Making Backups with Third-Party Snapshot Technologies* for more information.

Oracle RMAN

Oracle RMAN is an Oracle Database client that performs backup and recovery tasks on databases and automates administration of backup strategies. It greatly simplifies backing up, restoring, and recovering database files.

The RMAN environment consists of the utilities and databases that play a role in backing up data. Minimally, the environment for RMAN must include the following components:

- **A target database** – An Oracle database to which RMAN is connected with the **TARGET** keyword. A target database is a database on which RMAN is performing backup and recovery operations. RMAN always maintains metadata about its operations on a database in the control file of the database. The RMAN metadata is known as the RMAN repository.
- **The RMAN client** – An Oracle database executable that interprets commands, directs server sessions to execute those commands, and records its activity in the target database control file. The RMAN executable is automatically installed with the database and is typically located in the same directory as the other database executables.

Advantages of Oracle RMAN-based backups include:

- Only used space in the database is backed up
- RMAN does not put tablespaces in backup mode, saving on redo-generation overhead. RMAN will re-read database blocks until it gets a consistent image of it.

Learn more about *Oracle RMAN*.

Oracle Database Cloning

Cloning of an Oracle database is the process of making an exact copy of another database for various reasons. The cloned database is both fully functional and separate in its own right.

Use cases for cloning include making copies of the production database to use it:

- As a development database for developing new applications or adding new features to existing applications.
- As a QA database for testing existing software for bugs or testing new software features or versions.
- As a test database for backup and recovery scenarios.
- To provision a copy of a database for different business units.
- To test database patching, upgrade, and migration strategies.
- To benchmark for performance.

After cloning, the DBA may choose to mask sensitive data in the cloned database before releasing it for general consumption.

For example, a production database for a credit card company will have real customer data that cannot be revealed for security purposes, so Oracle data-masking is used to mask customer names and social security number.

Examples of database cloning include using Oracle Enterprise Manager Cloud Control or classic cloning using RMAN backups. See *Cloning Oracle Databases and Pluggable Databases* for more information.

The database cloning process may also occasionally include making copies of Oracle database home directories, along with a copy of the Oracle database, for those instances when testing database patching, upgrade, or migration strategies is needed.

Oracle Real Application Clusters on VMware vSphere

Oracle Clusterware is portable cluster software that provides comprehensive multi-tiered high availability and resource management for consolidated environments. It supports clustering of independent servers so that they cooperate as a single system.

Oracle Clusterware is the integrated foundation for Oracle Real Application Clusters (Oracle RAC), and the high-availability and resource management framework for all applications on any major platform.

Learn more about *Oracle Clusterware 19c*.

There are two key requirements for Oracle RAC:

- Shared storage
- Multicast Layer 2 networking

These requirements are fully addressed when running Oracle RAC on VMware vSphere, as both shared storage and Layer 2 networking are natively supported by vSphere.

vSphere high availability (HA) clusters enable a collection of ESXi hosts to work together so that, as a group, they provide higher levels of infrastructure-level availability for VMs than each ESXi host can provide individually.

vSphere HA provides high availability for VMs by pooling the VMs and the hosts they reside on into a cluster. Hosts in the cluster are monitored and, in the event of a failure, the VMs on a failed host are restarted on alternate hosts.

When creating a vSphere HA cluster, a single host is automatically elected as the master host. The master host communicates with vCenter Server and monitors the state of all protected VMs and of the slave hosts.

Learn more about *VMware vSphere HA*.

Oracle RAC and VMware HA solutions are completely complementary to each other. Running Oracle RAC on a VMware platform provides the application-level HA enabled by Oracle RAC, in addition to the infrastructure-level HA enabled by VMware vSphere.

Learn more about *Oracle RAC on VMware vSphere*.

Oracle Data Guard

Oracle Data Guard provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases to enable production Oracle databases to survive disasters and data corruptions. Oracle Data Guard maintains these standby databases as copies of the production database.

Then, if the production database becomes unavailable because of a planned or an unplanned outage, Oracle Data Guard can switch any standby database to the production role, minimizing the downtime associated with the outage. Oracle Data Guard can be used with traditional backup, restoration, and cluster techniques to provide a high level of data protection and data availability.

Learn more about *Oracle Data Guard*.

Solution Configuration

This section introduces the resources and configurations for the solution, including:

- Architecture diagram
- Hardware resources
- Software resources
- Network configuration
- Storage configuration
- Pure Storage Plugin for VMware vSphere client
- VM and Oracle configuration
- VMware Site Recovery Manager with vSphere Replication
- VMware Site Recovery Manager with Array-Based Replication (LUN level and vVOL Level)
- VMware Site Recovery
- VMware Cloud Disaster Recovery

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)
- VMware Cloud on AWS

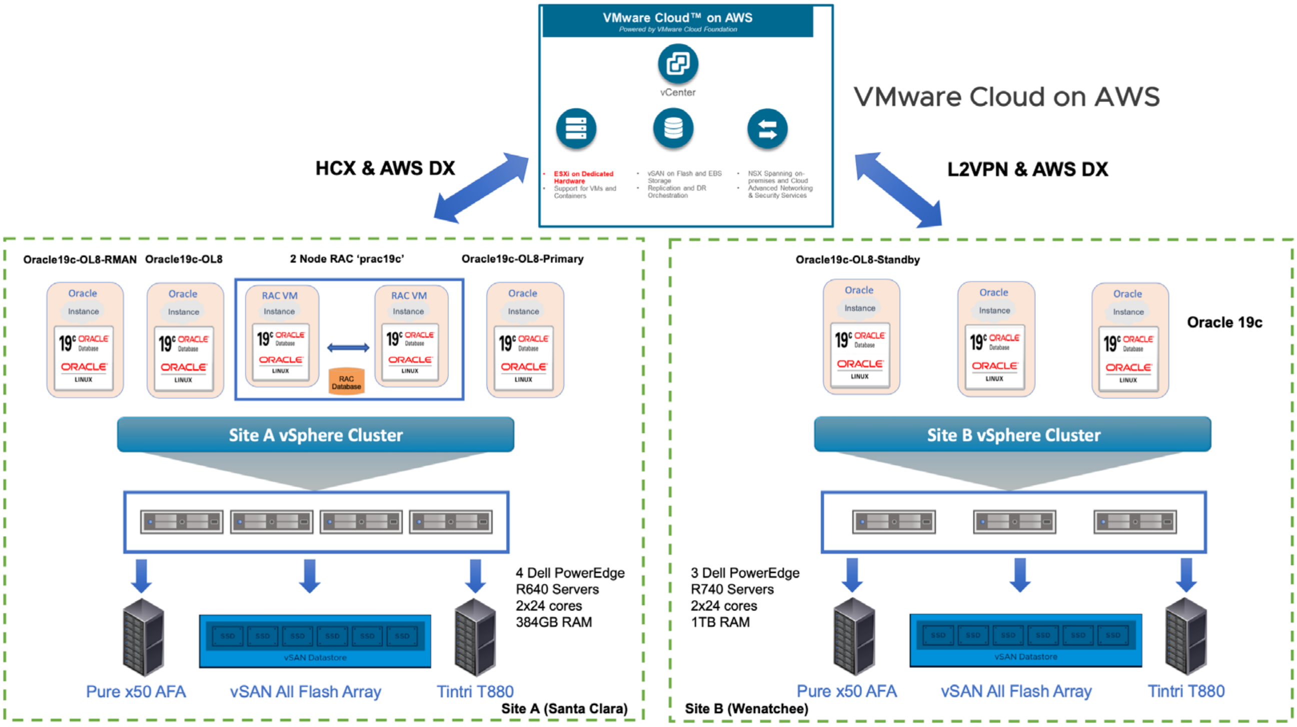


FIGURE 7. Site Architecture Diagram

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

- Site A is hosting production RAC and single-instance workloads.
- Site B is hosting non-production RAC and non-RAC workloads, including disaster recovery (DR).
- Both sites are connected to VMware Cloud on AWS.

Site A infrastructure details are as follows:

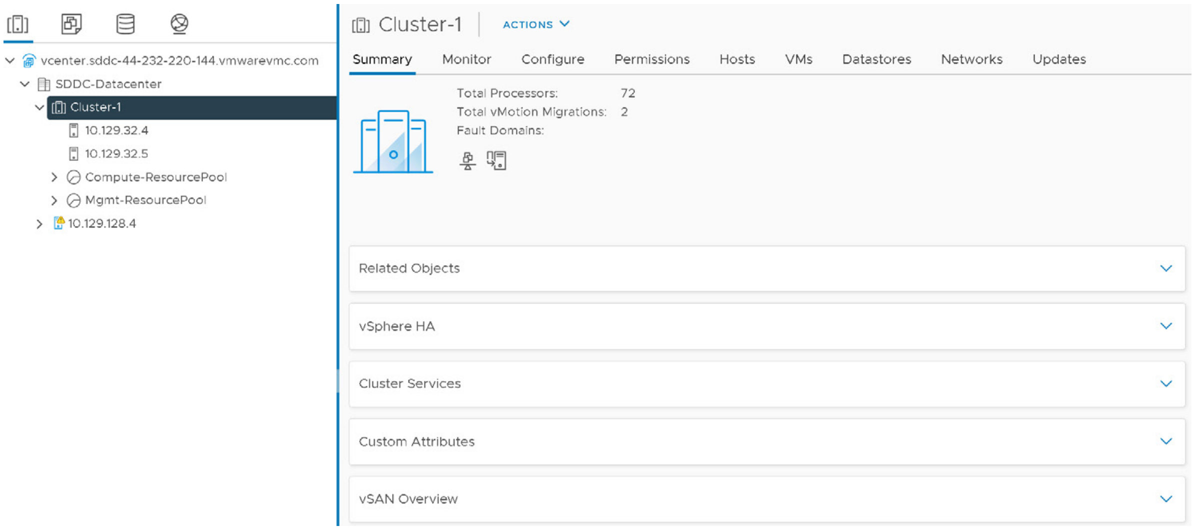
- vCenter **sc2wvc03.vslab.local** version 7.0.2 Build 17694817
- vSphere cluster **BCA-SiteC** with 4-nodes running ESXi version 7.0.2 Build 17867351
- Each ESXi server is a Dell PowerEdge R640 Server with Intel® Xeon® Platinum 8168 CPU @ 2.70GHz with 2x24 cores, and 384GB RAM with hyperthreading
- 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 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 two-node cluster for VMware Cloud on AWS setup, each ESXI server version 7.0.2 Build 18226209
- Each ESXi server is an Amazon EC2 i3.metal with 2 sockets, 18 cores each with Intel Xeon processor E5-2686 v4 at 2.30GHz without HyperThreading and 512GB RAM memory
- Storage provided by the HCI vSAN instance



Total Processors: 72
Total vMotion Migrations: 2
Fault Domains:

FIGURE 8. VMware Cloud on AWS Setup

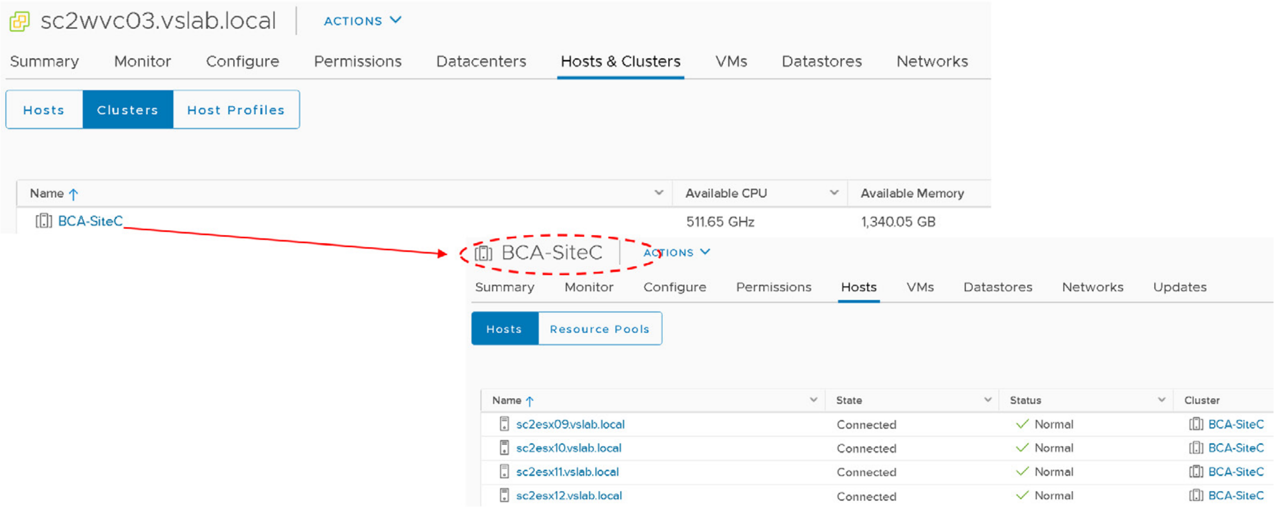
Hardware Resources

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

DESCRIPTION	SPECIFICATION
Server	4 x ESXi server
Server Model	Dell 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 2. Site A Hardware Resources

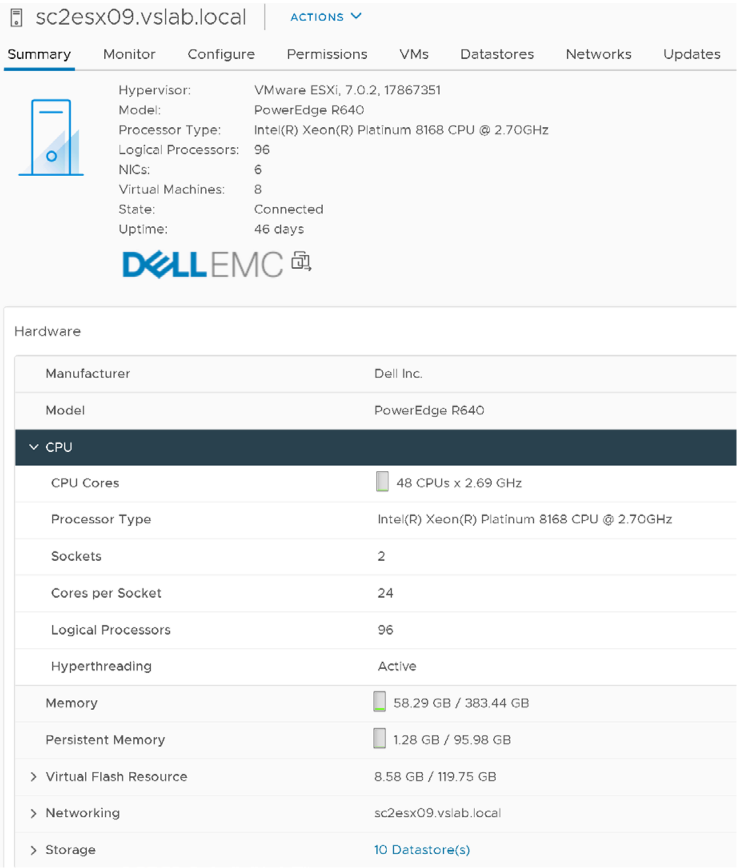
The following summarizes the vCenter **sc2wvc03.vslab.local**, vSphere cluster **BCA-SiteC** and one of the ESXi servers in the vSphere cluster on Site A:



Name ↑	Available CPU	Available Memory
BCA-SiteC	511.65 GHz	1,340.05 GB

Name ↑	State	Status	Cluster
sc2esx09.vslab.local	Connected	✓ Normal	BCA-SiteC
sc2esx10.vslab.local	Connected	✓ Normal	BCA-SiteC
sc2esx11.vslab.local	Connected	✓ Normal	BCA-SiteC
sc2esx12.vslab.local	Connected	✓ Normal	BCA-SiteC

FIGURE 9. Site A vCenter and vSphere Cluster



Hypervisor: VMware ESXi, 7.0.2, 17867351
Model: PowerEdge R640
Processor Type: Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz
Logical Processors: 96
NICs: 6
Virtual Machines: 8
State: Connected
Uptime: 46 days

Hardware

Manufacturer	Dell Inc.
Model	PowerEdge R640
CPU	
CPU Cores	48 CPUs x 2.69 GHz
Processor Type	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz
Sockets	2
Cores per Socket	24
Logical Processors	96
Hyperthreading	Active
Memory	58.29 GB / 383.44 GB
Persistent Memory	1.28 GB / 95.98 GB
Virtual Flash Resource	8.58 GB / 119.75 GB
Networking	sc2esx09.vslab.local
Storage	10 Datastore(s)

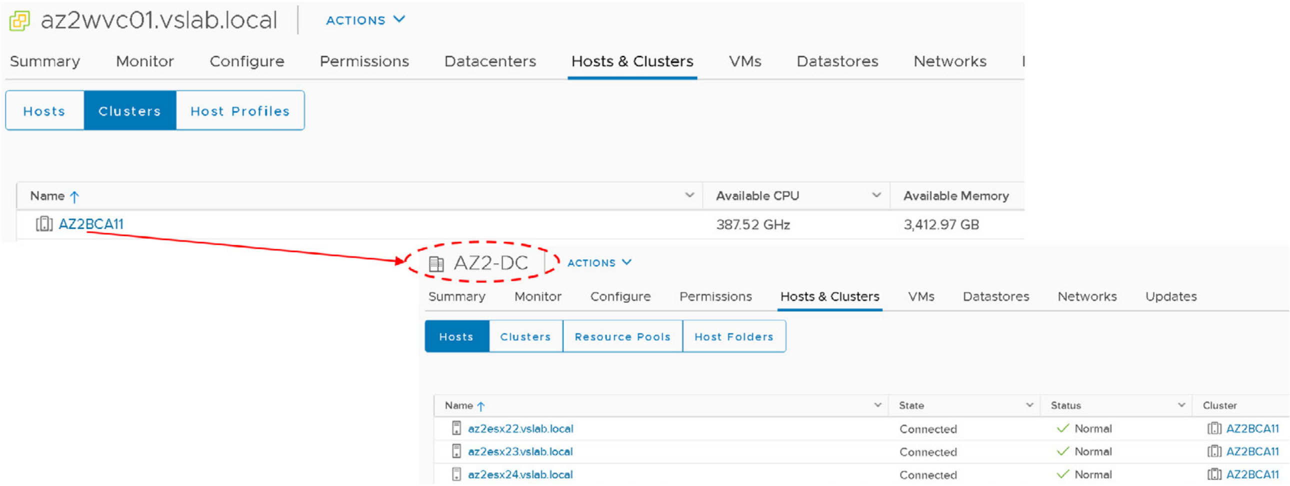
FIGURE 10. Site A VMware ESXI Server Summary

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

DESCRIPTION	SPECIFICATION
Server	3 x ESXi server
Server Model	Dell 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 3. Site B Hardware Resources

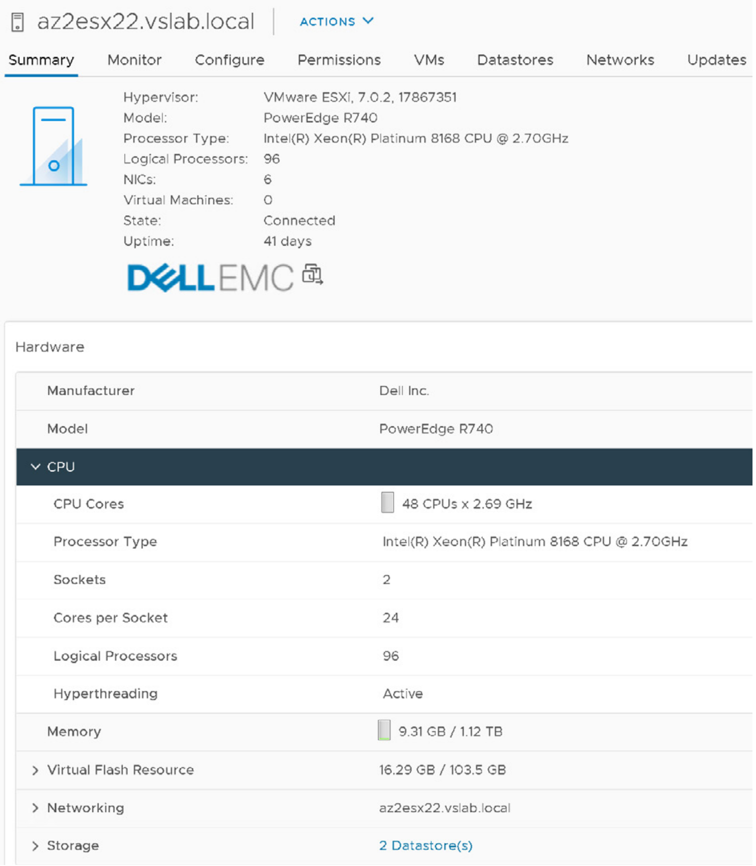
The following summarizes the vCenter **az2wvc01.vslab.local**, vSphere cluster **AZ2-DC** and one of the ESXi servers in the vSphere cluster on Site B:



Name ↑	Available CPU	Available Memory
AZ2BCA11	387.52 GHz	3,412.97 GB

Name ↑	State	Status	Cluster
az2esx22.vslab.local	Connected	✓ Normal	AZ2BCA11
az2esx23.vslab.local	Connected	✓ Normal	AZ2BCA11
az2esx24.vslab.local	Connected	✓ Normal	AZ2BCA11

FIGURE 11. Site B vCenter and vSphere Cluster



Hypervisor:	VMware ESXi, 7.0.2, 17867351
Model:	PowerEdge R740
Processor Type:	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz
Logical Processors:	96
NICs:	6
Virtual Machines:	0
State:	Connected
Uptime:	41 days

Hardware

Manufacturer	Dell Inc.
Model	PowerEdge R740
CPU	
CPU Cores	48 CPUs x 2.69 GHz
Processor Type	Intel(R) Xeon(R) Platinum 8168 CPU @ 2.70GHz
Sockets	2
Cores per Socket	24
Logical Processors	96
Hyperthreading	Active
Memory	9.31 GB / 1.12 TB
Virtual Flash Resource	16.29 GB / 103.5 GB
Networking	az2esx22.vslab.local
Storage	2 Datastore(s)

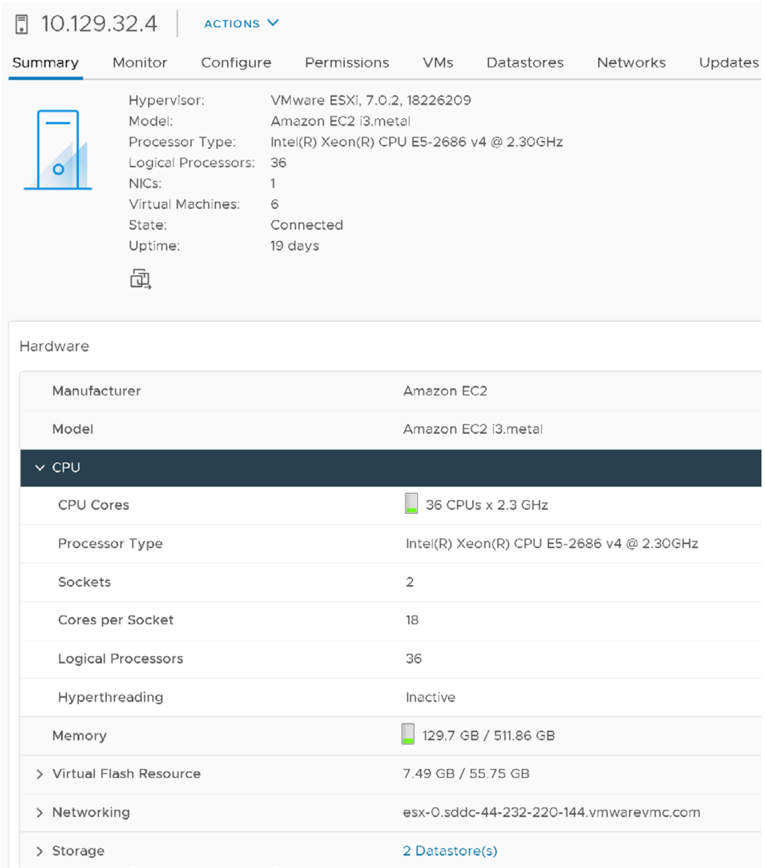
FIGURE 12. Site B Vmware Esxi Server Summary

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

DESCRIPTION	SPECIFICATION
Server	2 x ESXi servers
Server model	Amazon EC2 i3.metal
CPU	Two 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 two vSAN disk groups
vSAN disk groups	Two disk groups, each disk group with (1) NVMe for cache and (3) NVMe for capacity
Network	25G Amazon Elastic Network Adapter (ENA)

TABLE 4. VMware Cloud on AWS Hardware Resources

The following summarizes one of the ESXi servers in the VMware Cloud on AWS:



Hypervisor:	VMware ESXi, 7.0.2, 18226209
Model:	Amazon EC2 i3.metal
Processor Type:	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
Logical Processors:	36
NICs:	1
Virtual Machines:	6
State:	Connected
Uptime:	19 days

Hardware

Manufacturer	Amazon EC2
Model	Amazon EC2 i3.metal
CPU	
CPU Cores	36 CPUs x 2.3 GHz
Processor Type	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
Sockets	2
Cores per Socket	18
Logical Processors	36
Hyperthreading	Inactive
Memory	129.7 GB / 511.86 GB
Virtual Flash Resource	7.49 GB / 55.75 GB
Networking	esx-0.sddc-44-232-220-144.vmwarevmc.com
Storage	2 Datastore(s)

FIGURE 13. VMware Cloud on AWS ESXI Server Summary

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 5. Software Resources

Network Configuration

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.

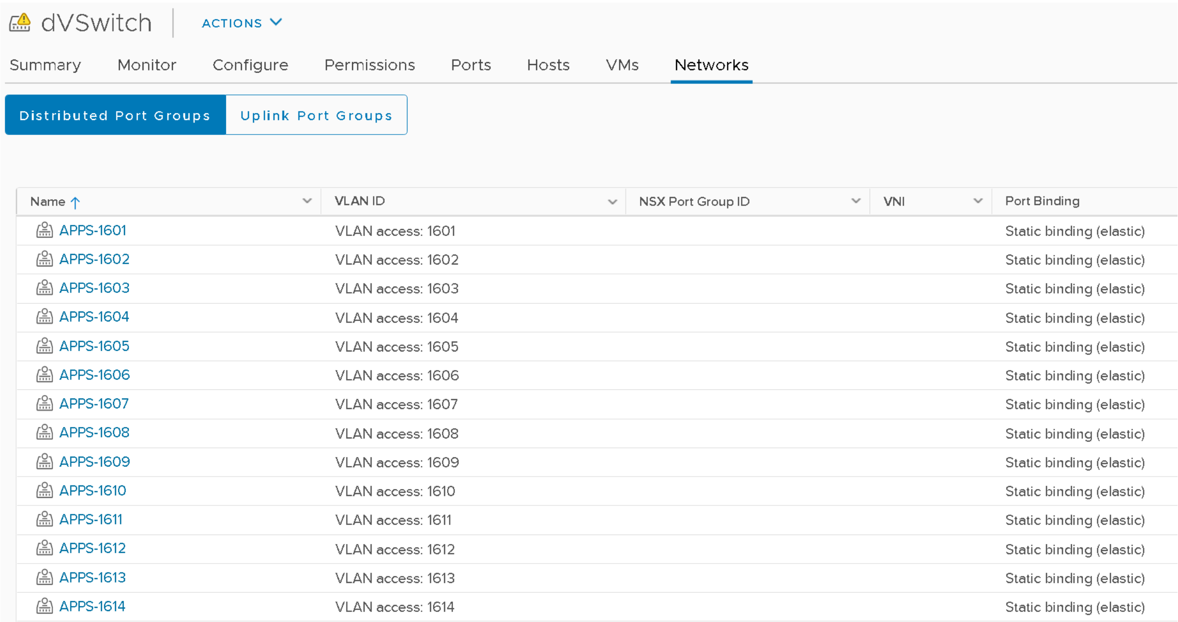
A port group defines properties regarding security, traffic-shaping, and network adapter-teaming. Jumbo frames (MTU=9000 bytes) are enabled on the vSphere vMotion interface and the default port group setting is used.

For Site A, vSphere Distributed Switch **dVSwitch** uses 2x 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 RAC and 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 RAC interconnect 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 14. Site A vSphere Distributed Switch Port Group Configuration

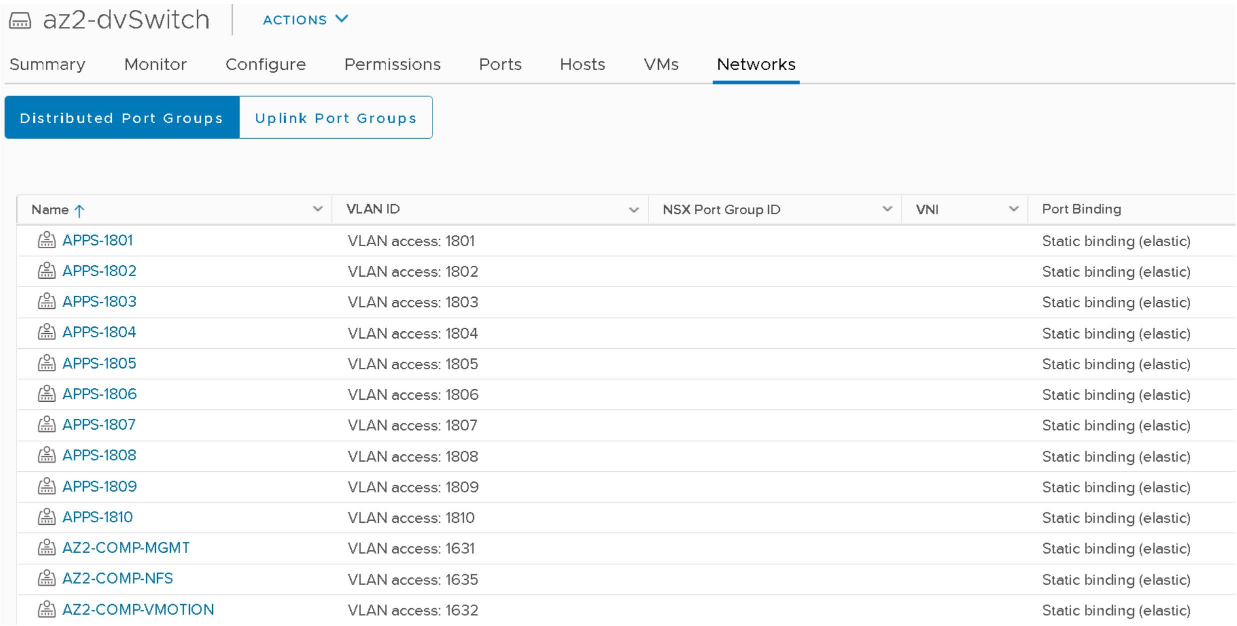
For Site B, vSphere Distributed Switch **az2-dvSwitch** uses 2x 10GbE adapter per host:

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

The following distributed switch-port groups were created for Oracle RAC and 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 RAC interconnect traffic with two active/active uplinks set to **Route based on originating virtual port**.

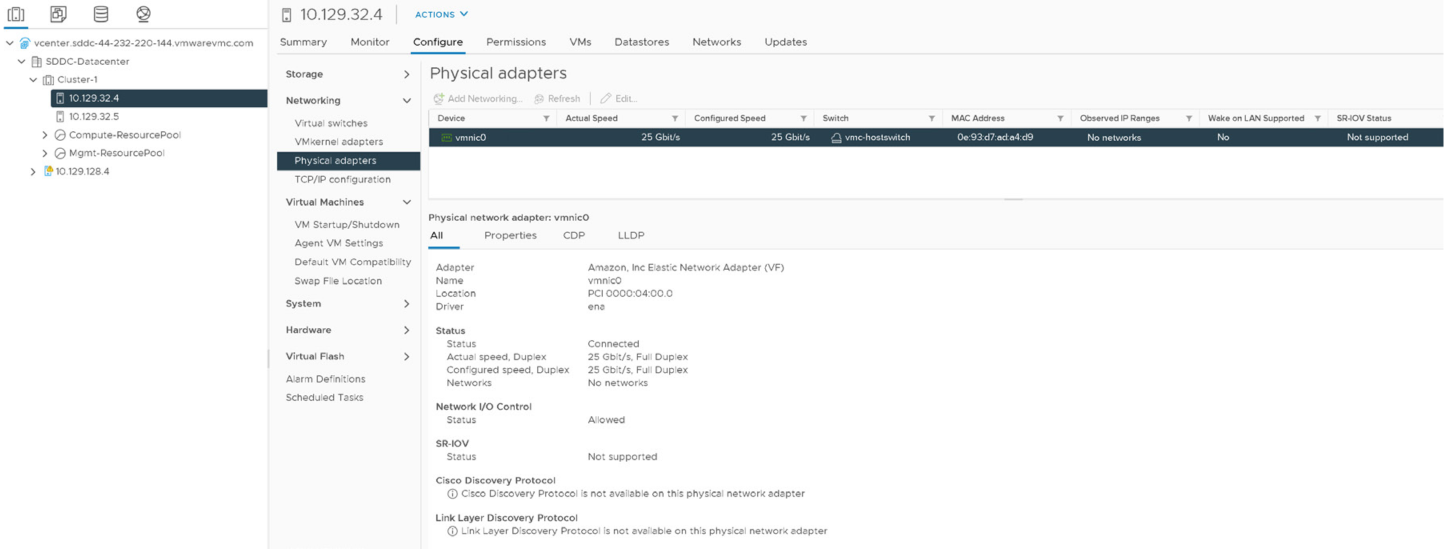
- Port group **APPS-1809** with VLAN ID 1809 (Subnet 172.18.09.1/24) is for Site Recovery Manager test network
- Port group **AZ2-COMP-MGMT** with VLAN ID 1631 for management traffic
- Port group **AZ2-COMP-VMOTION** with VLAN ID 1632 for vMotion traffic
- Port group **AZ2-COMP-NFS** with VLAN ID 1635 for NFS and vSAN traffic



Name ↑	VLAN ID	NSX Port Group ID	VNI	Port Binding
APPS-1801	VLAN access: 1801			Static binding (elastic)
APPS-1802	VLAN access: 1802			Static binding (elastic)
APPS-1803	VLAN access: 1803			Static binding (elastic)
APPS-1804	VLAN access: 1804			Static binding (elastic)
APPS-1805	VLAN access: 1805			Static binding (elastic)
APPS-1806	VLAN access: 1806			Static binding (elastic)
APPS-1807	VLAN access: 1807			Static binding (elastic)
APPS-1808	VLAN access: 1808			Static binding (elastic)
APPS-1809	VLAN access: 1809			Static binding (elastic)
APPS-1810	VLAN access: 1810			Static binding (elastic)
AZ2-COMP-MGMT	VLAN access: 1631			Static binding (elastic)
AZ2-COMP-NFS	VLAN access: 1635			Static binding (elastic)
AZ2-COMP-VMOTION	VLAN access: 1632			Static binding (elastic)

FIGURE 15. Site B vSphere Distributed Switch Port Group Configuration

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



Device	Actual Speed	Configured Speed	Switch	MAC Address	Observed IP Ranges	Wake on LAN Supported	SR-IOV Status
vmnic0	25 Gbit/s	25 Gbit/s	vmc-hostswitch	0e:93:d7:ad:a4:d9	No networks	No	Not supported

Physical network adapter: vmnic0

Adapter	Amazon, Inc Elastic Network Adapter (VF)
Name	vmnic0
Location	PCI 0000:04:00.0
Driver	ena
Status	
Status	Connected
Actual speed, Duplex	25 Gbit/s, Full Duplex
Configured speed, Duplex	25 Gbit/s, Full Duplex
Networks	No networks
Network I/O Control	
Status	Allowed
SR-IOV	
Status	Not supported

Cisco Discovery Protocol

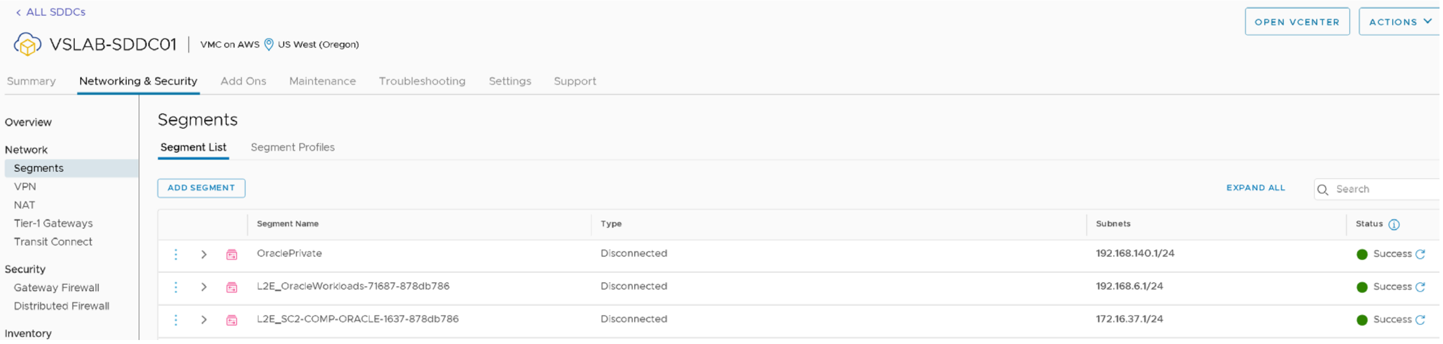
ⓘ Cisco Discovery Protocol is not available on this physical network adapter

Link Layer Discovery Protocol

ⓘ Link Layer Discovery Protocol is not available on this physical network adapter

FIGURE 16. VMware Cloud on AWS Physical Adapter Configuration

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 is an example:

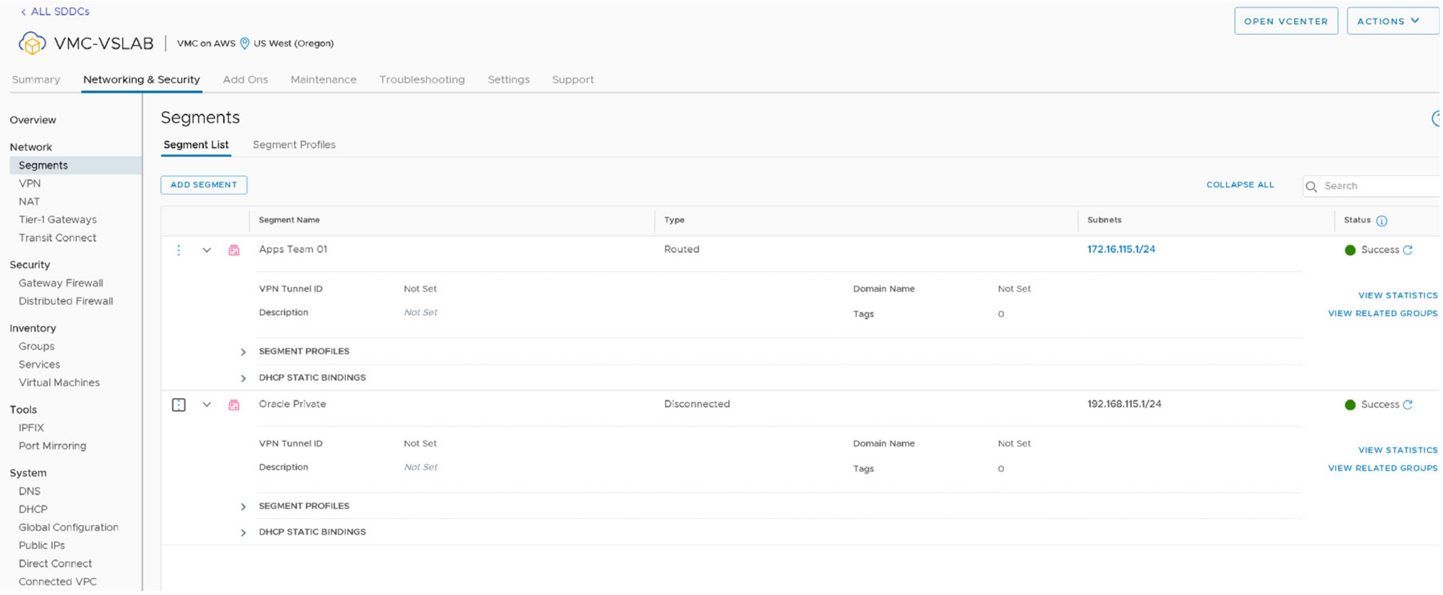


Segment Name	Type	Subnets	Status
OraclePrivate	Disconnected	192.168.140.1/24	● Success
L2E_OracleWorkloads-71687-878db786	Disconnected	192.168.6.1/24	● Success
L2E_SC2-COMP-ORACLE-1637-878db786	Disconnected	172.16.37.1/24	● Success

FIGURE 17. 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 VMs connected to it.



Segment Name	Type	Subnets	Status
Apps Team 01	Routed	172.16.115.1/24	● Success
Oracle Private	Disconnected	192.168.115.1/24	● Success

Apps Team 01: VPN Tunnel ID Not Set; Description *Not Set*; Domain Name Not Set; Tags 0

Oracle Private: VPN Tunnel ID Not Set; Description *Not Set*; Domain Name Not Set; Tags 0

FIGURE 18. Logical Segments for Public and Private network

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

The following are logical segments of 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 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, vSphere vMotion migration between on-premises VMs and VMware Cloud on AWS can be enabled across various vSphere Distributed Switch 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.

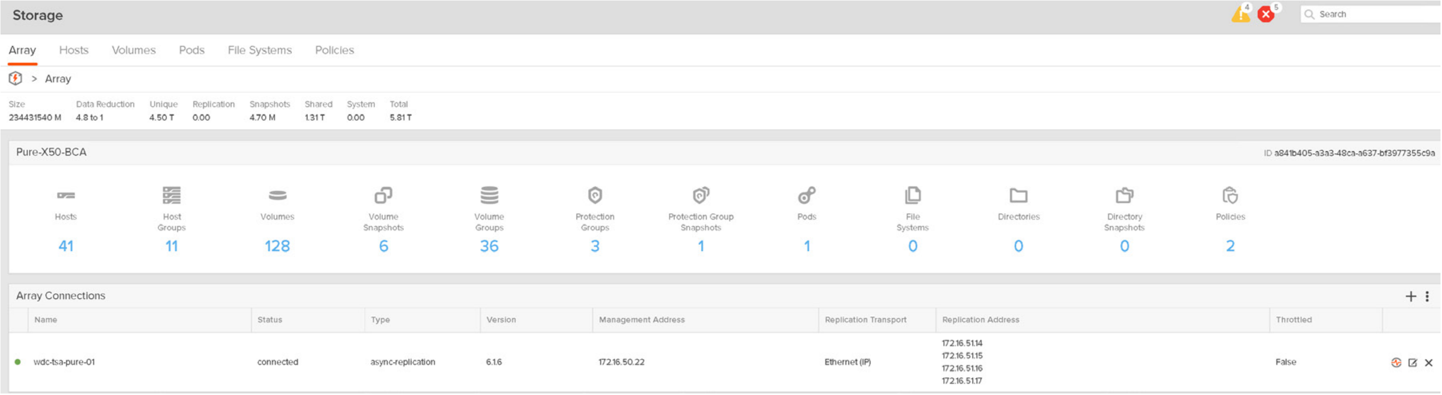
Learn more about *AWS Direct Connect*.

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

Storage Configuration

Storage Setup on Site A and Site B

Site A has access to a Pure Storage FlashArray//x50 all-flash storage (Purity/FA 6.1.6) for VMFS and vSphere Virtual Volumes named **Pure-X50-BCA**.



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
234431540 M	4.8 to 1	4.50 T	0.00	4.70 M	1.31 T	0.00	5.81 T

Pure-X50-BCA

ID a841b405-a3a3-48ca-a637-bf3977355c9a

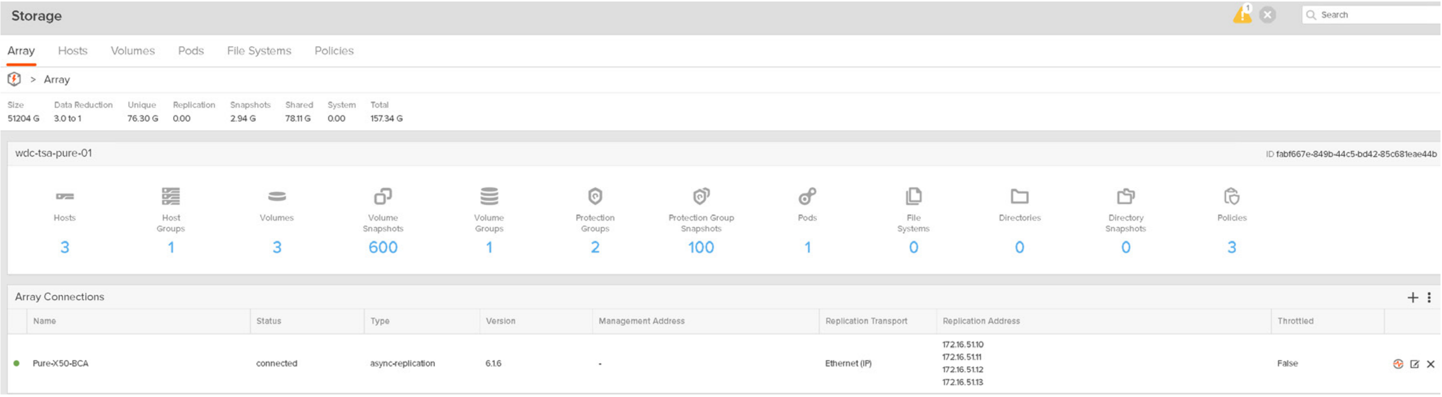
Hosts	Host Groups	Volumes	Volume Snapshots	Volume Groups	Protection Groups	Protection Group Snapshots	Pods	File Systems	Directories	Directory Snapshots	Policies
41	11	128	6	36	3	1	1	0	0	0	2

Array Connections

Name	Status	Type	Version	Management Address	Replication Transport	Replication Address	Throttled
wdc-tsa-pure-01	connected	async-replication	6.1.6	172.16.50.22	Ethernet (IP)	172.16.51.14 172.16.51.15 172.16.51.16 172.16.51.17	False

FIGURE 19. Site A Pure Storage

Site B has access to a Pure Storage FlashArray//x50 all-flash storage (Purity/FA 6.1.6) for VMFS and vSphere Virtual Volumes named **wdc-tsa-pure-01**.



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
51204 G	3.0 to 1	76.30 G	0.00	2.94 G	78.11 G	0.00	157.34 G

wdc-tsa-pure-01 ID fabf667e-849b-44c5-bd42-85c681eae44b

Hosts	Host Groups	Volumes	Volume Snapshots	Volume Groups	Protection Groups	Protection Group Snapshots	Pods	File Systems	Directories	Directory Snapshots	Policies
3	1	3	600	1	2	100	1	0	0	0	3

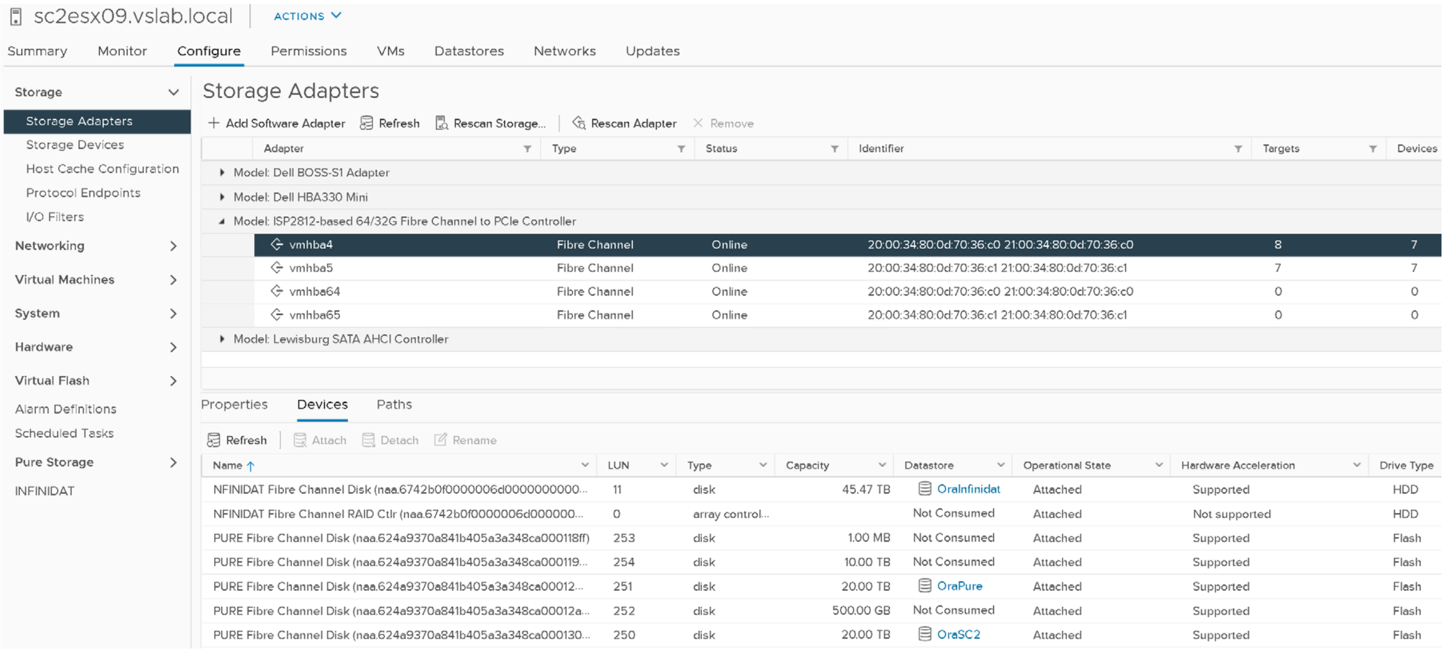
Array Connections

Name	Status	Type	Version	Management Address	Replication Transport	Replication Address	Throttled
Pure-X50-BCA	connected	async-replication	6.1.6	-	Ethernet (IP)	172.16.51.10 172.16.51.11 172.16.51.12 172.16.51.13	False

FIGURE 20. Site B Pure Storage

ESXi Storage Setup on Site A and Site B

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

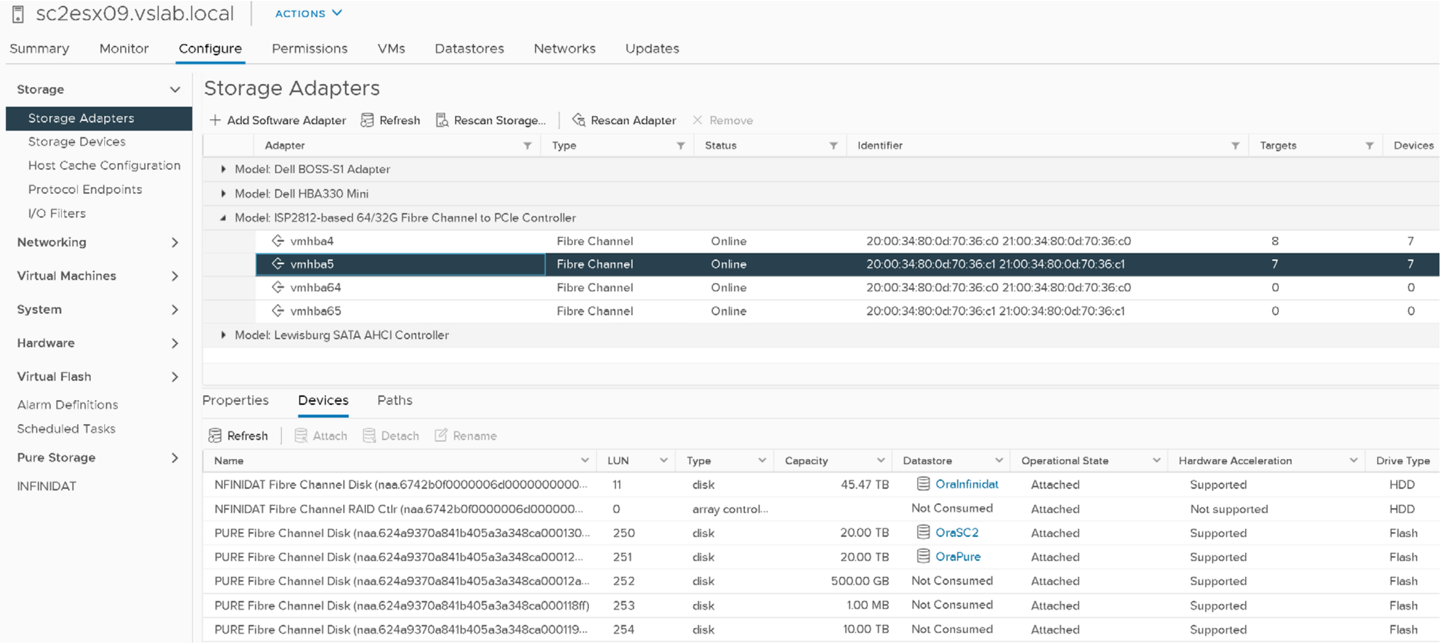


Storage Adapters

Adapter	Type	Status	Identifier	Targets	Devices
Model: Dell BOSS-S1 Adapter					
Model: Dell HBA330 Mini					
Model: ISP2812-based 64/32G Fibre Channel to PCIe Controller					
vmhba4	Fibre Channel	Online	20:00:34:80:0d:70:36:c0 21:00:34:80:0d:70:36:c0	8	7
vmhba5	Fibre Channel	Online	20:00:34:80:0d:70:36:c1 21:00:34:80:0d:70:36:c1	7	7
vmhba64	Fibre Channel	Online	20:00:34:80:0d:70:36:c0 21:00:34:80:0d:70:36:c0	0	0
vmhba65	Fibre Channel	Online	20:00:34:80:0d:70:36:c1 21:00:34:80:0d:70:36:c1	0	0
Model: Lewisburg SATA AHCI Controller					

Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type
NFINIDAT Fibre Channel Disk (naa.6742b0f0000006d0000000000...	11	disk	45.47 TB	OraInfinidat	Attached	Supported	HDD
NFINIDAT Fibre Channel RAID Ctlr (naa.6742b0f0000006d000000...	0	array control...		Not Consumed	Attached	Not supported	HDD
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca000118ff)	253	disk	1.00 MB	Not Consumed	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca000119...	254	disk	10.00 TB	Not Consumed	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00012...	251	disk	20.00 TB	OraPure	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00012a...	252	disk	500.00 GB	Not Consumed	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca000130...	250	disk	20.00 TB	OraSC2	Attached	Supported	Flash

FIGURE 21. Site A ESXi Server Storage Adapter



Storage Adapters

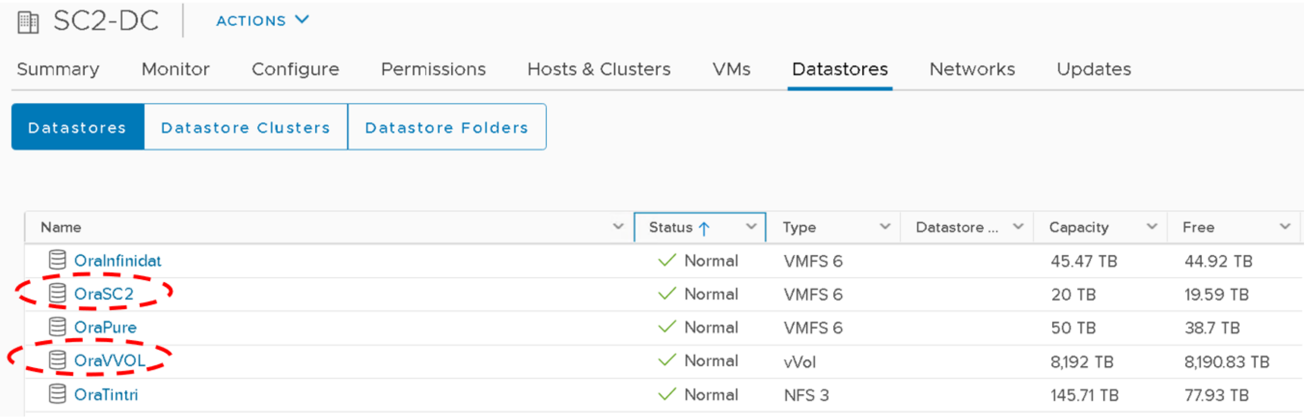
Adapter	Type	Status	Identifier	Targets	Devices
Model: Dell BOSS-S1 Adapter					
Model: Dell HBA330 Mini					
Model: ISP2812-based 64/32G Fibre Channel to PCIe Controller					
vmhba4	Fibre Channel	Online	20:00:34:80:0d:70:36:c0 21:00:34:80:0d:70:36:c0	8	7
vmhba5	Fibre Channel	Online	20:00:34:80:0d:70:36:c1 21:00:34:80:0d:70:36:c1	7	7
vmhba64	Fibre Channel	Online	20:00:34:80:0d:70:36:c0 21:00:34:80:0d:70:36:c0	0	0
vmhba65	Fibre Channel	Online	20:00:34:80:0d:70:36:c1 21:00:34:80:0d:70:36:c1	0	0
Model: Lewisburg SATA AHCI Controller					

Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type
NFINIDAT Fibre Channel Disk (naa.6742b0f0000006d0000000000...	11	disk	45.47 TB	OraInfinidat	Attached	Supported	HDD
NFINIDAT Fibre Channel RAID Ctlr (naa.6742b0f0000006d000000...	0	array control...		Not Consumed	Attached	Not supported	HDD
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca000130...	250	disk	20.00 TB	OraSC2	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00012...	251	disk	20.00 TB	OraPure	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00012a...	252	disk	500.00 GB	Not Consumed	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca000118ff)	253	disk	1.00 MB	Not Consumed	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca000119...	254	disk	10.00 TB	Not Consumed	Attached	Supported	Flash

FIGURE 22. Site A ESXi Server FC Storage Connections

On Site A, on the four-node vSphere cluster, the following VMFS and vSphere Virtual Volumes datastores were created on the Pure x50 array.

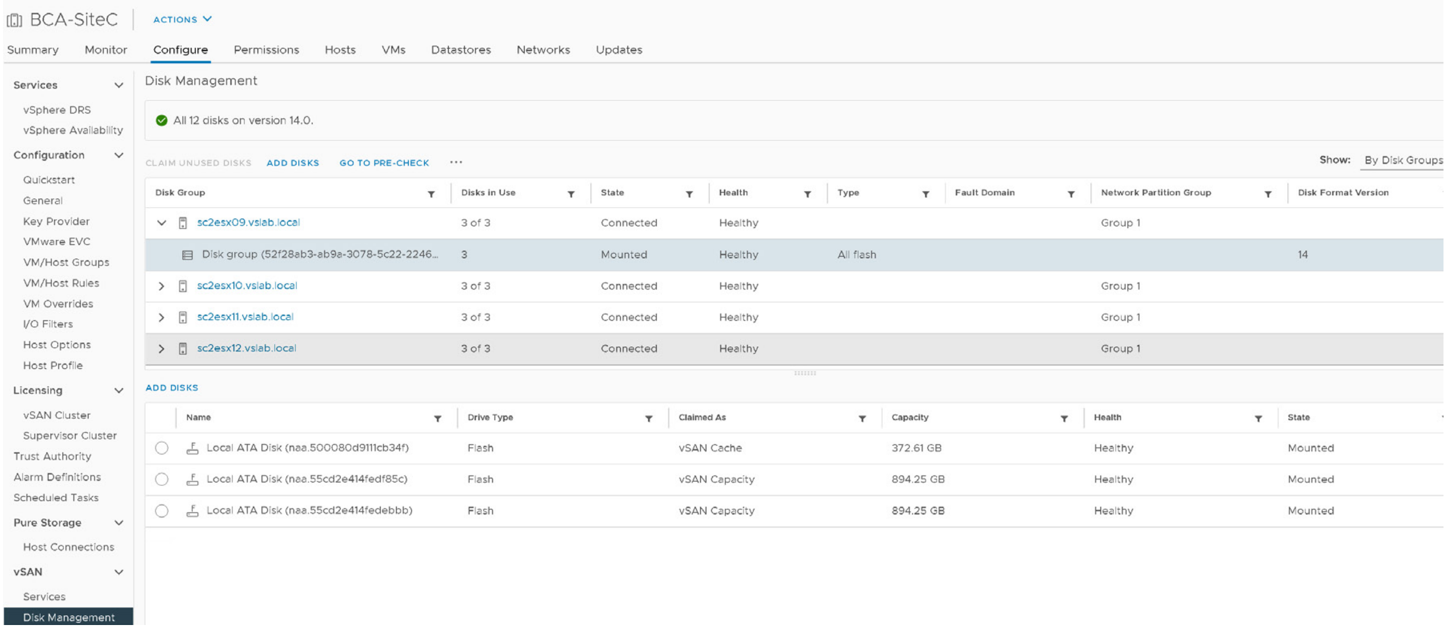
OraSC2 VMFS6 datastore and **OraVVOL** vSphere Virtual Volumes datastore on Site A were used in this reference architecture.



Name	Status ↑	Type	Datastore ...	Capacity	Free
OraInfinidat	✓ Normal	VMFS 6		45.47 TB	44.92 TB
OraSC2	✓ Normal	VMFS 6		20 TB	19.59 TB
OraPure	✓ Normal	VMFS 6		50 TB	38.7 TB
OraVVOL	✓ Normal	vVol		8,192 TB	8,190.83 TB
OraTintri	✓ Normal	NFS 3		145.71 TB	77.93 TB

FIGURE 23. Site A Datastores

In addition, Site A four-node vSphere cluster has a vSAN datastore **BCA-SiteC-vSAN**.



Disk Management

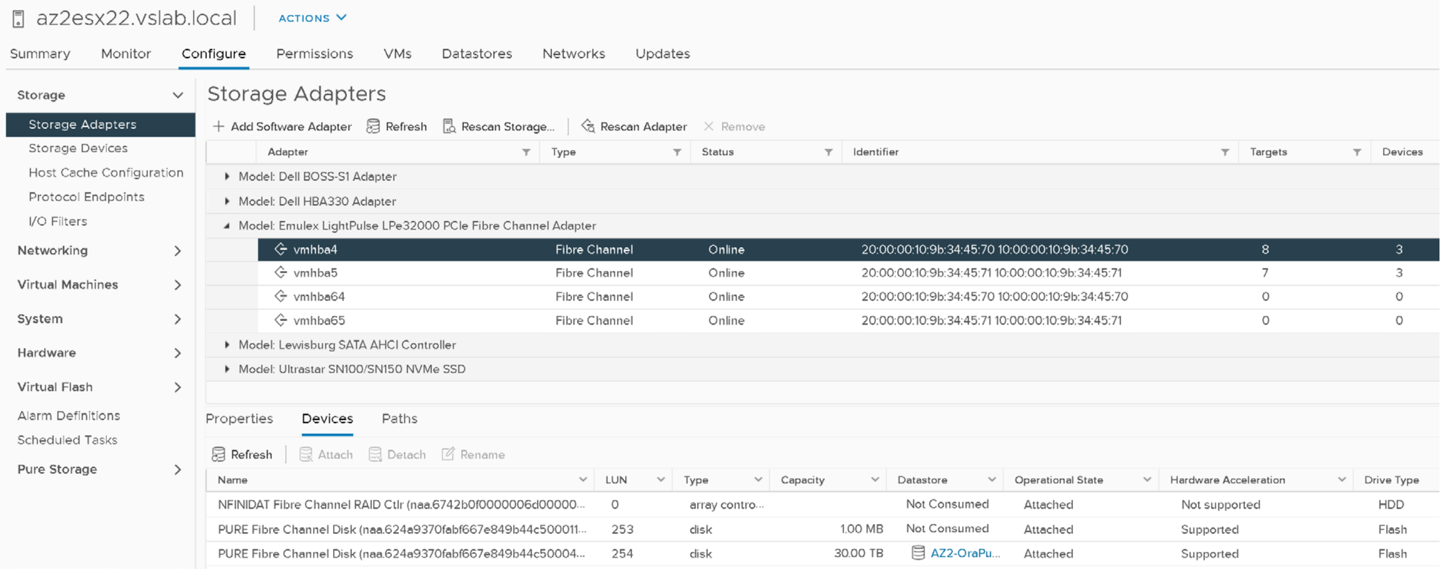
All 12 disks on version 14.0.

Disk Group	Disks in Use	State	Health	Type	Fault Domain	Network Partition Group	Disk Format Version
sc2esx09.vslab.local	3 of 3	Connected	Healthy			Group 1	
Disk group (52f28ab3-ab9a-3078-5c22-2246...	3	Mounted	Healthy	All flash			14
sc2esx10.vslab.local	3 of 3	Connected	Healthy			Group 1	
sc2esx11.vslab.local	3 of 3	Connected	Healthy			Group 1	
sc2esx12.vslab.local	3 of 3	Connected	Healthy			Group 1	

	Name	Drive Type	Claimed As	Capacity	Health	State
○	Local ATA Disk (naa.500080d9111cb34f)	Flash	vSAN Cache	372.61 GB	Healthy	Mounted
○	Local ATA Disk (naa.55cd2e414fedf85c)	Flash	vSAN Capacity	894.25 GB	Healthy	Mounted
○	Local ATA Disk (naa.55cd2e414fedebbb)	Flash	vSAN Capacity	894.25 GB	Healthy	Mounted

FIGURE 24. Site A vSAN Datastore

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

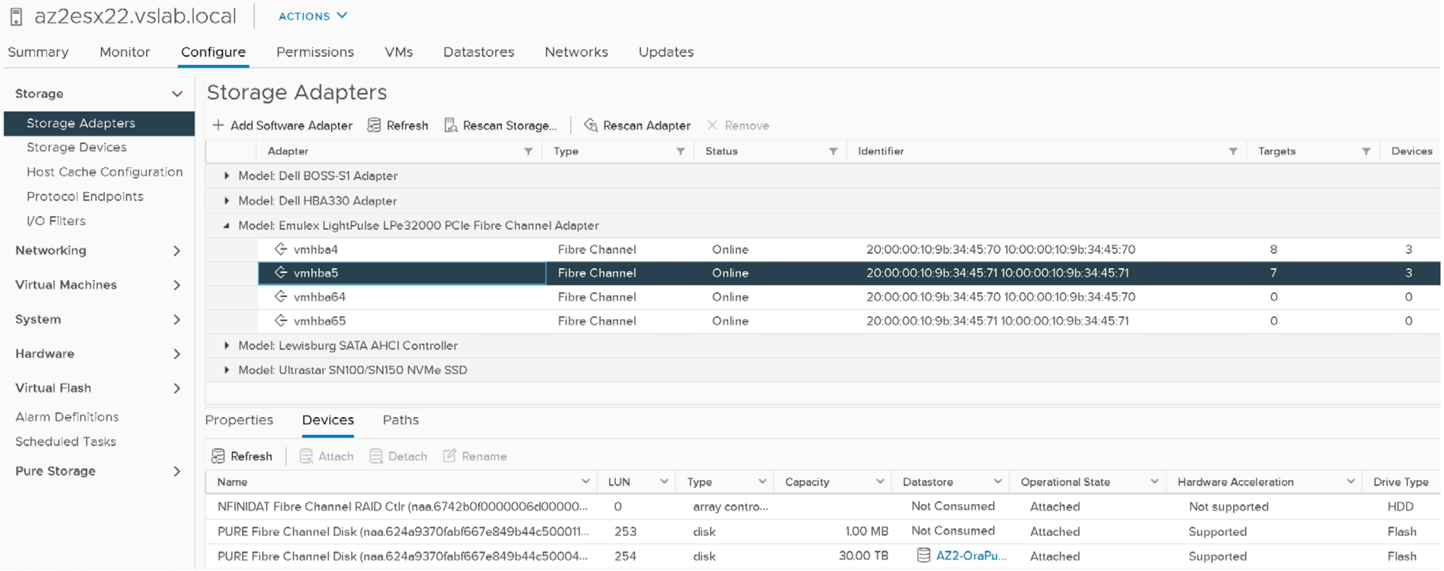


Storage Adapters

Adapter	Type	Status	Identifier	Targets	Devices
Model: Dell BOSS-S1 Adapter					
Model: Dell HBA330 Adapter					
Model: Emulex LightPulse LPe32000 PCIe Fibre Channel Adapter					
vmhba4	Fibre Channel	Online	20:00:00:10:9b:34:45:70 10:00:00:10:9b:34:45:70	8	3
vmhba5	Fibre Channel	Online	20:00:00:10:9b:34:45:71 10:00:00:10:9b:34:45:71	7	3
vmhba64	Fibre Channel	Online	20:00:00:10:9b:34:45:70 10:00:00:10:9b:34:45:70	0	0
vmhba65	Fibre Channel	Online	20:00:00:10:9b:34:45:71 10:00:00:10:9b:34:45:71	0	0
Model: Lewisburg SATA AHCI Controller					
Model: Ultrastar SN100/SN150 NVMe SSD					

Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type
NFINIDAT Fibre Channel RAID Ctlr (naa.6742b0f0000006d00000...	0	array contro...		Not Consumed	Attached	Not supported	HDD
PURE Fibre Channel Disk (naa.624a9370fabf667e849b44c500011...	253	disk	1.00 MB	Not Consumed	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370fabf667e849b44c50004...	254	disk	30.00 TB	AZ2-OraPu...	Attached	Supported	Flash

FIGURE 25. Site B ESXi Server Storage Adapter



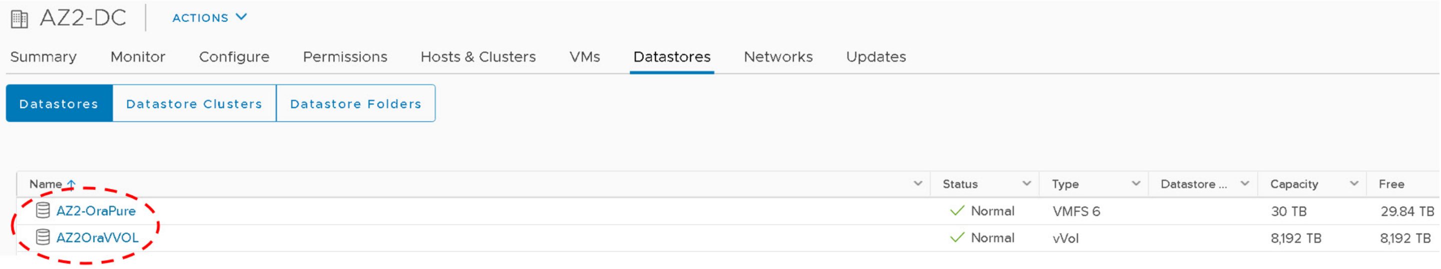
Adapter	Type	Status	Identifier	Targets	Devices
Model: Dell BOSS-S1 Adapter					
Model: Dell HBA330 Adapter					
Model: Emulex LightPulse LPe32000 PCIe Fibre Channel Adapter					
vmhba4	Fibre Channel	Online	20:00:00:10:9b:34:45:70 10:00:00:10:9b:34:45:70	8	3
vmhba5	Fibre Channel	Online	20:00:00:10:9b:34:45:71 10:00:00:10:9b:34:45:71	7	3
vmhba64	Fibre Channel	Online	20:00:00:10:9b:34:45:70 10:00:00:10:9b:34:45:70	0	0
vmhba65	Fibre Channel	Online	20:00:00:10:9b:34:45:71 10:00:00:10:9b:34:45:71	0	0
Model: Lewisburg SATA AHCI Controller					
Model: Ultrastar SN100/SN150 NVMe SSD					

Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type
NFINIDAT Fibre Channel RAID Ctlr (naa.6742b0f0000006d00000...	0	array contro...		Not Consumed	Attached	Not supported	HDD
PURE Fibre Channel Disk (naa.624a9370fabf667e849b44c500011...	253	disk	1.00 MB	Not Consumed	Attached	Supported	Flash
PURE Fibre Channel Disk (naa.624a9370fabf667e849b44c50004...	254	disk	30.00 TB	AZ2-OraPu...	Attached	Supported	Flash

FIGURE 26. Site B ESXi Server FC Storage Connections

On Site B, on the three-node vSphere cluster, the following VMFS and vSphere Virtual Volumes datastores were created on the Pure x50 array.

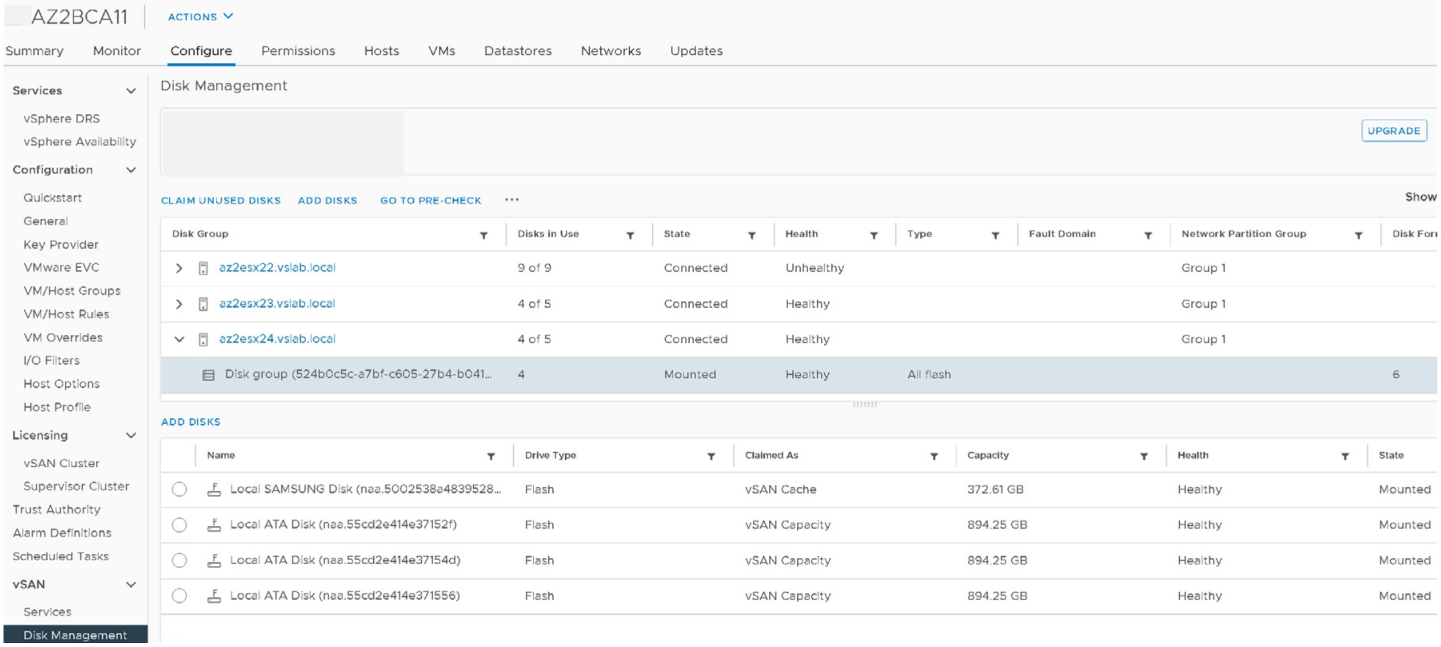
AZ2OraPure VMFS6 datastore and **AZ2OraVVOL** vSphere Virtual Volumes datastore on Site B were used in this reference architecture.



Name	Status	Type	Datastore ...	Capacity	Free
AZ2-OraPure	✓ Normal	VMFS 6		30 TB	29.84 TB
AZ2OraVVOL	✓ Normal	vVol		8,192 TB	8,192 TB

FIGURE 27. Site B Datastores

In addition, Site B three-node vSphere cluster also has a vSAN datastore AZ2-vSAN.



Disk Management

Disk Group	Disks in Use	State	Health	Type	Fault Domain	Network Partition Group	Disk Forı
az2esx22.vslab.local	9 of 9	Connected	Unhealthy			Group 1	
az2esx23.vslab.local	4 of 5	Connected	Healthy			Group 1	
az2esx24.vslab.local	4 of 5	Connected	Healthy			Group 1	
Disk group (524b0c5c-a7bf-c605-27b4-b041...	4	Mounted	Healthy	All flash			6

Name	Drive Type	Claimed As	Capacity	Health	State
Local SAMSUNG Disk (naa.5002538a4839528...	Flash	vSAN Cache	372.61 GB	Healthy	Mounted
Local ATA Disk (naa.55cd2e414e37152f)	Flash	vSAN Capacity	894.25 GB	Healthy	Mounted
Local ATA Disk (naa.55cd2e414e37154d)	Flash	vSAN Capacity	894.25 GB	Healthy	Mounted
Local ATA Disk (naa.55cd2e414e371556)	Flash	vSAN Capacity	894.25 GB	Healthy	Mounted

FIGURE 28. Site B vSAN Datastore

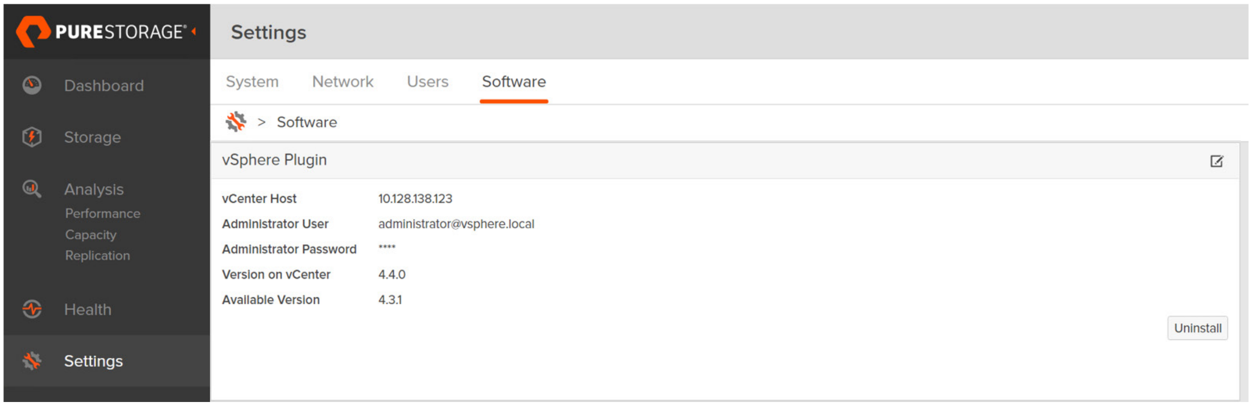
Pure Storage Plugin for VMware vSphere Client

The Pure Storage Plugin for the vSphere client enables VMware users to have insight into, and control of, their Pure Storage FlashArray environment while directly logged into the vSphere client.

The Pure Storage Plugin extends the vSphere client interface to include environmental statistics and objects that underpin the VMware objects in use and to provision new resources as needed.

Learn more about *installing the Pure Storage Plugin for the vSphere client*.

Pure Storage Plugin details are shown below:



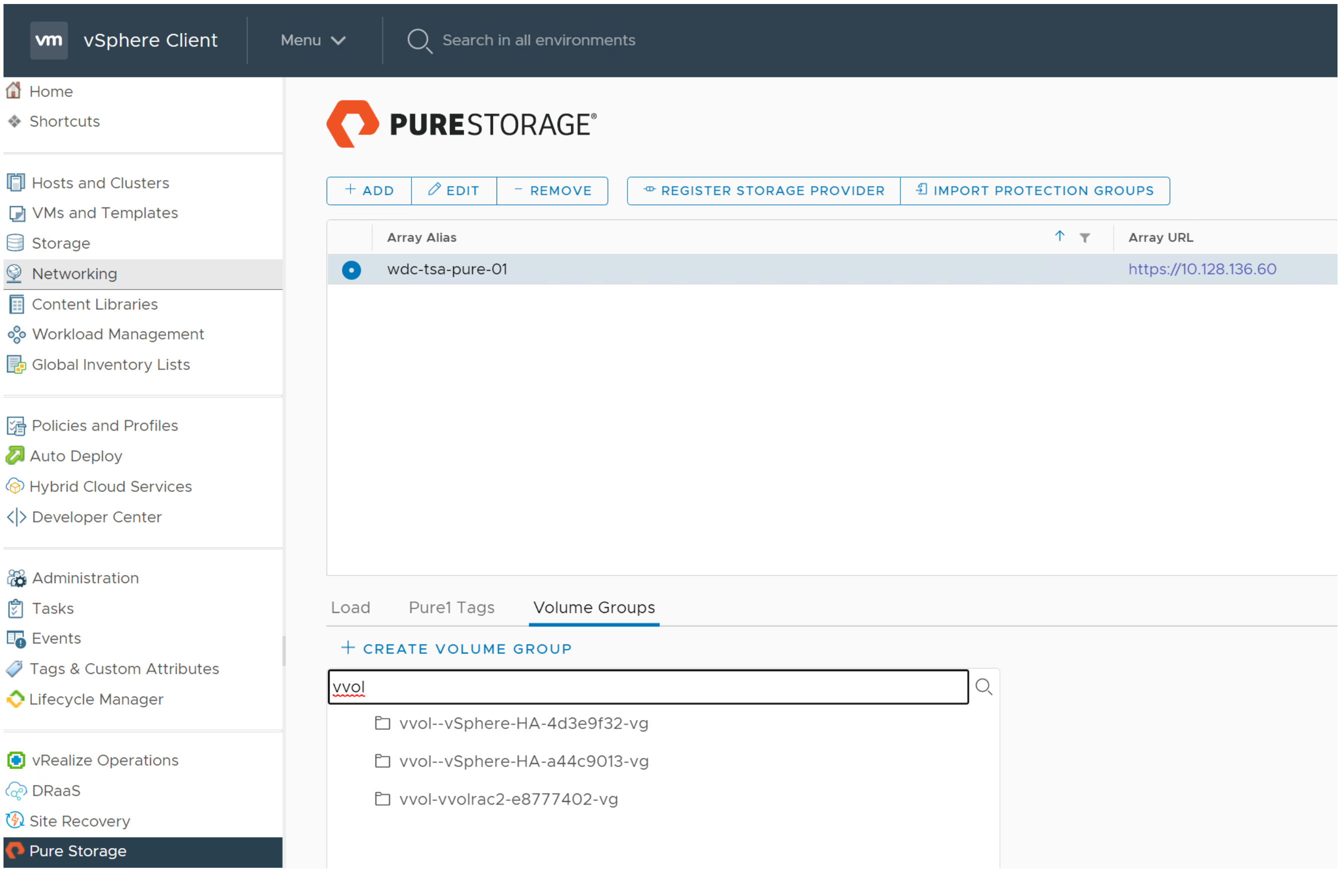
Settings

vSphere Plugin

vCenter Host	10.128.138.123
Administrator User	administrator@vsphere.local
Administrator Password	****
Version on vCenter	4.4.0
Available Version	4.3.1

FIGURE 29. Pure Storage Plugin Details

VMware vCenter and Pure Storage Plugin:



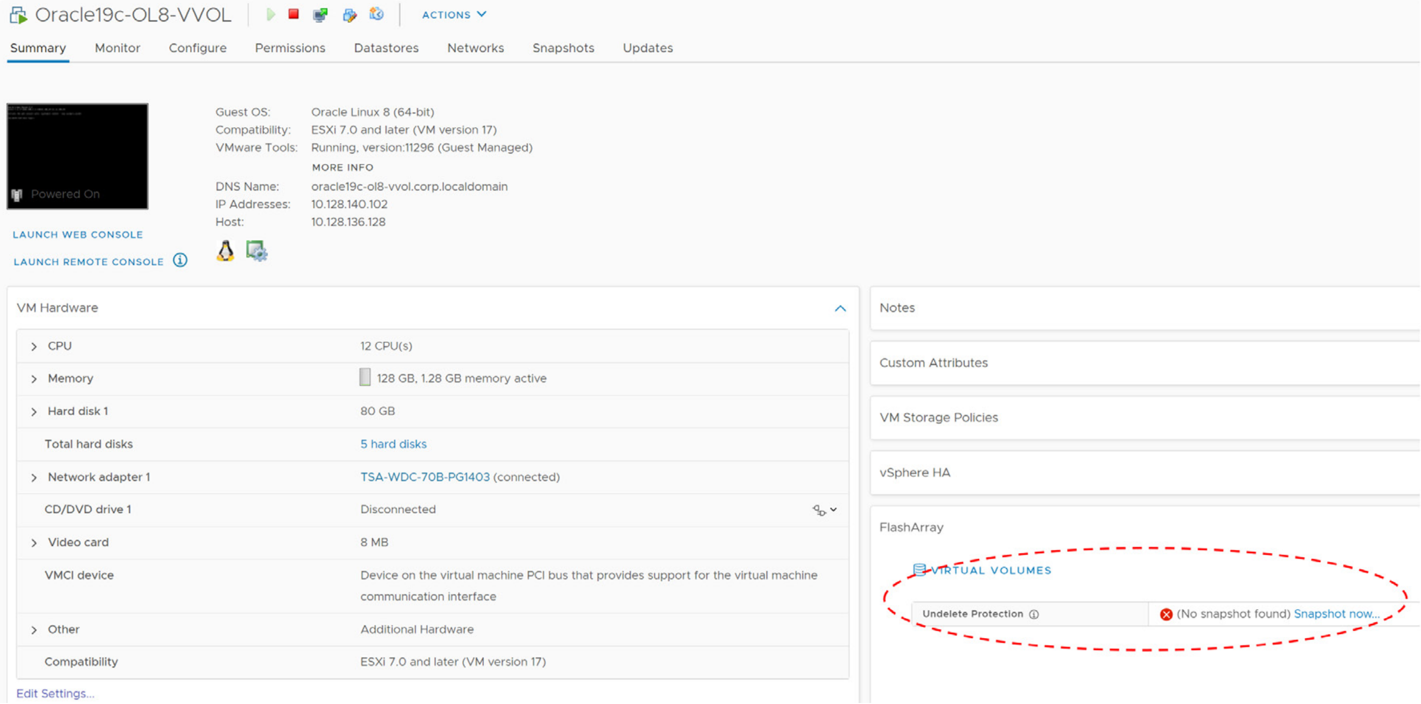
	Array Alias	Array URL
●	wdc-tsa-pure-01	https://10.128.136.60

vvol

- vvol--vSphere-HA-4d3e9f32-vg
- vvol--vSphere-HA-a44c9013-vg
- vvol-vvolrac2-e8777402-vg

FIGURE 30. VMware vCenter and Pure Storage Plugin

Once the plugin is installed, from the VM **Oracle19c-OL8-VVOL** view and summary tab, there is a FlashArray widget box indicating whether or not the VM has undelete protection. Undelete protection means that there is currently a FlashArray snapshot of the VM's config-virtual volumes.



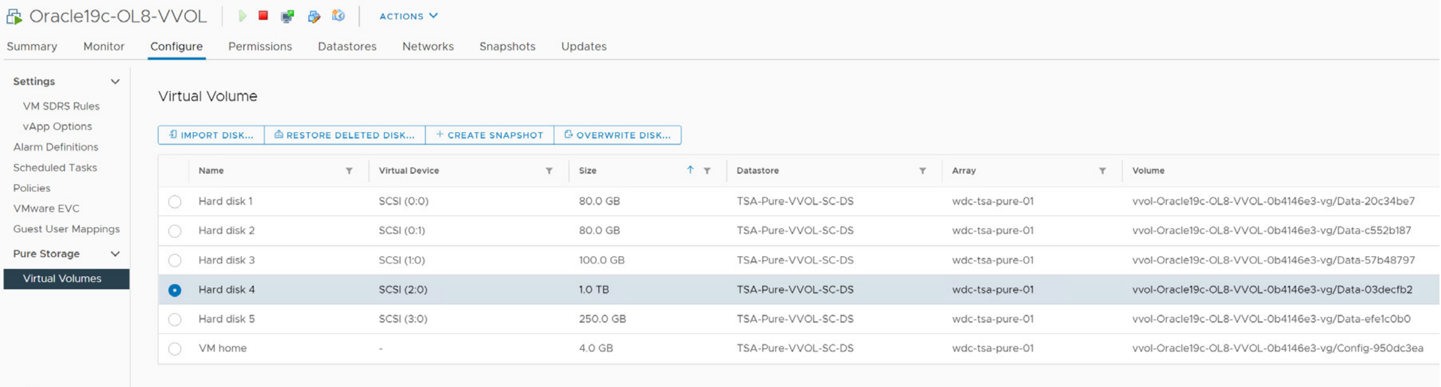
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol.corp.localdomain
IP Addresses: 10.128.140.102
Host: 10.128.136.128

VM Hardware	
CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	TSA-WDC-70B-PG1403 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Undelete Protection ⓘ ☒ (No snapshot found) Snapshot now...

FIGURE 31. Undelete Protection Widget

Navigate to VM **Oracle19c-OL8-VVOL's Configure** tab to see virtual volumes on Pure Storage.



Virtual Volume

	Name	Virtual Device	Size	Datastore	Array	Volume
○	Hard disk 1	SCSI (0:0)	80.0 GB	TSA-Pure-VVOL-SC-DS	wdc-tsa-pure-01	vvol-Oracle19c-OL8-VVOL-0b4146e3-vg/Data-20c34be7
○	Hard disk 2	SCSI (0:1)	80.0 GB	TSA-Pure-VVOL-SC-DS	wdc-tsa-pure-01	vvol-Oracle19c-OL8-VVOL-0b4146e3-vg/Data-c552b187
○	Hard disk 3	SCSI (1:0)	100.0 GB	TSA-Pure-VVOL-SC-DS	wdc-tsa-pure-01	vvol-Oracle19c-OL8-VVOL-0b4146e3-vg/Data-57b48797
●	Hard disk 4	SCSI (2:0)	1.0 TB	TSA-Pure-VVOL-SC-DS	wdc-tsa-pure-01	vvol-Oracle19c-OL8-VVOL-0b4146e3-vg/Data-03decfb2
○	Hard disk 5	SCSI (3:0)	250.0 GB	TSA-Pure-VVOL-SC-DS	wdc-tsa-pure-01	vvol-Oracle19c-OL8-VVOL-0b4146e3-vg/Data-efe1c0b0
○	VM home	-	4.0 GB	TSA-Pure-VVOL-SC-DS	wdc-tsa-pure-01	vvol-Oracle19c-OL8-VVOL-0b4146e3-vg/Config-950dc3ea

FIGURE 32. Virtual Volumes on Pure Storage

The Pure Storage Plugin enables the following operations:

- Import disk – to import a virtual disk (vVol)
- Restore deleted disk – to restore a destroyed vVol
- Create snapshot – to take a snapshot
- Overwrite disk – to overwrite an existing vVol

Learn more about *Pure Storage Plugin operations*.

Virtual Machine and Oracle Configuration

Two single-instance VMs were created on Site A as follows:

- VM Oracle19c-OL8
- VM Oracle19c-OL8-RMAN

Each VM was created with the following tools or characteristics:

- VM version 19 on ESXi 7.0 U2
- Guest operating system Oracle Enterprise Linux 8.3 UEK
- Oracle Grid and RDBMS binaries version 19.8
- ASM disk group for Oracle Grid Infrastructure Management Repository (GIMR) named **MGMT_DATA**
- Different names for DATA and FRA ASM disks on VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN**
  - On VM **Oracle19c-OL8**, ASM diskgroup DATA_DG contains a ASM disk **DATA_01** and ASM diskgroup FRA_DG has a ASM disk **FRA_01**
  - On VM Oracle19c-OL8-RMAN, ASM diskgroup RMAN_DATA_DG contains a ASM disk **RMAN_DATA_01**

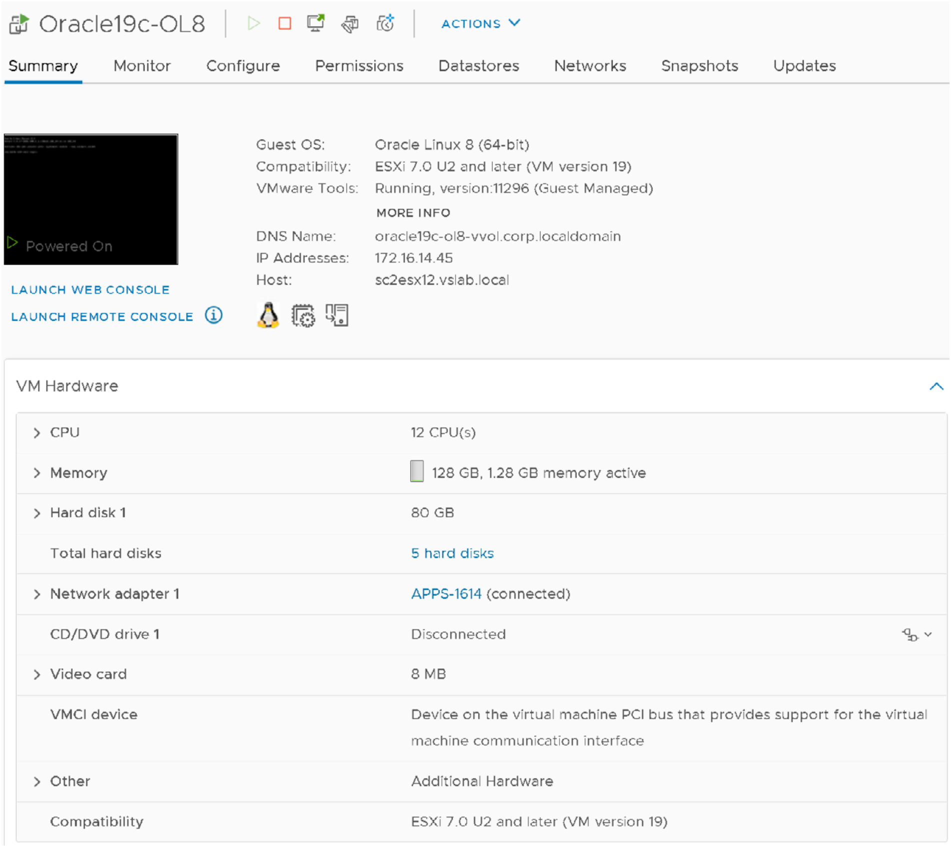
Storage for both VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** was provisioned on the VMFS datastore OraSC2.for all use cases except for storage-based replication using vSphere Virtual Volumes, these two VMs were provisioned on the vSphere Virtual Volumes datastore OraVVOL.

The use cases for application-based replication and VMware-based replication (VMware Site Recovery Manager with VMware vSphere Replication) can be applied to virtual machines with storage on any VMware datastore (NFS, VMFS, vSAN, vSphere Virtual Volumes).

Details for VM Oracle19c-OL8 are as follows:

- 12 vCPUs with 128GB RAM
- Oracle SGA set to 96GB with traditional HugePages and PGA set to 6GB
- VM hosts both Oracle Grid and RDBMS 19.8 multi-tenant production database **vvol19c** with a pluggable database **pdb1**
- 3 ASM disks groups:
  - MGMT_DATA for Oracle Grid Infrastructure Management Repository (GIMR) with ASM disk **MGMT_DATA01**
  - DATA_DG for data and redo log files with ASM disk **DATA_01**
  - FRA_DG for archive logs files with ASM disk **FRA_01**
- VM network adapter is connected to port group **APPS-1614** and assigned an IP address 172.16.14.45

All Oracle on VMware platform best practices were followed as per the *VMware Hybrid Cloud Best Practices Guide for Oracle Workloads*.



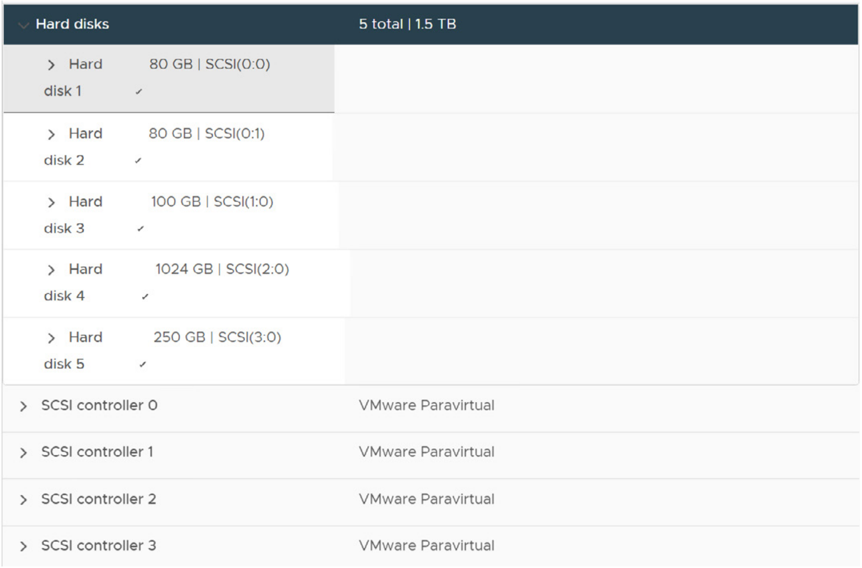
Guest OS:	Oracle Linux 8 (64-bit)
Compatibility:	ESXi 7.0 U2 and later (VM version 19)
VMware Tools:	Running, version:11296 (Guest Managed)
DNS Name:	oracle19c-ol8-vvol.corp.localdomain
IP Addresses:	172.16.14.45
Host:	sc2esx12.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 33. VM Oracle19c-OL8 Summary

VM **Oracle19c-OL8** VMDKs are shown below. All SCSI controllers are set to **VMware Paravirtual SCSI Controller** type.



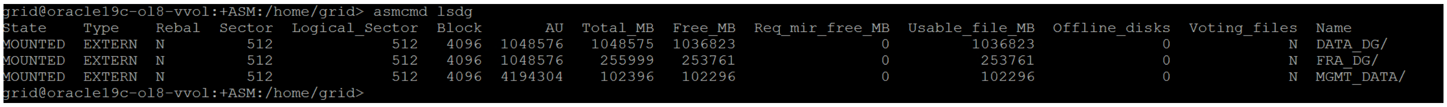
Hard disks	5 total | 1.5 TB
Hard disk 1	80 GB | SCSI(0:0)
Hard disk 2	80 GB | SCSI(0:1)
Hard disk 3	100 GB | SCSI(1:0)
Hard disk 4	1024 GB | SCSI(2:0)
Hard disk 5	250 GB | SCSI(3:0)
SCSI controller 0	VMware Paravirtual
SCSI controller 1	VMware Paravirtual
SCSI controller 2	VMware Paravirtual
SCSI controller 3	VMware Paravirtual

FIGURE 34. VM Oracle19c-OL8 VMDKs

VMKD details:

- Hard Disk 1 – 80GB for operating system
- Hard Disk 2 – 80GB for Oracle Grid and RDBMS binaries
- Hard Disk 3 – 100GB for Oracle Grid Infrastructure Management Repository (GIMR) (Management Database (MGMTDB)) (ASM Disk Group MGMT_DATA)
- Hard Disk 4 – 1TB for database **vvol19c** data and redo log files (ASM Disk Group DATA_DG)
- Hard Disk 5 – 250GB for database **vvol19c** archive logs files (ASM Disk Group FRA_DG)

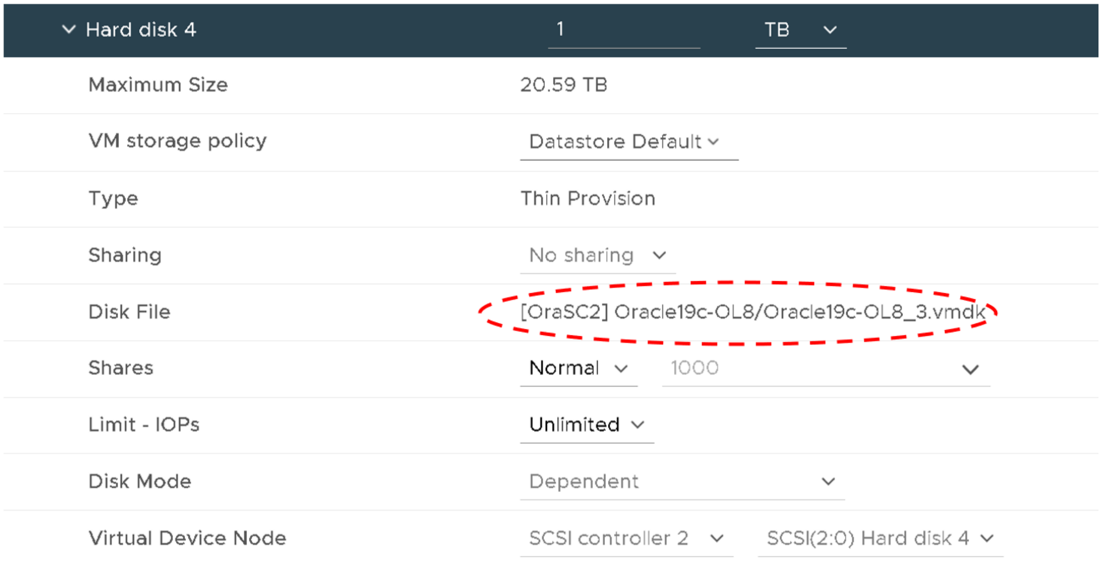
Oracle ASM disk group details:



```
grid@oracle19c-ol8-vvol:+ASM:/home/grid> asmcmd lsdg
State    Type    Rebal  Sector  Logical_Sector  Block       AU  Total_MB  Free_MB  Req_mir_free_MB  Usable_file_MB  Offline_disks  Voting_files  Name
MOUNTED  EXTERN  N         512             512   4096  1048576   1048575  1036823                0         1036823              0             N  DATA_DG/
MOUNTED  EXTERN  N         512             512   4096  1048576    255999   253761                0          253761              0             N  FRA_DG/
MOUNTED  EXTERN  N         512             512   4096  4194304    102396   102296                0          102296              0             N  MGMT_DATA/
grid@oracle19c-ol8-vvol:+ASM:/home/grid>
```

FIGURE 35. Oracle ASM Disk Group

Hard Disk 4 (1TB) details are shown below:



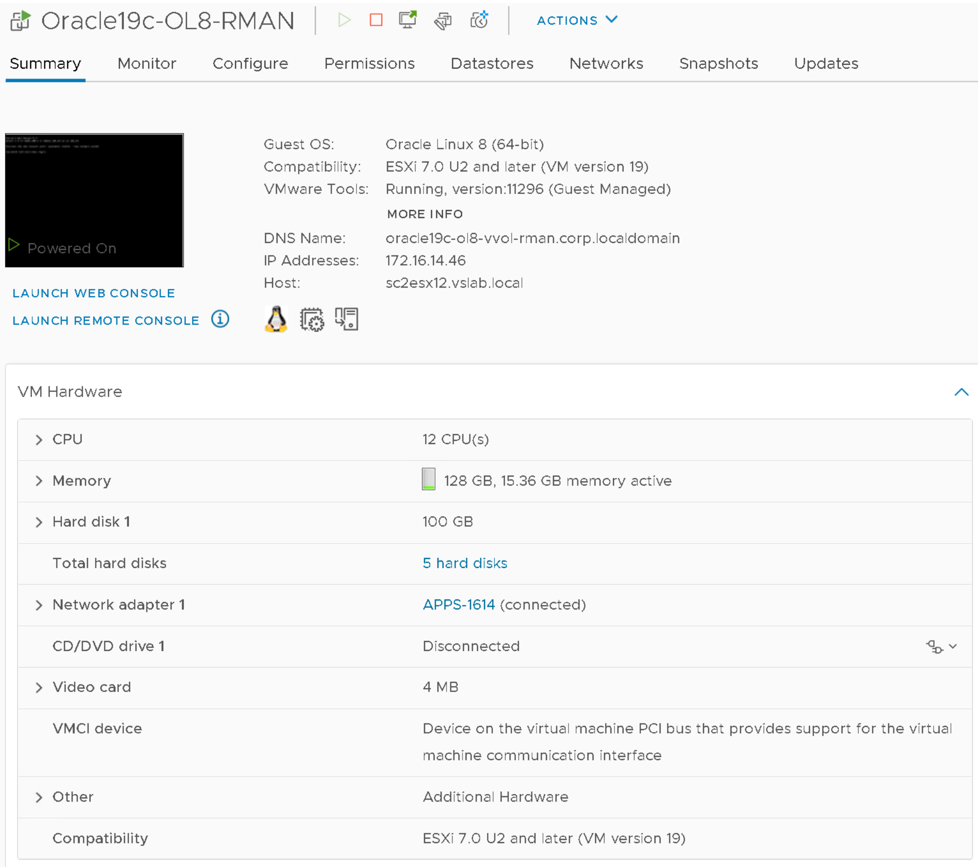
Hard disk 4	1 TB
Maximum Size	20.59 TB
VM storage policy	Datastore Default
Type	Thin Provision
Sharing	No sharing
Disk File	[OraSC2] Oracle19c-OL8/Oracle19c-OL8_3.vmdk
Shares	Normal 1000
Limit - IOPs	Unlimited
Disk Mode	Dependent
Virtual Device Node	SCSI controller 2 SCSI(2:0) Hard disk 4

FIGURE 36. Hard Disk 4 (1TB)

VM **Oracle19c-OL8-RMAN** details are as follows:

- 12 vCPUs with 128GB RAM
- Oracle SGA set to 96GB with traditional HugePages and PGA set to 6GB
- VM hosts both Oracle Grid and RDBMS 19.8 multi-tenant production database **rmandb** with a pluggable database **pdb1** for Oracle RMAN catalog purpose and an xfs file system **/rman** for holding Oracle RMAN backups
- 2 ASM disks groups
  - MGMT_DATA for Oracle Grid Infrastructure Management Repository (GIMR) with ASM disk **MGMT_DATA01**
  - RMAN_DATA_DG for data, redo log files and archive log files with ASM disk **RMAN_DATA_01**
- VM network adapter is connected to port group **APPS-1614** and assigned an IP address 172.16.14.46

All Oracle on VMware platform best practices were followed as outlined in *VMware Hybrid Cloud Best Practices Guide for Oracle Workloads*.

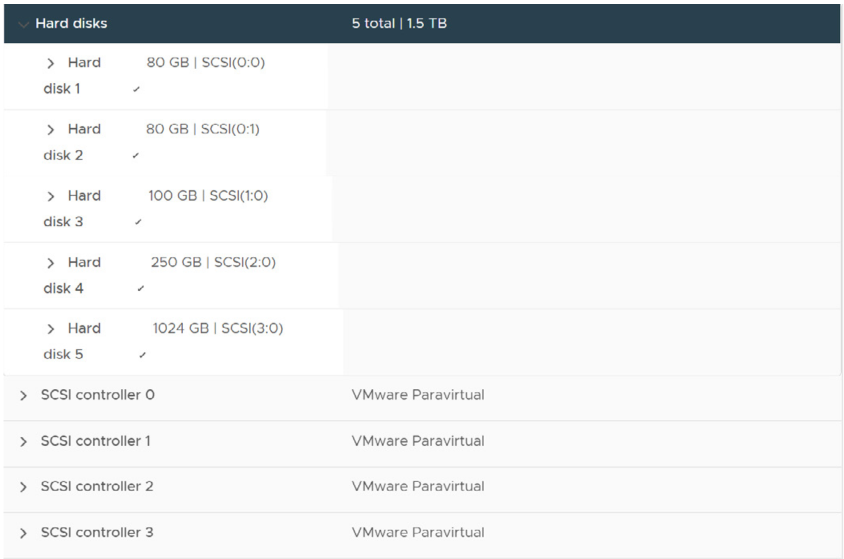


Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.16.14.46
Host: sc2esx12.vslab.local

CPU	12 CPU(s)
Memory	128 GB, 15.36 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 37. VM Oracle19c-OL8-RMAN Summary

VM **Oracle19c-OL8-RMAN** VMDKs are shown below. All SCSI controllers are set to **VMware Paravirtual SCSI Controller** type.



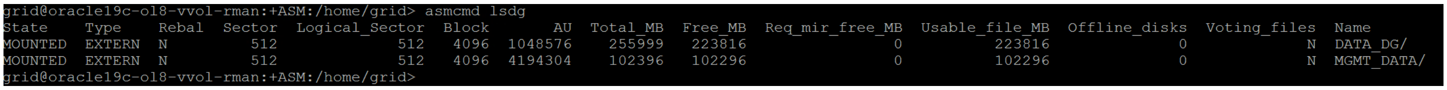
Hard disks	5 total | 1.5 TB
Hard disk 1	80 GB | SCSI(0:0) ✓
Hard disk 2	80 GB | SCSI(0:1) ✓
Hard disk 3	100 GB | SCSI(1:0) ✓
Hard disk 4	250 GB | SCSI(2:0) ✓
Hard disk 5	1024 GB | SCSI(3:0) ✓
SCSI controller 0	VMware Paravirtual
SCSI controller 1	VMware Paravirtual
SCSI controller 2	VMware Paravirtual
SCSI controller 3	VMware Paravirtual

FIGURE 38. VM Oracle19c-OL8-RMAN VMDKs

VMDK details:

- Hard Disk 1 - 80GB for operating system
- Hard Disk 2 - 80GB for Oracle Grid and RDBMS binaries
- Hard Disk 3 - 100GB for Oracle Grid Infrastructure Management Repository (GIMR) (Management Database (MGMTDB)) (ASM Disk Group MGMT_DATA)
- Hard Disk 4 – 250GB for Oracle Database **rmandb** database, redo log and archive log files (ASM Disk Group DATA_DG)
- Hard Disk 5 – 1TB for XFS filesystem **/rman** mount point for storing physical RMAN backups

Oracle ASM disk group details:



```
grid@oracle19c-ol8-vvol-rman:+ASM:/home/grid> asmcmd lsdg
State    Type    Rebal  Sector  Logical_Sector  Block       AU  Total_MB  Free_MB  Req_mir_free_MB  Usable_file_MB  Offline_disks  Voting_files  Name
MOUNTED  EXTERN  N         512             512   4096  1048576    255999   223816                0          223816              0             N  DATA_DG/
MOUNTED  EXTERN  N         512             512   4096  4194304    102396   102296                0          102296              0             N  MGMT_DATA/
grid@oracle19c-ol8-vvol-rman:+ASM:/home/grid>
```

FIGURE 39. Oracle ASM Disk Group

A two-node Oracle RAC was created on Site A as follows:

- VM prac19c1
- VM prac19c2

The basic steps for a RAC deployment on VMware can be found in
Oracle VMware Hybrid Cloud High Availability Guide Reference Architecture.

For simplicity, and for sake of illustration, the RAC cluster was created with one shared VMDK.

Storage for the Oracle RAC **prac19c** VMs was provisioned on the VMFS datastore **OraSC2** for all use cases except storage-based replication using vSphere Virtual Volumes. Oracle RAC **prac19c** VMs were provisioned on the vSphere Virtual Volumes datastore **OraVVOL**.

The use cases for application-based replication and VMware-based replication (VMware Site Recovery Manager with VMware vSphere Replication) can be applied to virtual machines with storage on any VMware datastore (NFS, VMFS, vSAN, vSphere Virtual Volumes).

Details of Oracle RAC VMs **prac19c1** and **prac19c2** are as follows:

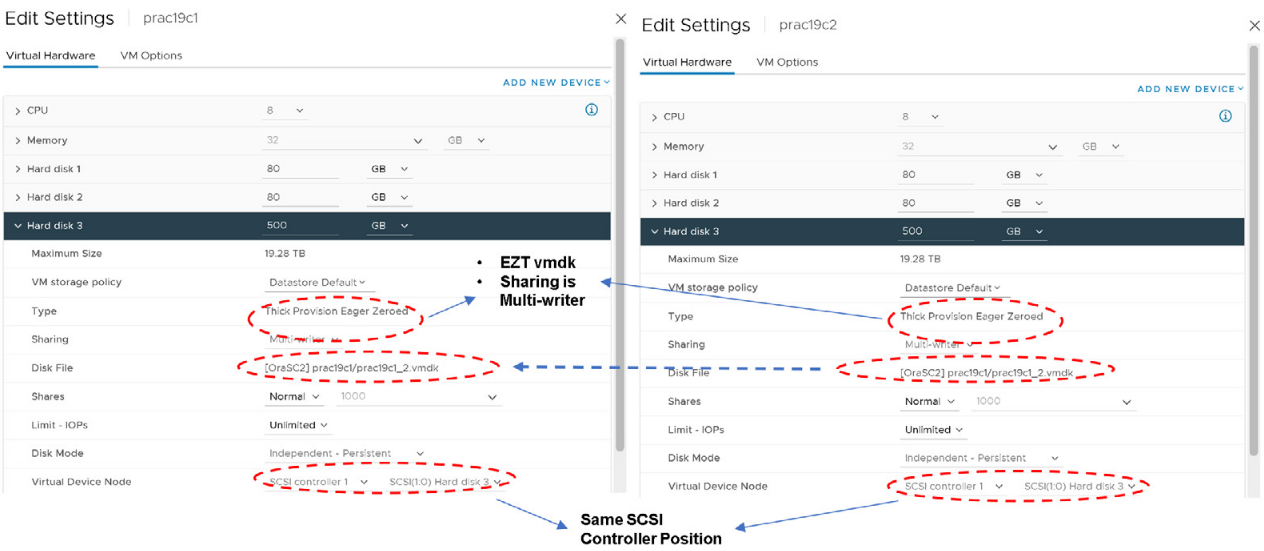
- 12 vCPUs with 128GB RAM
- Oracle SGA set to 96GB with traditional HugePages and PGA set to 6GB
- VM hosts both Oracle Grid and RDBMS 19.8 multi-tenant production database **vvol19c** with a pluggable database **pdb1**
- For purposes of simplicity and illustration, one ASM disk group was created (**DATA_DG**) housing all data files, control files, redo log files, archive log files, CRS and vote disks.
- Separate ASM disk groups are recommended for the RAC and database components as a best practice. Refer to *Oracle VMware Hybrid Cloud High Availability Guide* for more information.
- VM prac19c1 public network adapter is connected to port group **APPS-1614** and assigned an IP address 172.16.14.191. The private network adapter is connected to port group **APPS-1605** and assigned an IP address 192.168.14.191
- VM prac19c2 public network adapter is connected to port group **APPS-1614** and assigned an IP address 172.16.14.192. The private network adapter is connected to port group **APPS-1605** and assigned an IP address 192.168.14.192

All Oracle on VMware platform best practices were followed as described in
VMware Hybrid Cloud Best Practices Guide for Oracle Workloads.

Oracle RAC **prac19c** VM's VMDKs are shown below. All SCSI controllers are set to **VMware Paravirtual SCSI Controller** type:

- Two non-shared VMDKs
  - – Hard Disk 1 80GB for Operating System with disk mode **Dependent**
  - – Hard Disk 1 80GB for Oracle Grid Infrastructure and RDBMS binaries with disk mode **Dependent**
- One shared VMDK (500 GB) with multi-writer attribute and disk mode **Independent-Persistent** for RAC cluster

Details of the shared VMDK with **multi-writer flag** and disk mode **Independent-Persistent** are shown below:



Edit Settings | prac19c1

Virtual Hardware | VM Options

CPU	8	
Memory	32	GB
Hard disk 1	80	GB
Hard disk 2	80	GB
Hard disk 3	500	GB
Maximum Size	19.28 TB	
VM storage policy	Datastore Default	
Type	Thick Provision Eager Zeroed	
Sharing	Multi-writer	
Disk File	[OraSC2] prac19c1/prac19c1_2.vmdk	
Shares	Normal	1000
Limit - IOPs	Unlimited	
Disk Mode	Independent - Persistent	
Virtual Device Node	SCSI controller 1	SCSI(1:0) Hard disk 3

Edit Settings | prac19c2

Virtual Hardware | VM Options

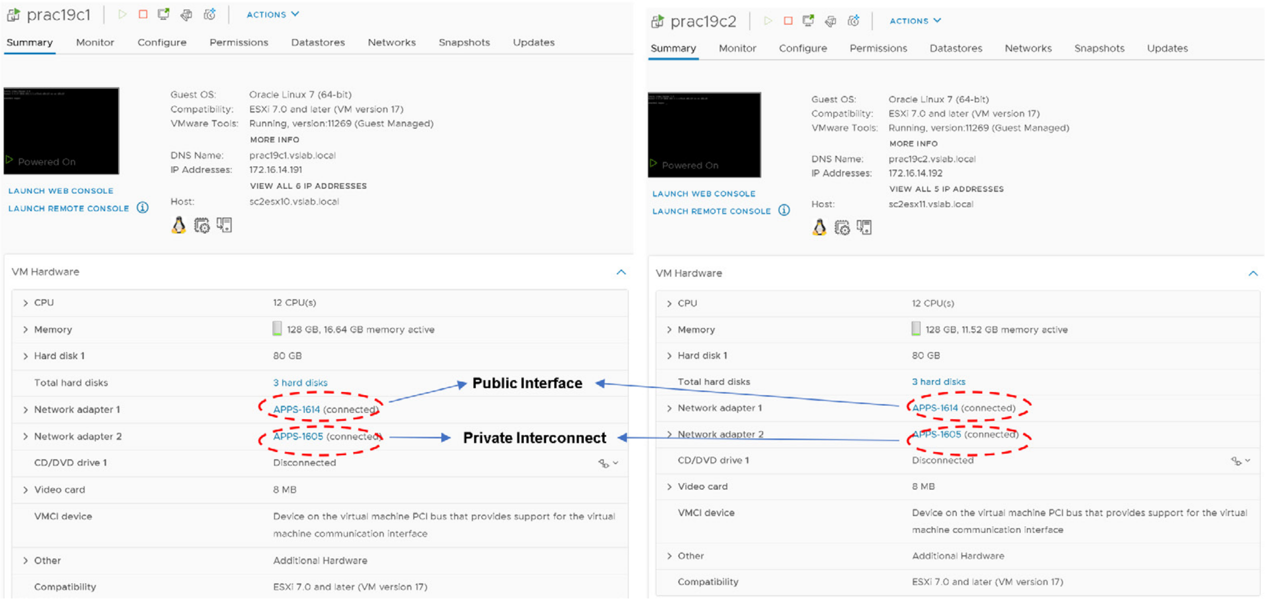
CPU	8	
Memory	32	GB
Hard disk 1	80	GB
Hard disk 2	80	GB
Hard disk 3	500	GB
Maximum Size	19.28 TB	
VM storage policy	Datastore Default	
Type	Thick Provision Eager Zeroed	
Sharing	Multi-writer	
Disk File	[OraSC2] prac19c1/prac19c1_2.vmdk	
Shares	Normal	1000
Limit - IOPs	Unlimited	
Disk Mode	Independent - Persistent	
Virtual Device Node	SCSI controller 1	SCSI(1:0) Hard disk 3

FIGURE 40. Oracle RAC prac19c Shared VMDK Details

Details of the RAC public network and private interconnect are shown below:

SERVER	prac19c1	prac19c2	PORTGROUP
IP	172.16.14.191	172.16.14.192	
Public FDQN	prac19c1.vslab.local	prac19c2.vslab.local	APPS-1614
Public IP	172.16.14.191	172.16.14.192	
Private FDQN	prac19c1-priv1.vslab.local	prac19c2-priv1.vslab.local	APPS-1605
Private IP	192.168.14.191	192.168.14.192	
VIP FDQN	prac19c1-vip.vslab.local	prac19c2-vip.vslab.local	APPS-1605
VIP IP	172.16.14.193	172.16.14.194	
SCAN	prac19c-scan.vslab.local		
	172.16.14.195		
	172.16.14.196		
	172.16.14.197		

TABLE 6. Oracle RAC Public and Private Network Details



prac19c1

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.16.14.191
Host: sc2esx10.vslab.local

CPU	12 CPU(s)
Memory	128 GB, 16.64 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

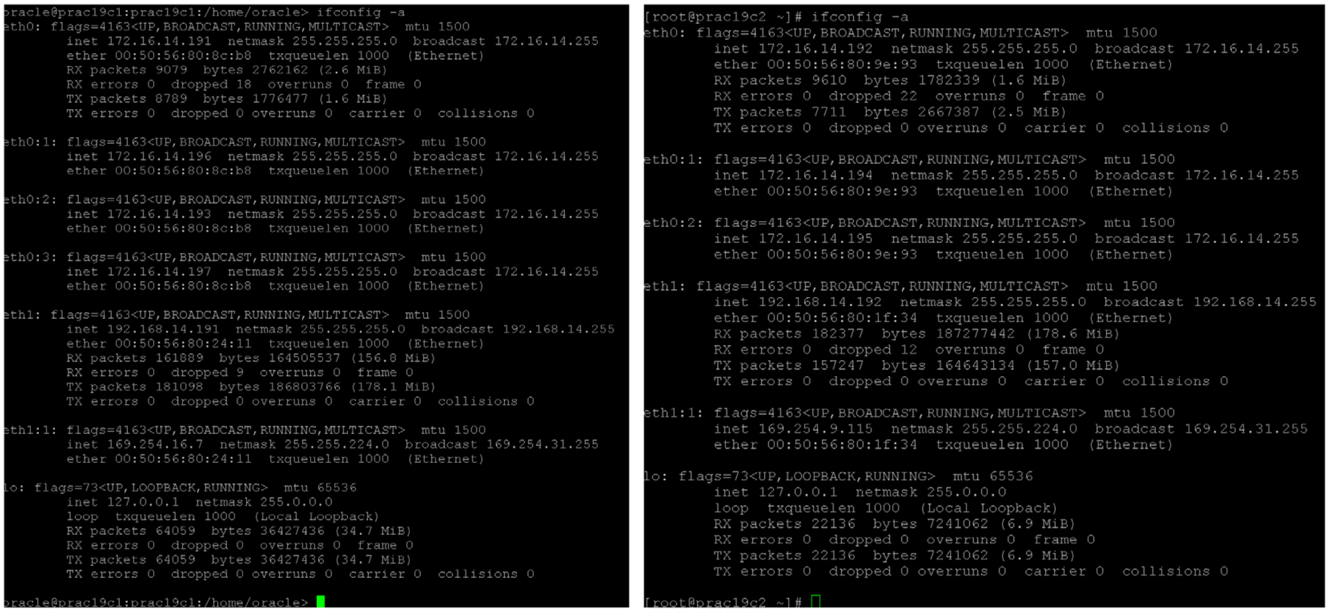
prac19c2

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.16.14.192
Host: sc2esx11.vslab.local

CPU	12 CPU(s)
Memory	128 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 41. Oracle RAC prac19c Public Network and Private Interconnect

Details of the RAC public network, private interconnect, VIP and HAIP IP address are shown below:

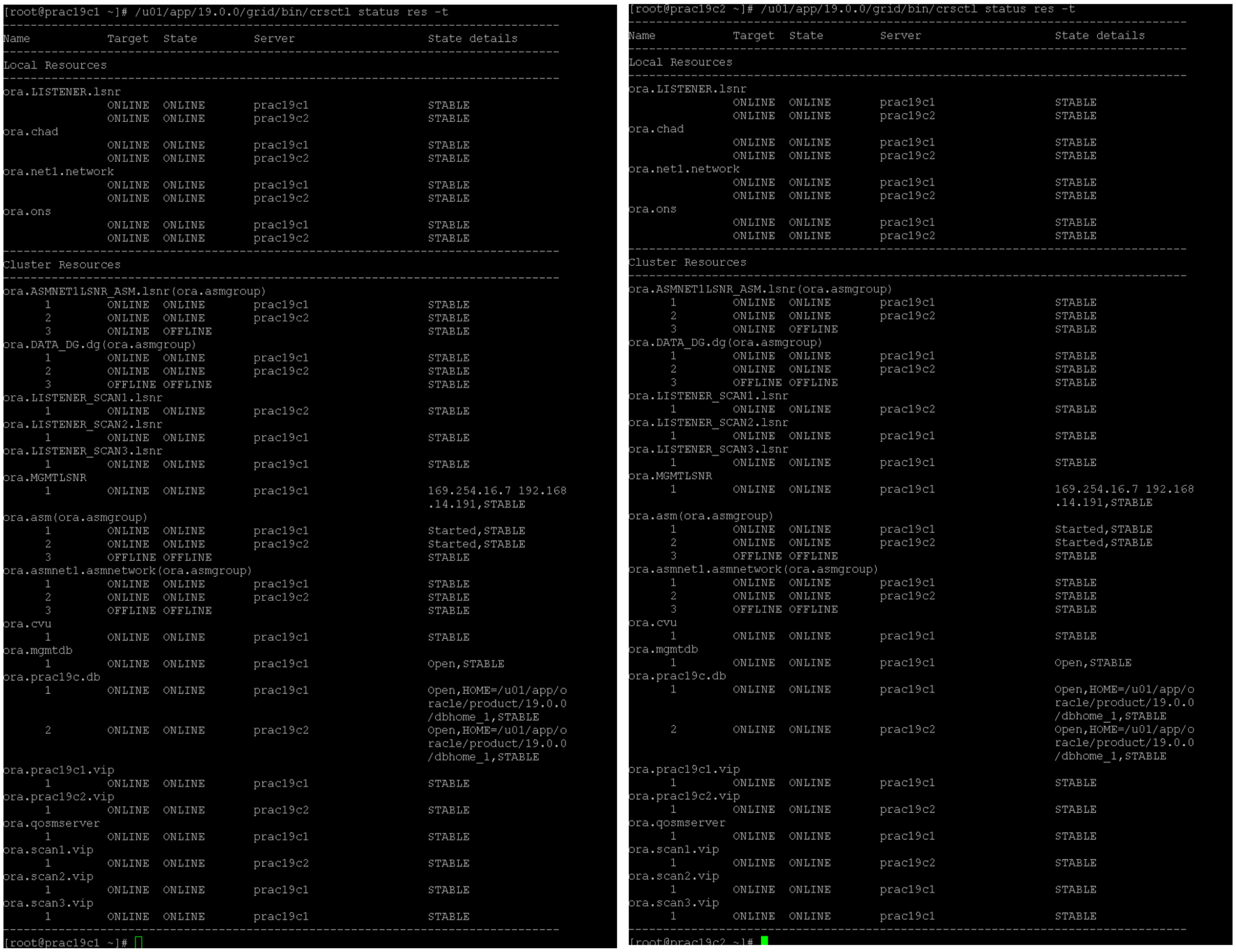


```
oracle@prac19c1:prac19c1:/home/oracle> ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.191  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:8c:b8  txqueuelen 1000  (Ethernet)
        RX packets 9079  bytes 2762162 (2.6 MiB)
        RX errors 0  dropped 18  overruns 0  frame 0
        TX packets 8789  bytes 1776477 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.196  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:8c:b8  txqueuelen 1000  (Ethernet)

eth0:2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.193  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:8c:b8  txqueuelen 1000  (Ethernet)

eth0:3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.197  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:8c:b8  txqueuelen 1000  (Ethernet)

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.14.191  netmask 255.255.255.0  broadcast 192.168.14.255
        ether 00:50:56:80:24:11  txqueuelen 1000  (Ethernet)
        RX packets 161889  bytes 164505537 (156.8 MiB)
        RX errors 0  dropped 9  overruns 0  frame 0
        TX packets 181098  bytes 186803766 (178.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 169.254.16.7  netmask 255.255.224.0  broadcast 169.254.31.255
        ether 00:50:56:80:24:11  txqueuelen 1000  (Ethernet)

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 64059  bytes 36427436 (34.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64059  bytes 36427436 (34.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

oracle@prac19c1:prac19c1:/home/oracle>
```

```
[root@prac19c2 ~]# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.192  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:9e:93  txqueuelen 1000  (Ethernet)
        RX packets 9610  bytes 1782339 (1.6 MiB)
        RX errors 0  dropped 22  overruns 0  frame 0
        TX packets 7711  bytes 2667387 (2.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.194  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:9e:93  txqueuelen 1000  (Ethernet)

eth0:2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.14.195  netmask 255.255.255.0  broadcast 172.16.14.255
        ether 00:50:56:80:9e:93  txqueuelen 1000  (Ethernet)

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.14.192  netmask 255.255.255.0  broadcast 192.168.14.255
        ether 00:50:56:80:1f:34  txqueuelen 1000  (Ethernet)
        RX packets 182377  bytes 187277442 (178.6 MiB)
        RX errors 0  dropped 12  overruns 0  frame 0
        TX packets 157247  bytes 164643134 (157.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1:1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 169.254.9.115  netmask 255.255.224.0  broadcast 169.254.31.255
        ether 00:50:56:80:1f:34  txqueuelen 1000  (Ethernet)

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 22136  bytes 7241062 (6.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22136  bytes 7241062 (6.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@prac19c2 ~]#
```

FIGURE 42. Oracle RAC prac19c Networking Details

Details of the RAC cluster services are shown below:



```
[root@prac19c1 ~]# /u01/app/19.0.0/grid/bin/crsctl status res -t
--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.LISTENER.lsnr
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.chad
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.net1.network
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.ons
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.ASMNET1LSNR_ASM.lsnr(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        ONLINE  OFFLINE                               STABLE
ora.DATA_DG.dg(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.LISTENER_SCAN1.lsnr
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.LISTENER_SCAN2.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.LISTENER_SCAN3.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.MGMTLSNR
      1        ONLINE  ONLINE       prac19c1                 169.254.16.7 192.168
                                                             .14.191,STABLE
ora.asm(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 Started,STABLE
      2        ONLINE  ONLINE       prac19c2                 Started,STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.asmnet1.asmnetwork(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.cvu
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.mgmtdb
      1        ONLINE  ONLINE       prac19c1                 Open,STABLE
ora.prac19c.db
      1        ONLINE  ONLINE       prac19c1                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
      2        ONLINE  ONLINE       prac19c2                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
ora.prac19c1.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.prac19c2.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.qosmserver
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan1.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.scan2.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan3.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
--------------------------------------------------------------------------------
[root@prac19c1 ~]#
```

```
[root@prac19c2 ~]# /u01/app/19.0.0/grid/bin/crsctl status res -t
--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.LISTENER.lsnr
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.chad
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.net1.network
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.ons
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.ASMNET1LSNR_ASM.lsnr(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        ONLINE  OFFLINE                               STABLE
ora.DATA_DG.dg(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.LISTENER_SCAN1.lsnr
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.LISTENER_SCAN2.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.LISTENER_SCAN3.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.MGMTLSNR
      1        ONLINE  ONLINE       prac19c1                 169.254.16.7 192.168
                                                             .14.191,STABLE
ora.asm(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 Started,STABLE
      2        ONLINE  ONLINE       prac19c2                 Started,STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.asmnet1.asmnetwork(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.cvu
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.mgmtdb
      1        ONLINE  ONLINE       prac19c1                 Open,STABLE
ora.prac19c.db
      1        ONLINE  ONLINE       prac19c1                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
      2        ONLINE  ONLINE       prac19c2                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
ora.prac19c1.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.prac19c2.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.qosmserver
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan1.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.scan2.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan3.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
--------------------------------------------------------------------------------
[root@prac19c2 ~]#
```

FIGURE 43. Oracle RAC prac19c Cluster Services

For the Oracle Data Guard use case, two VMs were created with one VM on Site A and one VM on Site B as follows:

- VM **Oracle19c-OL8-Primary** on Site A with IP address 172.16.14.50
- VM **Oracle19c-OL8-Standby** on Site B with IP address 172.16.14.51

Each VM was created with the following tools or characteristics:

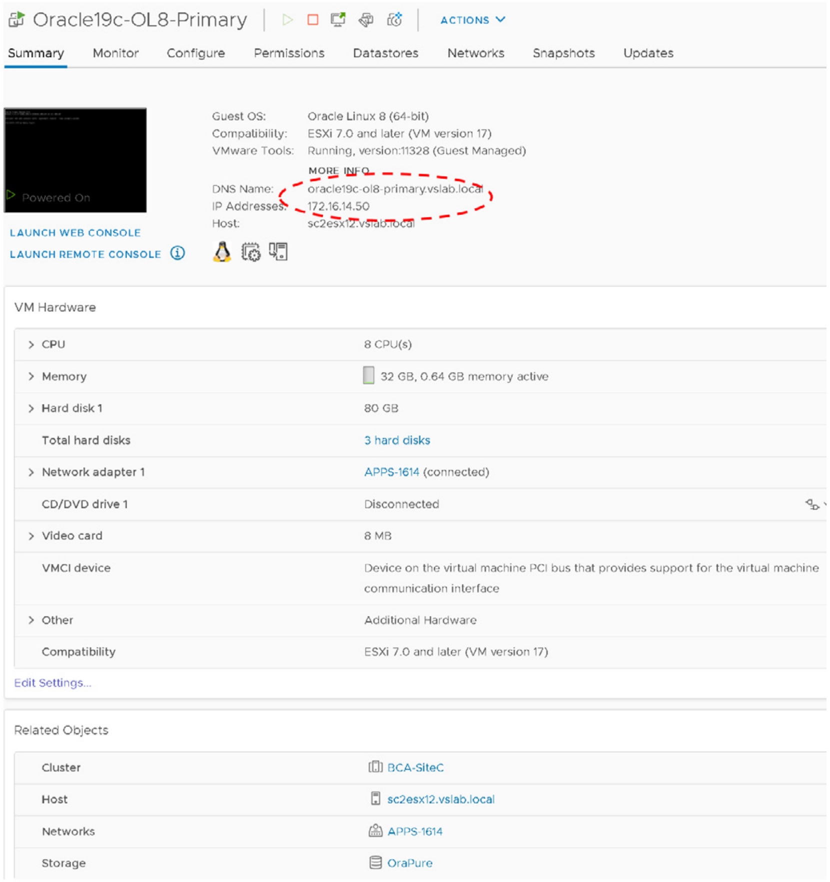
- VM version 19 on ESXi 7.0 U2
- Guest operating system Oracle Enterprise Linux 8.3 UEK
- Oracle Grid and RDBMS binaries version 19.12
- For sake of simplicity and illustration, one ASM disk group was created called DATA_DG which houses all the data files, control files, redo log files and archive log files. Creating separate ASM disk groups for these components is recommended as a best practice.

Storage for VM **Oracle19c-OL8-Primary** was provisioned on the VMFS datastore **OraPure**. Storage for VM **Oracle19c-OL8-Standby** was provisioned on the NFS datastore **AZ2-TINTRI-EC6090**.

Details for VM **Oracle19c-OL8-Primary** are as follows:

- 8 vCPUs with 32 GB RAM
- Oracle SGA set to 16B with traditional HugePages and PGA set to 6GB
- VM hosts both Oracle Grid and RDBMS 19.12 multi-tenant production database **ora19c** with a pluggable database **pdb1**
- For the sake of simplicity and illustration, one ASM disk group was created called DATA_DG which houses all the datafiles, control files, redo log files and archive log files. Creating separate ASM disk groups for these components is recommended as a best practice.
- VM network adapter is connected to port group **APPS-1614** and assigned an IP address 172.16.14.50

All Oracle on VMware platform best practices were followed as described in *VMware Hybrid Cloud Best Practices Guide for Oracle Workloads*.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11328 (Guest Managed)
DNS Name: oracle19c-ol8-primary.vslab.local
IP Addresses: 172.16.14.50
Host: sc2esx12.vslab.local

VM Hardware

> CPU	8 CPU(s)
> Memory	32 GB, 0.64 GB memory active
> Hard disk 1	80 GB
Total hard disks	3 hard disks
> Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
> Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
> Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Related Objects

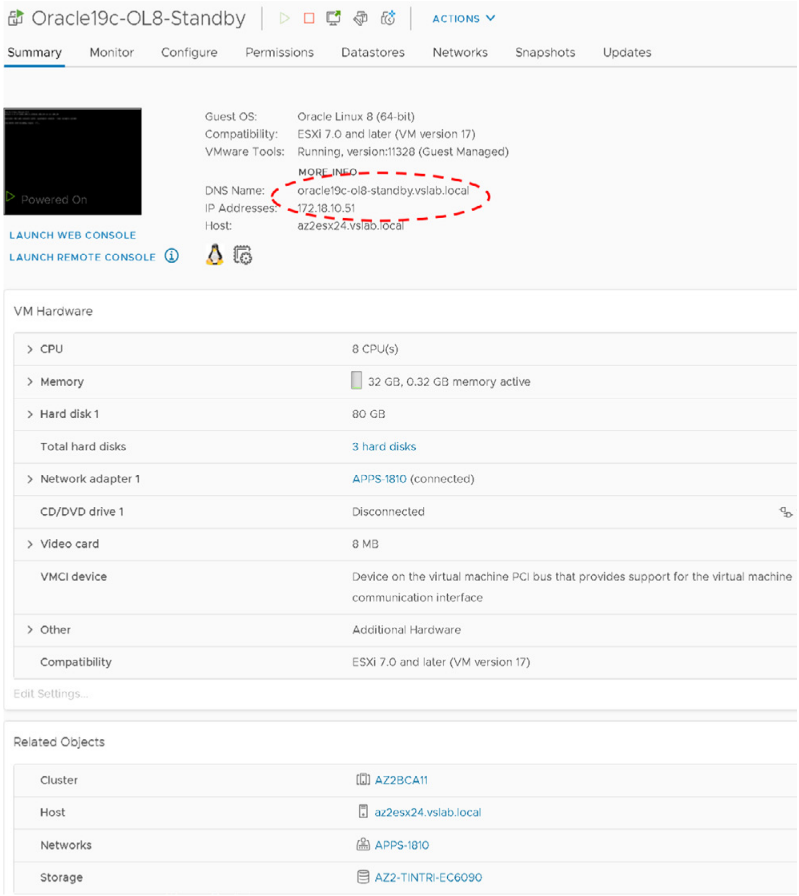
Cluster	BCA-SiteC
Host	sc2esx12.vslab.local
Networks	APPS-1614
Storage	OraPure

FIGURE 44. Primary Database VM Oracle19C-OL8-Primary

Details of VM **Oracle19c-OL8-Standby** are as follows:

- 8 vCPUs with 32 GB RAM
- Oracle SGA set to 16B with traditional HugePages and PGA set to 6GB
- VM hosts both Oracle Grid and RDBMS 19.12 multi-tenant standby production database ora19c with a pluggable database **pdb1**
- For sake of simplicity and illustration, one ASM disk group was created called DATA_DG which houses all the datafiles, control files, redo log files and archive log files. Creating separate ASM disk groups for these components is recommended as a best practice.
- VM network adapter is connected to port group **APPS-1810** and assigned an IP address 172.18.10.51

All Oracle on VMware platform best practices were followed as outlined in *VMware Hybrid Cloud Best Practices Guide for Oracle Workloads*.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11328 (Guest Managed)
DNS Name: oracle19c-ol8-standby.vslab.local
IP Addresses: 172.18.10.51
Host: az2esx24.vslab.local

VM Hardware

CPU	8 CPU(s)
Memory	32 GB, 0.32 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

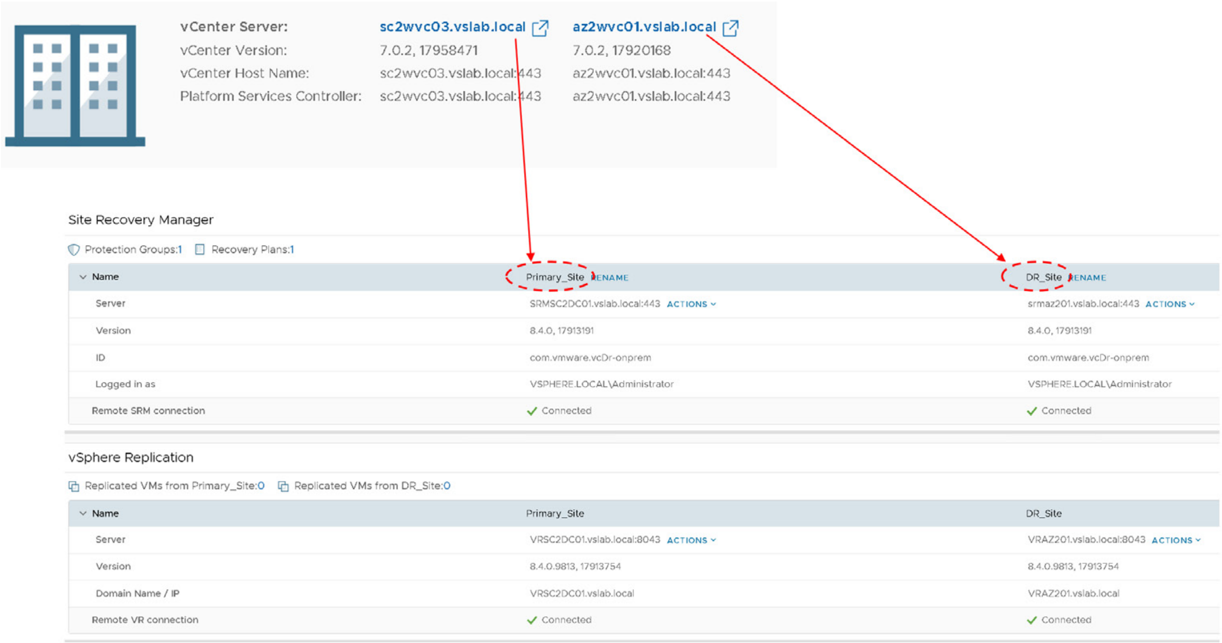
Related Objects

Cluster	AZ2BCA11
Host	az2esx24.vslab.local
Networks	APPS-1810
Storage	AZ2-TINTRI-EC6090

FIGURE 45. Physical Standby VM Oracle19C-OL8-Standby

VMware Site Recovery Manager with vSphere Replication and VMware Site Recovery Manager with Array Based Replication

The Site Recovery Manager and vSphere Replication Appliance information Site Pair Summary for Site A and Site B are as shown below:



vCenter Server:	sc2wvc03.vslab.local	az2wvc01.vslab.local
vCenter Version:	7.0.2, 17958471	7.0.2, 17920168
vCenter Host Name:	sc2wvc03.vslab.local:443	az2wvc01.vslab.local:443
Platform Services Controller:	sc2wvc03.vslab.local:443	az2wvc01.vslab.local:443

Site Recovery Manager

Protection Groups:1 Recovery Plans:1

Name	Primary_Site RENAME	DR_Site RENAME
Server	SRMSC2DC01.vslab.local:443 ACTIONS	srmaz201.vslab.local:443 ACTIONS
Version	8.4.0, 17913191	8.4.0, 17913191
ID	com.vmware.vcDr-onprem	com.vmware.vcDr-onprem
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

vSphere Replication

Replicated VMs from Primary_Site:0 Replicated VMs from DR_Site:0

Name	Primary_Site	DR_Site
Server	VRSC2DC01.vslab.local:8043 ACTIONS	VRAZ201.vslab.local:8043 ACTIONS
Version	8.4.0.9813, 17913754	8.4.0.9813, 17913754
Domain Name / IP	VRSC2DC01.vslab.local	VRAZ201.vslab.local
Remote VR connection	✓ Connected	✓ Connected

FIGURE 46. Site A and Site B Pairing Summary

The network mappings, folder mappings, resource mappings and placeholder datastore mappings must be setup for both use cases below:

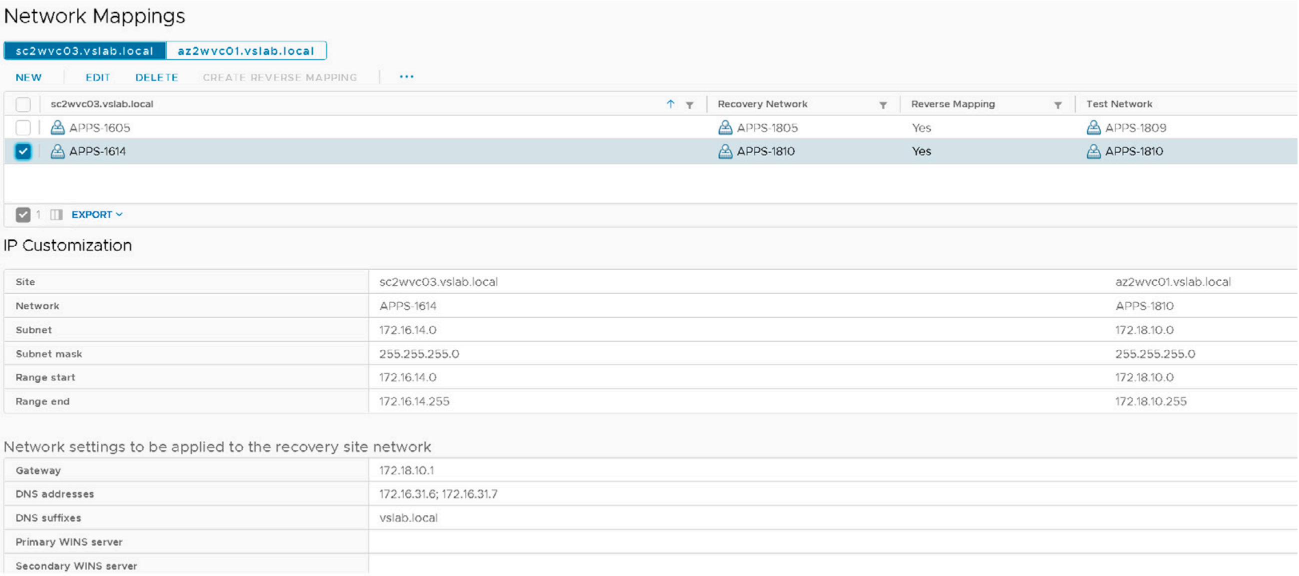
- Site Recovery Manager with vSphere Replication
- Site Recovery Manager with array-based replication (LUN OR vVOL level)

The network-mapping port groups between Site A and Site B is as shown below:

NETWORK	SOURCE SITE	PORT GROUP	DESTINATION SITE	DESTINATION TEST NETWORK	DESTINATION RECOVERY NETWORK
Public Network	Site A	APPS-1614	Site B	APPS-1810	APPS-1810
Private Interconnect	Site A	APPS-1605	Site B	APPS-1809	APPS-1805
Public Network	Site B	APPS-1810	Site A	APPS-1614	APPS-1614
Private Interconnect	Site B	APPS-1805	Site A	APPS-1605	APPS-1605

TABLE 7. Network-Mapping Details between Site A and Site B

The network-mapping for protected site public network **APPS-1614** to recovery site recovery network **APPS-1810** is as shown below. The recovery site test network is also **APPS-1810**.



Network Mappings

	sc2wvc03.vslab.local	Recovery Network	Reverse Mapping	Test Network
□	APPS-1605	APPS-1805	Yes	APPS-1809
☑	APPS-1614	APPS-1810	Yes	APPS-1810

☑ 1

IP Customization

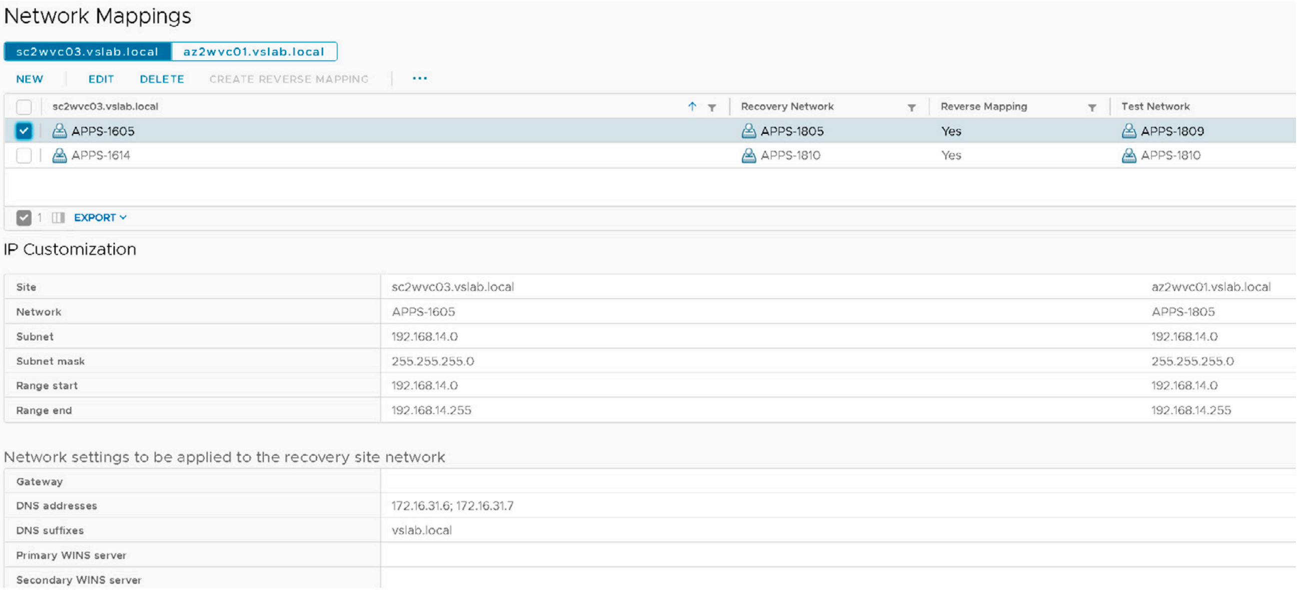
Site	sc2wvc03.vslab.local	az2wvc01.vslab.local
Network	APPS-1614	APPS-1810
Subnet	172.16.14.0	172.18.10.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	172.16.14.0	172.18.10.0
Range end	172.16.14.255	172.18.10.255

Network settings to be applied to the recovery site network

Gateway	172.18.10.1
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 47. Network Mapping Between Site A and Site B for Planned Recovery Use Case

The network mapping for protected site private interconnect network **APPS-1605** to recovery site recovery network **APPS-1805** is as shown below. The recovery site test network is **APPS-1809**.



Network Mappings

	sc2wvc03.vslab.local	Recovery Network	Reverse Mapping	Test Network
☑	APPS-1605	APPS-1805	Yes	APPS-1809
□	APPS-1614	APPS-1810	Yes	APPS-1810

☑ 1

IP Customization

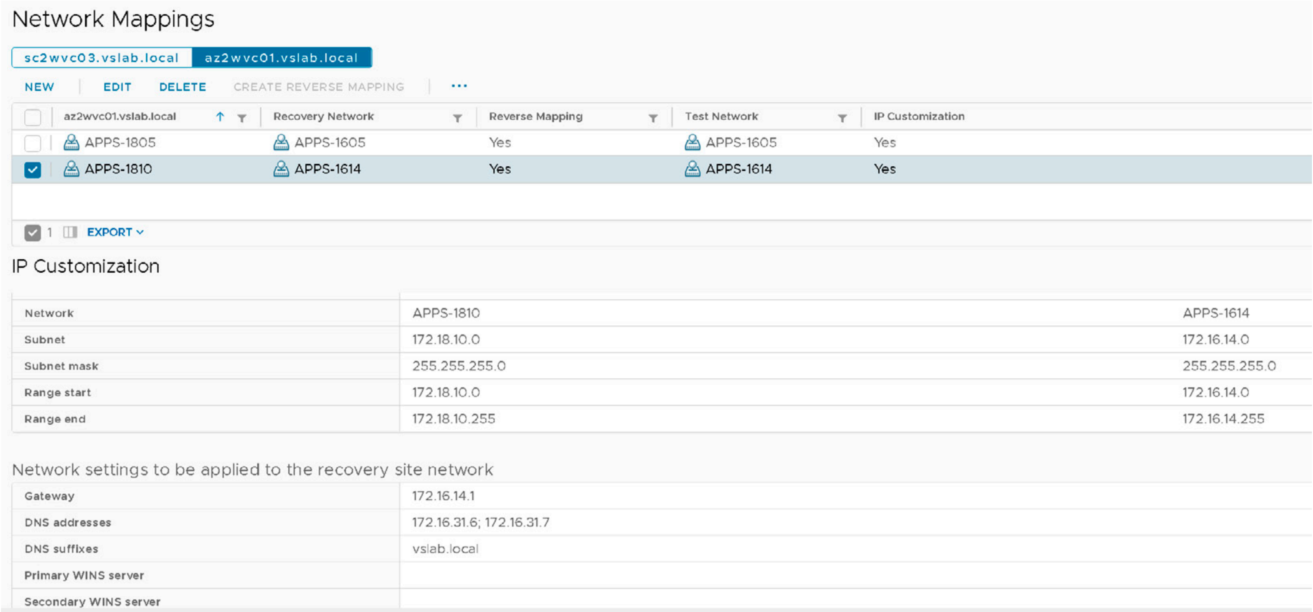
Site	sc2wvc03.vslab.local	az2wvc01.vslab.local
Network	APPS-1605	APPS-1805
Subnet	192.168.14.0	192.168.14.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	192.168.14.0	192.168.14.0
Range end	192.168.14.255	192.168.14.255

Network settings to be applied to the recovery site network

Gateway	
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 48. Network Mapping Between Site A and Site B for Test Recovery Use Case

The network mapping for recovery site public network **APPS-1810** to protected site recovery network **APPS-1614** is as shown below. The recovery site test network is **APPS-1614**.


Network Mappings

sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW | EDIT | DELETE | CREATE REVERSE MAPPING | ...

	az2wvc01.vslab.local	Recovery Network	Reverse Mapping	Test Network	IP Customization
□	APPS-1805	APPS-1605	Yes	APPS-1605	Yes
☑	APPS-1810	APPS-1614	Yes	APPS-1614	Yes

☑ 1 EXPORT

IP Customization

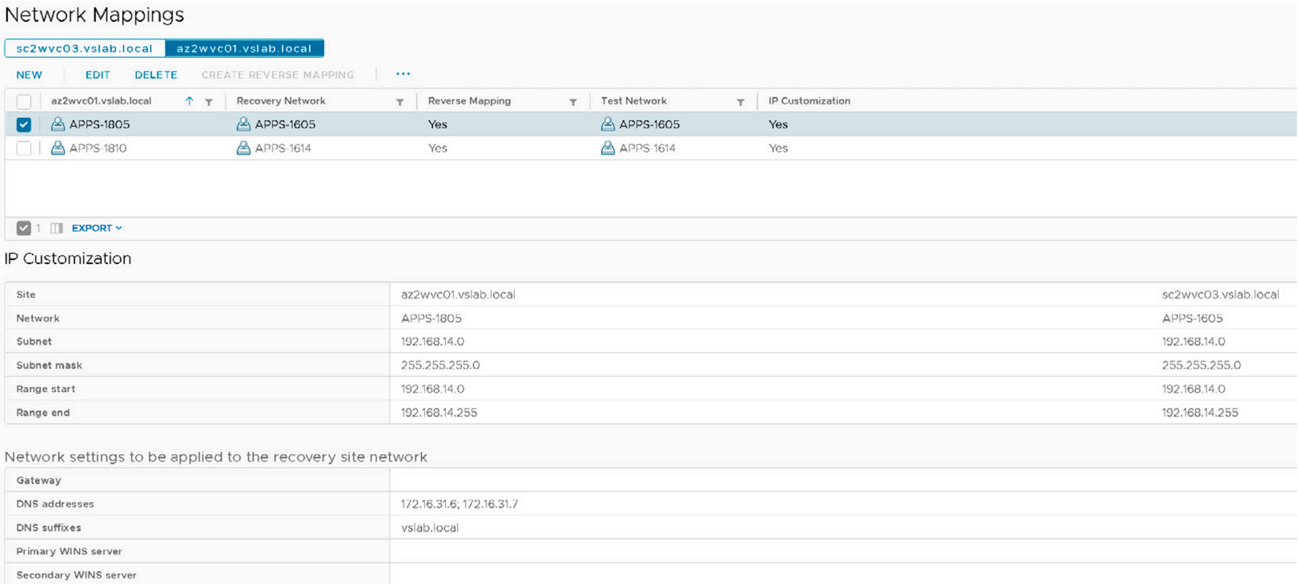
Network	APPS-1810	APPS-1614
Subnet	172.18.10.0	172.16.14.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	172.18.10.0	172.16.14.0
Range end	172.18.10.255	172.16.14.255

Network settings to be applied to the recovery site network

Gateway	172.16.14.1
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 49. Network Mapping Between Site B and Site A for Planned Recovery Use Case

The network mapping for recovery site private interconnect network **APPS-1805** to protected site recovery network **APPS-1605** is as shown below. The recovery site test network is **APPS-1605**.


Network Mappings

sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW | EDIT | DELETE | CREATE REVERSE MAPPING | ...

	az2wvc01.vslab.local	Recovery Network	Reverse Mapping	Test Network	IP Customization
☑	APPS-1805	APPS-1605	Yes	APPS-1605	Yes
□	APPS-1810	APPS-1614	Yes	APPS-1614	Yes

☑ 1 EXPORT

IP Customization

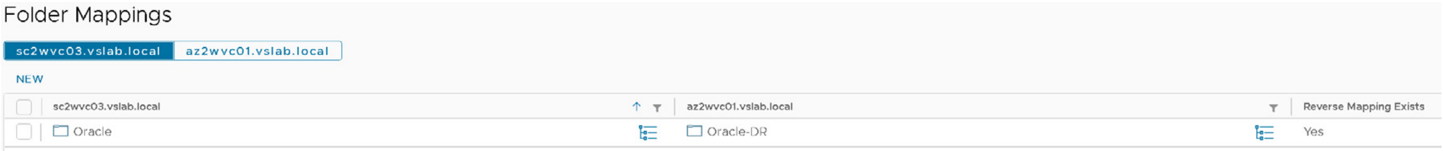
Site	az2wvc01.vslab.local	sc2wvc03.vslab.local
Network	APPS-1805	APPS-1605
Subnet	192.168.14.0	192.168.14.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	192.168.14.0	192.168.14.0
Range end	192.168.14.255	192.168.14.255

Network settings to be applied to the recovery site network

Gateway	
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 50. Network Mapping Between Site B and Site A for Test Recovery Use Case

The folder mapping from Site A to Site B is as shown below:



Folder Mappings

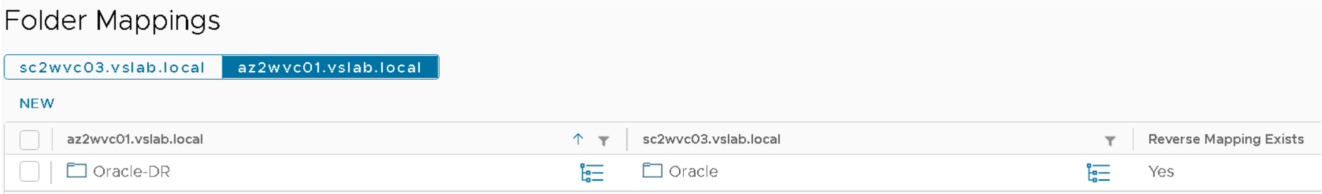
sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW

sc2wvc03.vslab.local	az2wvc01.vslab.local	Reverse Mapping Exists
Oracle	Oracle-DR	Yes

FIGURE 51. Folder Mappings from Site A to Site B

The folder mapping from Site B to Site A is as shown below:



Folder Mappings

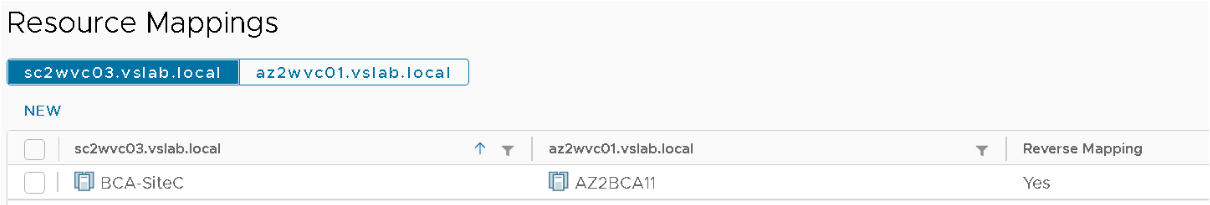
sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW

az2wvc01.vslab.local	sc2wvc03.vslab.local	Reverse Mapping Exists
Oracle-DR	Oracle	Yes

FIGURE 52. Folder Mappings from Site B to Site A

The resource mapping from Site A to Site B is as shown below:



Resource Mappings

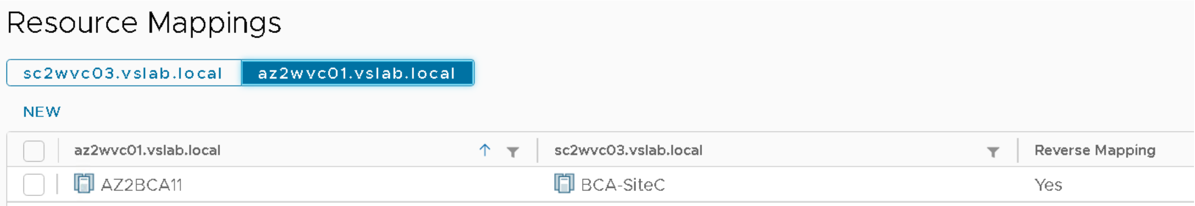
sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW

sc2wvc03.vslab.local	az2wvc01.vslab.local	Reverse Mapping
BCA-SiteC	AZ2BCA11	Yes

FIGURE 53. Resource Mappings from Site A to Site B

The resource mapping from Site B to Site A is as shown below:



Resource Mappings

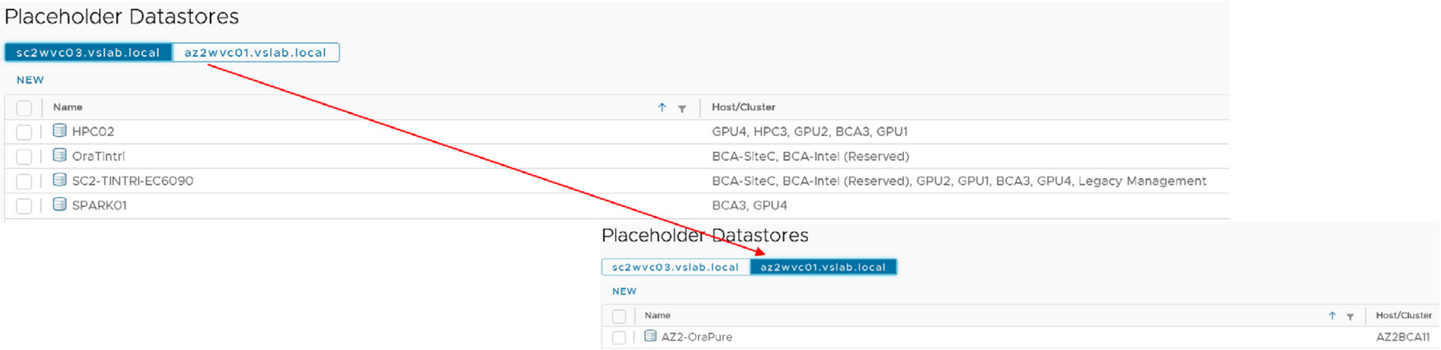
sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW

az2wvc01.vslab.local	sc2wvc03.vslab.local	Reverse Mapping
AZ2BCA11	BCA-SiteC	Yes

FIGURE 54. Resource Mappings from Site B to Site A

The placeholder datastore mapping between Site A and Site B is as shown below. The placeholder datastore on the recovery site is used by Site Recovery Manager to store placeholder VMs.



Placeholder Datastores

Name	Host/Cluster
HPC02	GPU4, HPC3, GPU2, BCA3, GPU1
OraTintri	BCA-SiteC, BCA-Intel (Reserved)
SC2-TINTRI-EC6090	BCA-SiteC, BCA-Intel (Reserved), GPU2, GPU1, BCA3, GPU4, Legacy Management
SPARK01	BCA3, GPU4

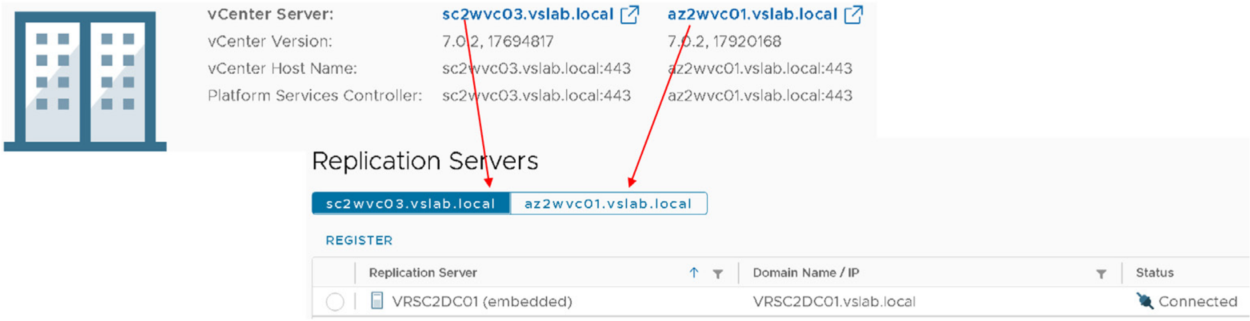
Placeholder Datastores

Name	Host/Cluster
AZ2-OraPure	AZ2BCA11

FIGURE 55. Placeholder Datastore Mappings between Site A and Site B

VMware Site Recovery Manager with vSphere Replication

The graphic below illustrates Site Recovery Manager and vSphere Replication setup between on-premises Site A and Site B:

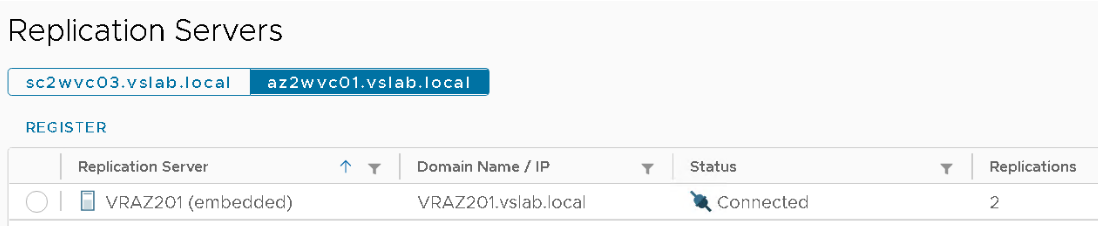


vCenter Server:	sc2wvc03.vslab.local	az2wvc01.vslab.local
vCenter Version:	7.0.2, 17694817	7.0.2, 17920168
vCenter Host Name:	sc2wvc03.vslab.local:443	az2wvc01.vslab.local:443
Platform Services Controller:	sc2wvc03.vslab.local:443	az2wvc01.vslab.local:443

Replication Servers

Replication Server	Domain Name / IP	Status
VRSC2DC01 (embedded)	VRSC2DC01.vslab.local	Connected

FIGURE 56. Site A Replication Server Details



Replication Servers

Replication Server	Domain Name / IP	Status	Replications
VRAZ201 (embedded)	VRAZ201.vslab.local	Connected	2

FIGURE 57. Site B Replication Server Details

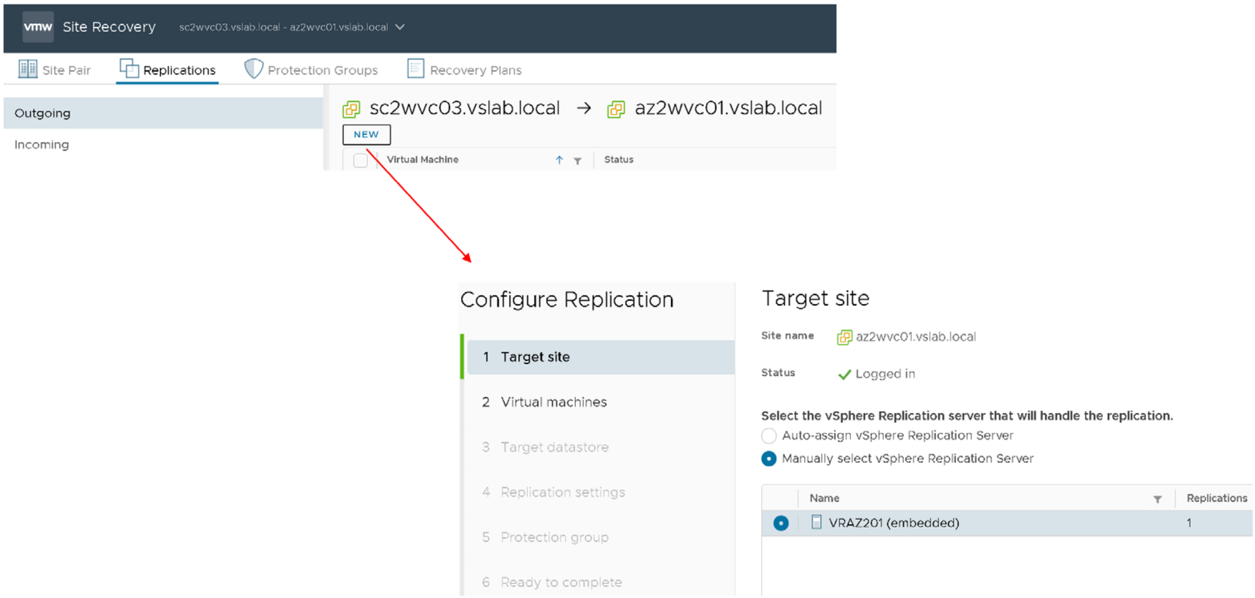
Site Recovery Manager and vSphere Replication pairings and IP addresses for on-premises and VMware Cloud on AWS are shown below:

COMPONENT	SOURCE SITE	APPLIANCE	DESTINATION SITE	APPLIANCE
SRM Appliance	Site A	SRMSC2DC01.vslab.local	Site B	SRMAZ01.vslab.local
IP Address		172.16.31.145		172.16.31.147
vSphere Replication Appliance	Site A	VRSC2DC01.vslab.local	Site B	VRAZ01.vslab.local
IP Address		172.16.31.144		172.16.31.146
SRM Appliance	Site A	SRMSC2DC03.vslab.local	VMware Cloud on AWS	srm.sddc-44-232-220-144.vmwarevmc.com
IP Address		172.16.31.149		10.129.224.24
vSphere Replication Appliance	Site A	VRSC2DC01.vslab.local	VMware Cloud on AWS	vr.sddc-44-232-220-144.vmwarevmc.com
IP Address		172.16.31.144		10.129.224.23

TABLE 8. VSPHERE REPLICATION NETWORK PAIRING DETAILS

Setup of Site Recovery Manager and vSphere Replication is beyond the scope of this paper.

The steps to configure replication are as shown below:



sc2wvc03.vslab.local → az2wvc01.vslab.local

Configure Replication

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Ready to complete

Target site

Site name: az2wvc01.vslab.local

Status: ✓ Logged in

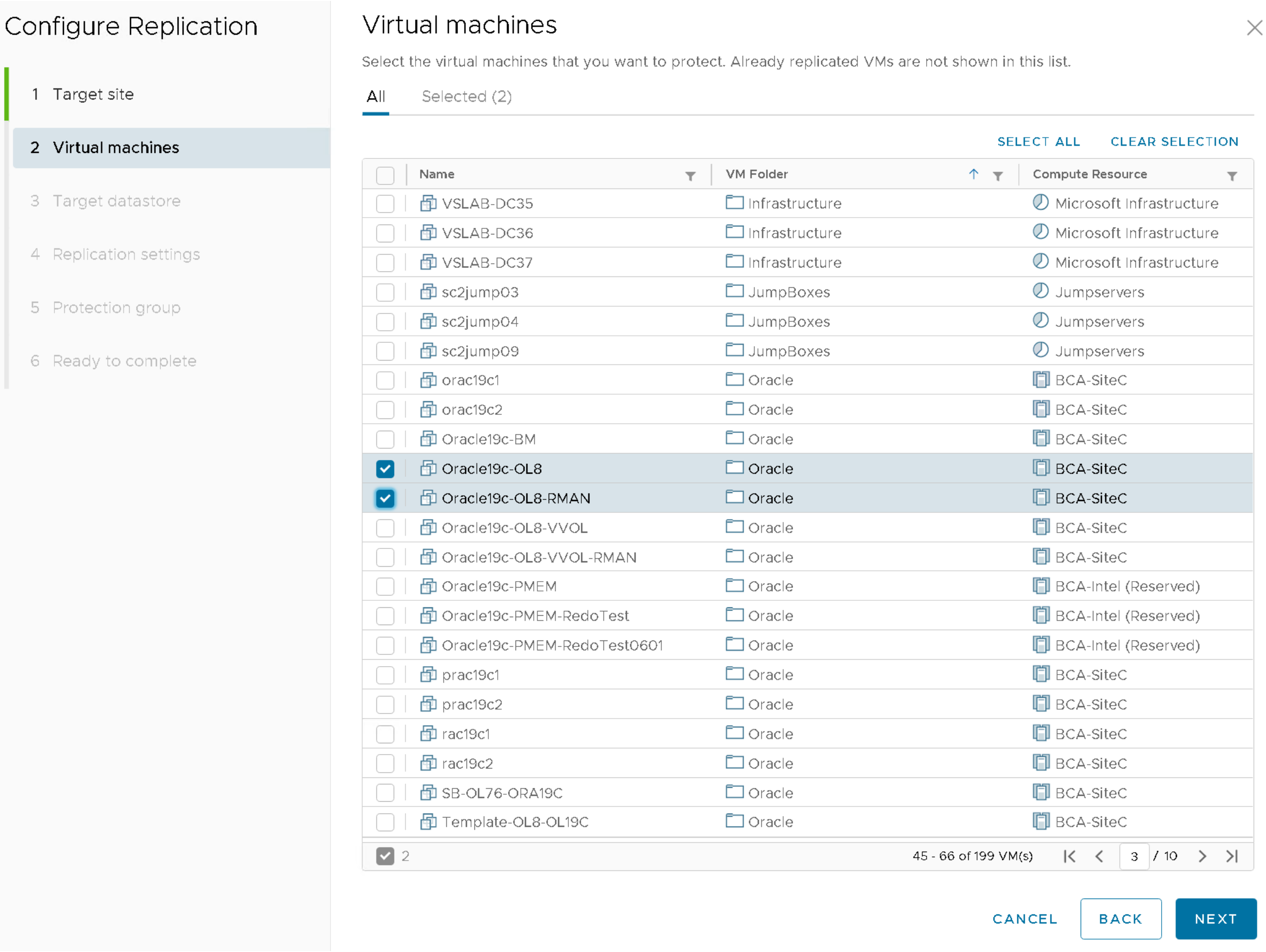
Select the vSphere Replication server that will handle the replication.

○ Auto-assign vSphere Replication Server
● Manually select vSphere Replication Server

	Name	Replications
●	VRAZ201 (embedded)	1

FIGURE 58. SITE A: Configure Replication Start Steps

Choose the VMs to protect.



Configure Replication

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Ready to complete

Virtual machines

Select the virtual machines that you want to protect. Already replicated VMs are not shown in this list.

All | Selected (2)

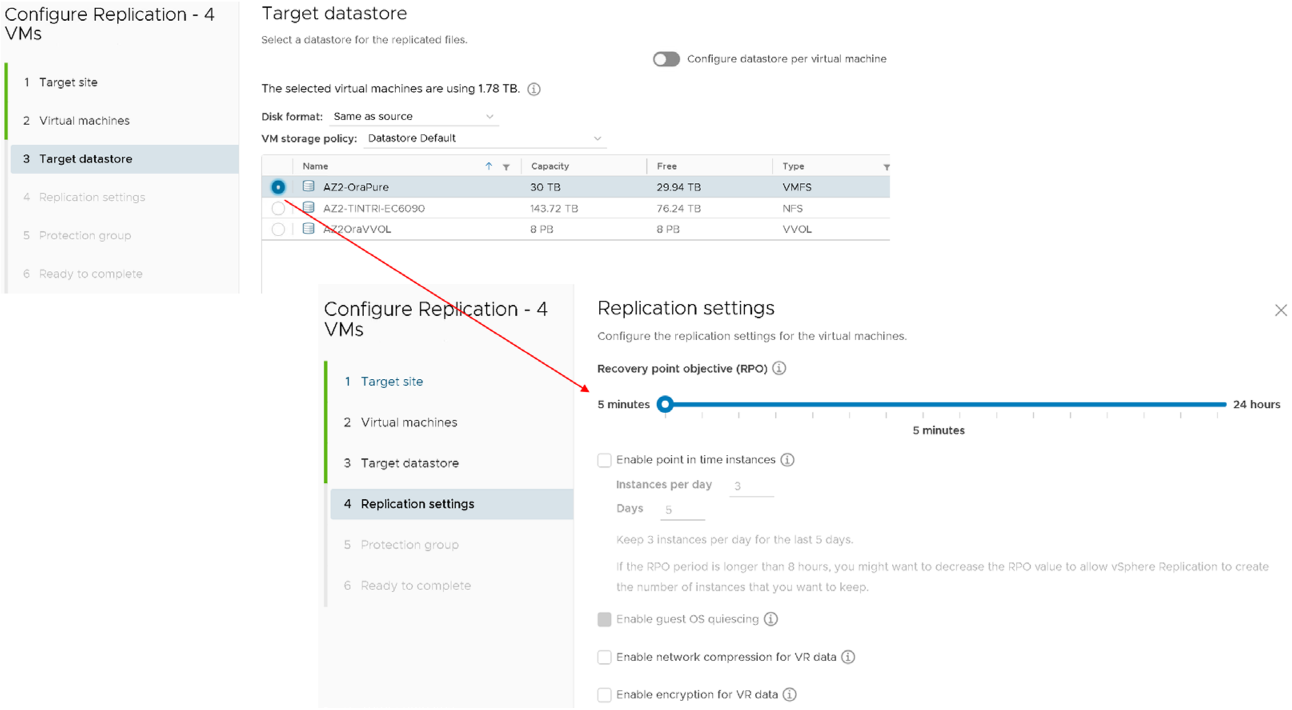
SELECT ALL | CLEAR SELECTION

□	Name	VM Folder	Compute Resource
□	VSLAB-DC35	Infrastructure	Microsoft Infrastructure
□	VSLAB-DC36	Infrastructure	Microsoft Infrastructure
□	VSLAB-DC37	Infrastructure	Microsoft Infrastructure
□	sc2jump03	JumpBoxes	Jumpservers
□	sc2jump04	JumpBoxes	Jumpservers
□	sc2jump09	JumpBoxes	Jumpservers
□	orac19c1	Oracle	BCA-SiteC
□	orac19c2	Oracle	BCA-SiteC
□	Oracle19c-BM	Oracle	BCA-SiteC
☑	Oracle19c-OL8	Oracle	BCA-SiteC
☑	Oracle19c-OL8-RMAN	Oracle	BCA-SiteC
□	Oracle19c-OL8-VVOL	Oracle	BCA-SiteC
□	Oracle19c-OL8-VVOL-RMAN	Oracle	BCA-SiteC
□	Oracle19c-PMEM	Oracle	BCA-Intel (Reserved)
□	Oracle19c-PMEM-RedoTest	Oracle	BCA-Intel (Reserved)
□	Oracle19c-PMEM-RedoTest0601	Oracle	BCA-Intel (Reserved)
□	prac19c1	Oracle	BCA-SiteC
□	prac19c2	Oracle	BCA-SiteC
□	rac19c1	Oracle	BCA-SiteC
□	rac19c2	Oracle	BCA-SiteC
□	SB-OL76-ORA19C	Oracle	BCA-SiteC
□	Template-OL8-OL19C	Oracle	BCA-SiteC

☑ 2 | 45 - 66 of 199 VM(s) | 3 / 10

FIGURE 59. SITE A: Choose VMs to Protect

Choose the target datastore and RPO.



Configure Replication - 4 VMs

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Ready to complete

Target datastore

Select a datastore for the replicated files.

Configure datastore per virtual machine

The selected virtual machines are using 1.78 TB.

Disk format: Same as source

VM storage policy: Datastore Default

	Name	Capacity	Free	Type
●	AZ2-OraPure	30 TB	29.94 TB	VMFS
○	AZ2-TINTRI-EC6090	143.72 TB	76.24 TB	NFS
○	AZ2OraVVOL	8 PB	8 PB	VVOL

Configure Replication - 4 VMs

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Ready to complete

Replication settings

Configure the replication settings for the virtual machines.

Recovery point objective (RPO)

5 minutes — 24 hours

5 minutes

□ Enable point in time instances

Instances per day 3

Days 5

Keep 3 instances per day for the last 5 days.

If the RPO period is longer than 8 hours, you might want to decrease the RPO value to allow vSphere Replication to create the number of instances that you want to keep.

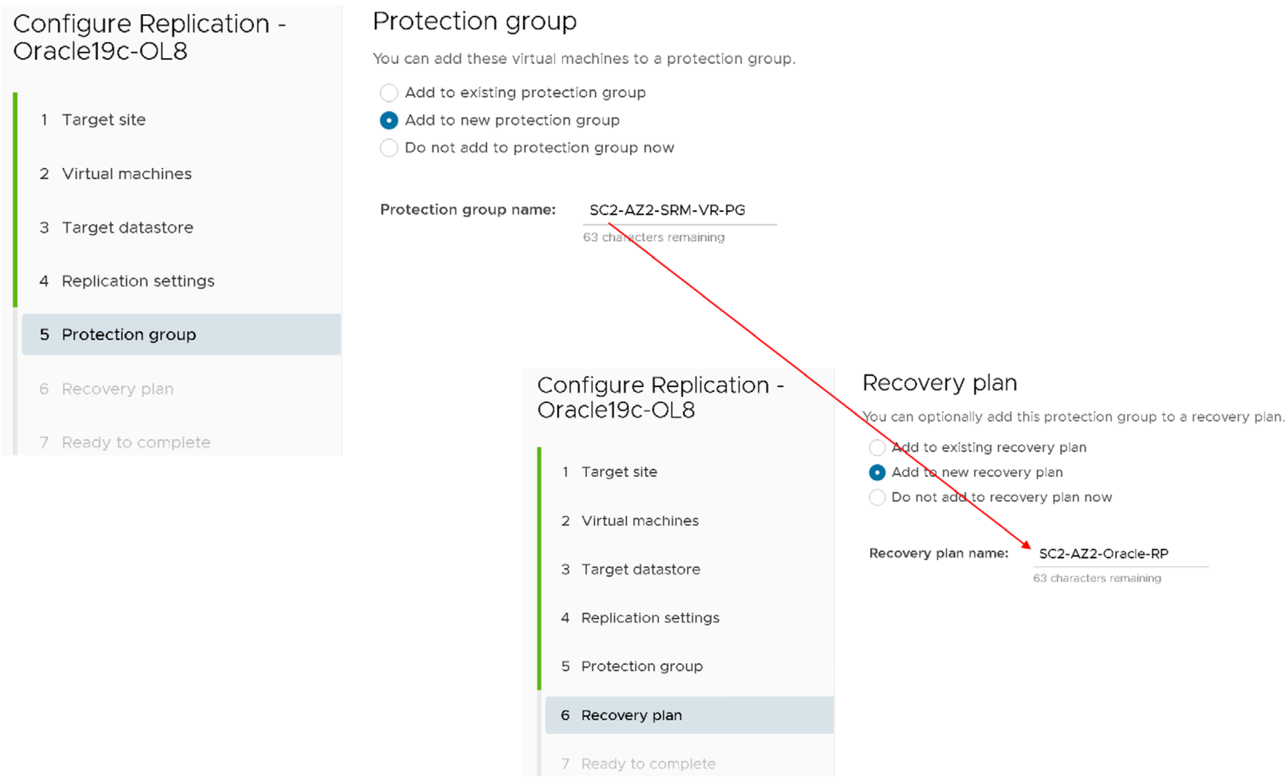
□ Enable guest OS quiescing

□ Enable network compression for VR data

□ Enable encryption for VR data

FIGURE 60. SITE A: Pick Target Datastore and RPO

Create protection group **SC2-AZ2-SRM-VR-PG** and recovery plan **SC2-AZ2-Oracle-RP**.



Configure Replication - Oracle19c-OL8

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Recovery plan
7 Ready to complete

Protection group

You can add these virtual machines to a protection group.

○ Add to existing protection group
● Add to new protection group
○ Do not add to protection group now

Protection group name: SC2-AZ2-SRM-VR-PG
63 characters remaining

Configure Replication - Oracle19c-OL8

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Recovery plan
7 Ready to complete

Recovery plan

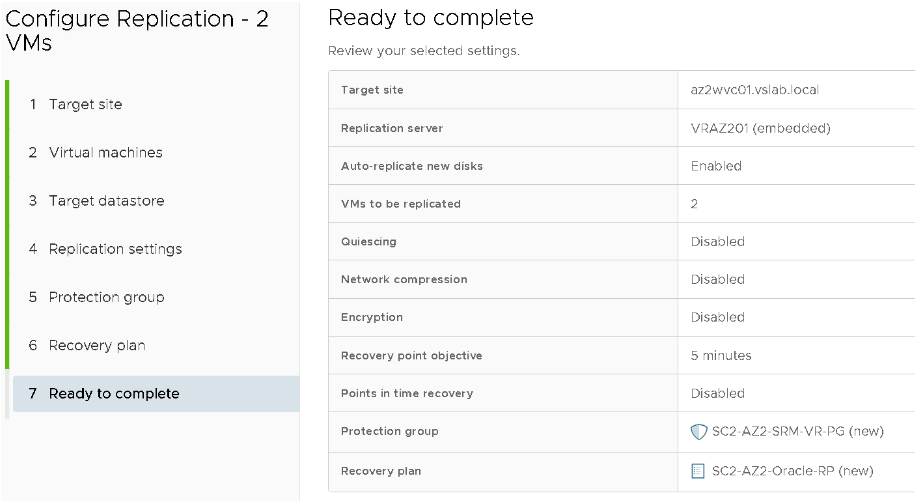
You can optionally add this protection group to a recovery plan.

○ Add to existing recovery plan
● Add to new recovery plan
○ Do not add to recovery plan now

Recovery plan name: SC2-AZ2-Oracle-RP
63 characters remaining

FIGURE 61. SITE A: Create Protection Group and Recovery Plan

The replication configuration summary is as shown below:



Configure Replication - 2 VMs

1 Target site
2 Virtual machines
3 Target datastore
4 Replication settings
5 Protection group
6 Recovery plan
7 Ready to complete

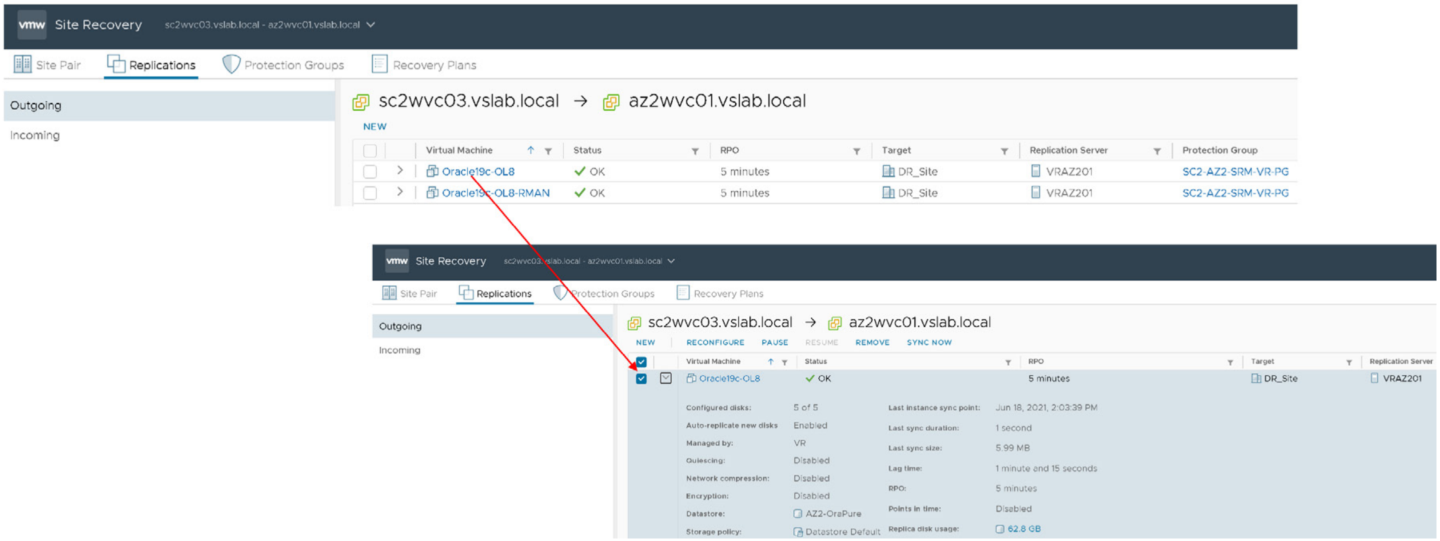
Ready to complete

Review your selected settings.

Target site	az2wvc01.vslab.local
Replication server	VRAZ201 (embedded)
Auto-replicate new disks	Enabled
VMs to be replicated	2
Quiescing	Disabled
Network compression	Disabled
Encryption	Disabled
Recovery point objective	5 minutes
Points in time recovery	Disabled
Protection group	SC2-AZ2-SRM-VR-PG (new)
Recovery plan	SC2-AZ2-Oracle-RP (new)

FIGURE 62. SITE A: Ready to Configure Replication

After the setup completes, vSphere Replication will automatically seed the source data to target as baseline first **OR** we can force a sync.



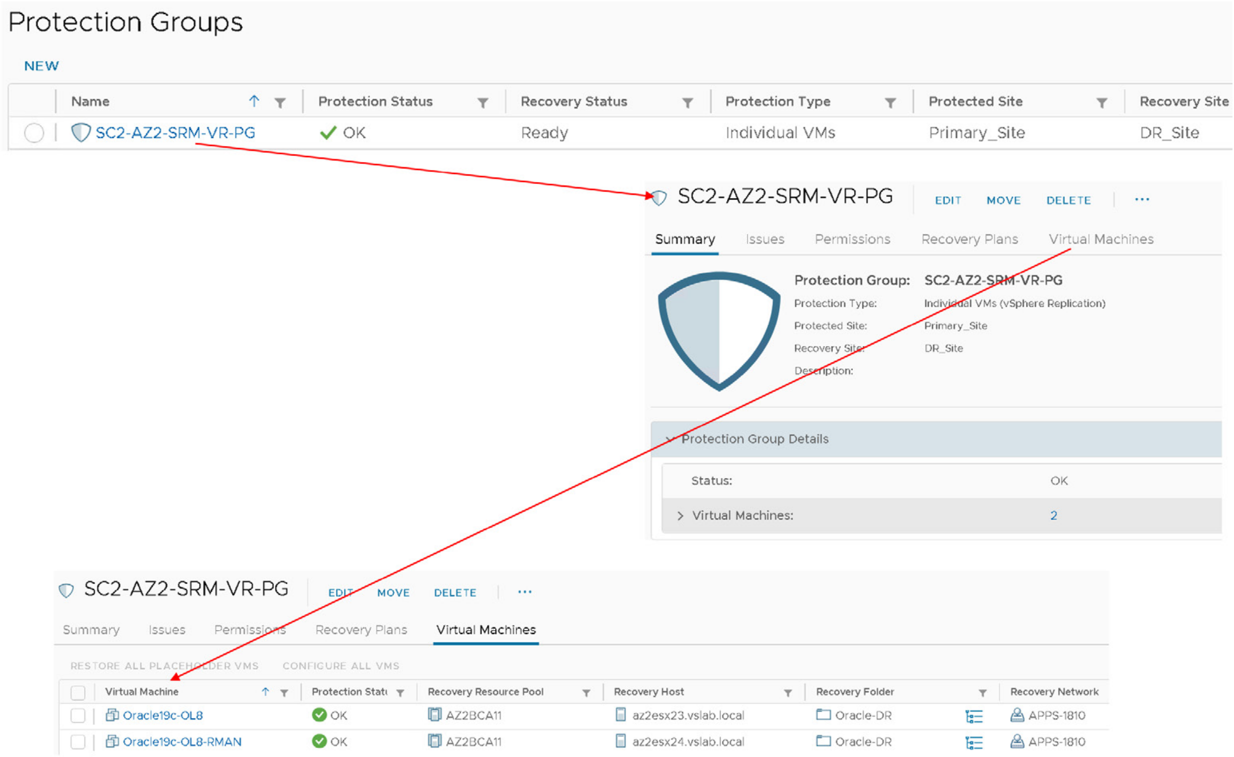
	Virtual Machine	Status	RPO	Target	Replication Server	Protection Group
□	Oracle19c-OL8	✓ OK	5 minutes	DR_Site	VRAZ201	SC2-AZ2-SRM-VR-PG
□	Oracle19c-OL8-RMAN	✓ OK	5 minutes	DR_Site	VRAZ201	SC2-AZ2-SRM-VR-PG

☑	Virtual Machine	Status	RPO	Target	Replication Server
☑	Oracle19c-OL8	✓ OK	5 minutes	DR_Site	VRAZ201

Configured disks:	5 of 5	Last instance sync point:	Jun 18, 2021, 2:03:39 PM
Auto-replicate new disks	Enabled	Last sync duration:	1 second
Managed by:	VR	Last sync size:	5.99 MB
Quiescing:	Disabled	Lag time:	1 minute and 15 seconds
Network compression:	Disabled	RPO:	5 minutes
Encryption:	Disabled	Points in time:	Disabled
Datastore:	AZ2-OraPure	Replica disk usage:	62.8 GB
Storage policy:	Datastore Default		

FIGURE 63. SITE A: vSphere Replication Seed Process

The protection group is as shown below:



	Name	Protection Status	Recovery Status	Protection Type	Protected Site	Recovery Site
○	SC2-AZ2-SRM-VR-PG	✓ OK	Ready	Individual VMs	Primary_Site	DR_Site

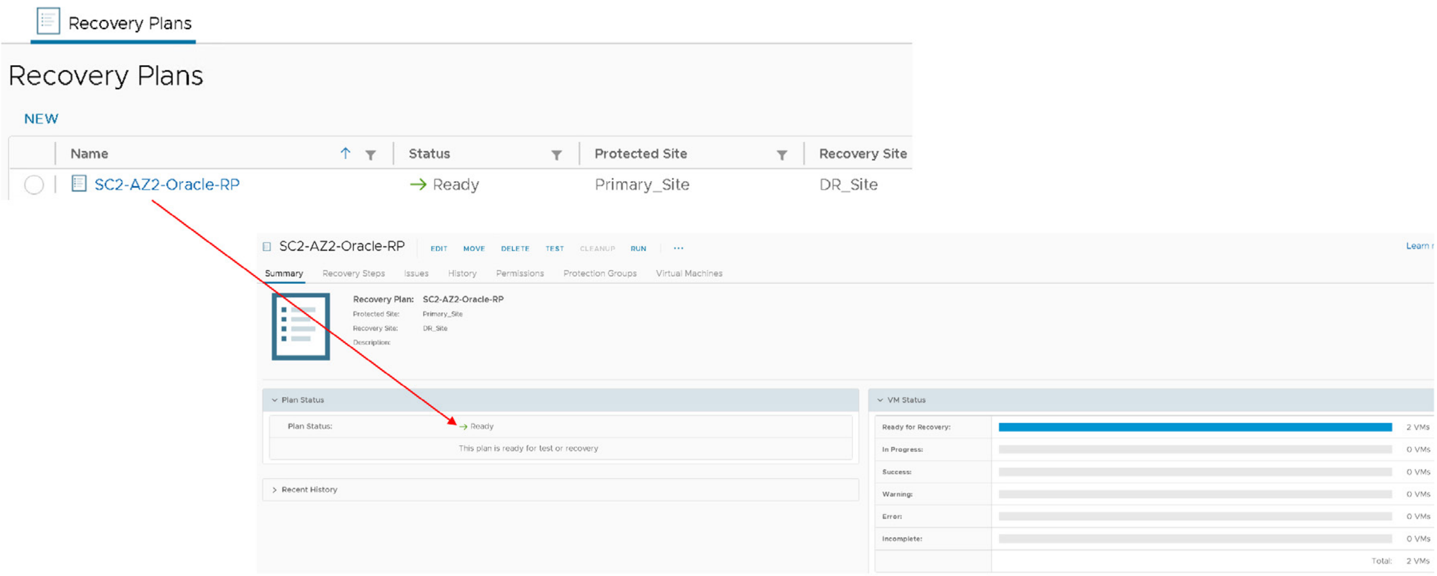
Protection Group: SC2-AZ2-SRM-VR-PG
Protection Type: Individual VMs (vSphere Replication)
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Status: OK
Virtual Machines: 2

□	Virtual Machine	Protection Stat	Recovery Resource Pool	Recovery Host	Recovery Folder	Recovery Network
□	Oracle19c-OL8	✓ OK	AZ2BCA11	az2esx23.vslab.local	Oracle-DR	APPS-1810
□	Oracle19c-OL8-RMAN	✓ OK	AZ2BCA11	az2esx24.vslab.local	Oracle-DR	APPS-1810

FIGURE 64. SITE A: Protection Group and Virtual Machines

The recovery plan is as shown below:



Recovery Plans

Name	Status	Protected Site	Recovery Site
SC2-AZ2-Oracle-RP	→ Ready	Primary_Site	DR_Site

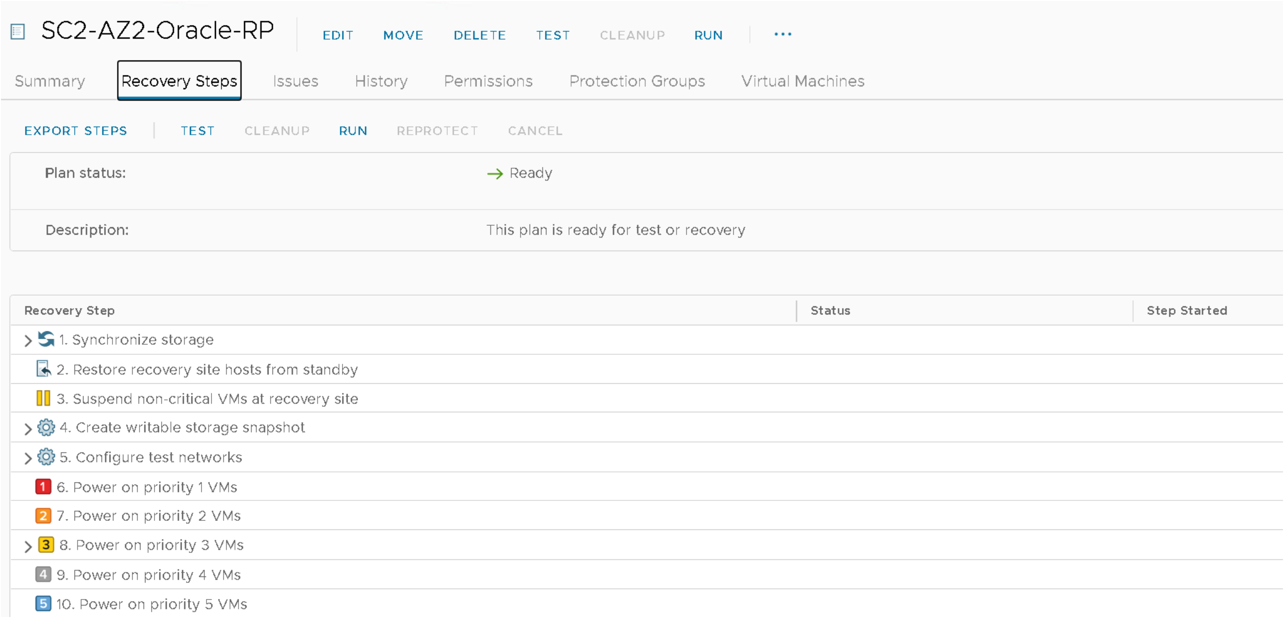
Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

FIGURE 65. SITE A: Recovery Plan

The recovery steps of the recovery plan are as shown below:



Plan status: → Ready

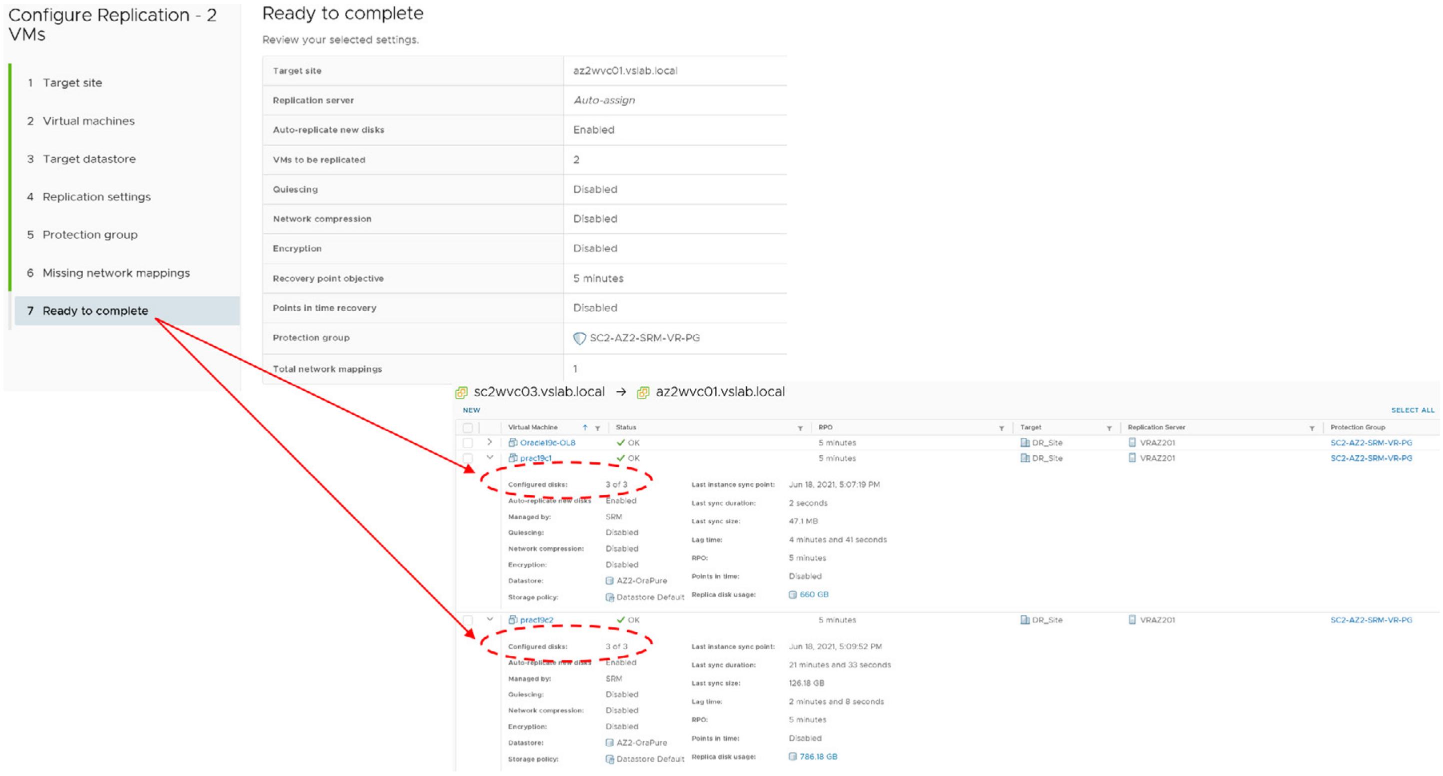
Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby		
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
5. Configure test networks		
1 6. Power on priority 1 VMs		
2 7. Power on priority 2 VMs		
3 8. Power on priority 3 VMs		
4 9. Power on priority 4 VMs		
5 10. Power on priority 5 VMs		

FIGURE 66. SITE A: Recovery Plan Steps

Currently, VMware vSphere Replication 8.4 cannot replicate VMs that share VMDK files. This limitation can be found in *VMware vSphere Replication 8.4 Release Notes*.

Attempting to use vSphere Replication of Oracle RAC **prac19c** results in two shadow VMs created at the DR site, each with three standalone VMDKs (two 80GB VMDKs and one 500GB VMDK), which is inconsistent with the Oracle RAC VMDK layout. The 500GB VMDK is shared between the two Oracle RAC VMs.



Ready to complete

Review your selected settings.

Target site	az2wvc01.vslab.local
Replication server	*Auto-assign*
Auto-replicate new disks	Enabled
VMs to be replicated	2
Quiescing	Disabled
Network compression	Disabled
Encryption	Disabled
Recovery point objective	5 minutes
Points in time recovery	Disabled
Protection group	SC2-AZ2-SRM-VR-PG
Total network mappings	1

sc2wvc03.vslab.local → az2wvc01.vslab.local

Virtual Machine	Status	RPO	Target	Replication Server	Protection Group
Oracle19c-OL8	✓ OK	5 minutes	DR_Site	VRAZ201	SC2-AZ2-SRM-VR-PG
prac19c1	✓ OK	5 minutes	DR_Site	VRAZ201	SC2-AZ2-SRM-VR-PG

Configured disks:	3 of 3	Last instance sync point:	Jun 18, 2021, 5:07:19 PM
Auto-replicate new disks	Enabled	Last sync duration:	2 seconds
Managed by:	SRM	Last sync size:	47.1 MB
Quiescing:	Disabled	Lag time:	4 minutes and 41 seconds
Network compression:	Disabled	RPO:	5 minutes
Encryption:	Disabled	Points in time:	Disabled
Datastore:	AZ2-OraPure	Replica disk usage:	660 GB
Storage policy:	Datastore Default		

Virtual Machine	Status	RPO	Target	Replication Server	Protection Group
prac19c2	✓ OK	5 minutes	DR_Site	VRAZ201	SC2-AZ2-SRM-VR-PG

Configured disks:	3 of 3	Last instance sync point:	Jun 18, 2021, 5:09:52 PM
Auto-replicate new disks	Enabled	Last sync duration:	21 minutes and 33 seconds
Managed by:	SRM	Last sync size:	126.18 GB
Quiescing:	Disabled	Lag time:	2 minutes and 8 seconds
Network compression:	Disabled	RPO:	5 minutes
Encryption:	Disabled	Points in time:	Disabled
Datastore:	AZ2-OraPure	Replica disk usage:	786.18 GB
Storage policy:	Datastore Default		

FIGURE 67. Limitations with Clustered VMDKs

Keep in mind, both Oracle RAC VMs **prac19c1** and **prac19c2** contain three VMDKs:

- Two non-shared VMDKs
  - Hard Disk 1 80GB for operating system with disk mode **Dependent**
  - Hard Disk 1 80GB for Oracle Grid Infrastructure and RDBMS binaries with disk mode **Dependent**
- One shared VMDK (500GB) with multi-writer attribute and disk mode **Independent-Persistent**

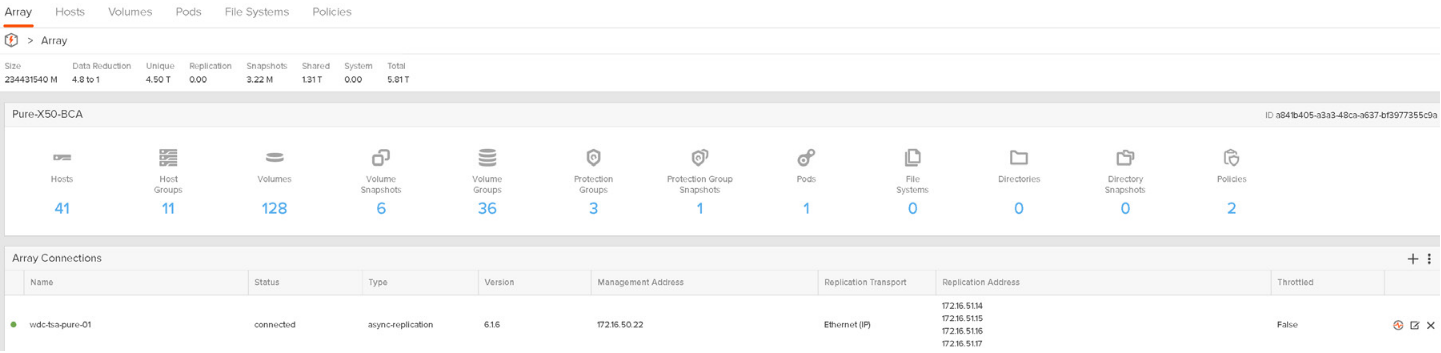
VMware Site Recovery Manager with Array-Based Replication (LUN Level)

The Site Recovery Manager and Pure Storage Array pairings between on-premises Site A and Site B are shown below:

COMPONENT	SOURCE SITE	APPLIANCE	DESTINATION SITE	APPLIANCE
SRM Appliance	Site A	SRMSC2DC01.vslab.local	Site B	SRMAZ01.vslab.local
IP Address		172.16.31.145		172.16.31.147
Pure Storage	Site A	Pure-X50-BCA	Site B	wdc-tsa-pure-01

TABLE 9. Site Recovery Manager Site A and B Network Pairing

Site A Pure Storage **Pure-X50-BCA** and Site B Pure Storage **wdc-tsa-pure-01** are paired as indicated below:



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
234431540 M	4.8 to 1	4.50 T	0.00	3.22 M	1.31 T	0.00	5.81 T

Pure-X50-BCA

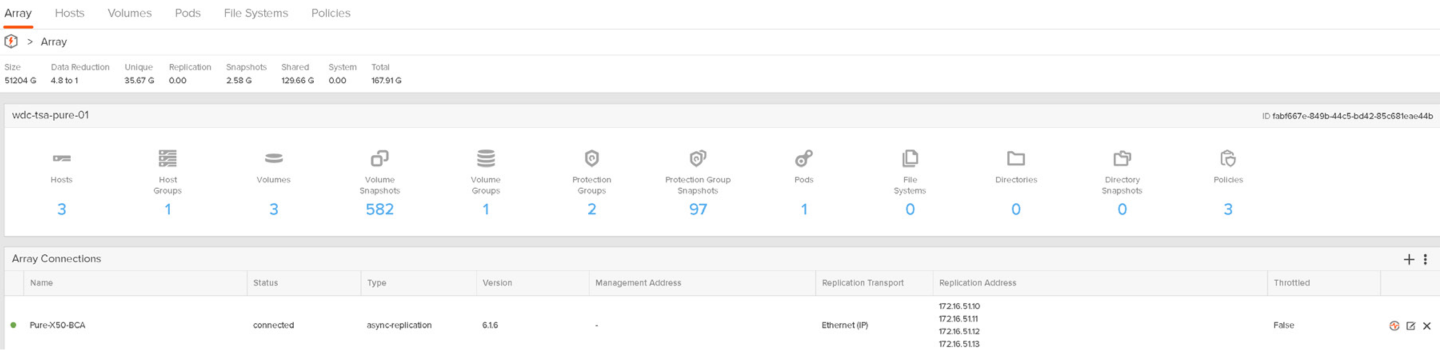
ID a841b405-a3a3-48ca-a637-bf3977355c9a

Hosts	Host Groups	Volumes	Volume Snapshots	Volume Groups	Protection Groups	Protection Group Snapshots	Pods	File Systems	Directories	Directory Snapshots	Policies
41	11	128	6	36	3	1	1	0	0	0	2

Array Connections

Name	Status	Type	Version	Management Address	Replication Transport	Replication Address	Throttled
wdc-tsa-pure-01	connected	async-replication	6.1.6	172.16.50.22	Ethernet (IP)	172.16.51.14 172.16.51.15 172.16.51.16 172.16.51.17	False

FIGURE 68. SITE A: Pure Storage Pure-X50-BCA



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
51204 G	4.8 to 1	35.67 G	0.00	2.58 G	129.66 G	0.00	167.91 G

wdc-tsa-pure-01

ID fabf667e-849b-44c5-bd42-85c681eae44b

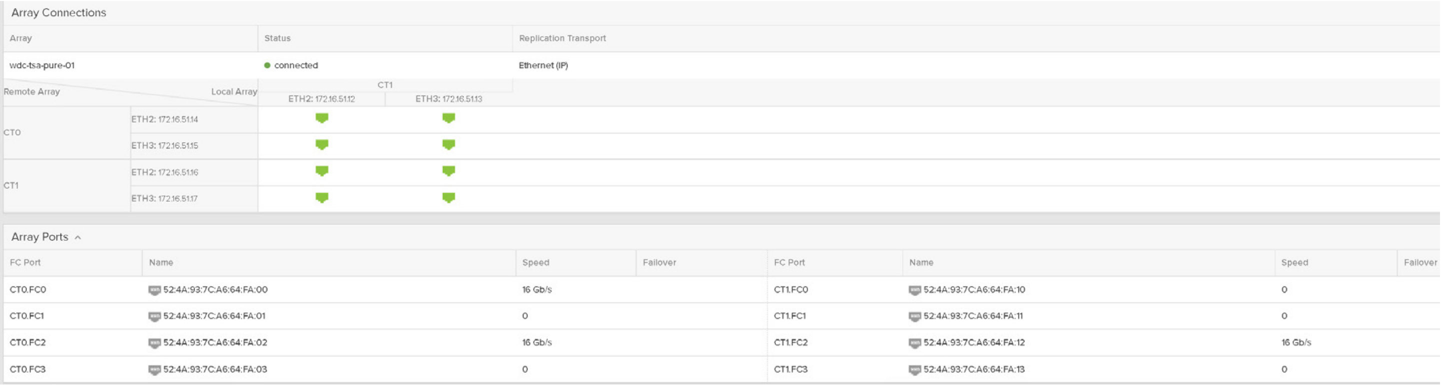
Hosts	Host Groups	Volumes	Volume Snapshots	Volume Groups	Protection Groups	Protection Group Snapshots	Pods	File Systems	Directories	Directory Snapshots	Policies
3	1	3	582	1	2	97	1	0	0	0	3

Array Connections

Name	Status	Type	Version	Management Address	Replication Transport	Replication Address	Throttled
Pure-X50-BCA	connected	async-replication	6.1.6	-	Ethernet (IP)	172.16.51.10 172.16.51.11 172.16.51.12 172.16.51.13	False

FIGURE 69. SITE B: Pure Storage wdc-tsa-pure-01

Site A Pure Storage **Pure-X50-BCA** and Site B Pure Storage **wdc-tsa-pure-01** Replication links are as shown below:



Array Connections

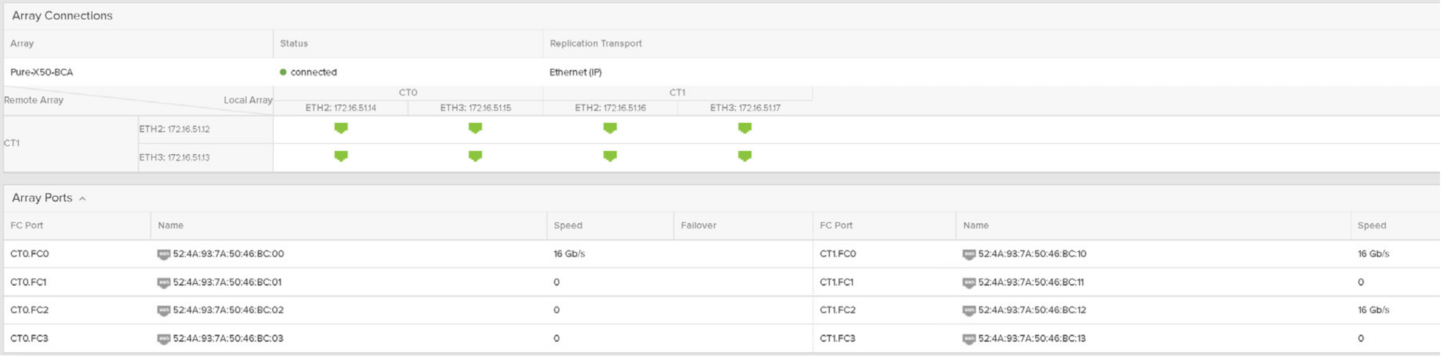
Array	Status	Replication Transport
wdc-tsa-pure-01	● connected	Ethernet (IP)

Remote Array	Local Array	CT1 ETH2: 172.16.51.12	CT1 ETH3: 172.16.51.13
CT0	ETH2: 172.16.51.14	✓	✓
	ETH3: 172.16.51.15	✓	✓
CT1	ETH2: 172.16.51.16	✓	✓
	ETH3: 172.16.51.17	✓	✓

Array Ports ^

FC Port	Name	Speed	Failover	FC Port	Name	Speed	Failover
CT0.FC0	52:4A:93:7C:A6:64:FA:00	16 Gb/s		CT1.FC0	52:4A:93:7C:A6:64:FA:10	0	
CT0.FC1	52:4A:93:7C:A6:64:FA:01	0		CT1.FC1	52:4A:93:7C:A6:64:FA:11	0	
CT0.FC2	52:4A:93:7C:A6:64:FA:02	16 Gb/s		CT1.FC2	52:4A:93:7C:A6:64:FA:12	16 Gb/s	
CT0.FC3	52:4A:93:7C:A6:64:FA:03	0		CT1.FC3	52:4A:93:7C:A6:64:FA:13	0	

FIGURE 70. SITE A: Pure Storage Pure-X50-BCA Replication Links



Array Connections

Array	Status	Replication Transport
Pure-X50-BCA	● connected	Ethernet (IP)

Remote Array	Local Array	CT0 ETH2: 172.16.51.14	CT0 ETH3: 172.16.51.15	CT1 ETH2: 172.16.51.16	CT1 ETH3: 172.16.51.17
CT1	ETH2: 172.16.51.12	✓	✓	✓	✓
	ETH3: 172.16.51.13	✓	✓	✓	✓

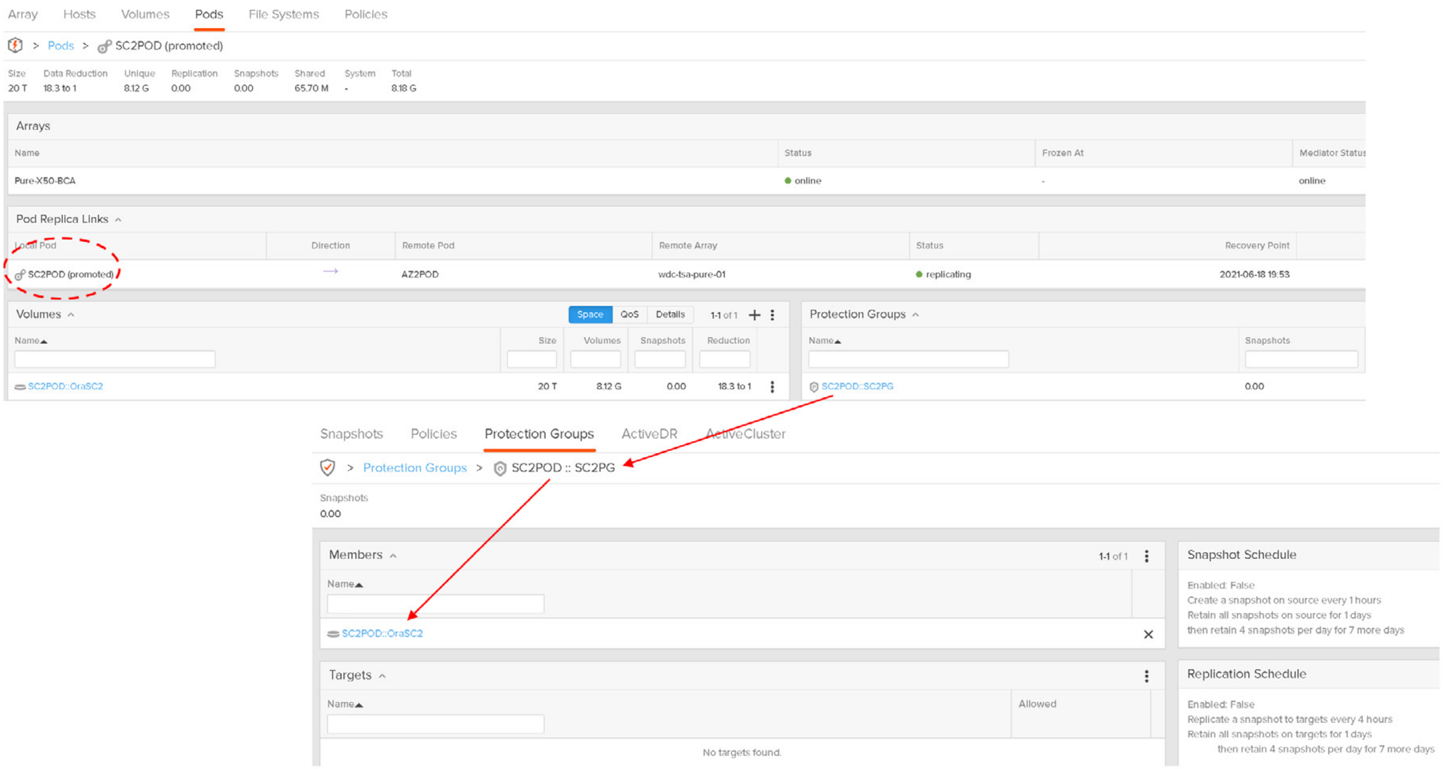
Array Ports ^

FC Port	Name	Speed	Failover	FC Port	Name	Speed
CT0.FC0	52:4A:93:7A:50:46:BC:00	16 Gb/s		CT1.FC0	52:4A:93:7A:50:46:BC:10	16 Gb/s
CT0.FC1	52:4A:93:7A:50:46:BC:01	0		CT1.FC1	52:4A:93:7A:50:46:BC:11	0
CT0.FC2	52:4A:93:7A:50:46:BC:02	0		CT1.FC2	52:4A:93:7A:50:46:BC:12	16 Gb/s
CT0.FC3	52:4A:93:7A:50:46:BC:03	0		CT1.FC3	52:4A:93:7A:50:46:BC:13	0

FIGURE 71. SITE B: Pure Storage wdc-tsa-pure-01 Replication Links

Follow steps in the *FlashRecover Replication Configuration and Best Practices Guide* to connect the two Pure Storage arrays for replication.

Site A Pure Storage **Pure-X50-BCA** has storage pod **SC2POD** and protection group **SC2PG**. Volume **OraSC2** (20TB) is part of the storage pod **SC2POD**.



> Pods > SC2POD (promoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	18.3 to 1	8.12 G	0.00	0.00	65.70 M	-	8.18 G

Arrays

Name	Status	Frozen At	Mediator Status
Pure-X50-BCA	● online	-	online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status	Recovery Point
SC2POD (promoted)	→	AZ2POD	wdc-tsa-pure-01	● replicating	2021-06-18 19:53

Volumes

Name▲	Size	Volumes	Snapshots	Reduction
SC2POD::OraSC2	20 T	8.12 G	0.00	18.3 to 1

Protection Groups

Name▲	Snapshots
SC2POD::SC2PG	0.00

> Protection Groups > SC2POD :: SC2PG

Snapshots
0.00

Members

Name▲
SC2POD::OraSC2

Snapshot Schedule

Enabled: False
Create a snapshot on source every 1 hours
Retain all snapshots on source for 1 days
then retain 4 snapshots per day for 7 more days

Targets

Name▲	Allowed

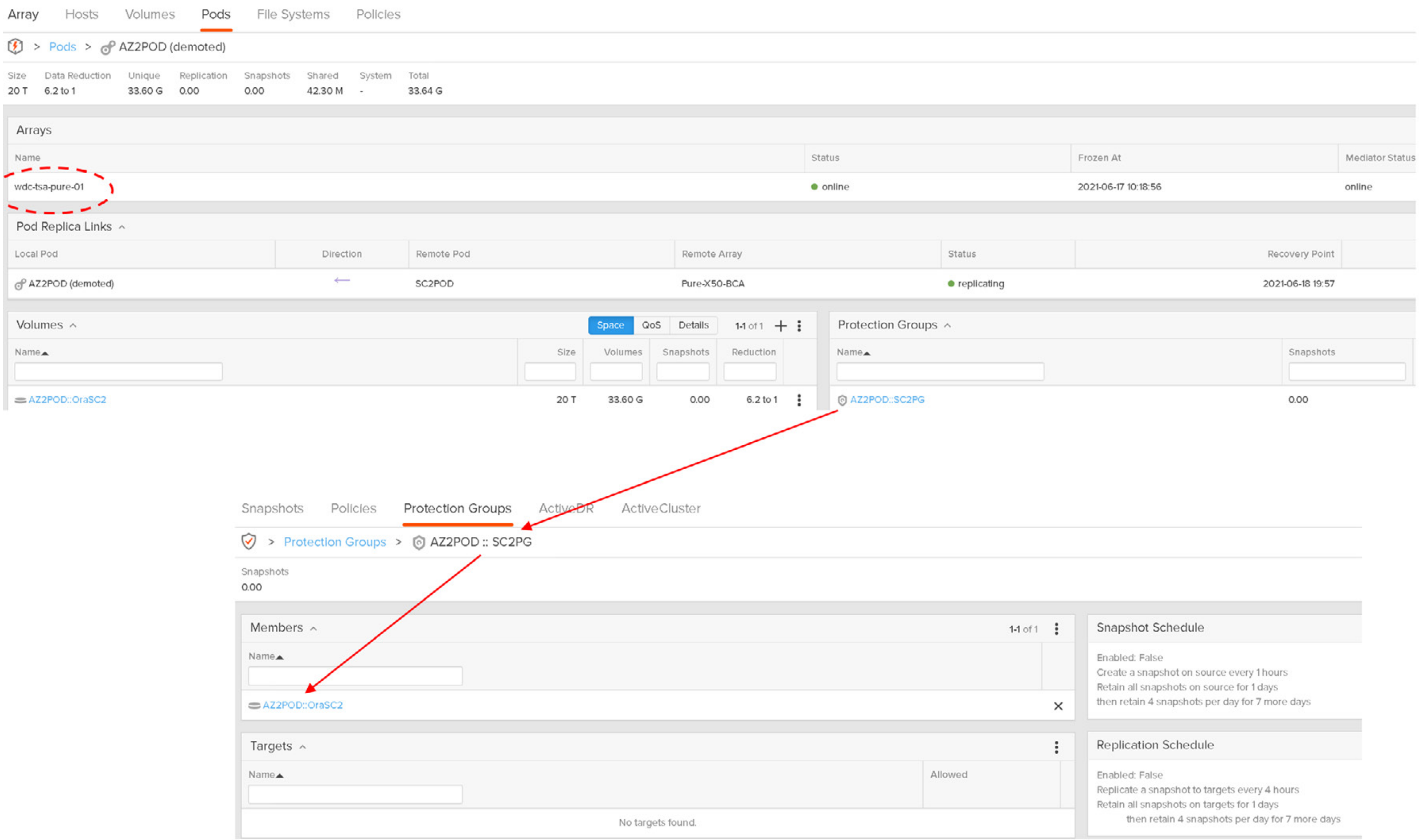
No targets found.

Replication Schedule

Enabled: False
Replicate a snapshot to targets every 4 hours
Retain all snapshots on targets for 1 days
then retain 4 snapshots per day for 7 more days

FIGURE 72. SITE A: Pure Storage POD, Protection Group and Protected Volume

Site B Pure Storage **wdc-tsa-pure-01** has storage pod **AZ2POD**. Volume **A2POD::OraSC2** is the corresponding recovery volume in the storage pod **AZ2POD**.



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	6.2 to 1	33.60 G	0.00	0.00	42.30 M	-	33.64 G

Arrays

Name	Status	Frozen At	Mediator Status
wdc-tsa-pure-01	● online	2021-06-17 10:18:56	online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status	Recovery Point
AZ2POD (demoted)	←	SC2POD	Pure-X50-BCA	● replicating	2021-06-18 19:57

Volumes

Name	Size	Volumes	Snapshots	Reduction
AZ2POD::OraSC2	20 T	33.60 G	0.00	6.2 to 1

Protection Groups

Name	Snapshots
AZ2POD::SC2PG	0.00

Snapshots
0.00

Members

Name
AZ2POD::OraSC2

Snapshot Schedule

Enabled: False
Create a snapshot on source every 1 hours
Retain all snapshots on source for 1 days
then retain 4 snapshots per day for 7 more days

Targets

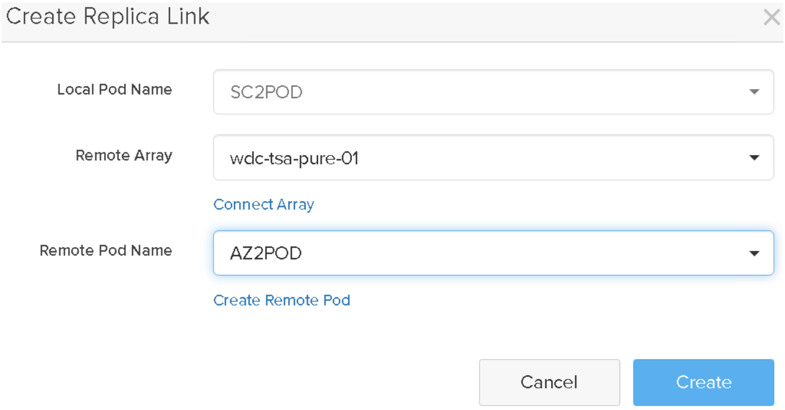
Name	Allowed
No targets found.	

Replication Schedule

Enabled: False
Replicate a snapshot to targets every 4 hours
Retain all snapshots on targets for 1 days
then retain 4 snapshots per day for 7 more days

FIGURE 73. SITE B: Pure Storage POD, Protection Group and Protected Volume

A replica link is created between Site A storage pod **SC2POD** and Site B storage pod **AZ2POD**.

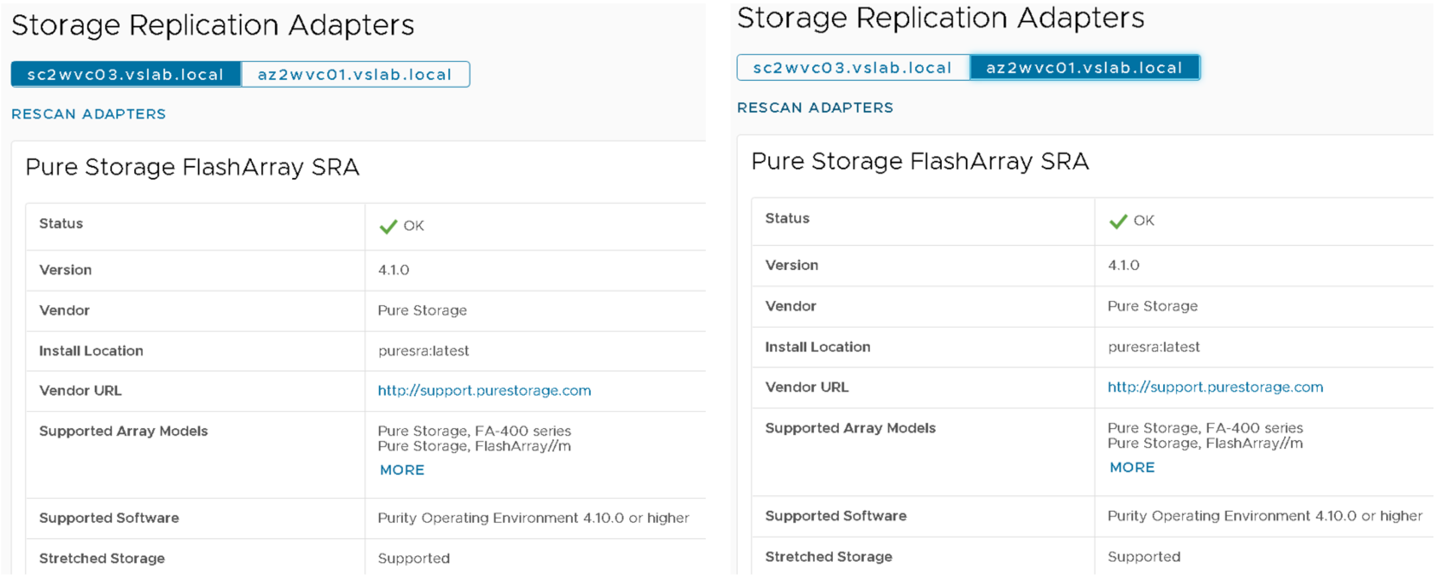

Create Replica Link

Local Pod Name	SC2POD
Remote Array	wdc-tsa-pure-01
Remote Pod Name	AZ2POD

FIGURE 74. Pure Storage Replica Link Between Site A and Site B

Information on configuring the replica link can be found in
SRM User Guide: FlashArray Continuous Replication (ActiveDR) Workflows guide.

Site Recovery Manager includes two important features that allow discovery of the Pure Storage replication environment—the Pure Storage SRA and Array Managers.



Storage Replication Adapters

Pure Storage FlashArray SRA

Status	✓ OK
Version	4.1.0
Vendor	Pure Storage
Install Location	puresra:latest
Vendor URL	http://support.purestorage.com
Supported Array Models	Pure Storage, FA-400 series Pure Storage, FlashArray//m MORE
Supported Software	Purity Operating Environment 4.10.0 or higher
Stretched Storage	Supported

Storage Replication Adapters

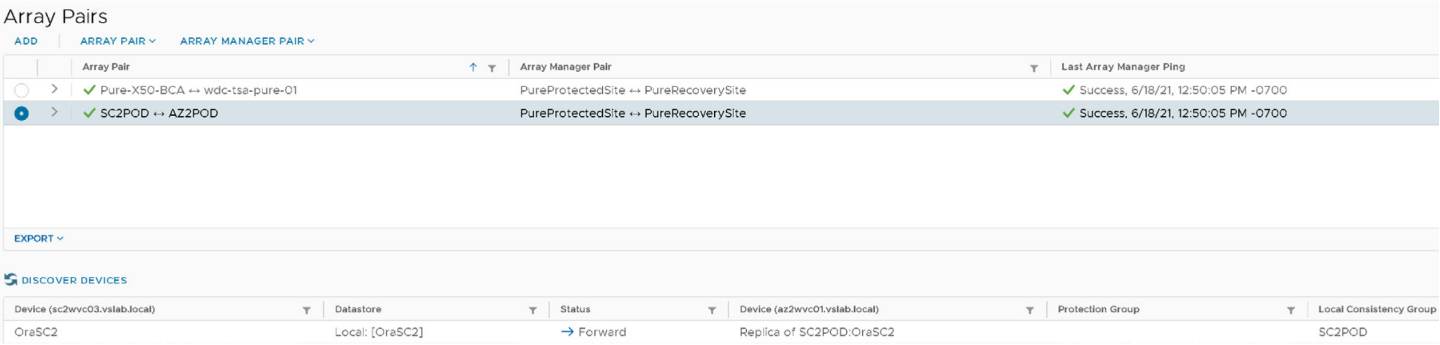
Pure Storage FlashArray SRA

Status	✓ OK
Version	4.1.0
Vendor	Pure Storage
Install Location	puresra:latest
Vendor URL	http://support.purestorage.com
Supported Array Models	Pure Storage, FA-400 series Pure Storage, FlashArray//m MORE
Supported Software	Purity Operating Environment 4.10.0 or higher
Stretched Storage	Supported

FIGURE 75. Site A and Site B Storage Replication Adapters

Details regarding configuration of Pure Storage SRA can be found in
SRM User Guide: Installing the FlashArray Storage Replication Adapter.

After the protected site and recovery site are paired up, the array managers are configured so that Site Recovery Manager can discover replicated devices, compute datastore groups, and initiate storage operations.



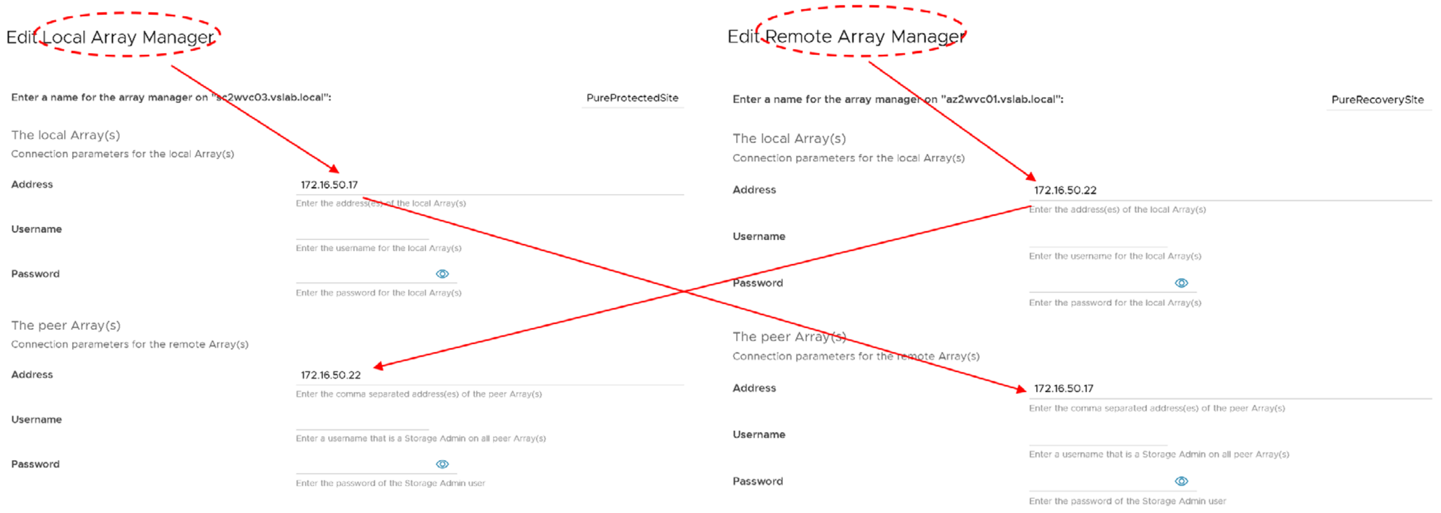
Array Pairs

	Array Pair	Array Manager Pair	Last Array Manager Ping
○	✓ Pure-X50-BCA ↔ wdc-tsa-pure-01	PureProtectedSite ↔ PureRecoverySite	✓ Success, 6/18/21, 12:50:05 PM -0700
●	✓ SC2POD ↔ AZ2POD	PureProtectedSite ↔ PureRecoverySite	✓ Success, 6/18/21, 12:50:05 PM -0700

Device (sc2wvc03.vslab.local)	Datastore	Status	Device (az2wvc01.vslab.local)	Protection Group	Local Consistency Group
OraSC2	Local: [OraSC2]	→ Forward	Replica of SC2POD:OraSC2		SC2POD

Figure 76. Site A and Site B Array Managers

Additional array managers details are shown below:



Edit Local Array Manager

Enter a name for the array manager on "sc2wvc03.vslab.local": PureProtectedSite

The local Array(s)

Connection parameters for the local Array(s)

Address	172.16.50.17 Enter the address(es) of the local Array(s)
Username	Enter the username for the local Array(s)
Password	Enter the password for the local Array(s)

The peer Array(s)

Connection parameters for the remote Array(s)

Address	172.16.50.22 Enter the comma separated address(es) of the peer Array(s)
Username	Enter a username that is a Storage Admin on all peer Array(s)
Password	Enter the password of the Storage Admin user

Edit Remote Array Manager

Enter a name for the array manager on "az2wvc01.vslab.local": PureRecoverySite

The local Array(s)

Connection parameters for the local Array(s)

Address	172.16.50.22 Enter the address(es) of the local Array(s)
Username	Enter the username for the local Array(s)
Password	Enter the password for the local Array(s)

The peer Array(s)

Connection parameters for the remote Array(s)

Address	172.16.50.17 Enter the comma separated address(es) of the peer Array(s)
Username	Enter a username that is a Storage Admin on all peer Array(s)
Password	Enter the password of the Storage Admin user

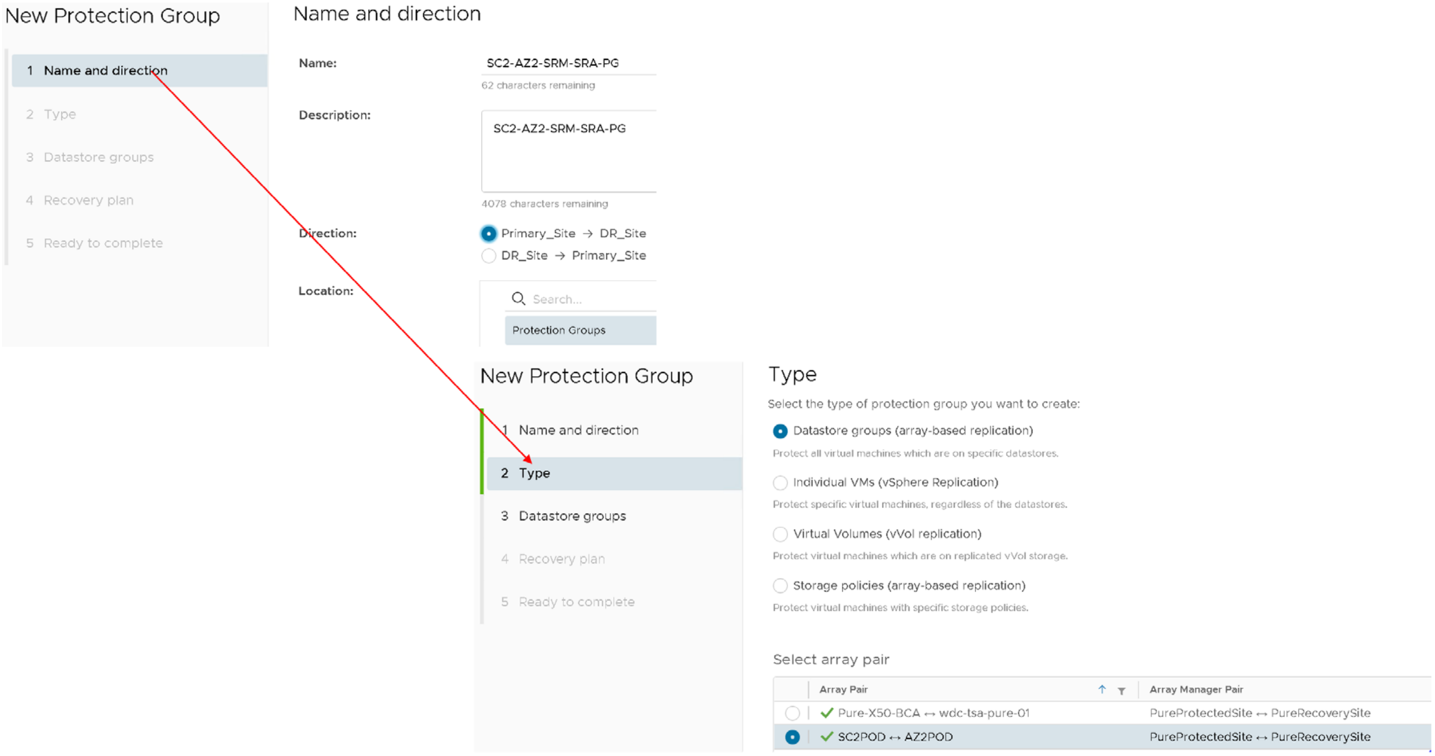
FIGURE 77. Site A and Site B Array Managers Details

Information regarding configuration of Pure Storage Array Manager can be found in *SRM User Guide: Configuring the FlashArray SRA Array Managers*.

Installing Pure Storage SRA and Pure Storage Array Manager is beyond the scope of this paper.

Site A protection group **SC2-AZ2-SRM-SRA-PG** for array-based replication is created as shown below.

The steps to create the protection group for array-based replication are as shown below:



New Protection Group

1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete

Name and direction

Name: SC2-AZ2-SRM-SRA-PG
62 characters remaining

Description: SC2-AZ2-SRM-SRA-PG
4078 characters remaining

Direction:
● Primary_Site → DR_Site
○ DR_Site → Primary_Site

Location:
Search...
Protection Groups

New Protection Group

1 Name and direction
2 Type
3 Datastore groups
4 Recovery plan
5 Ready to complete

Type

Select the type of protection group you want to create:

● Datastore groups (array-based replication)
Protect all virtual machines which are on specific datastores.

○ Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.

○ Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

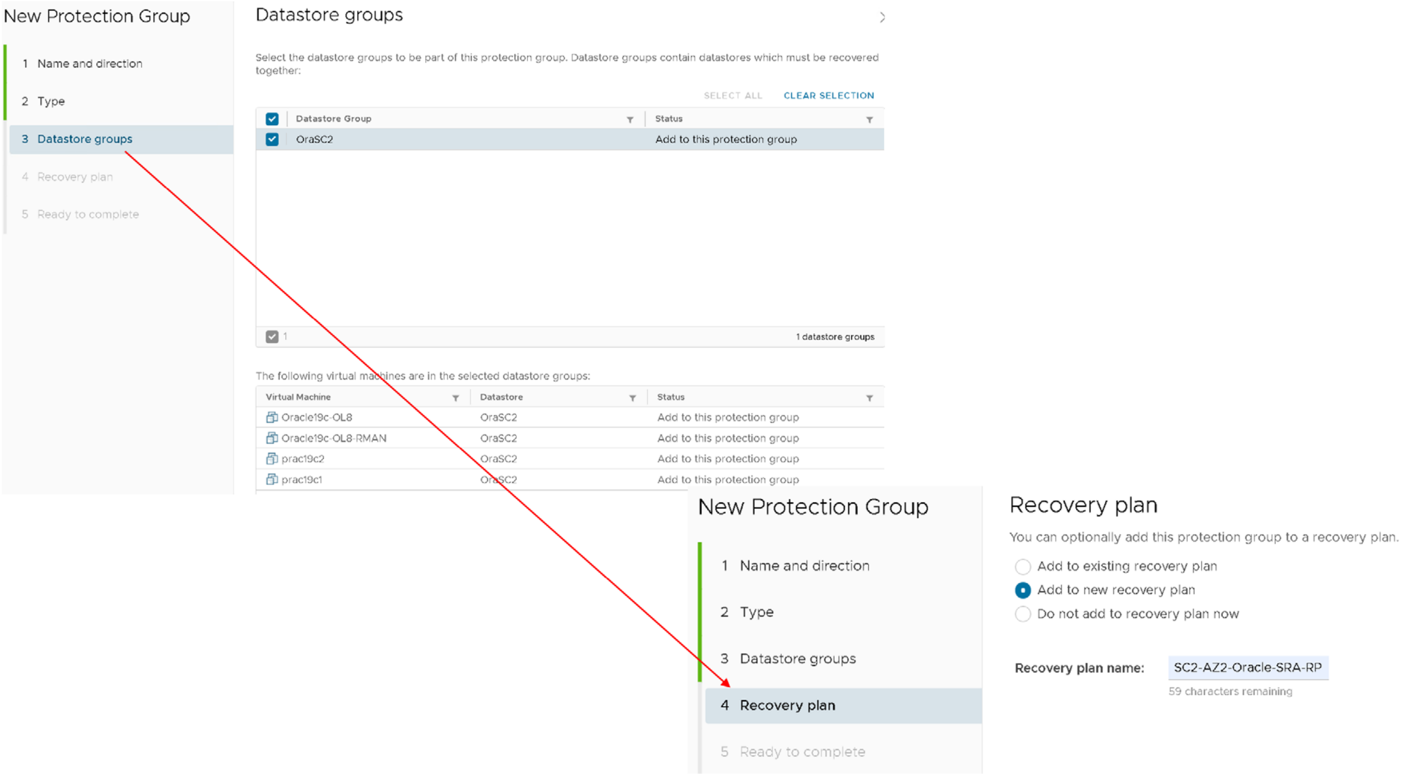
○ Storage policies (array-based replication)
Protect virtual machines with specific storage policies.

Select array pair

	Array Pair	Array Manager Pair
○	✓ Pure-X50-BCA ↔ wdc-tsa-pure-01	PureProtectedSite ↔ PureRecoverySite
●	✓ SC2POD ↔ AZ2POD	PureProtectedSite ↔ PureRecoverySite

FIGURE 78. SITE A: Array Based Replication Create Protection Group

Choose the protected datastore and create a new recovery plan **SC2-AZ2-Oracle-SRA-RP**.



Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together:

	Datastore Group	Status
☑	OraSC2	Add to this protection group

☑ 1 — 1 datastore groups

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
Oracle19c-OL8	OraSC2	Add to this protection group
Oracle19c-OL8-RMAN	OraSC2	Add to this protection group
prac19c2	OraSC2	Add to this protection group
prac19c1	OraSC2	Add to this protection group

Recovery plan

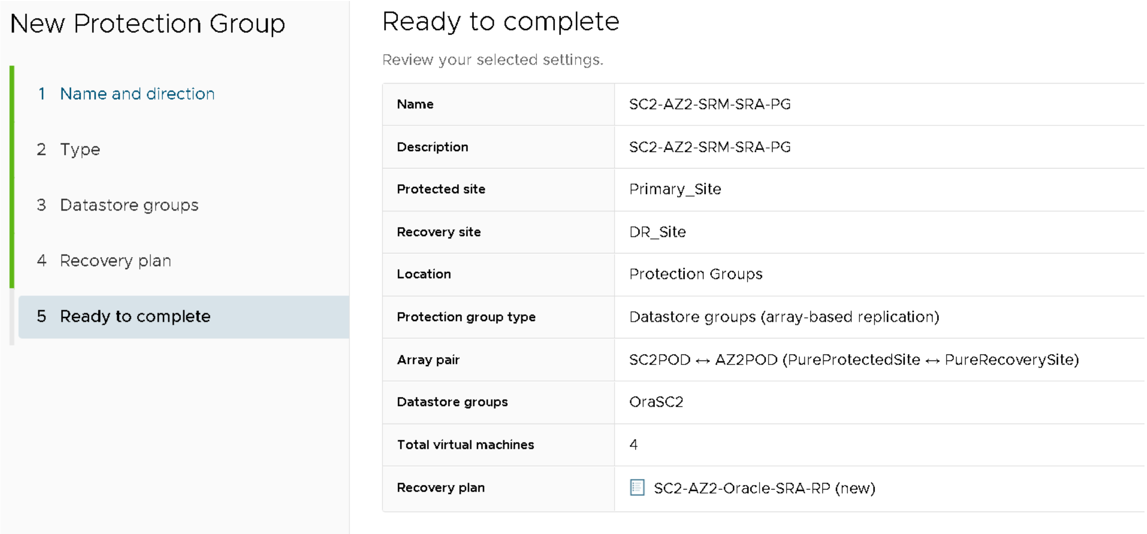
You can optionally add this protection group to a recovery plan.

○ Add to existing recovery plan
● Add to new recovery plan
○ Do not add to recovery plan now

Recovery plan name: SC2-AZ2-Oracle-SRA-RP
59 characters remaining

FIGURE 79. SITE A: Pick Protected Datastore and Create New recovery plan

The protection group summary and recovery plan details are as shown below:



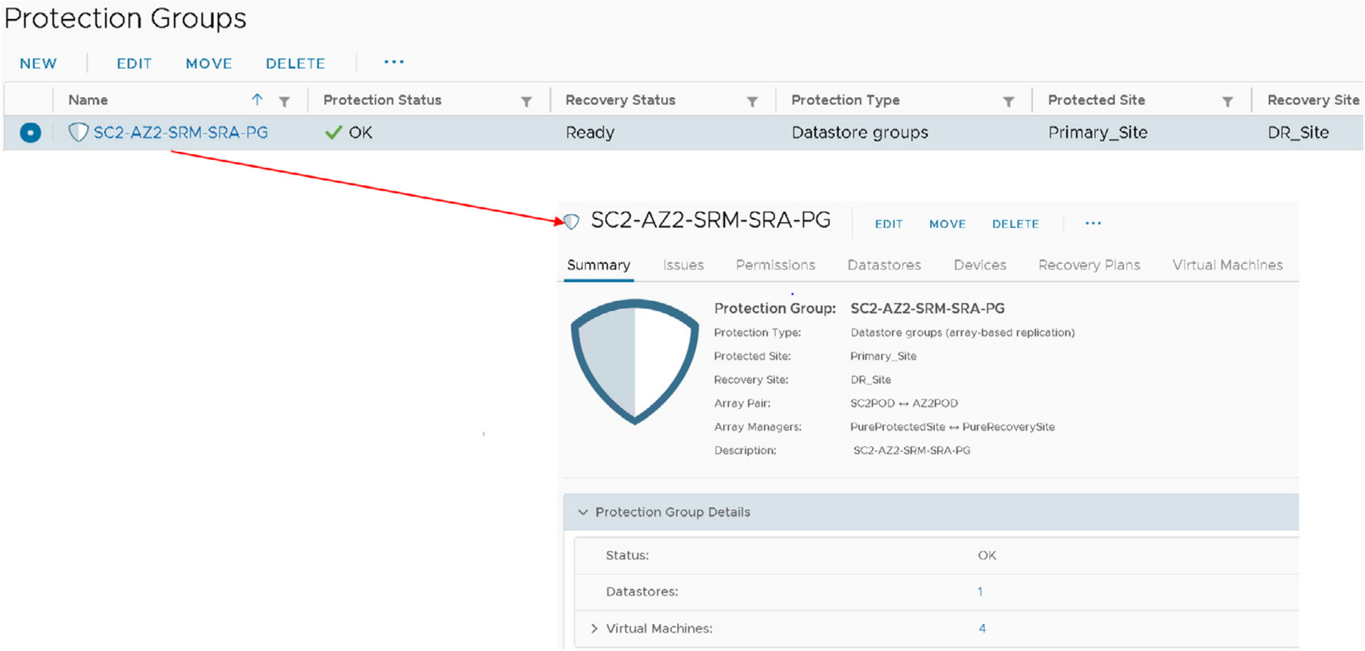
Ready to complete

Review your selected settings.

Name	SC2-AZ2-SRM-SRA-PG
Description	SC2-AZ2-SRM-SRA-PG
Protected site	Primary_Site
Recovery site	DR_Site
Location	Protection Groups
Protection group type	Datastore groups (array-based replication)
Array pair	SC2POD ↔ AZ2POD (PureProtectedSite ↔ PureRecoverySite)
Datastore groups	OraSC2
Total virtual machines	4
Recovery plan	SC2-AZ2-Oracle-SRA-RP (new)

FIGURE 80. Protection Group and Recovery Plan Details

The details of protection group **SC2-AZ2-SRM-SRA-PG** are as shown below:



Protection Groups

NEW EDIT MOVE DELETE ···

Name	Protection Status	Recovery Status	Protection Type	Protected Site	Recovery Site
SC2-AZ2-SRM-SRA-PG	✓ OK	Ready	Datastore groups	Primary_Site	DR_Site

SC2-AZ2-SRM-SRA-PG EDIT MOVE DELETE ···

Summary Issues Permissions Datastores Devices Recovery Plans Virtual Machines

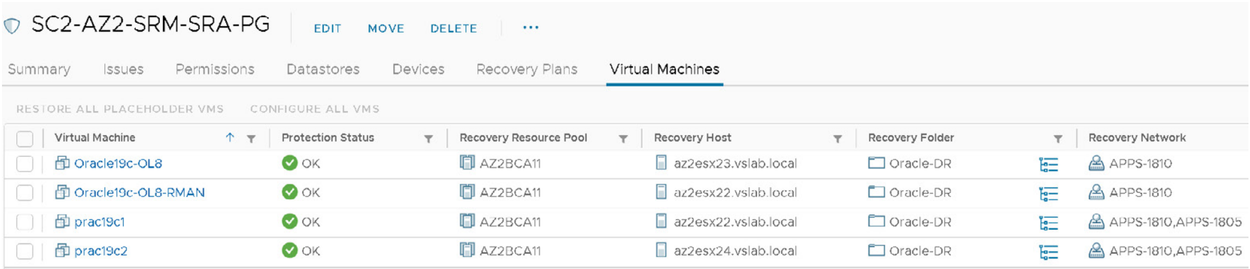
Protection Group: **SC2-AZ2-SRM-SRA-PG**
Protection Type: Datastore groups (array-based replication)
Protected Site: Primary_Site
Recovery Site: DR_Site
Array Pair: SC2POD ↔ AZ2POD
Array Managers: PureProtectedSite ↔ PureRecoverySite
Description: SC2-AZ2-SRM-SRA-PG

Protection Group Details

Status:	OK
Datastores:	1
Virtual Machines:	4

FIGURE 81. Protection Group Details

Protection group **SC2-AZ2-SRM-SRA-PG** for array-based replication is protecting both single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** and Oracle RAC **prac19c** VMs.



SC2-AZ2-SRM-SRA-PG EDIT MOVE DELETE ···

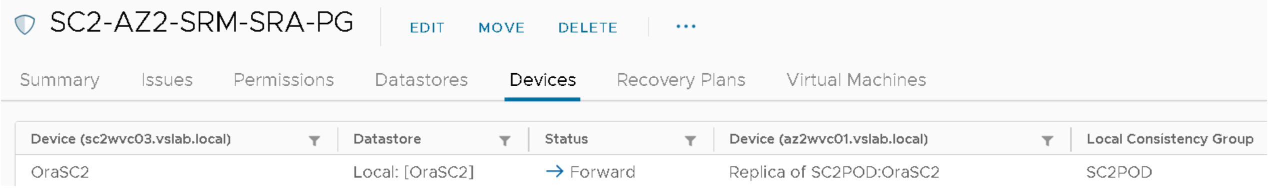
Summary Issues Permissions Datastores Devices Recovery Plans Virtual Machines

RESTORE ALL PLACEHOLDER VMS CONFIGURE ALL VMS

Virtual Machine	Protection Status	Recovery Resource Pool	Recovery Host	Recovery Folder	Recovery Network
Oracle19c-OL8	OK	AZ2BCA11	az2esx23.vslab.local	Oracle-DR	APPS-1810
Oracle19c-OL8-RMAN	OK	AZ2BCA11	az2esx22.vslab.local	Oracle-DR	APPS-1810
prac19c1	OK	AZ2BCA11	az2esx22.vslab.local	Oracle-DR	APPS-1810,APPS-1805
prac19c2	OK	AZ2BCA11	az2esx24.vslab.local	Oracle-DR	APPS-1810,APPS-1805

FIGURE 82. Protection Group Virtual Machine Details

The discovered devices are as shown below:



SC2-AZ2-SRM-SRA-PG EDIT MOVE DELETE ···

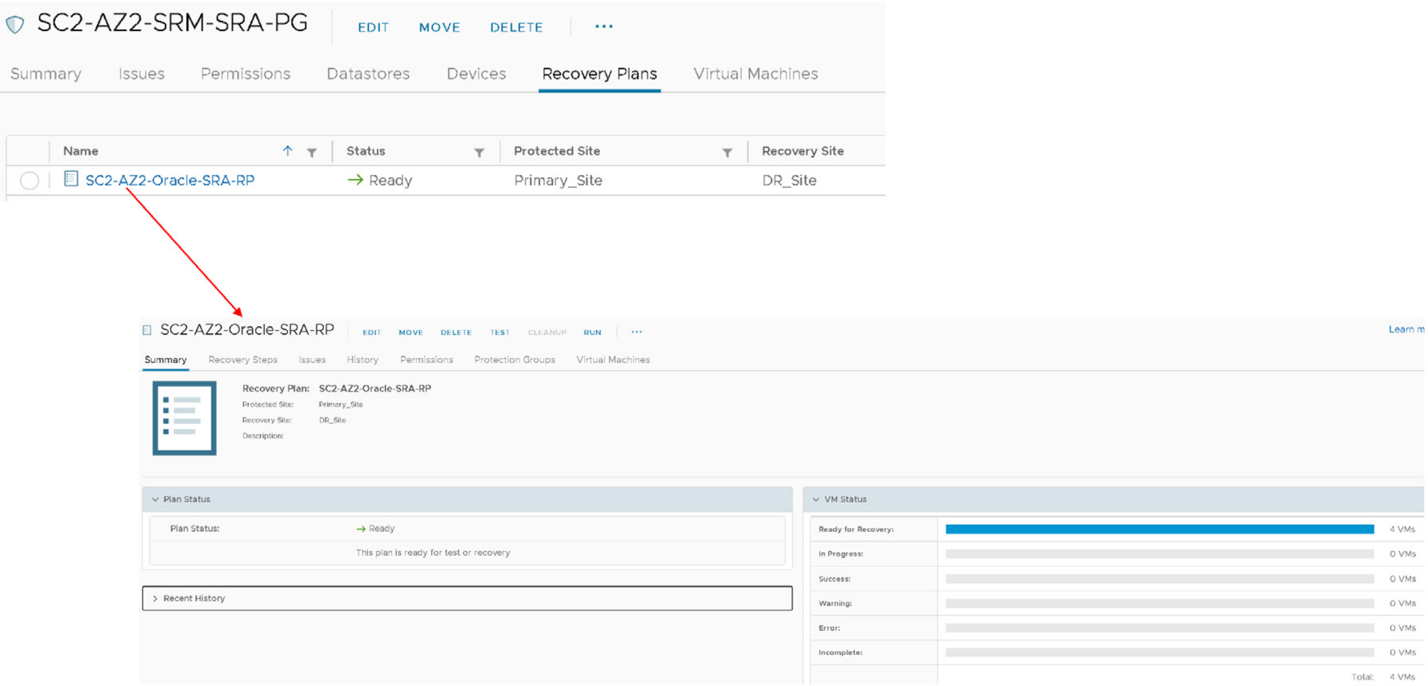
Summary Issues Permissions Datastores Devices Recovery Plans Virtual Machines

Device (sc2wvc03.vslab.local)	Datastore	Status	Device (az2wvc01.vslab.local)	Local Consistency Group
OraSC2	Local: [OraSC2]	→ Forward	Replica of SC2POD:OraSC2	SC2POD

FIGURE 83. Site A Discovered Devices

Information regarding discovered devices can be found in *SRM User Guide: Discovering Replicated Devices with the FlashArray SRA*.

Recovery plan **SC2-AZ2-Oracle-SRA-RP** for array-based replication is as shown below:



Name	Status	Protected Site	Recovery Site
SC2-AZ2-Oracle-SRA-RP	→ Ready	Primary_Site	DR_Site

Recovery Plan: SC2-AZ2-Oracle-SRA-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

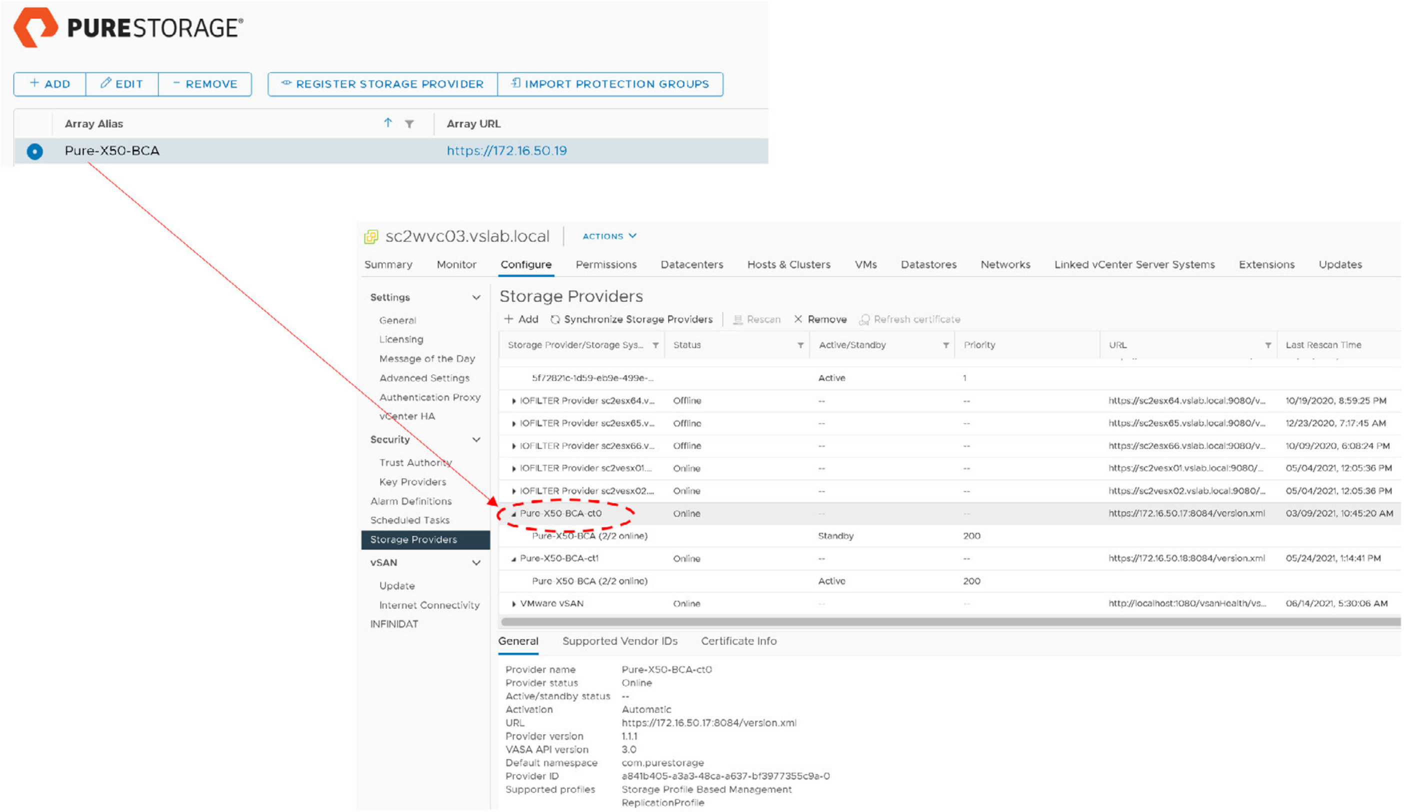
FIGURE 84. Array-Based Replication Recovery Plan Details

More information regarding testing a recovery plan can be found in *SRM User Guide: FlashArray Continuous Replication (ActiveDR) Workflows*.

Further information regarding Site Recovery Manager with array-based replication can be found in *Using Array-Based Replication with Site Recovery Manager*.

VMware Site Recovery Manager with Array-Based Replication (vVOL Level)

Details of Site A Pure Storage **Pure-X50-BCA** vVOL storage providers are as shown below:



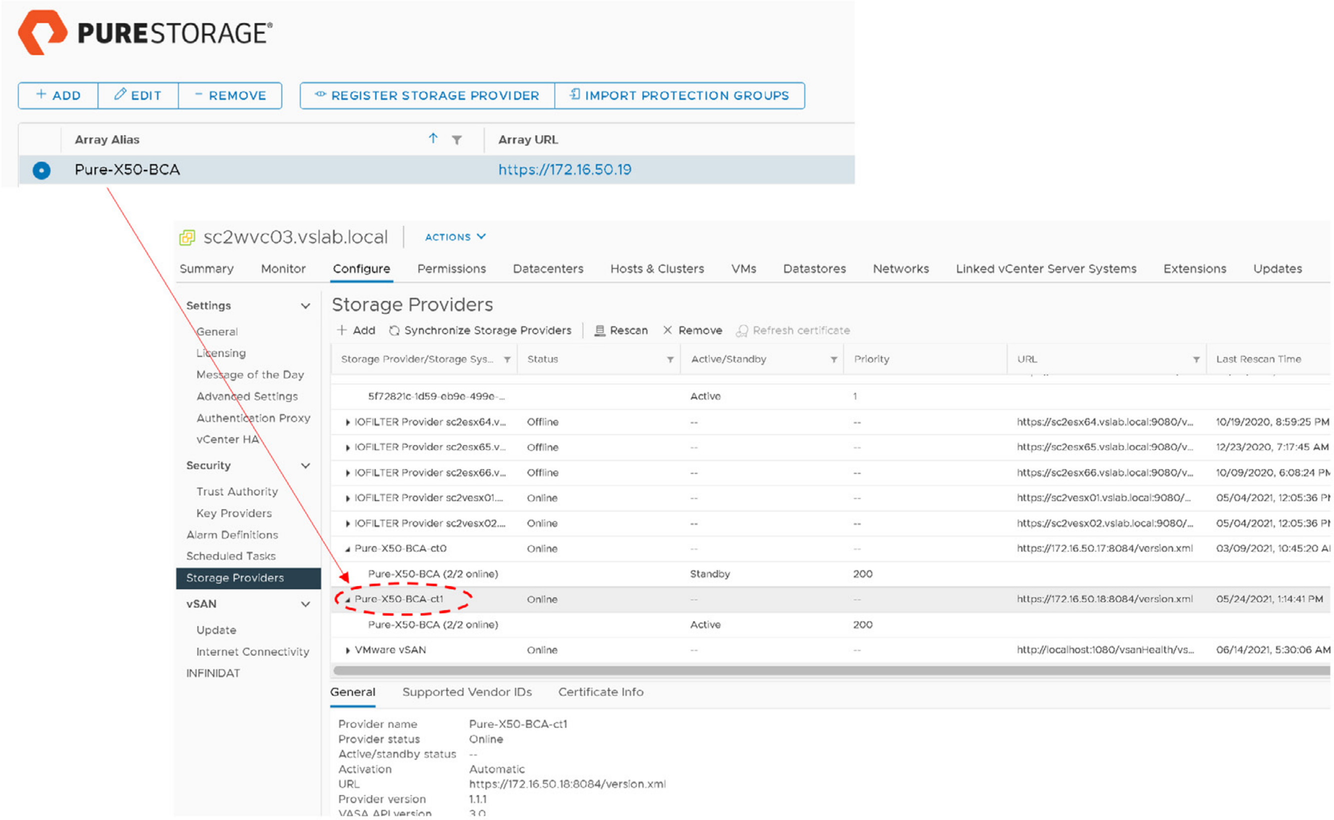
	Array Alias	Array URL
●	Pure-X50-BCA	https://172.16.50.19

Storage Providers

Storage Provider/Storage Sys...	Status	Active/Standby	Priority	URL	Last Rescan Time
5f72821c-1d59-eb9e-499e-...		Active	1		
IOFILTER Provider sc2esx64.v...	Offline	--	--	https://sc2esx64.vslab.local:9080/v...	10/19/2020, 8:59:25 PM
IOFILTER Provider sc2esx65.v...	Offline	--	--	https://sc2esx65.vslab.local:9080/v...	12/23/2020, 7:17:45 AM
IOFILTER Provider sc2esx66.v...	Offline	--	--	https://sc2esx66.vslab.local:9080/v...	10/09/2020, 6:08:24 PM
IOFILTER Provider sc2vesx01....	Online	--	--	https://sc2vesx01.vslab.local:9080/...	05/04/2021, 12:05:36 PM
IOFILTER Provider sc2vesx02....	Online	--	--	https://sc2vesx02.vslab.local:9080/...	05/04/2021, 12:05:36 PM
Pure-X50-BCA-ct0	Online	--	--	https://172.16.50.17:8084/version.xml	03/09/2021, 10:45:20 AM
Pure-X50-BCA (2/2 online)		Standby	200		
Pure-X50-BCA-ct1	Online	--	--	https://172.16.50.18:8084/version.xml	05/24/2021, 1:14:41 PM
Pure-X50-BCA (2/2 online)		Active	200		
VMware vSAN	Online	--	--	http://localhost:1080/vsanHealth/vs...	06/14/2021, 5:30:06 AM

Provider name	Pure-X50-BCA-ct0
Provider status	Online
Active/standby status	--
Activation	Automatic
URL	https://172.16.50.17:8084/version.xml
Provider version	1.1.1
VASA API version	3.0
Default namespace	com.purestorage
Provider ID	a841b405-a3a3-48ca-a637-bf3977355c9a-0
Supported profiles	Storage Profile Based Management ReplicationProfile

FIGURE 85. SITE A: Storage Provider Details—ct0



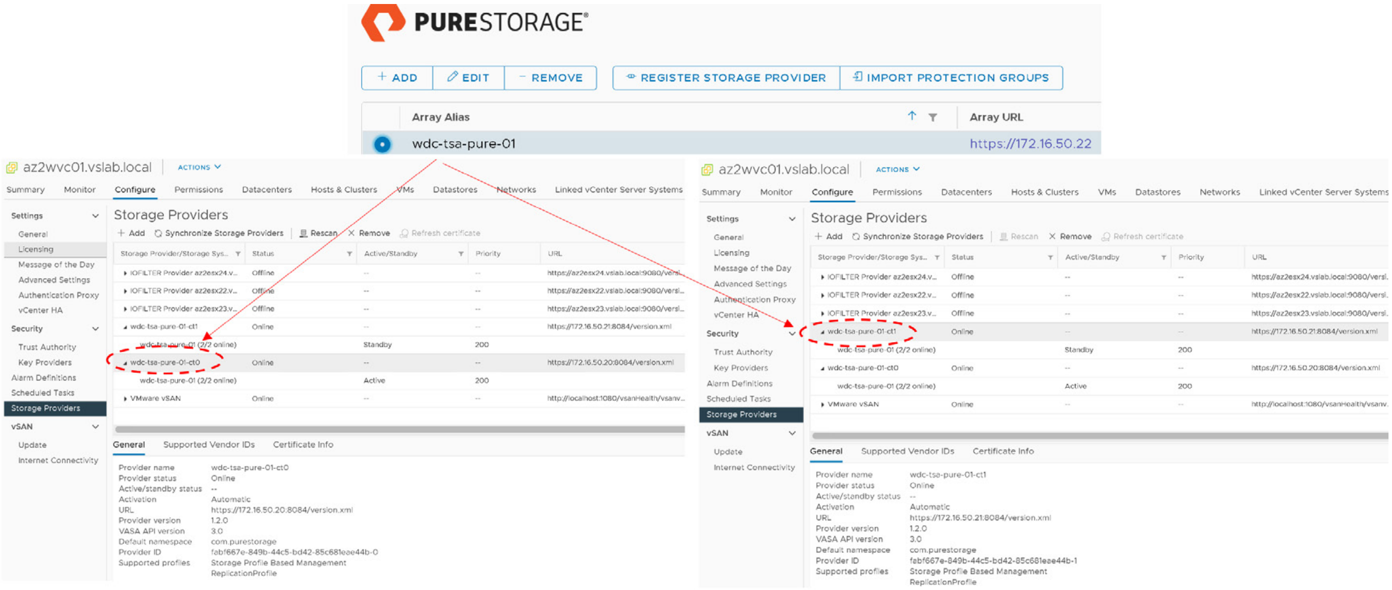
Array Alias	Array URL
Pure-X50-BCA	https://172.16.50.19

Storage Provider/Storage Sys...	Status	Active/Standby	Priority	URL	Last Rescan Time
5f72821c-1d59-eb9e-499e-...		Active	1		
IOFILTER Provider sc2esx64.v...	Offline	--	--	https://sc2esx64.vslab.local:9080/v...	10/19/2020, 8:59:25 PM
IOFILTER Provider sc2esx65.v...	Offline	--	--	https://sc2esx65.vslab.local:9080/v...	12/23/2020, 7:17:45 AM
IOFILTER Provider sc2esx66.v...	Offline	--	--	https://sc2esx66.vslab.local:9080/v...	10/09/2020, 6:08:24 PM
IOFILTER Provider sc2vesx01....	Online	--	--	https://sc2vesx01.vslab.local:9080/...	05/04/2021, 12:05:36 PI
IOFILTER Provider sc2vesx02....	Online	--	--	https://sc2vesx02.vslab.local:9080/...	05/04/2021, 12:05:36 PI
Pure-X50-BCA-ct0	Online	--	--	https://172.16.50.17:8084/version.xml	03/09/2021, 10:45:20 AI
Pure-X50-BCA (2/2 online)		Standby	200		
Pure-X50-BCA-ct1	Online	--	--	https://172.16.50.18:8084/version.xml	05/24/2021, 1:14:41 PM
Pure-X50-BCA (2/2 online)		Active	200		
VMware vSAN	Online	--	--	http://localhost:1080/vsanHealth/vs...	06/14/2021, 5:30:06 AM

Provider name Pure-X50-BCA-ct1
Provider status Online
Active/standby status --
Activation Automatic
URL https://172.16.50.18:8084/version.xml
Provider version 1.1.1
VASA API version 3.0

FIGURE 86. SITE A: Storage Provider Details—ct1

Details of Site B Pure Storage **wdc-tsa-pure-01** vVOL storage providers are as shown below:



Array Alias	Array URL
wdc-tsa-pure-01	https://172.16.50.22

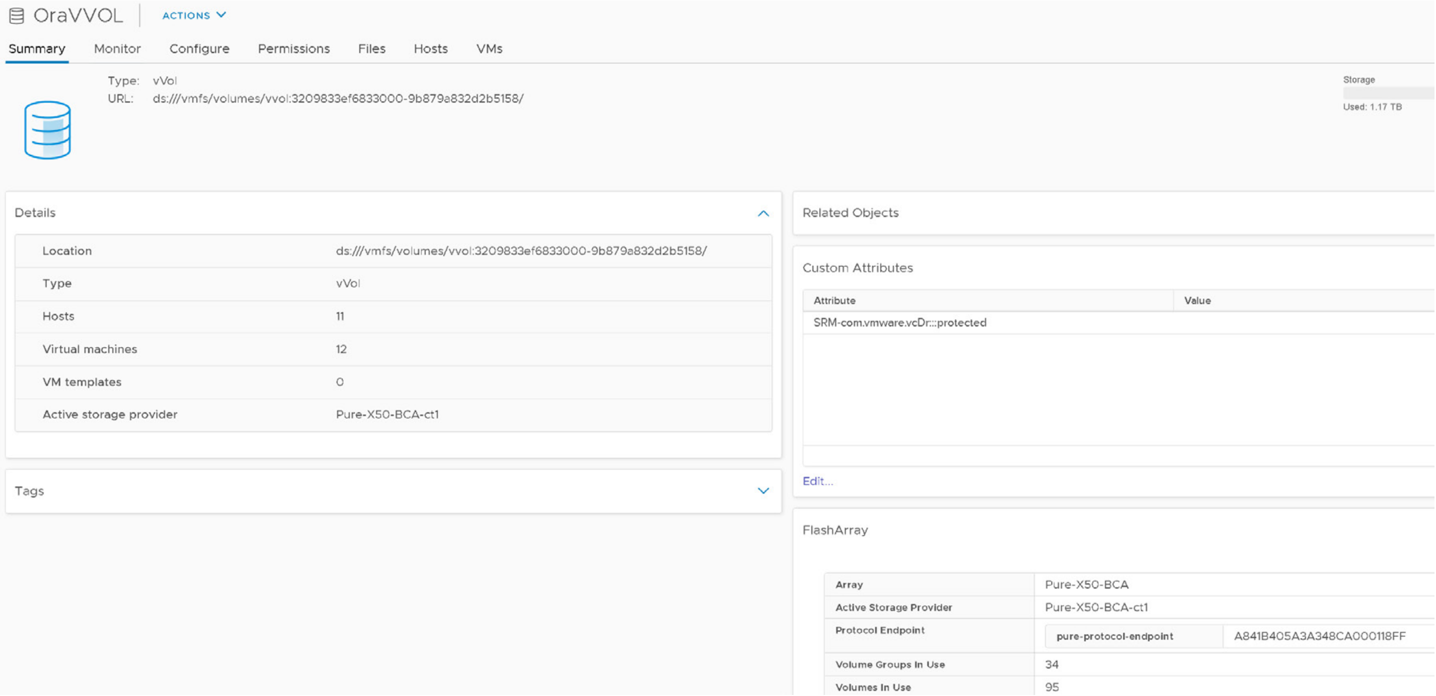
Storage Provider/Storage Sys...	Status	Active/Standby	Priority	URL
IOFILTER Provider az2esx24.v...	Offline	--	--	https://az2esx24.vslab.local:9080/versi...
IOFILTER Provider az2esx22.v...	Offline	--	--	https://az2esx22.vslab.local:9080/versi...
IOFILTER Provider az2esx23.v...	Offline	--	--	https://az2esx23.vslab.local:9080/versi...
wdc-tsa-pure-01-ct1	Online	--	--	https://172.16.50.21:8084/version.xml
wdc-tsa-pure-01 (2/2 online)		Standby	200	
wdc-tsa-pure-01-ct0	Online	--	--	https://172.16.50.20:8084/version.xml
wdc-tsa-pure-01 (2/2 online)		Active	200	
VMware vSAN	Online	--	--	http://localhost:1080/vsanHealth/vsanv...

Provider name wdc-tsa-pure-01-ct0
Provider status Online
Active/standby status --
Activation Automatic
URL https://172.16.50.20:8084/version.xml
Provider version 1.2.0
VASA API version 3.0
Default namespace com.purestorage
Provider ID fabf667e-849b-44c5-bd42-85c681eae44b-0
Supported profiles Storage Profile Based Management
ReplicationProfile

Provider name wdc-tsa-pure-01-ct1
Provider status Online
Active/standby status --
Activation Automatic
URL https://172.16.50.21:8084/version.xml
Provider version 1.2.0
VASA API version 3.0
Default namespace com.purestorage
Provider ID fabf667e-849b-44c5-bd42-85c681eae44b-1
Supported profiles Storage Profile Based Management
ReplicationProfile

FIGURE 87. SITE B: Storage Provider Details

Site A Pure Storage vVOL datastore **OraVVOL** is as shown below:



Type: vVol
URL: ds:///vmfs/volumes/vvol:3209833ef6833000-9b879a832d2b5158/

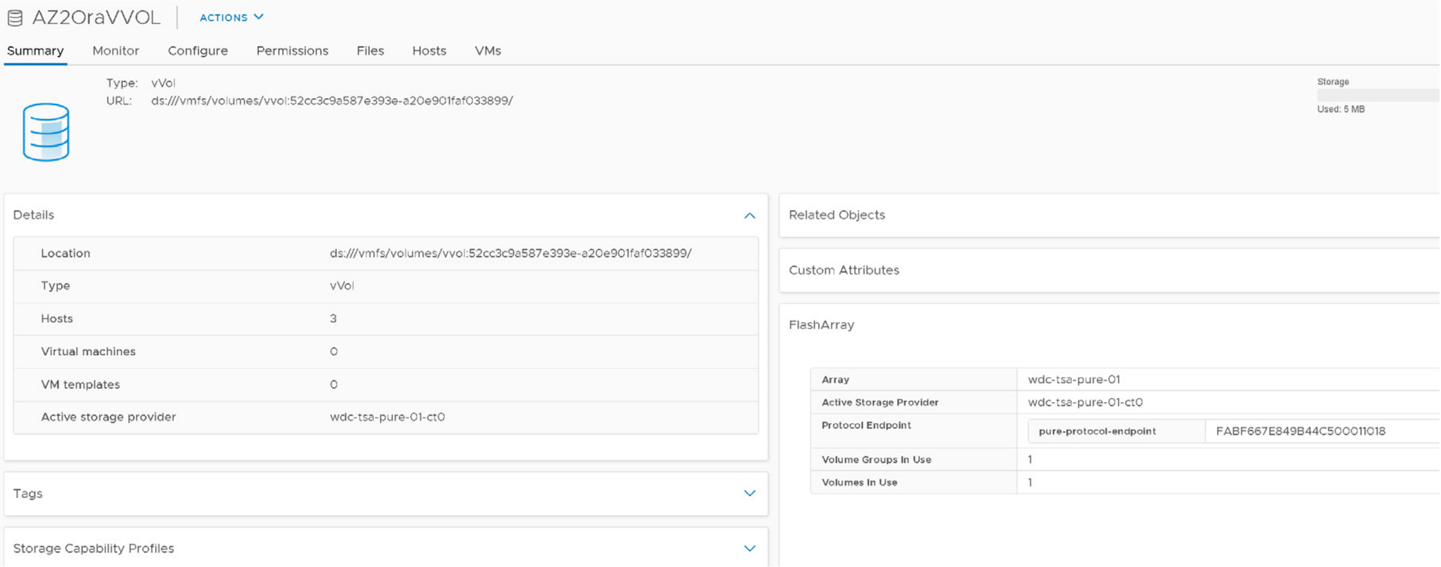
Location	ds:///vmfs/volumes/vvol:3209833ef6833000-9b879a832d2b5158/
Type	vVol
Hosts	11
Virtual machines	12
VM templates	0
Active storage provider	Pure-X50-BCA-ct1

Attribute	Value
SRM-com.vmware.vcDr:::protected	

Array	Pure-X50-BCA
Active Storage Provider	Pure-X50-BCA-ct1
Protocol Endpoint	pure-protocol-endpoint A841B405A3A348CA000118FF
Volume Groups In Use	34
Volumes In Use	95

FIGURE 88. SITE A: vVOL Datastore

Site B Pure Storage vVOL datastore **AZ2OraVVOL** is as shown below:



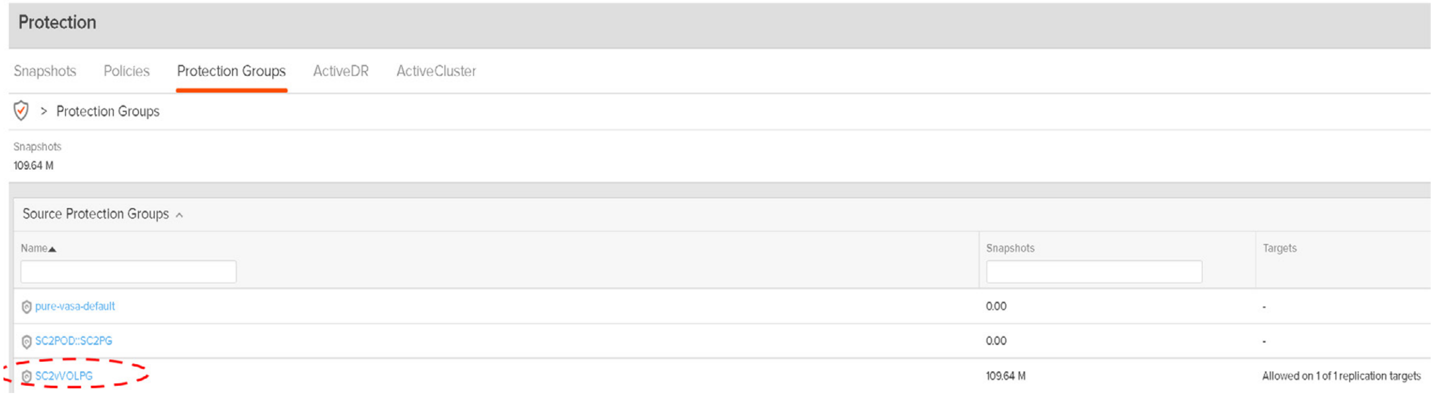
Type: vVol
URL: ds:///vmfs/volumes/vvol:52cc3c9a587e393e-a20e901faf033899/

Location	ds:///vmfs/volumes/vvol:52cc3c9a587e393e-a20e901faf033899/
Type	vVol
Hosts	3
Virtual machines	0
VM templates	0
Active storage provider	wdc-tsa-pure-01-ct0

Array	wdc-tsa-pure-01
Active Storage Provider	wdc-tsa-pure-01-ct0
Protocol Endpoint	pure-protocol-endpoint FABF667E849B44C500011018
Volume Groups In Use	1
Volumes In Use	1

FIGURE 89. SITE B: vVOL Datastore

Create a Pure Storage protection group **SC2vVOLPG** on Site A. We do not need to create a Pure Storage protection group on Site B.


Protection

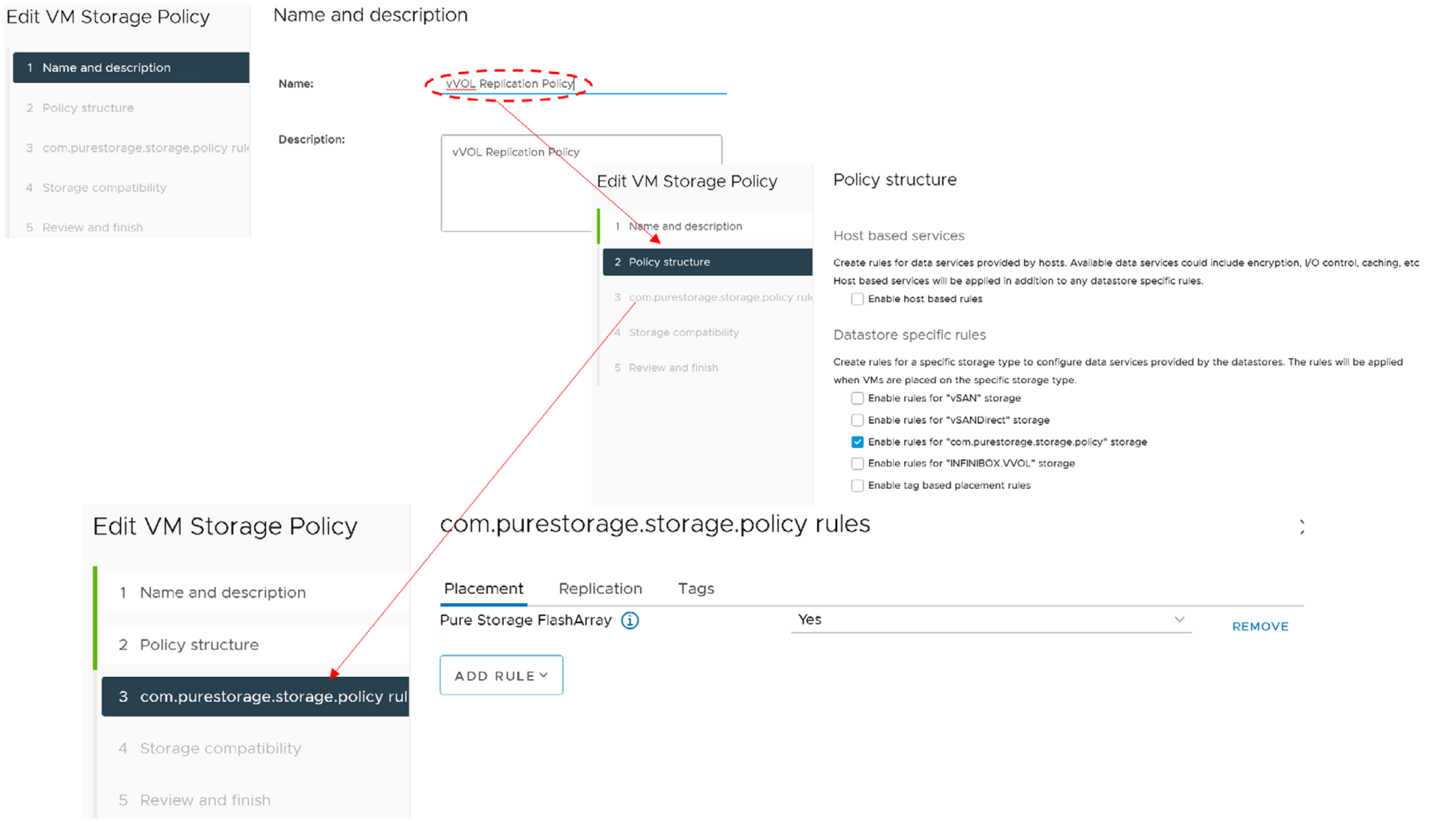
Snapshots
109.64 M

Source Protection Groups

Name	Snapshots	Targets
pure-vasa-default	0.00	-
SC2POD::SC2PG	0.00	-
SC2vVOLPG	109.64 M	Allowed on 1 of 1 replication targets

FIGURE 90. SITE A: Storage Protection Group

Create the VMware replication-based VM storage policy **vVOL Replication Policy** for Site A.



Name and description

Name: vVOL Replication Policy

Description: vVOL Replication Policy

Policy structure

Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc Host based services will be applied in addition to any datastore specific rules.

☐ Enable host based rules

Datastore specific rules

Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

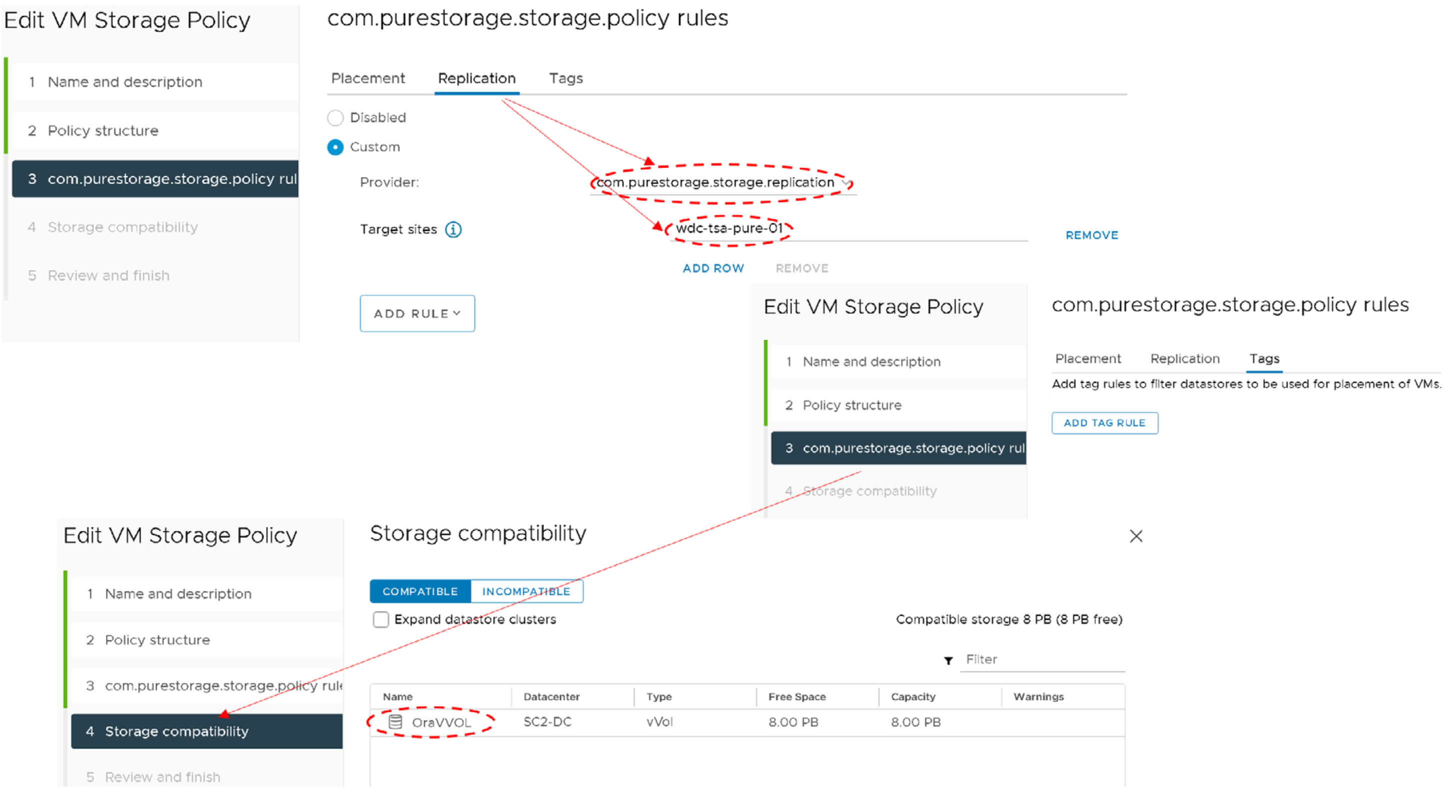
☐ Enable rules for "vSAN" storage
☐ Enable rules for "vSANDirect" storage
☑ Enable rules for "com.purestorage.storage.policy" storage
☐ Enable rules for "INFINIBOX.VVOL" storage
☐ Enable tag based placement rules

com.purestorage.storage.policy rules

Pure Storage FlashArray: Yes

FIGURE 91. Site A vVOL Storage Replication Policy

The following is a continuation of the steps needed to create VMware replication-based VM storage policy **vVOL Replication Policy** for Site A.



Edit VM Storage Policy

1 Name and description
2 Policy structure
3 com.purestorage.storage.policy rul
4 Storage compatibility
5 Review and finish

com.purestorage.storage.policy rules

Placement | Replication | Tags

○ Disabled
● Custom

Provider: com.purestorage.storage.replication

Target sites: wdc-tsa-pure-01 REMOVE

ADD ROW REMOVE

ADD RULE

Edit VM Storage Policy

1 Name and description
2 Policy structure
3 com.purestorage.storage.policy rul
4 Storage compatibility

com.purestorage.storage.policy rules

Placement | Replication | Tags

Add tag rules to filter datastores to be used for placement of VMs.

ADD TAG RULE

Edit VM Storage Policy

1 Name and description
2 Policy structure
3 com.purestorage.storage.policy rule
4 Storage compatibility
5 Review and finish

Storage compatibility

COMPATIBLE | INCOMPATIBLE

□ Expand datastore clusters

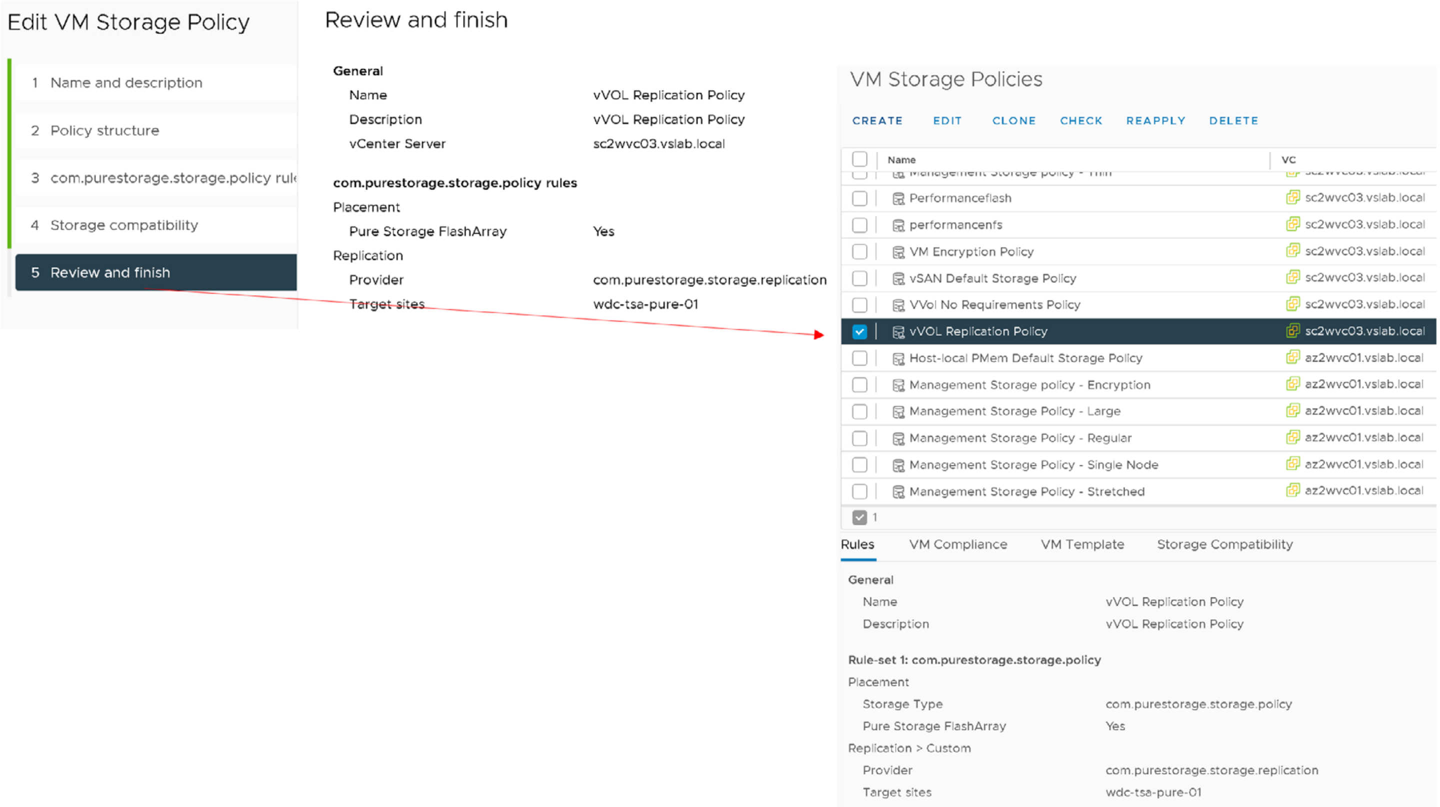
Compatible storage 8 PB (8 PB free)

Filter

Name	Datacenter	Type	Free Space	Capacity	Warnings
OraVVOL	SC2-DC	vVol	8.00 PB	8.00 PB	

FIGURE 92. SITE A: vVOL Storage Replication Policy Continued

The vVOL storage replication policy is created as shown below:



Edit VM Storage Policy

1 Name and description
2 Policy structure
3 com.purestorage.storage.policy rul
4 Storage compatibility
5 Review and finish

Review and finish

General	
Name	vVOL Replication Policy
Description	vVOL Replication Policy
vCenter Server	sc2wvc03.vslab.local
com.purestorage.storage.policy rules	
Placement	
Pure Storage FlashArray	Yes
Replication	
Provider	com.purestorage.storage.replication
Target sites	wdc-tsa-pure-01

VM Storage Policies

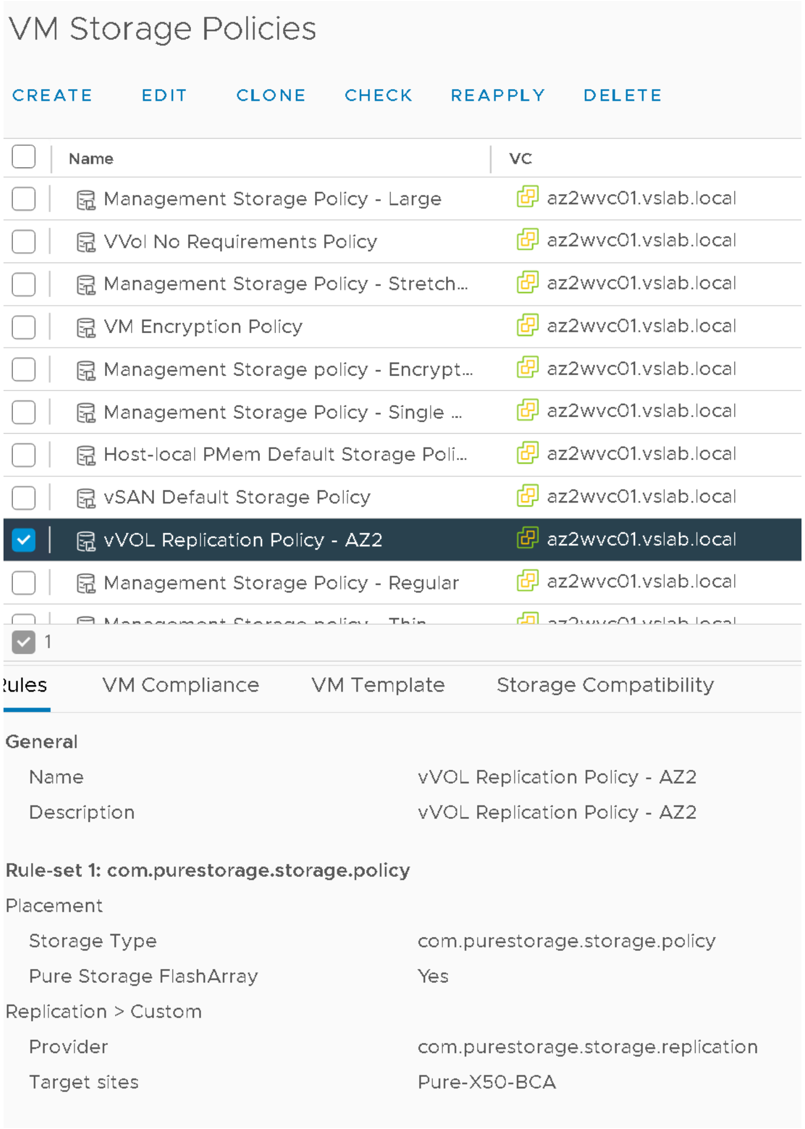
	Name	VC
□	Management Storage policy - Thin	sc2wvc03.vslab.local
□	Performanceflash	sc2wvc03.vslab.local
□	performancenfs	sc2wvc03.vslab.local
□	VM Encryption Policy	sc2wvc03.vslab.local
□	vSAN Default Storage Policy	sc2wvc03.vslab.local
□	VVol No Requirements Policy	sc2wvc03.vslab.local
☑	vVOL Replication Policy	sc2wvc03.vslab.local
□	Host-local PMem Default Storage Policy	az2wvc01.vslab.local
□	Management Storage policy - Encryption	az2wvc01.vslab.local
□	Management Storage Policy - Large	az2wvc01.vslab.local
□	Management Storage Policy - Regular	az2wvc01.vslab.local
□	Management Storage Policy - Single Node	az2wvc01.vslab.local
□	Management Storage Policy - Stretched	az2wvc01.vslab.local

☑ 1

General	
Name	vVOL Replication Policy
Description	vVOL Replication Policy
Rule-set 1: com.purestorage.storage.policy	
Placement	
Storage Type	com.purestorage.storage.policy
Pure Storage FlashArray	Yes
Replication > Custom	
Provider	com.purestorage.storage.replication
Target sites	wdc-tsa-pure-01

FIGURE 93. SITE A: vVOL Storage Replication Policy Complete

Create the VMware replication-based VM storage policy **vVOL Replication Policy** for Site B in the same way.



VM Storage Policies

□	Name	VC
□	Management Storage Policy - Large	az2wvc01.vslab.local
□	VVol No Requirements Policy	az2wvc01.vslab.local
□	Management Storage Policy - Stretch...	az2wvc01.vslab.local
□	VM Encryption Policy	az2wvc01.vslab.local
□	Management Storage policy - Encrypt...	az2wvc01.vslab.local
□	Management Storage Policy - Single ...	az2wvc01.vslab.local
□	Host-local PMem Default Storage Poli...	az2wvc01.vslab.local
□	vSAN Default Storage Policy	az2wvc01.vslab.local
☑	vVOL Replication Policy - AZ2	az2wvc01.vslab.local
□	Management Storage Policy - Regular	az2wvc01.vslab.local
□	Management Storage policy - Thin	az2wvc01.vslab.local

☑ 1

General

Name	vVOL Replication Policy - AZ2
Description	vVOL Replication Policy - AZ2

Rule-set 1: com.purestorage.storage.policy

Placement

Storage Type	com.purestorage.storage.policy
Pure Storage FlashArray	Yes

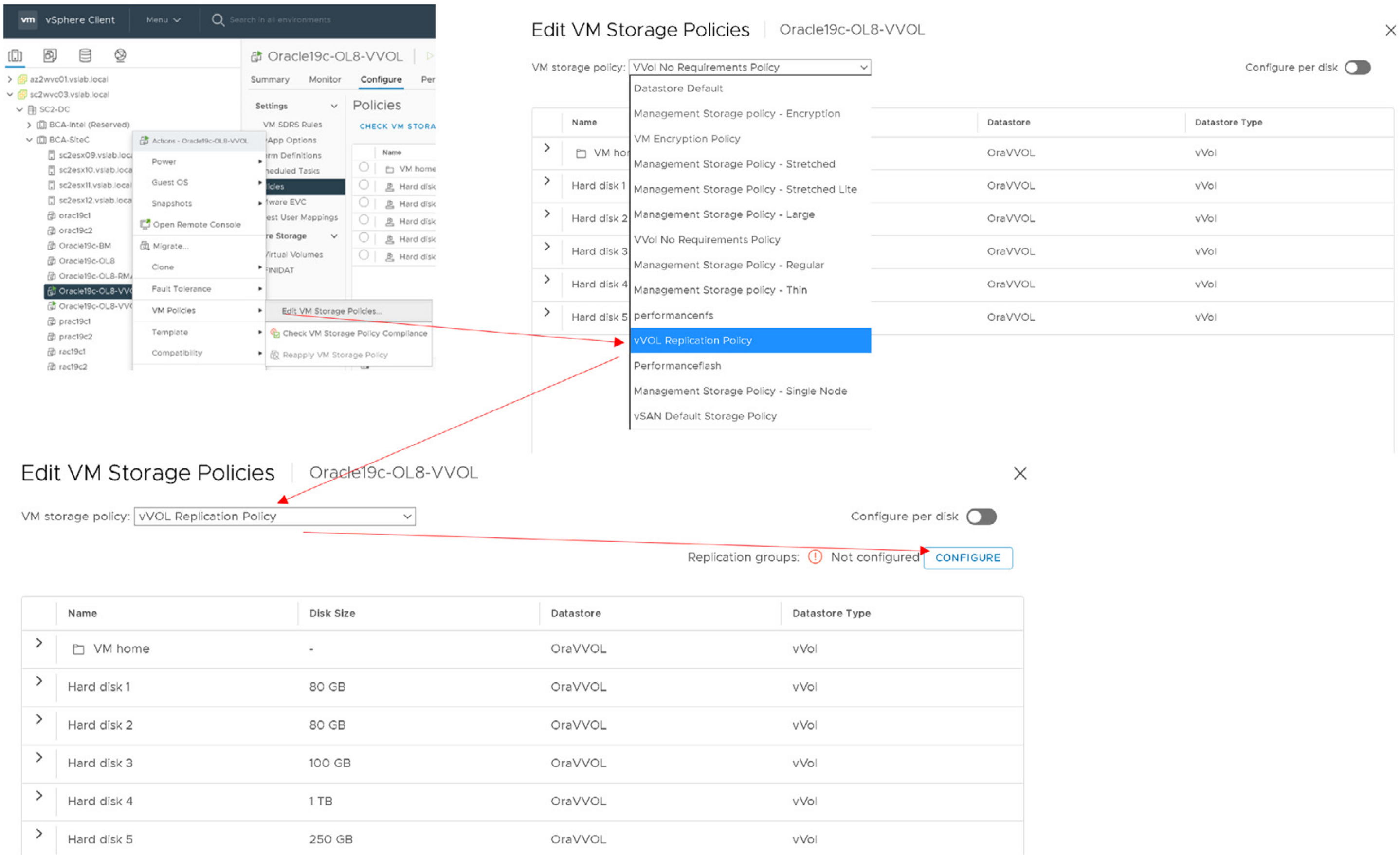
Replication > Custom

Provider	com.purestorage.storage.replication
Target sites	Pure-X50-BCA

FIGURE 94. SITE B: vVOL Storage Replication Policy Details

On Site A, we need to assign the VMware replication-based VM storage policy **vVOL Replication Policy** to both single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** and Oracle RAC **prac19c** VMs to be protected by FlashArray periodic replication.

Steps to assign the VMware replication-based VM storage policy **vVOL Replication Policy** to single-instance Oracle VM **Oracle19c-OL8** are shown below:



Edit VM Storage Policies | Oracle19c-OL8-VVOL

VM storage policy: VVol No Requirements Policy

Configure per disk

Datastore Default
Management Storage policy - Encryption
VM Encryption Policy
Management Storage Policy - Stretched
Management Storage Policy - Stretched Lite
Management Storage Policy - Large
VVol No Requirements Policy
Management Storage Policy - Regular
Management Storage policy - Thin
performancenfs
vVOL Replication Policy
Performanceflash
Management Storage Policy - Single Node
vSAN Default Storage Policy

Name	Datastore	Datastore Type
VM ho	OraVVOL	vVol
Hard disk 1	OraVVOL	vVol
Hard disk 2	OraVVOL	vVol
Hard disk 3	OraVVOL	vVol
Hard disk 4	OraVVOL	vVol
Hard disk 5	OraVVOL	vVol

Edit VM Storage Policies | Oracle19c-OL8-VVOL

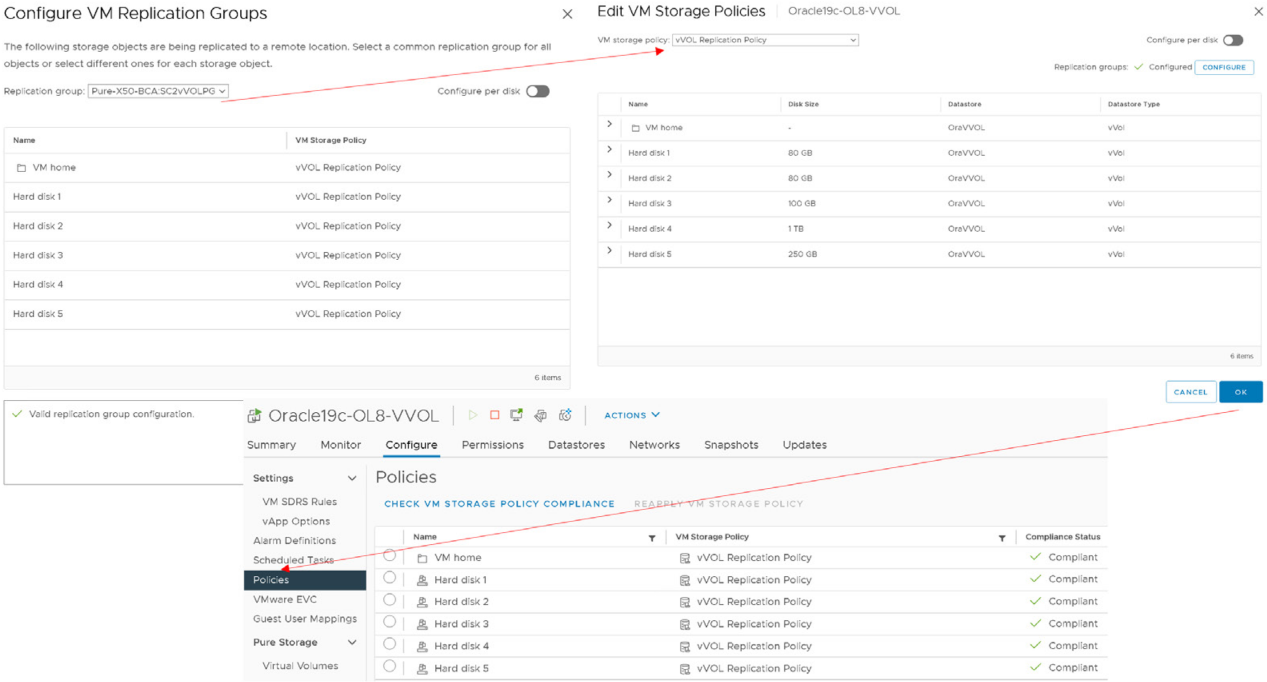
VM storage policy: vVOL Replication Policy

Configure per disk

Replication groups: ⓘ Not configured CONFIGURE

Name	Disk Size	Datastore	Datastore Type
VM home	-	OraVVOL	vVol
Hard disk 1	80 GB	OraVVOL	vVol
Hard disk 2	80 GB	OraVVOL	vVol
Hard disk 3	100 GB	OraVVOL	vVol
Hard disk 4	1 TB	OraVVOL	vVol
Hard disk 5	250 GB	OraVVOL	vVol

FIGURE 95. SITE A: Assign Storage Policy vVOL Replication Policy to VMs



Configure VM Replication Groups

The following storage objects are being replicated to a remote location. Select a common replication group for all objects or select different ones for each storage object.

Replication group: Pure-X50-BCA:SC2vVOLPG

Configure per disk

Name	VM Storage Policy
VM home	vVOL Replication Policy
Hard disk 1	vVOL Replication Policy
Hard disk 2	vVOL Replication Policy
Hard disk 3	vVOL Replication Policy
Hard disk 4	vVOL Replication Policy
Hard disk 5	vVOL Replication Policy

6 items

✓ Valid replication group configuration.

Edit VM Storage Policies | Oracle19c-OL8-VVOL

VM storage policy: vVOL Replication Policy

Configure per disk

Replication groups: ✓ Configured CONFIGURE

Name	Disk Size	Datastore	Datastore Type
VM home	-	OraVVOL	vVol
Hard disk 1	80 GB	OraVVOL	vVol
Hard disk 2	80 GB	OraVVOL	vVol
Hard disk 3	100 GB	OraVVOL	vVol
Hard disk 4	1 TB	OraVVOL	vVol
Hard disk 5	250 GB	OraVVOL	vVol

6 items

CANCEL OK

Oracle19c-OL8-VVOL

Policies

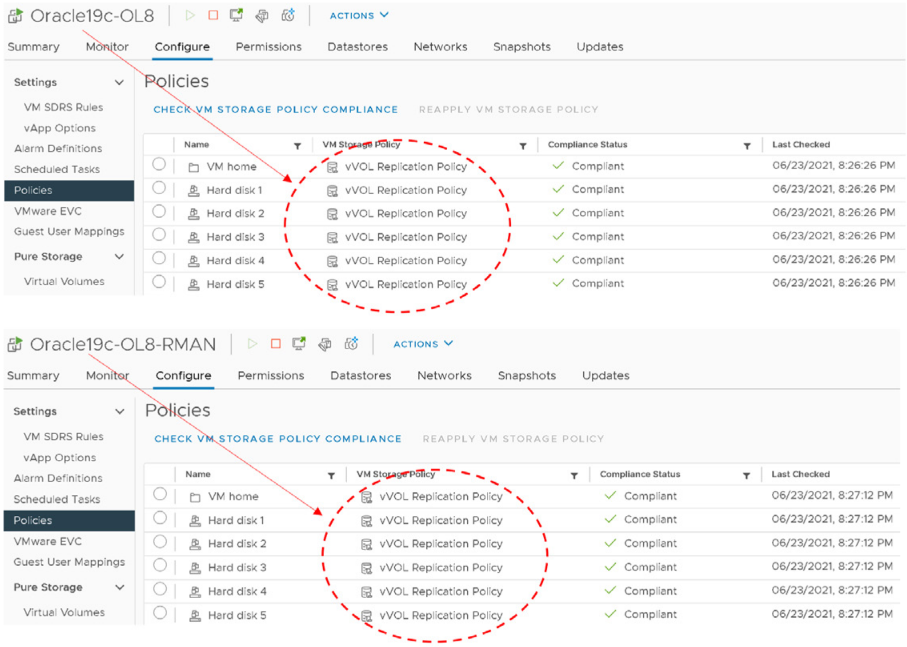
CHECK VM STORAGE POLICY COMPLIANCE REAPPLY VM STORAGE POLICY

Name	VM Storage Policy	Compliance Status
VM home	vVOL Replication Policy	✓ Compliant
Hard disk 1	vVOL Replication Policy	✓ Compliant
Hard disk 2	vVOL Replication Policy	✓ Compliant
Hard disk 3	vVOL Replication Policy	✓ Compliant
Hard disk 4	vVOL Replication Policy	✓ Compliant
Hard disk 5	vVOL Replication Policy	✓ Compliant

FIGURE 96. SITE A: Assign Storage Policy vVOL Replication Policy to VMs Continued

Steps to assign the replication-based VM to single-instance Oracle VM **Oracle19c-OL8-RMAN** and Oracle RAC **prac19c** VMs are the same as shown above.

Single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** now have storage policy **vVOL Replication Policy** applied.



Oracle19c-OL8

Policies

CHECK VM STORAGE POLICY COMPLIANCE REAPPLY VM STORAGE POLICY

Name	VM Storage Policy	Compliance Status	Last Checked
VM home	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:26:26 PM
Hard disk 1	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:26:26 PM
Hard disk 2	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:26:26 PM
Hard disk 3	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:26:26 PM
Hard disk 4	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:26:26 PM
Hard disk 5	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:26:26 PM

Oracle19c-OL8-RMAN

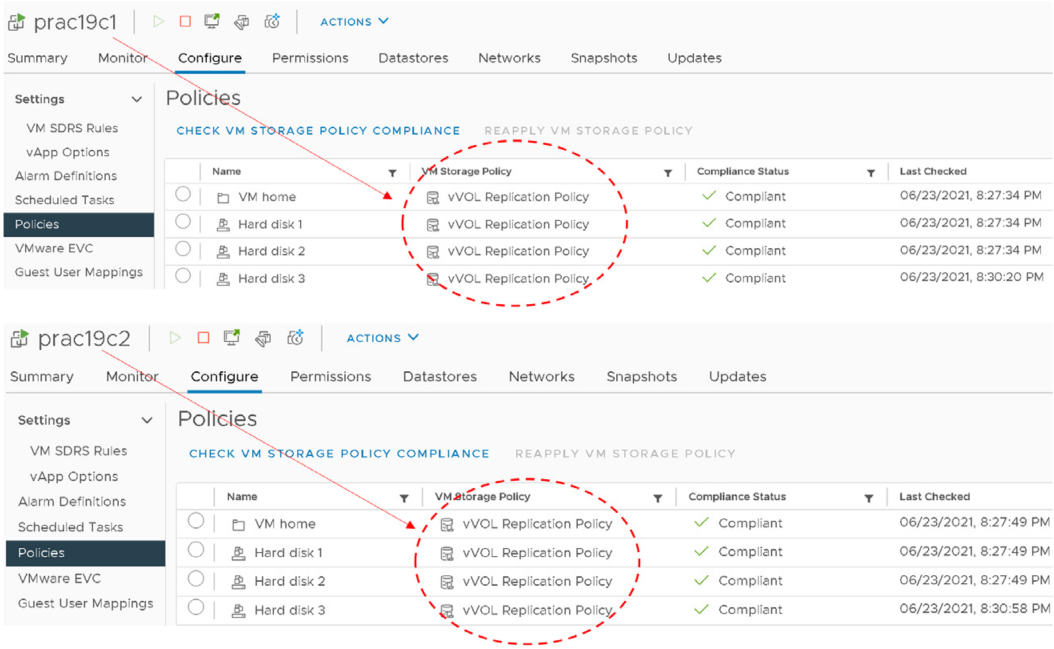
Policies

CHECK VM STORAGE POLICY COMPLIANCE REAPPLY VM STORAGE POLICY

Name	VM Storage Policy	Compliance Status	Last Checked
VM home	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:12 PM
Hard disk 1	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:12 PM
Hard disk 2	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:12 PM
Hard disk 3	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:12 PM
Hard disk 4	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:12 PM
Hard disk 5	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:12 PM

FIGURE 97. SITE A: Single-Instance VM’s Storage Policy vVOL Replication Policy

Oracle RAC **prac19c** VMs now have storage policy **vVOL Replication Policy** applied.



prac19c1

Policies

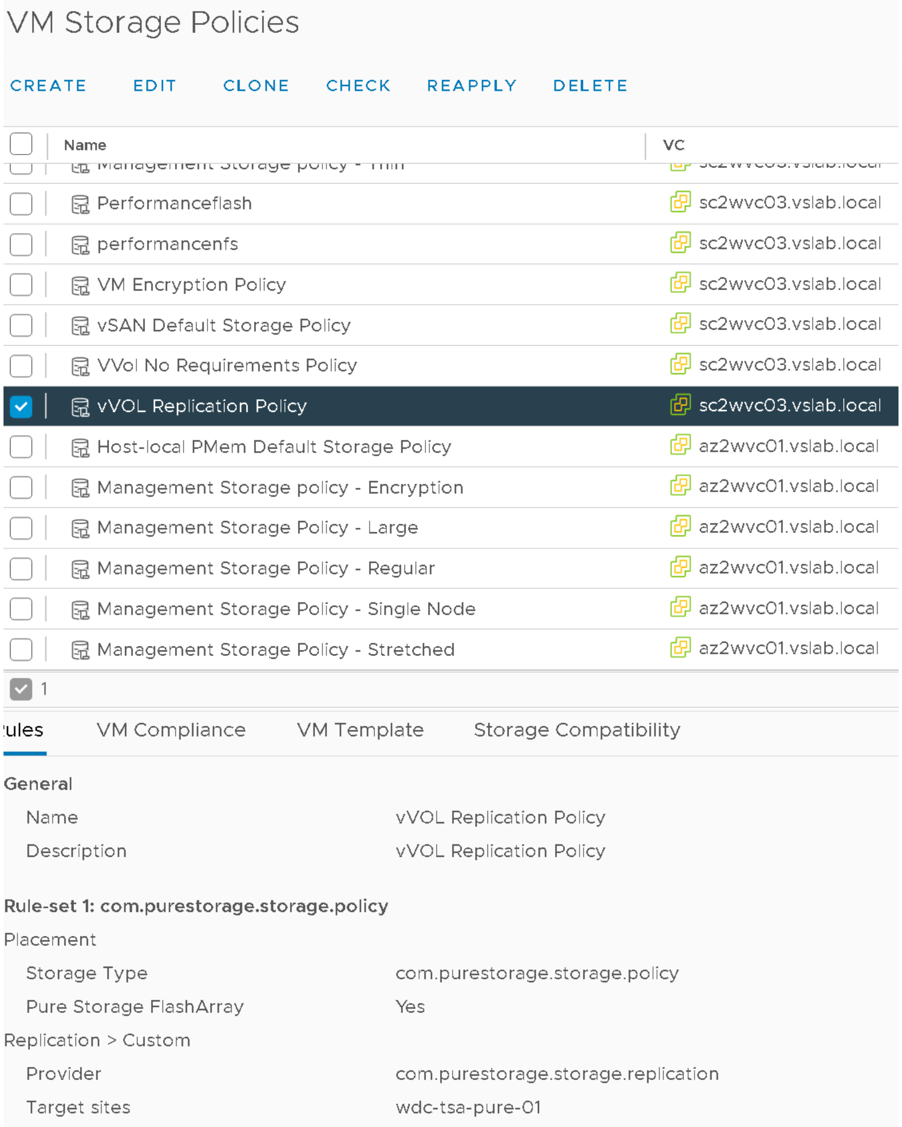
Name	VM Storage Policy	Compliance Status	Last Checked
VM home	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:34 PM
Hard disk 1	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:34 PM
Hard disk 2	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:34 PM
Hard disk 3	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:30:20 PM

prac19c2

Policies

Name	VM Storage Policy	Compliance Status	Last Checked
VM home	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:49 PM
Hard disk 1	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:49 PM
Hard disk 2	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:27:49 PM
Hard disk 3	vVOL Replication Policy	✓ Compliant	06/23/2021, 8:30:58 PM

FIGURE 98. SITE A: Oracle RAC VM’s Storage Policy vVOL Replication Policy



VM Storage Policies

☐	Name	VC
☐	Management Storage policy - Thin	sc2wvc03.vslab.local
☐	Performanceflash	sc2wvc03.vslab.local
☐	performancenfs	sc2wvc03.vslab.local
☐	VM Encryption Policy	sc2wvc03.vslab.local
☐	vSAN Default Storage Policy	sc2wvc03.vslab.local
☐	VVol No Requirements Policy	sc2wvc03.vslab.local
☑	vVOL Replication Policy	sc2wvc03.vslab.local
☐	Host-local PMem Default Storage Policy	az2wvc01.vslab.local
☐	Management Storage policy - Encryption	az2wvc01.vslab.local
☐	Management Storage Policy - Large	az2wvc01.vslab.local
☐	Management Storage Policy - Regular	az2wvc01.vslab.local
☐	Management Storage Policy - Single Node	az2wvc01.vslab.local
☐	Management Storage Policy - Stretched	az2wvc01.vslab.local

☑ 1

General

Name: vVOL Replication Policy

Description: vVOL Replication Policy

Rule-set 1: com.purestorage.storage.policy

Placement

Storage Type: com.purestorage.storage.policy

Pure Storage FlashArray: Yes

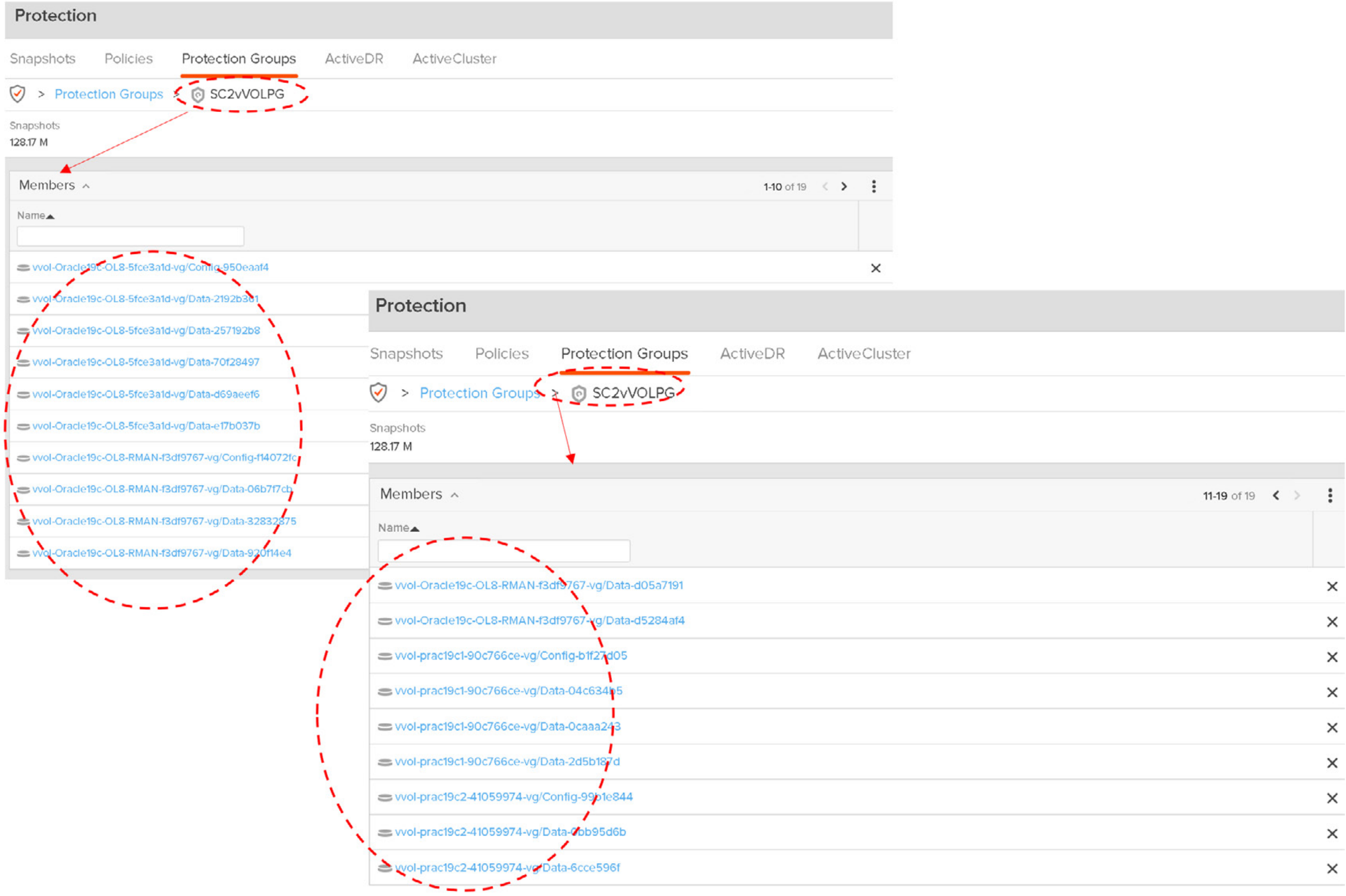
Replication > Custom

Provider: com.purestorage.storage.replication

Target sites: wdc-tsa-pure-01

FIGURE 99. SITE B: Storage Policy vVOL Replication Policy

The single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** VM and the Oracle RAC **vvolrac** VMs to be protected by FlashArray periodic replication are now part of the Site A Pure Storage protection group **SC2vVOLPG**.

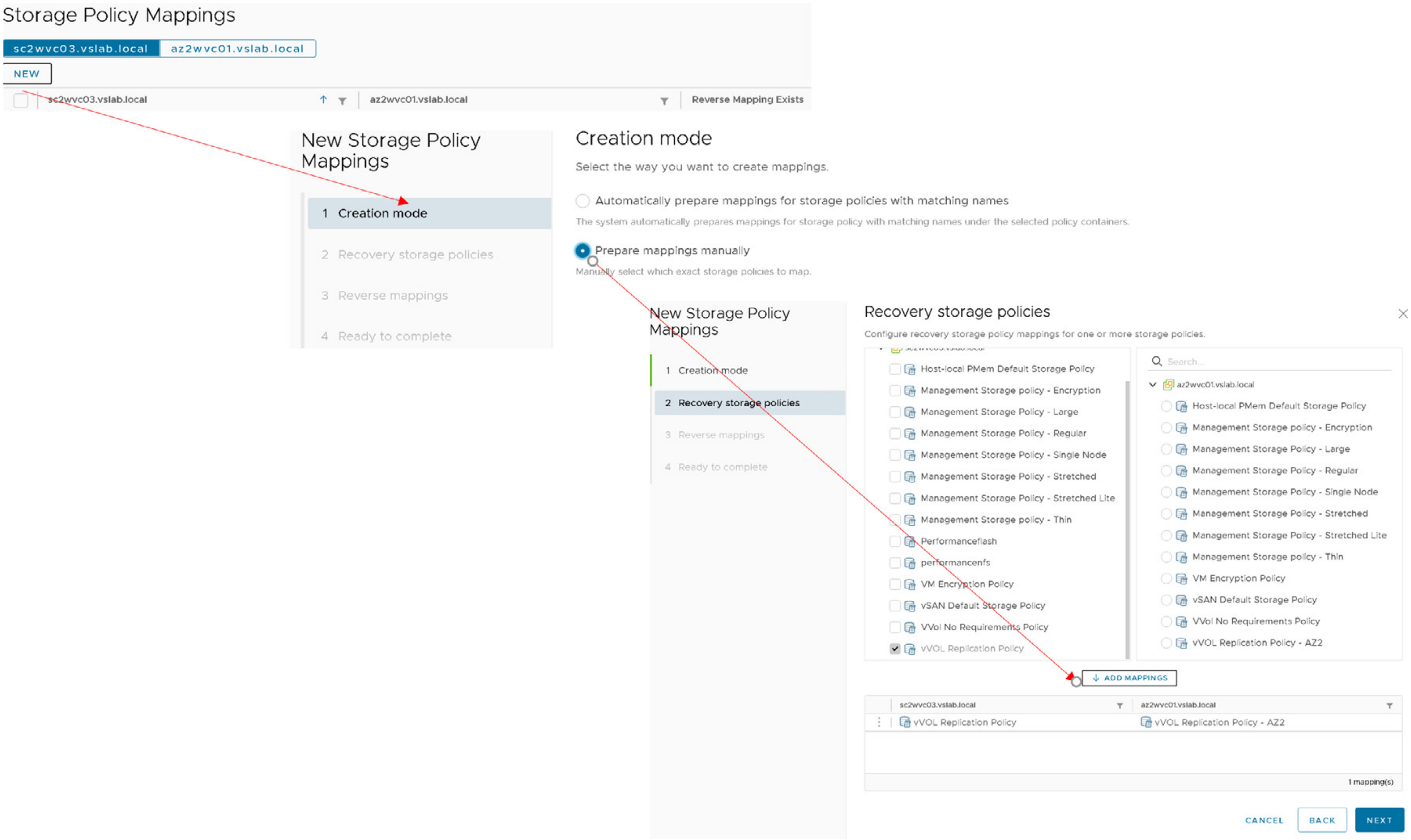


vvol-Oracle19c-OL8-5fce3a1d-vg/Config-950eaaf4
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-2192b381
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-257192b8
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-70f28497
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-d69aeef6
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-e17b037b
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Config-f14072fc
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-06b7f7cb
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-32832875
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-920f14e4

vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d05a7191
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d5284af4
vvol-prac19c1-90c766ce-vg/Config-b1f27d05
vvol-prac19c1-90c766ce-vg/Data-04c634b5
vvol-prac19c1-90c766ce-vg/Data-0caaa243
vvol-prac19c1-90c766ce-vg/Data-2d5b187d
vvol-prac19c2-41059974-vg/Config-99b1e844
vvol-prac19c2-41059974-vg/Data-0bb95d6b
vvol-prac19c2-41059974-vg/Data-6cce596f

FIGURE 100. SITE B: Storage Protection Groups and vVOLs

Create vSphere Virtual Volumes replication storage policy mappings between Site A and Site B.



Storage Policy Mappings

New Storage Policy Mappings

1 Creation mode
2 Recovery storage policies
3 Reverse mappings
4 Ready to complete

Creation mode

Select the way you want to create mappings.

○ Automatically prepare mappings for storage policies with matching names

The system automatically prepares mappings for storage policy with matching names under the selected policy containers.

● Prepare mappings manually

Manually select which exact storage policies to map.

New Storage Policy Mappings

1 Creation mode
2 Recovery storage policies
3 Reverse mappings
4 Ready to complete

Recovery storage policies

Configure recovery storage policy mappings for one or more storage policies.

- □ Host-local PMem Default Storage Policy
- □ Management Storage policy - Encryption
- □ Management Storage Policy - Large
- □ Management Storage Policy - Regular
- □ Management Storage Policy - Single Node
- □ Management Storage Policy - Stretched
- □ Management Storage Policy - Stretched Lite
- □ Management Storage policy - Thin
- □ Performanceflash
- □ performancenfs
- □ VM Encryption Policy
- □ vSAN Default Storage Policy
- □ VVol No Requirements Policy
- ☑ vVOL Replication Policy

Search...

az2wvc01.vslab.local

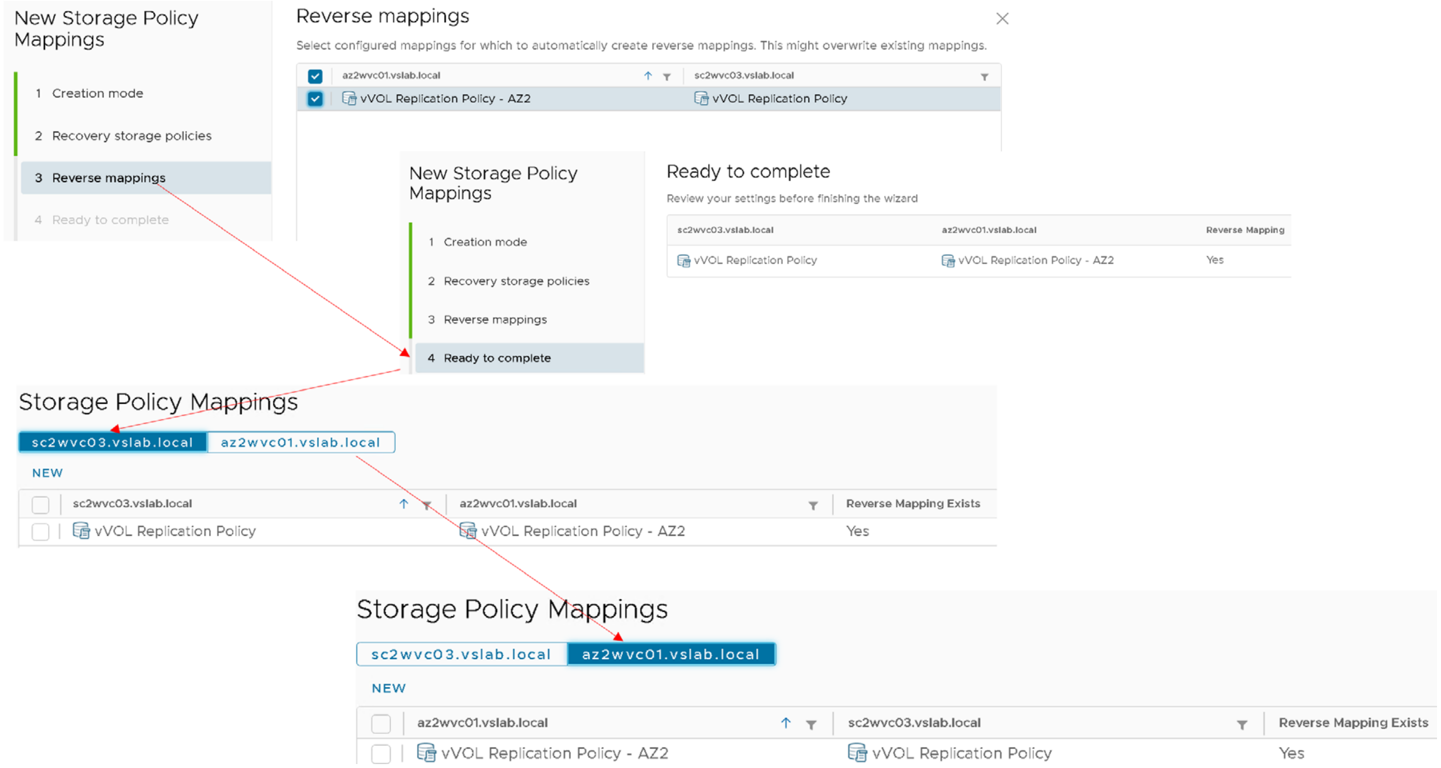
- ○ Host-local PMem Default Storage Policy
- ○ Management Storage policy - Encryption
- ○ Management Storage Policy - Large
- ○ Management Storage Policy - Regular
- ○ Management Storage Policy - Single Node
- ○ Management Storage Policy - Stretched
- ○ Management Storage Policy - Stretched Lite
- ○ Management Storage policy - Thin
- ○ VM Encryption Policy
- ○ vSAN Default Storage Policy
- ○ VVol No Requirements Policy
- ○ vVOL Replication Policy - AZ2

sc2wvc03.vslab.local	az2wvc01.vslab.local
vVOL Replication Policy	vVOL Replication Policy - AZ2

1 mapping(s)

FIGURE 101. vVOL Replication Storage Policy Mapping Between Site A and B

Further steps to create vSphere Virtual Volumes replication storage policy mappings between Site A and Site B are as shown below:



New Storage Policy Mappings

1 Creation mode
2 Recovery storage policies
3 Reverse mappings
4 Ready to complete

Reverse mappings

Select configured mappings for which to automatically create reverse mappings. This might overwrite existing mappings.

	az2wvc01.vslab.local	sc2wvc03.vslab.local
☑	vVOL Replication Policy - AZ2	vVOL Replication Policy

New Storage Policy Mappings

1 Creation mode
2 Recovery storage policies
3 Reverse mappings
4 Ready to complete

Ready to complete

Review your settings before finishing the wizard

sc2wvc03.vslab.local	az2wvc01.vslab.local	Reverse Mapping
vVOL Replication Policy	vVOL Replication Policy - AZ2	Yes

Storage Policy Mappings

sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW

	sc2wvc03.vslab.local	az2wvc01.vslab.local	Reverse Mapping Exists
□	vVOL Replication Policy	vVOL Replication Policy - AZ2	Yes

Storage Policy Mappings

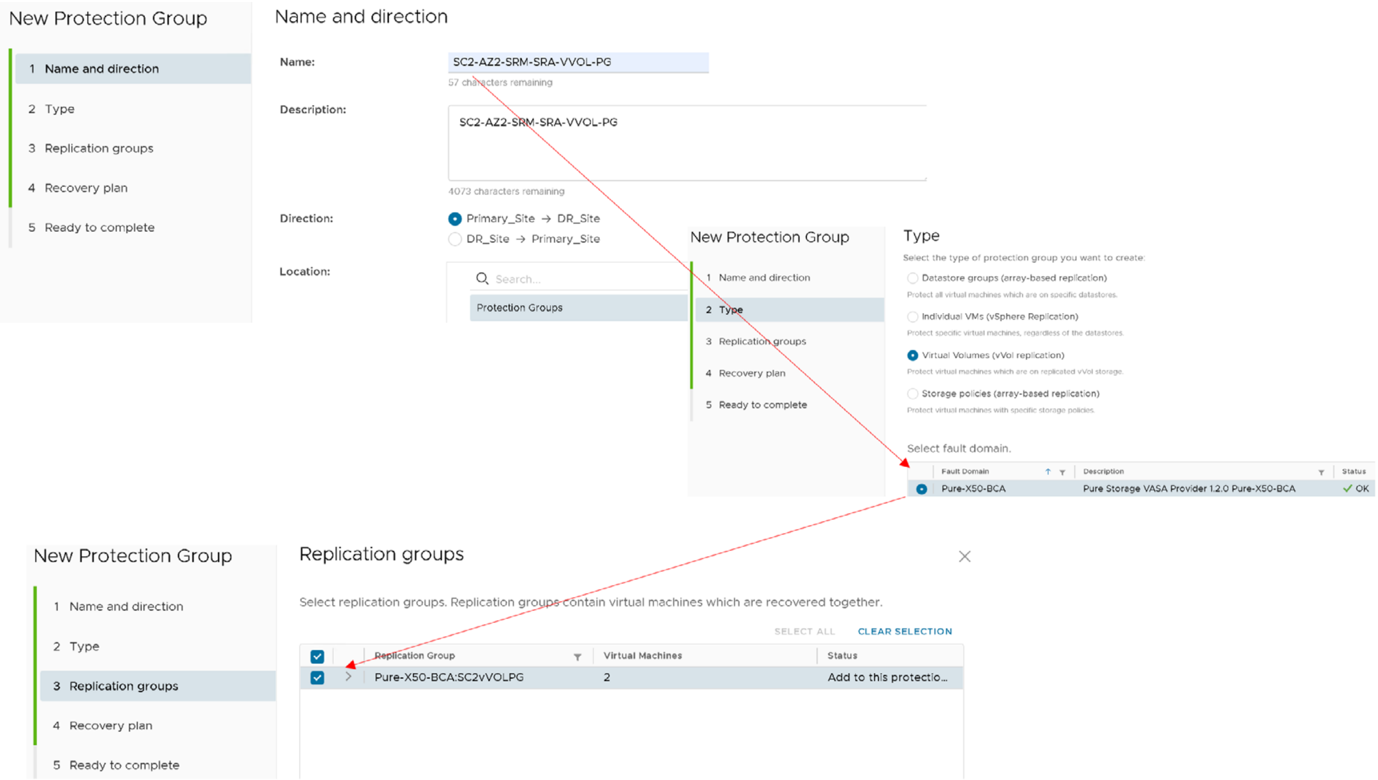
sc2wvc03.vslab.local | az2wvc01.vslab.local

NEW

	az2wvc01.vslab.local	sc2wvc03.vslab.local	Reverse Mapping Exists
□	vVOL Replication Policy - AZ2	vVOL Replication Policy	Yes

FIGURE 102. vVOL Replication Storage Policy Mapping Between Site A and B Continued

Create a new VMware Site Recovery Manager protection group **SC2-AZ2-SRM-SRA-VVOL-PG** on Site A for vVOL-based replication.



Name and direction

Name: SC2-AZ2-SRM-SRA-VVOL-PG
57 characters remaining

Description: SC2-AZ2-SRM-SRA-VVOL-PG
4073 characters remaining

Direction:
● Primary_Site → DR_Site
○ DR_Site → Primary_Site

Location: Protection Groups

Type

Select the type of protection group you want to create:

○ Datastore groups (array-based replication)
Protect all virtual machines which are on specific datastores.

○ Individual VMs (vSphere Replication)
Protect specific virtual machines, regardless of the datastores.

● Virtual Volumes (vVol replication)
Protect virtual machines which are on replicated vVol storage.

○ Storage policies (array-based replication)
Protect virtual machines with specific storage policies.

Select fault domain.

	Fault Domain	Description	Status
●	Pure-X50-BCA	Pure Storage VASA Provider 1.2.0 Pure-X50-BCA	✓ OK

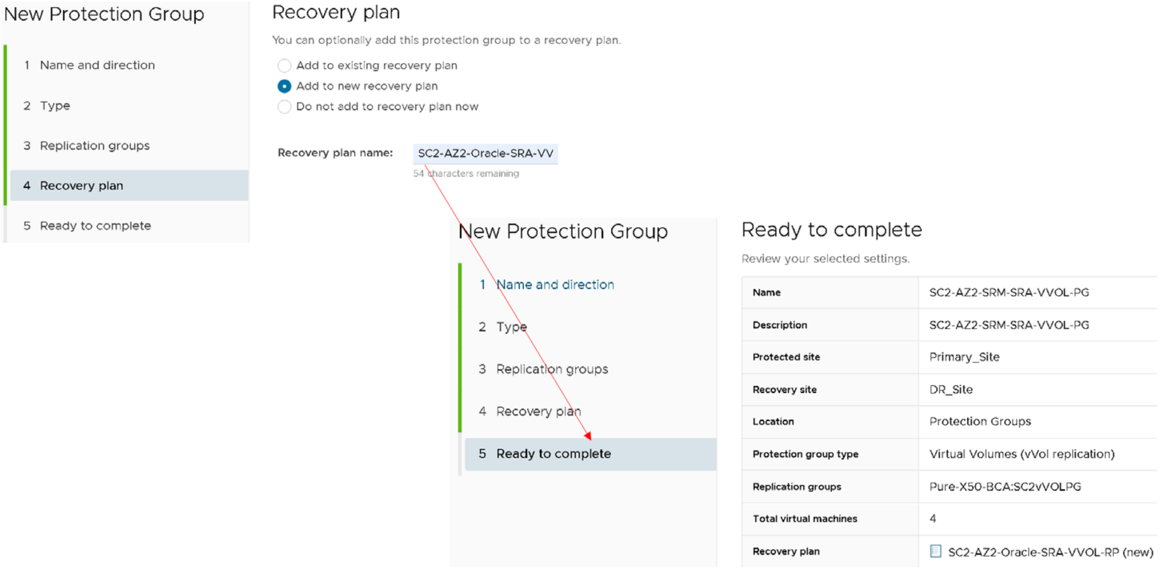
Replication groups

Select replication groups. Replication groups contain virtual machines which are recovered together.

☑		Replication Group	Virtual Machines	Status
☑	>	Pure-X50-BCA:SC2vVOLPG	2	Add to this protectio...

FIGURE 103. SITE A: Site Recovery Manager Protection Group for vVOL

Create a new VMware Site Recovery Manager recovery plan **SC2-AZ2-Oracle-SRA-VV** on Site A for vVOL-based replication.



Recovery plan

You can optionally add this protection group to a recovery plan.

○ Add to existing recovery plan
● Add to new recovery plan
○ Do not add to recovery plan now

Recovery plan name: SC2-AZ2-Oracle-SRA-VV
54 characters remaining

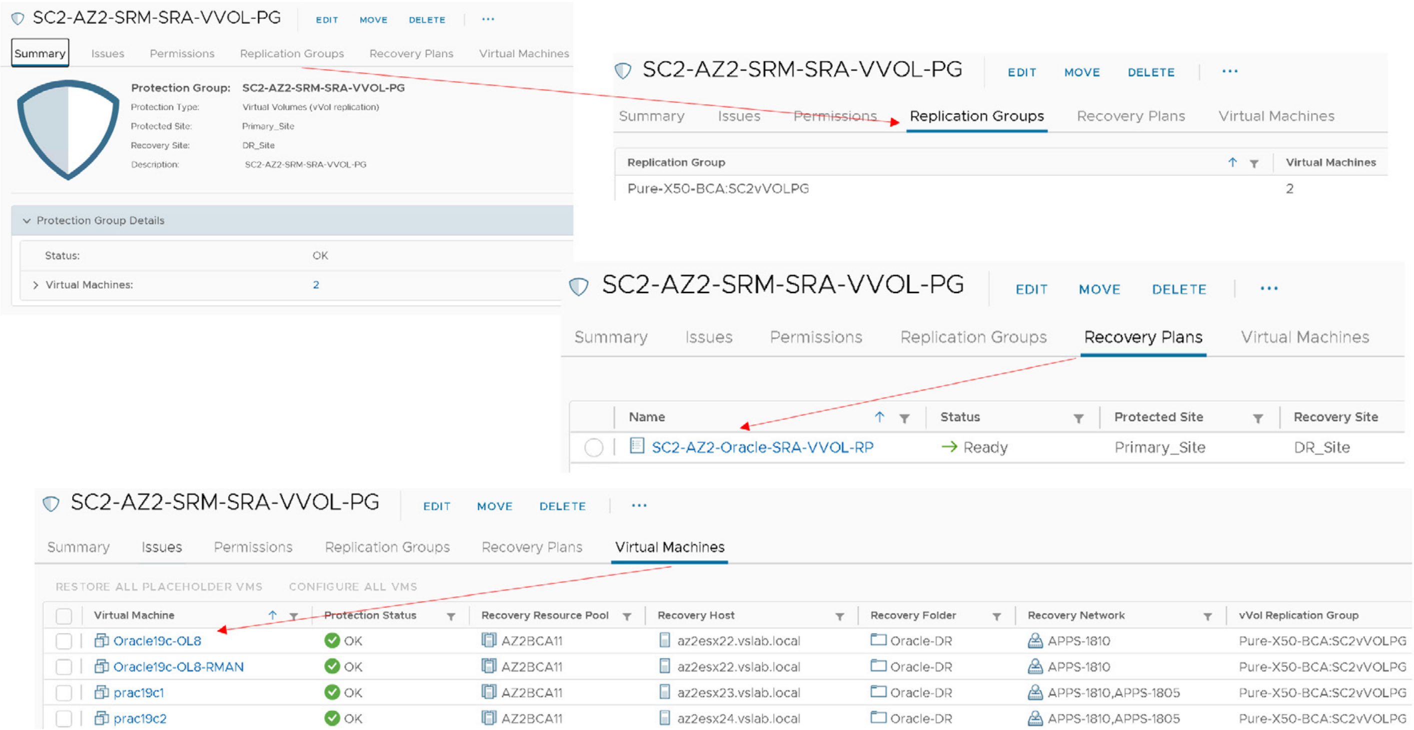
Ready to complete

Review your selected settings.

Name	SC2-AZ2-SRM-SRA-VVOL-PG
Description	SC2-AZ2-SRM-SRA-VVOL-PG
Protected site	Primary_Site
Recovery site	DR_Site
Location	Protection Groups
Protection group type	Virtual Volumes (vVol replication)
Replication groups	Pure-X50-BCA:SC2vVOLPG
Total virtual machines	4
Recovery plan	SC2-AZ2-Oracle-SRA-VVOL-RP (new)

FIGURE 104. SITE A: Site Recovery Manager Protection Group for vVOL Continued

The Site Recovery Manager protection group on Site A **SC2-AZ2-SRM-SRA-VVOL-PG** and the protected VMs are shown below:



Protection Group: SC2-AZ2-SRM-SRA-VVOL-PG
Protection Type: Virtual Volumes (vVol replication)
Protected Site: Primary_Site
Recovery Site: DR_Site
Description: SC2-AZ2-SRM-SRA-VVOL-PG

Status: OK
Virtual Machines: 2

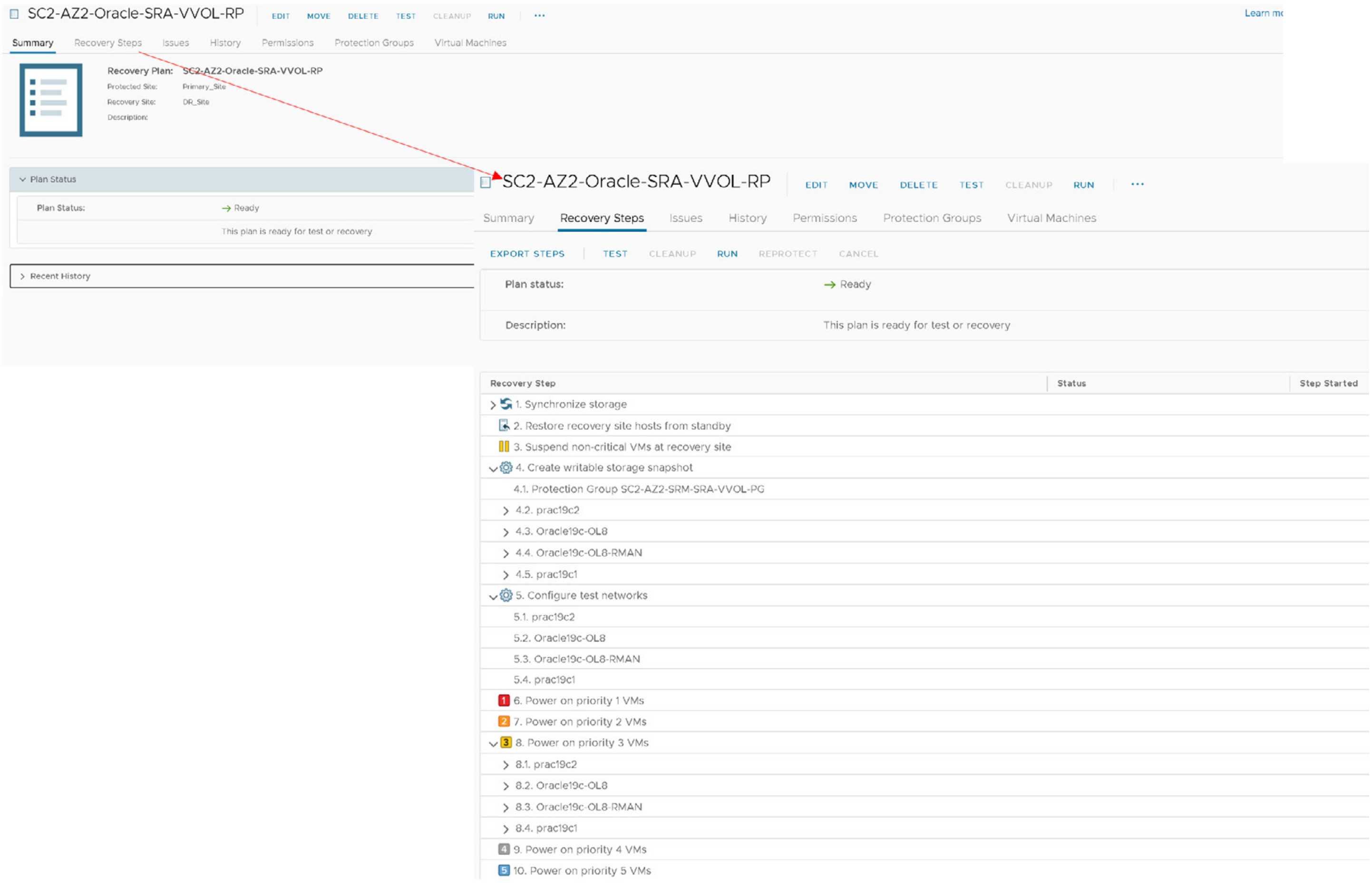
Replication Group	Virtual Machines
Pure-X50-BCA:SC2vVOLPG	2

Name	Status	Protected Site	Recovery Site
SC2-AZ2-Oracle-SRA-VVOL-RP	→ Ready	Primary_Site	DR_Site

Virtual Machine	Protection Status	Recovery Resource Pool	Recovery Host	Recovery Folder	Recovery Network	vVol Replication Group
Oracle19c-OL8	✓ OK	AZ2BCA11	az2esx22.vslab.local	Oracle-DR	APPS-1810	Pure-X50-BCA:SC2vVOLPG
Oracle19c-OL8-RMAN	✓ OK	AZ2BCA11	az2esx22.vslab.local	Oracle-DR	APPS-1810	Pure-X50-BCA:SC2vVOLPG
prac19c1	✓ OK	AZ2BCA11	az2esx23.vslab.local	Oracle-DR	APPS-1810,APPS-1805	Pure-X50-BCA:SC2vVOLPG
prac19c2	✓ OK	AZ2BCA11	az2esx24.vslab.local	Oracle-DR	APPS-1810,APPS-1805	Pure-X50-BCA:SC2vVOLPG

FIGURE 105. SITE A: Site Recovery Manager Protection Group and Protected VMs

The Site Recovery Manager recovery plan on Site A **SC2-AZ2-Oracle-SRA-VVOL-RP** is shown below:



SC2-AZ2-Oracle-SRA-VVOL-RP

Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status

Plan Status: → Ready
This plan is ready for test or recovery

Recent History

SC2-AZ2-Oracle-SRA-VVOL-RP

Plan status: → Ready

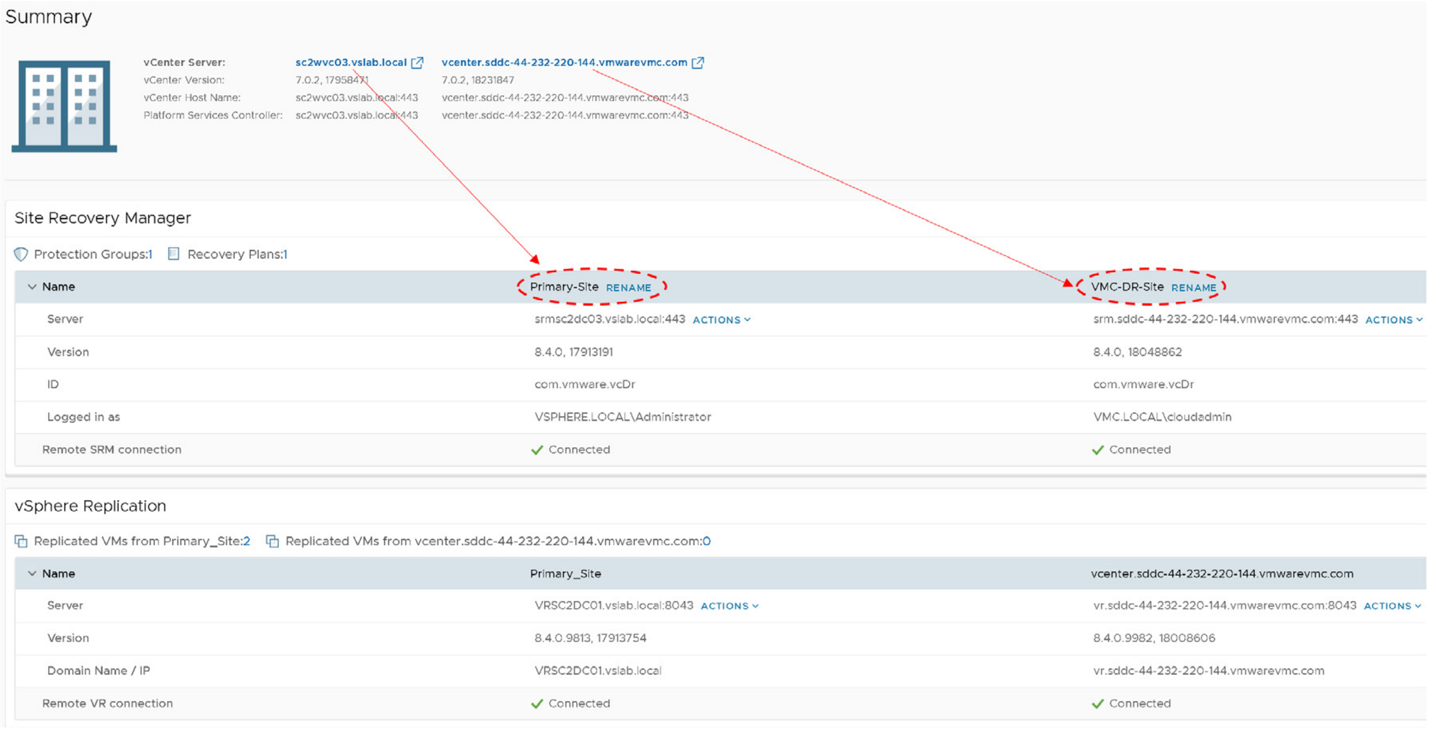
Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby		
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
4.1. Protection Group SC2-AZ2-SRM-SRA-VVOL-PG		
4.2. prac19c2		
4.3. Oracle19c-OL8		
4.4. Oracle19c-OL8-RMAN		
4.5. prac19c1		
5. Configure test networks		
5.1. prac19c2		
5.2. Oracle19c-OL8		
5.3. Oracle19c-OL8-RMAN		
5.4. prac19c1		
1 6. Power on priority 1 VMs		
2 7. Power on priority 2 VMs		
3 8. Power on priority 3 VMs		
8.1. prac19c2		
8.2. Oracle19c-OL8		
8.3. Oracle19c-OL8-RMAN		
8.4. prac19c1		
4 9. Power on priority 4 VMs		
5 10. Power on priority 5 VMs		

FIGURE 106. SITE A: Site Recovery Manager Recovery Plan

VMware Site Recovery

The Site Recovery Manager and vSphere Replication appliance information site pairing summary for Site A and VMware Cloud on AWS are as shown below:



Summary

vCenter Server:	sc2wvc03.vslab.local	vcenter.sddc-44-232-220-144.vmwarevmc.com
vCenter Version:	7.0.2, 17958471	7.0.2, 18231847
vCenter Host Name:	sc2wvc03.vslab.local:443	vcenter.sddc-44-232-220-144.vmwarevmc.com:443
Platform Services Controller:	sc2wvc03.vslab.local:443	vcenter.sddc-44-232-220-144.vmwarevmc.com:443

Site Recovery Manager

Protection Groups:1 Recovery Plans:1

Name	Primary-Site RENAME	VMC-DR-Site RENAME
Server	srmsc2dc03.vslab.local:443 ACTIONS	srm.sddc-44-232-220-144.vmwarevmc.com:443 ACTIONS
Version	8.4.0, 17913191	8.4.0, 18048862
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VMC.LOCAL\cloudadmin
Remote SRM connection	✓ Connected	✓ Connected

vSphere Replication

Replicated VMs from Primary_Site:2 Replicated VMs from vcenter.sddc-44-232-220-144.vmwarevmc.com:0

Name	Primary_Site	vcenter.sddc-44-232-220-144.vmwarevmc.com
Server	VRSC2DC01.vslab.local:8043 ACTIONS	vr.sddc-44-232-220-144.vmwarevmc.com:8043 ACTIONS
Version	8.4.0.9813, 17913754	8.4.0.9982, 18008606
Domain Name / IP	VRSC2DC01.vslab.local	vr.sddc-44-232-220-144.vmwarevmc.com
Remote VR connection	✓ Connected	✓ Connected

FIGURE 107. Site A and VMware Cloud on AWS Pairing Summary

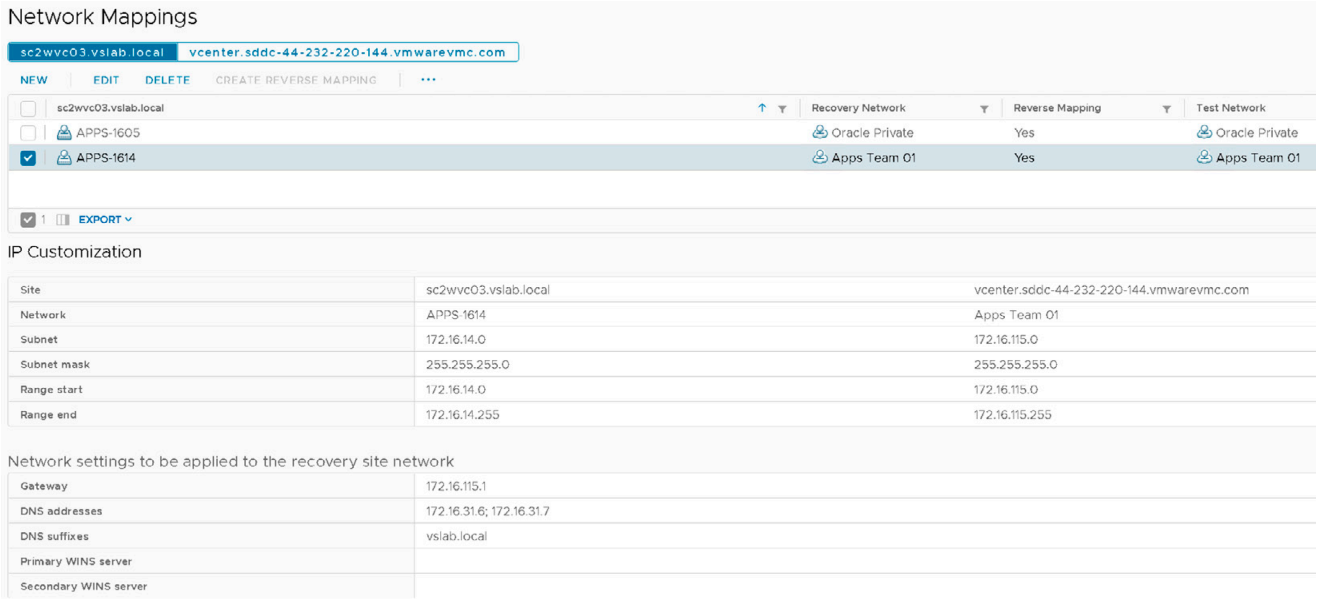
The network mappings, folder mappings, resource mappings and placeholder datastore mappings must be setup for Site Recovery Manager with vSphere Replication.

The network mapping port groups between Site A and VMware Cloud on AWS are as shown below:

NETWORK	SOURCE SITE	PORT GROUP	DESTINATION SITE	DESTINATION TEST NETWORK	DESTINATION RECOVERY NETWORK
Public Network	Site A	APPS-1614	VMware Cloud on AWS	Apps Team 01	Apps Team 01
Private Interconnect	Site A	APPS-1605	VMware Cloud on AWS	Oracle Private	Oracle Private
Public Network	VMware Cloud on AWS	Apps Team 01	Site A	APPS-1614	APPS-1614
Private Interconnect	VMware Cloud on AWS	Oracle Private	Site A	APPS-1605	APPS-1605

TABLE 10. Network Mapping Details between Site A and VMware Cloud on AWS

The network mapping for protected site public network **APPS-1614** to recovery site **Recovery Network Apps Team 01** is as shown below. The recovery site test network is also **Apps Team 01**.



Network Mappings

	sc2wvc03.vslab.local	Recovery Network	Reverse Mapping	Test Network
□	APPS-1605	Oracle Private	Yes	Oracle Private
☑	APPS-1614	Apps Team 01	Yes	Apps Team 01

IP Customization

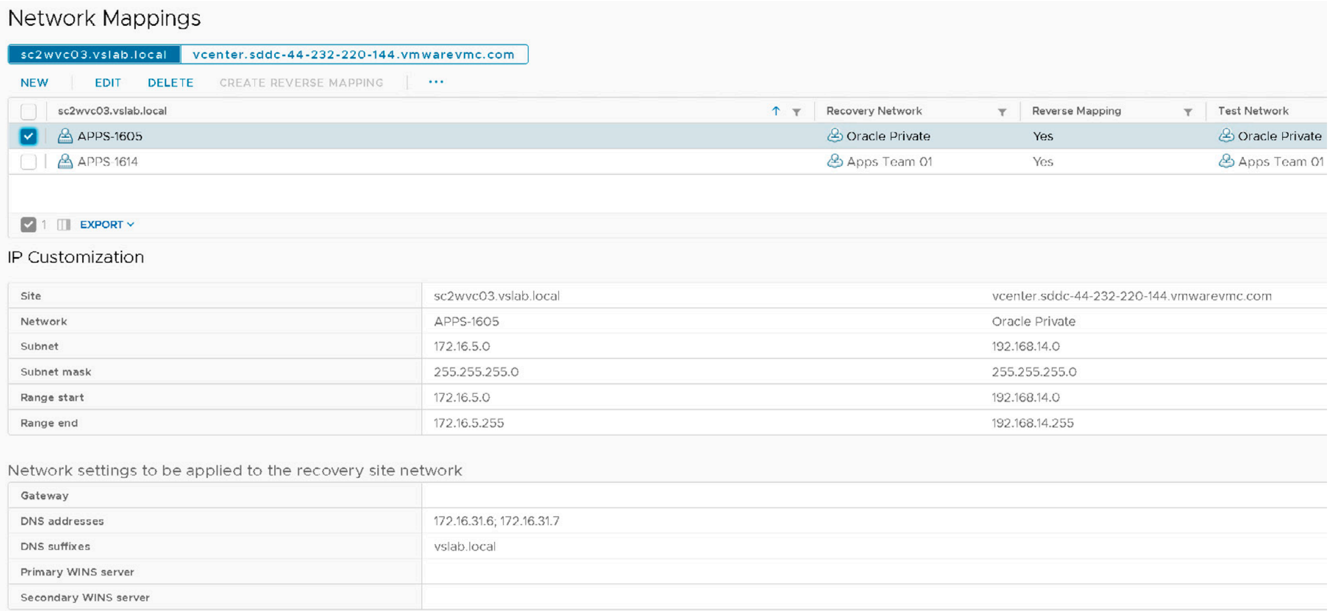
Site	sc2wvc03.vslab.local	vcenter.sddc-44-232-220-144.vmwarevmc.com
Network	APPS-1614	Apps Team 01
Subnet	172.16.14.0	172.16.115.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	172.16.14.0	172.16.115.0
Range end	172.16.14.255	172.16.115.255

Network settings to be applied to the recovery site network

Gateway	172.16.115.1
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 108. Network Mapping Between Site A and VMware Cloud on AWS for Planned Recovery Use Case

The network mapping for protected site private interconnect network **APPS-1605** to recovery site **Recovery Network Oracle Private** is as shown below. The recovery site test network is **Oracle Private**.



Network Mappings

	sc2wvc03.vslab.local	Recovery Network	Reverse Mapping	Test Network
☑	APPS-1605	Oracle Private	Yes	Oracle Private
□	APPS 1614	Apps Team 01	Yes	Apps Team 01

IP Customization

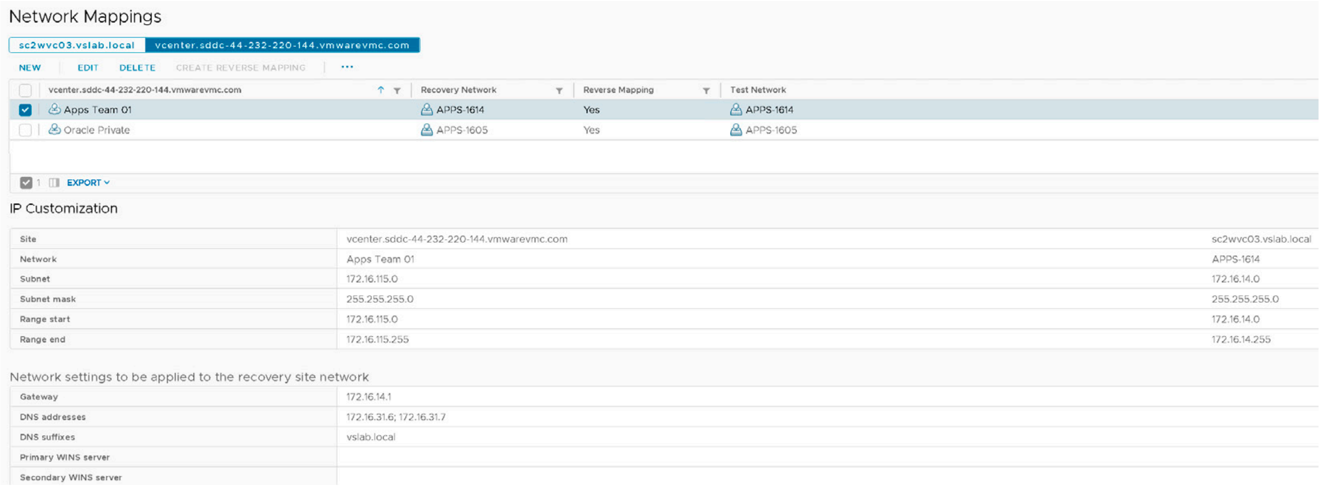
Site	sc2wvc03.vslab.local	vcenter.sddc-44-232-220-144.vmwarevmc.com
Network	APPS-1605	Oracle Private
Subnet	172.16.5.0	192.168.14.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	172.16.5.0	192.168.14.0
Range end	172.16.5.255	192.168.14.255

Network settings to be applied to the recovery site network

Gateway	
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 109. Network Mapping Between Site A and VMware Cloud on AWS For Test Recovery Use Case

The network mapping for recovery site **Public Network Apps Team 01** to protected site **Recovery Network APPS-1614** is as shown below. The recovery site test network is **APPS-1614**.



Network Mappings

	vcenter.sddc-44-232-220-144.vmwarevmc.com	Recovery Network	Reverse Mapping	Test Network
☑	Apps Team 01	APPS-1614	Yes	APPS-1614
□	Oracle Private	APPS-1605	Yes	APPS-1605

IP Customization

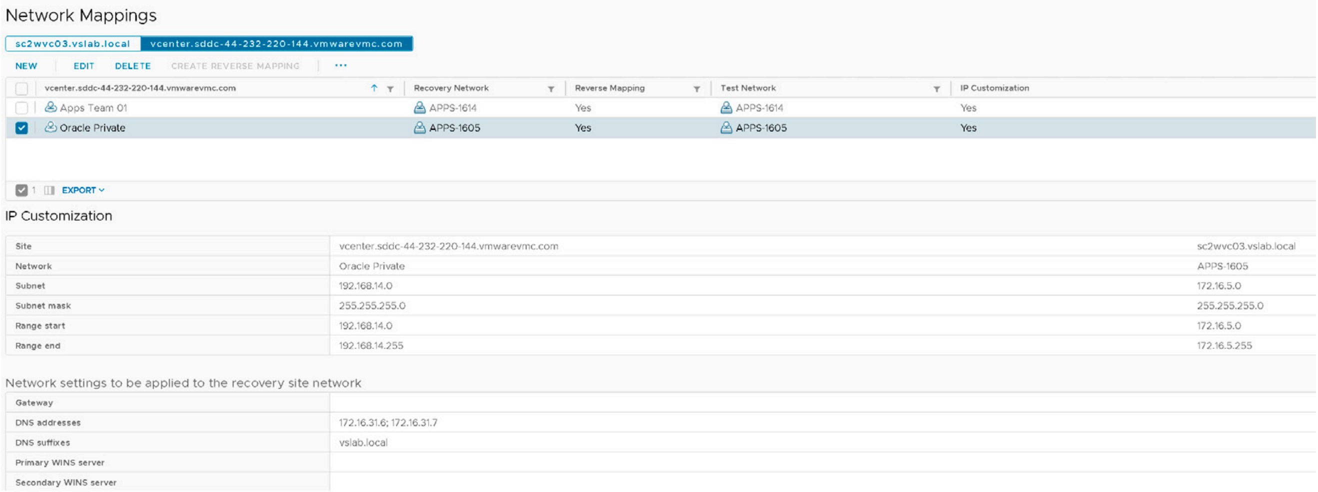
Site	vcenter.sddc-44-232-220-144.vmwarevmc.com	sc2wvc03.vslab.local
Network	Apps Team 01	APPS-1614
Subnet	172.16.115.0	172.16.14.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	172.16.115.0	172.16.14.0
Range end	172.16.115.255	172.16.14.255

Network settings to be applied to the recovery site network

Gateway	172.16.14.1
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 110. Network Mapping Between VMware Cloud on AWS and Site A for Planned Recovery Use Case

The network mapping for recovery site private network **Oracle Private** to protected site **Recovery Network APPS-1605** is as shown below. The recovery site test network is **APPS-1605**.



Network Mappings

	vcenter.sddc-44-232-220-144.vmwarevmc.com	Recovery Network	Reverse Mapping	Test Network	IP Customization
□	Apps Team 01	APPS-1614	Yes	APPS-1614	Yes
☑	Oracle Private	APPS-1605	Yes	APPS-1605	Yes

IP Customization

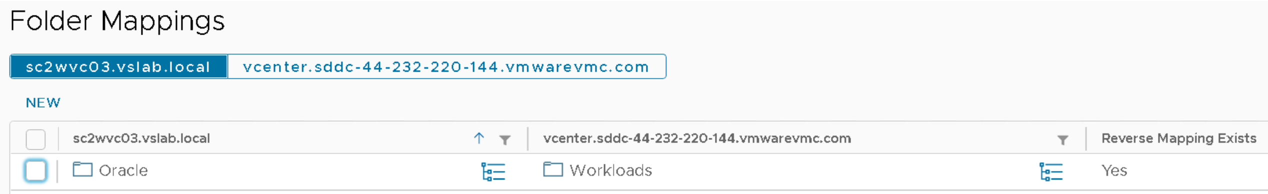
Site	vcenter.sddc-44-232-220-144.vmwarevmc.com	sc2wvc03.vslab.local
Network	Oracle Private	APPS-1605
Subnet	192.168.14.0	172.16.5.0
Subnet mask	255.255.255.0	255.255.255.0
Range start	192.168.14.0	172.16.5.0
Range end	192.168.14.255	172.16.5.255

Network settings to be applied to the recovery site network

Gateway	
DNS addresses	172.16.31.6; 172.16.31.7
DNS suffixes	vslab.local
Primary WINS server	
Secondary WINS server	

FIGURE 111. Network Mapping Between VMware Cloud on AWS and Site A for Test Recovery Use Case

The folder mapping from Site A to VMware Cloud on AWS is as shown below:

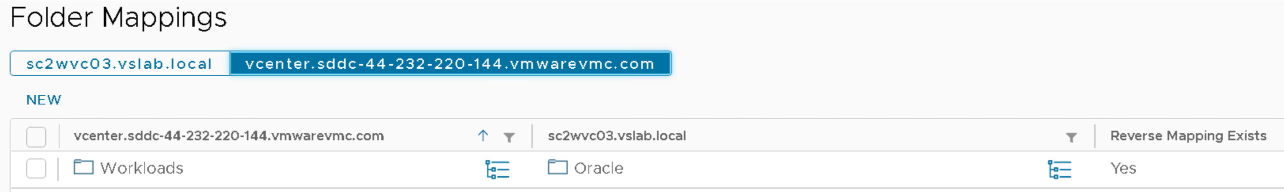


Folder Mappings

□	sc2wvc03.vslab.local	vcenter.sddc-44-232-220-144.vmwarevmc.com	Reverse Mapping Exists
□	Oracle	Workloads	Yes

FIGURE 112. Folder Mappings from Site A to VMware Cloud on AWS

Folder mapping from VMware Cloud on AWS to Site A is as shown below:

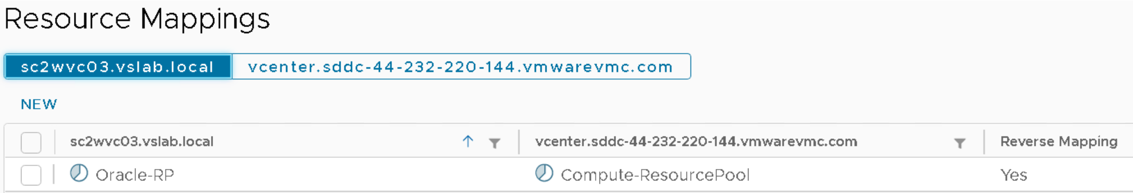


Folder Mappings

□	vcenter.sddc-44-232-220-144.vmwarevmc.com	sc2wvc03.vslab.local	Reverse Mapping Exists
□	Workloads	Oracle	Yes

FIGURE 113. Folder Mappings from VMware Cloud on AWS to Site A

Resource mapping from Site A to VMware Cloud on AWS is as shown below:

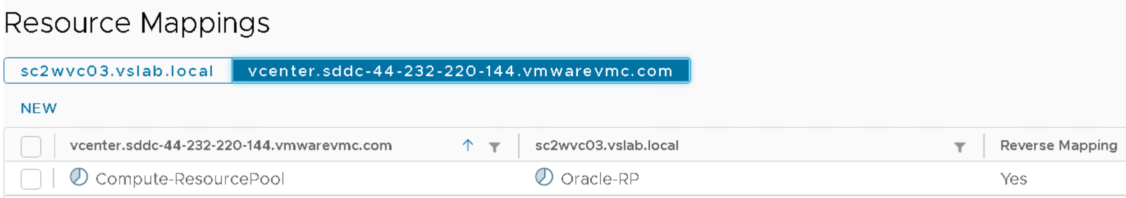


Resource Mappings

□	sc2wvc03.vslab.local	vcenter.sddc-44-232-220-144.vmwarevmc.com	Reverse Mapping
□	Oracle-RP	Compute-ResourcePool	Yes

FIGURE 114. Resource Mappings from Site A to VMware Cloud on AWS

The Resource mapping from VMware Cloud on AWS to Site A is as shown below:

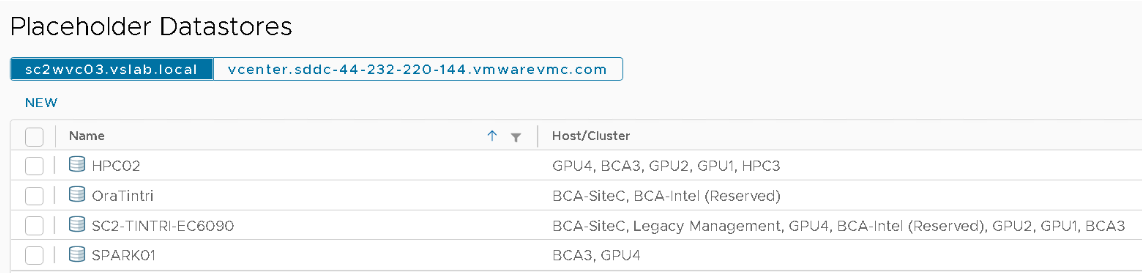


Resource Mappings

□	vcenter.sddc-44-232-220-144.vmwarevmc.com	sc2wvc03.vslab.local	Reverse Mapping
□	Compute-ResourcePool	Oracle-RP	Yes

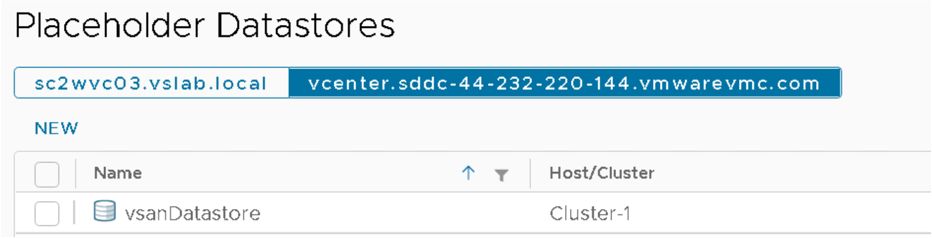
FIGURE 115. Resource Mappings from VMware Cloud on AWS to Site A

The placeholder datastore mapping between Site A and Site B is as shown below. The placeholder datastore on the recovery site is used by Site Recovery Manager to store placeholder VMs.


Placeholder Datastores

□	Name	Host/Cluster
□	HPC02	GPU4, BCA3, GPU2, GPU1, HPC3
□	OraTintri	BCA-SiteC, BCA-Intel (Reserved)
□	SC2-TINTRI-EC6090	BCA-SiteC, Legacy Management, GPU4, BCA-Intel (Reserved), GPU2, GPU1, BCA3
□	SPARK01	BCA3, GPU4

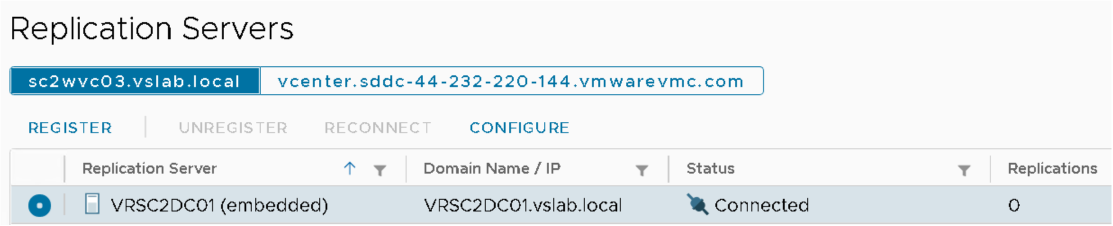
FIGURE 116. Placeholder Datastore Mappings from Site A to VMware Cloud on AWS


Placeholder Datastores

□	Name	Host/Cluster
□	vsanDatastore	Cluster-1

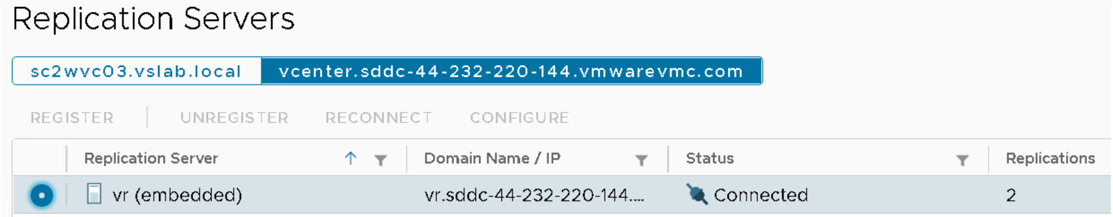
FIGURE 117. Placeholder Datastore Mappings from VMware Cloud on AWS and Site B

The graphic below illustrates vSphere Replication setup between on-premises Site A and VMware Cloud on AWS.


Replication Servers

	Replication Server	Domain Name / IP	Status	Replications
●	VRSC2DC01 (embedded)	VRSC2DC01.vslab.local	Connected	0

FIGURE 118. SITE A: Replication Server Details


Replication Servers

	Replication Server	Domain Name / IP	Status	Replications
●	vr (embedded)	vr.sddc-44-232-220-144....	Connected	2

FIGURE 119. VMware Cloud on AWS Replication Server Details

Site Recovery Manager and Sphere Replication pairings and IP addresses for Site A and VMware Cloud on AWS are as shown below:

COMPONENT	SOURCE SITE	APPLIANCE	DESTINATION SITE	APPLIANCE
SRM Appliance	Site A	SRMSC2DC03.vslab.local	VMware Cloud on AWS	srm.sddc-44-232-220-144.vmwarevmc.com
IP Address		172.16.31.149		10.129.224.24
vSphere Replication Appliance	Site A	VRSC2DC01.vslab.local	VMware Cloud on AWS	vr.sddc-44-232-220-144.vmwarevmc.com
IP Address		172.16.31.144		10.129.224.23

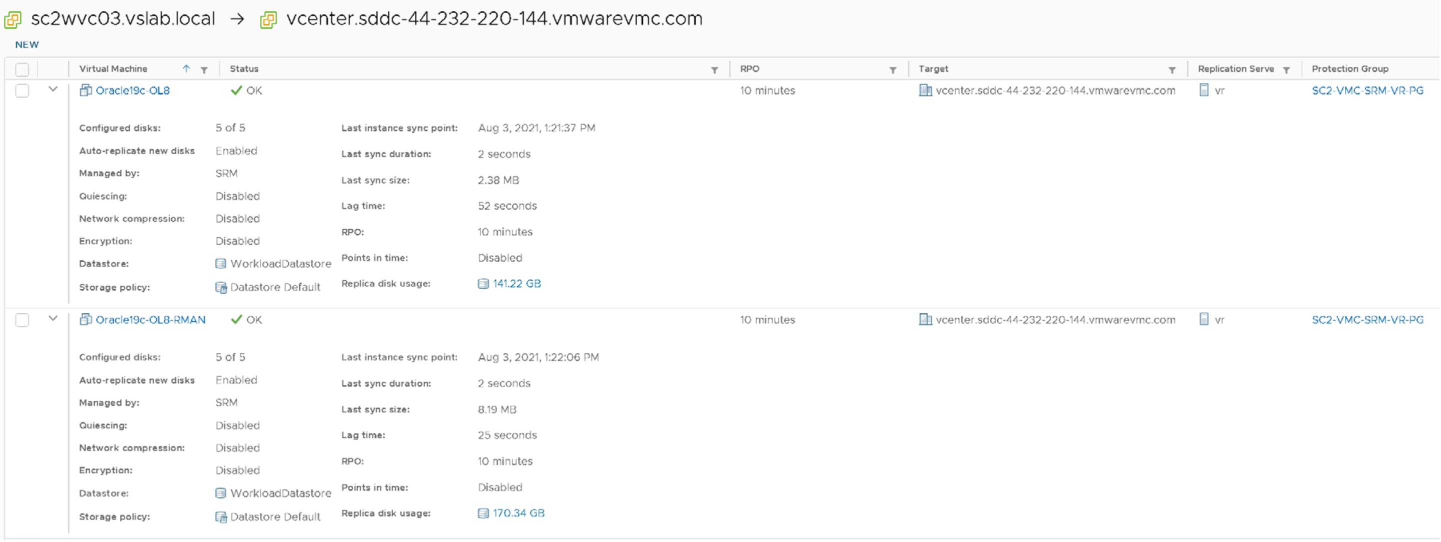
TABLE 11. vSphere Replication Network Pairing Details

Setup of Site Recovery Manager and vSphere Replication is beyond the scope of this paper.

The steps to set up replication between Site A and VMware Cloud on AWS are the same as those required to set up replication between Site A and Site B.

To enable site recovery on VMware Cloud in an AWS SDDC environment that uses VMware NSX-T, firewall rules must be created between on-premises and VMware Cloud on AWS management gateway. After the initial firewall rules configuration, one can add, edit or delete any rules as needed. *Learn more about firewall rules*.

After setup is complete, vSphere Replication will automatically seed the source data to target as baseline first **OR** we can force a sync.



sc2wvc03.vslab.local → vcenter.sddc-44-232-220-144.vmwarevmc.com

NEW

□	Virtual Machine	Status	RPO	Target	Replication Serve	Protection Group
□	Oracle19c-OL8	✓ OK	10 minutes	vcenter.sddc-44-232-220-144.vmwarevmc.com	vr	SC2-VMC-SRM-VR-PG

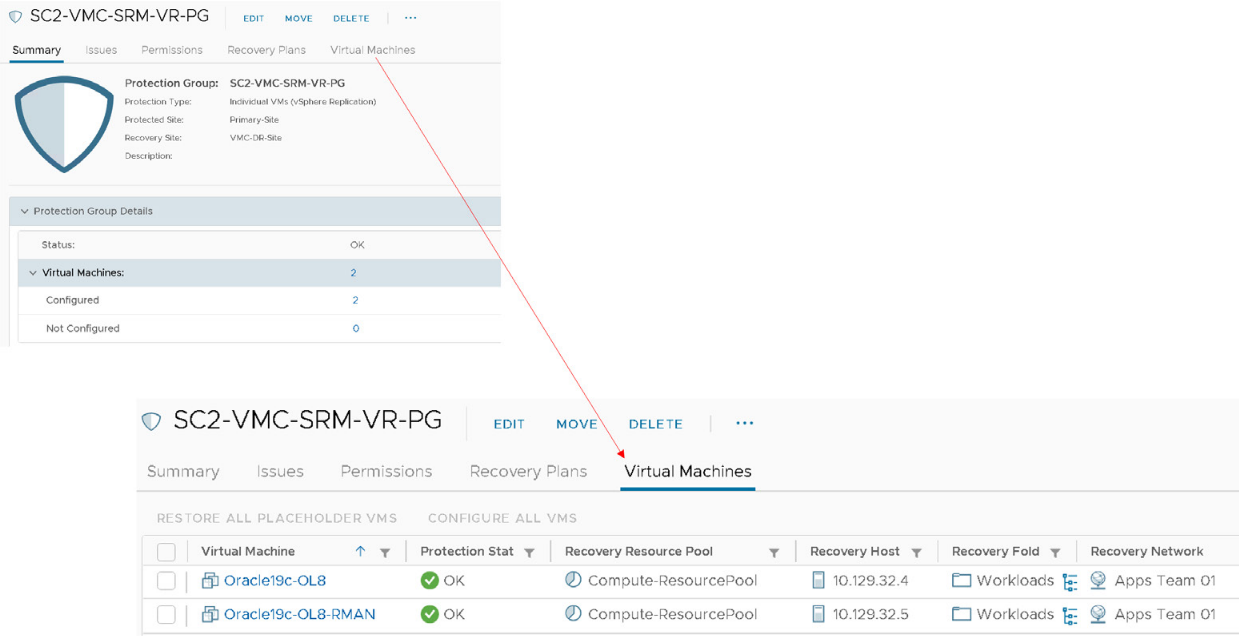
Configured disks:	5 of 5	Last instance sync point:	Aug 3, 2021, 1:21:37 PM
Auto-replicate new disks	Enabled	Last sync duration:	2 seconds
Managed by:	SRM	Last sync size:	2.38 MB
Quiescing:	Disabled	Lag time:	52 seconds
Network compression:	Disabled	RPO:	10 minutes
Encryption:	Disabled	Points in time:	Disabled
Datastore:	WorkloadDatastore	Replica disk usage:	141.22 GB
Storage policy:	Datastore Default		

□	Virtual Machine	Status	RPO	Target	Replication Serve	Protection Group
□	Oracle19c-OL8-RMAN	✓ OK	10 minutes	vcenter.sddc-44-232-220-144.vmwarevmc.com	vr	SC2-VMC-SRM-VR-PG

Configured disks:	5 of 5	Last instance sync point:	Aug 3, 2021, 1:22:06 PM
Auto-replicate new disks	Enabled	Last sync duration:	2 seconds
Managed by:	SRM	Last sync size:	8.19 MB
Quiescing:	Disabled	Lag time:	25 seconds
Network compression:	Disabled	RPO:	10 minutes
Encryption:	Disabled	Points in time:	Disabled
Datastore:	WorkloadDatastore	Replica disk usage:	170.34 GB
Storage policy:	Datastore Default		

FIGURE 120. vSphere Replication Source Data Seeding

The protection group and VMs are as shown below:



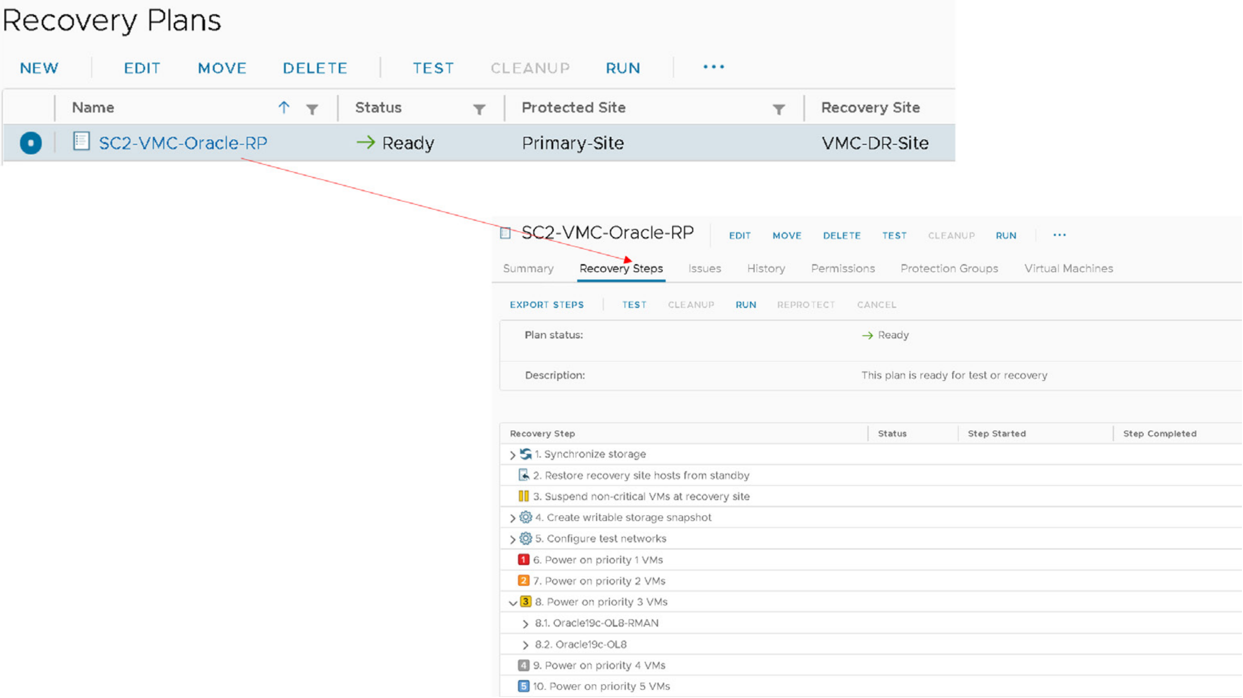
Protection Group: SC2-VMC-SRM-VR-PG
Protection Type: Individual VMs (vSphere Replication)
Protected Site: Primary-Site
Recovery Site: VMC-DR-Site
Description:

Status:	OK
Virtual Machines:	2
Configured	2
Not Configured	0

Virtual Machine	Protection Stat	Recovery Resource Pool	Recovery Host	Recovery Fold	Recovery Network
Oracle19c-OL8	OK	Compute-ResourcePool	10.129.32.4	Workloads	Apps Team 01
Oracle19c-OL8-RMAN	OK	Compute-ResourcePool	10.129.32.5	Workloads	Apps Team 01

FIGURE 121. Site A Protection Group and Virtual Machines

The recovery plan is as shown below:



Name	Status	Protected Site	Recovery Site
SC2-VMC-Oracle-RP	→ Ready	Primary-Site	VMC-DR-Site

Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage			
2. Restore recovery site hosts from standby			
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot			
5. Configure test networks			
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs			
8.1. Oracle19c-OL8-RMAN			
8.2. Oracle19c-OL8			
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

FIGURE 122. Site A Recovery Plan and Recovery Steps

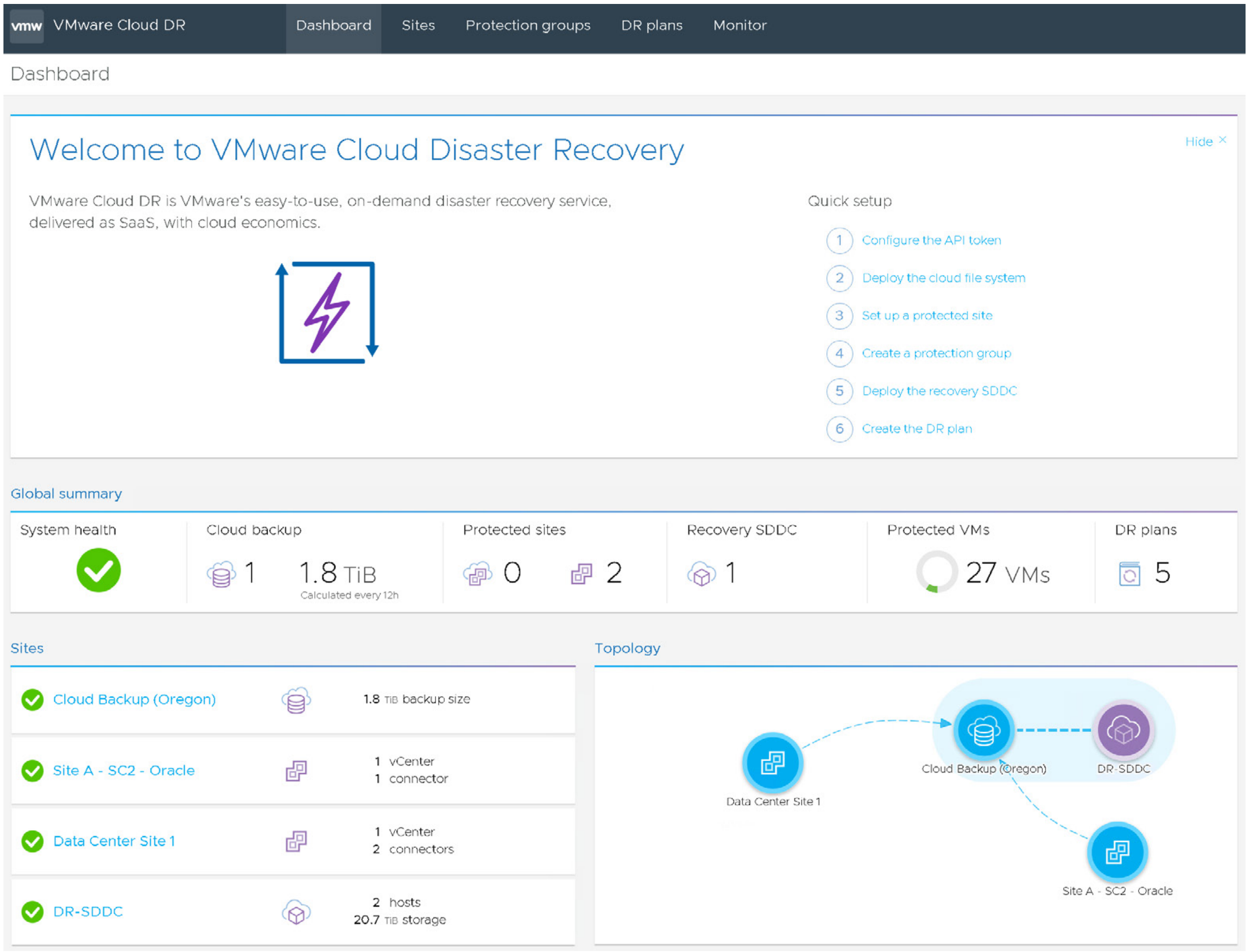
As mentioned before, vSphere Replication 8.4 cannot replicate VMs that share VMDK files. This limitation can be found in *VMware vSphere Replication 8.4 Release Notes*.

VMware Cloud Disaster Recovery

The illustration below shows VMware Cloud Disaster Recovery setup between Site A and VMware Cloud on AWS.

The dashboard for VMware Cloud Disaster Recovery is as shown below. Using VMware Cloud Disaster Recovery with VMware Cloud on AWS, the recovery SDDC is already provisioned and configured.

Setting up the recovery SDDC is beyond the scope of this paper. Learn more about *Deploying a Recovery SDDC*.



Dashboard

Welcome to VMware Cloud Disaster Recovery

VMware Cloud DR is VMware's easy-to-use, on-demand disaster recovery service, delivered as SaaS, with cloud economics.

Quick setup

1. Configure the API token
2. Deploy the cloud file system
3. Set up a protected site
4. Create a protection group
5. Deploy the recovery SDDC
6. Create the DR plan

Global summary

System health	Cloud backup	Protected sites	Recovery SDDC	Protected VMs	DR plans
✓	1 1.8 TiB Calculated every 12h	0 2	1	27 VMs	5

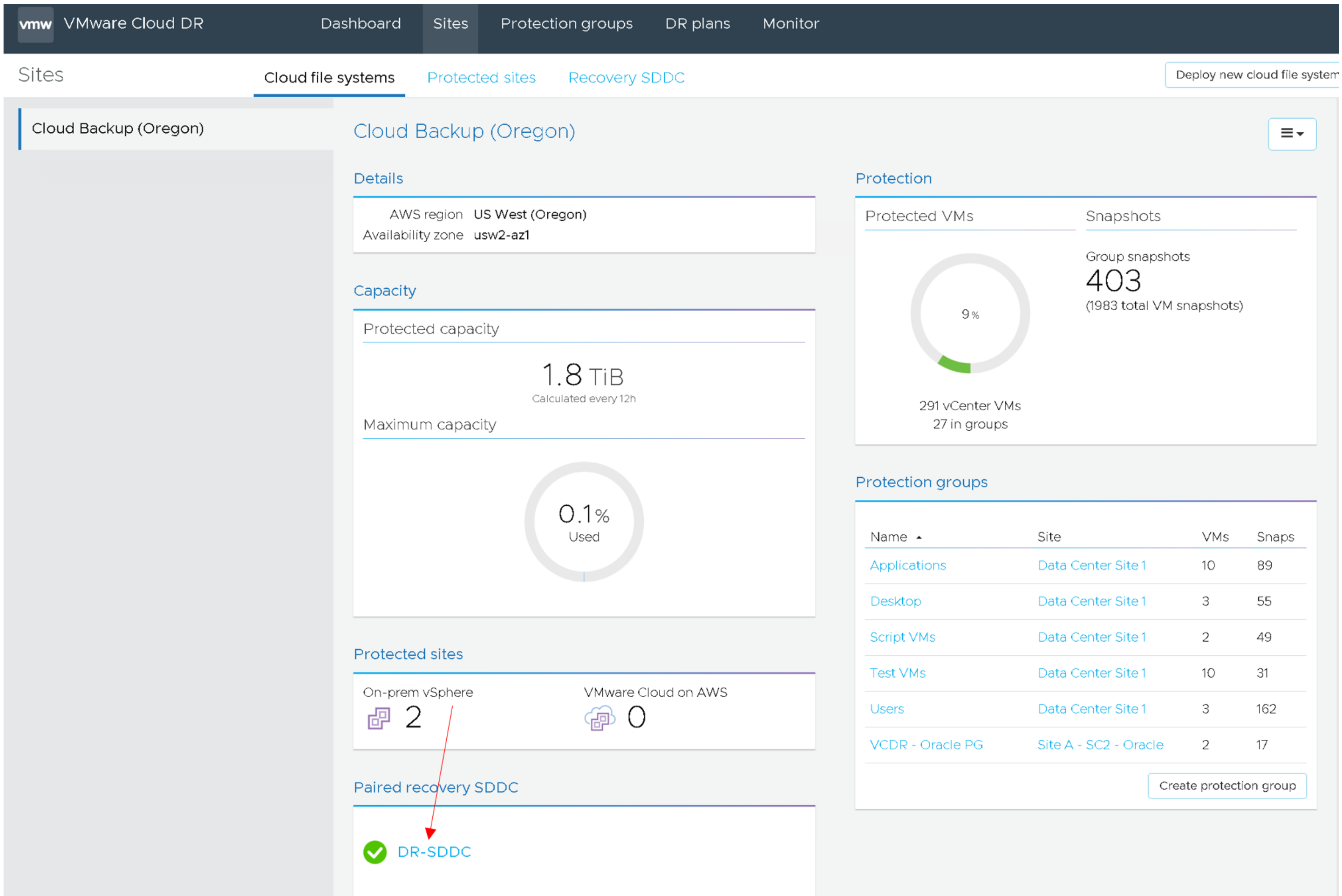
Sites

✓ Cloud Backup (Oregon)		1.8 TiB backup size
✓ Site A - SC2 - Oracle		1 vCenter 1 connector
✓ Data Center Site 1		1 vCenter 2 connectors
✓ DR-SDDC		2 hosts 20.7 TiB storage

Topology

FIGURE 123. VMware Cloud Disaster Recovery Dashboard

Cloud backup (Oregon) is as shown below:



Cloud Backup (Oregon)

Details

AWS region: US West (Oregon)
Availability zone: usw2-az1

Capacity

Protected capacity: 1.8 TiB
Calculated every 12h

Maximum capacity: 0.1% Used

Protected sites

On-prem vSphere: 2
VMware Cloud on AWS: 0

Paired recovery SDDC

✓ DR-SDDC

Protection

Protected VMs: 9%
291 vCenter VMs
27 in groups

Snapshots

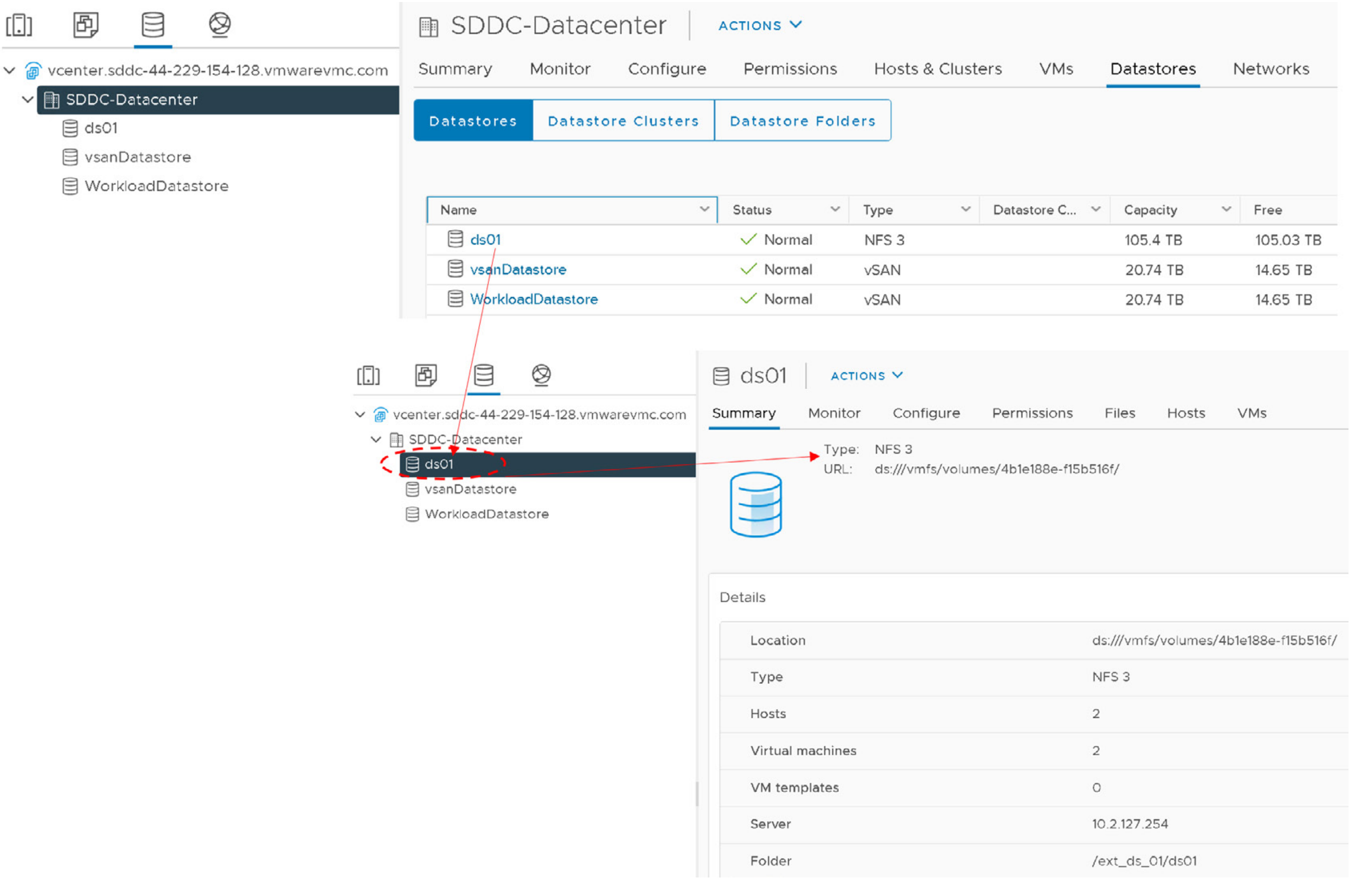
Group snapshots
403
(1983 total VM snapshots)

Protection groups

Name ▲	Site	VMs	Snaps
Applications	Data Center Site 1	10	89
Desktop	Data Center Site 1	3	55
Script VMs	Data Center Site 1	2	49
Test VMs	Data Center Site 1	10	31
Users	Data Center Site 1	3	162
VCDR - Oracle PG	Site A - SC2 - Oracle	2	17

FIGURE 124. VMware Cloud Disaster Recovery Cloud Backup

On the recovery VMware Cloud on AWS SDDC, there are tree datastores. Datastore **ds01** is scale-out cloud file system (SCFS) storage mounted as an NFS datastore on the recovery VMware Cloud on AWS SDDC. This datastore should only be used by VMware Cloud DR.



Name	Status	Type	Datastore C...	Capacity	Free
ds01	✓ Normal	NFS 3		105.4 TB	105.03 TB
vsanDatastore	✓ Normal	vSAN		20.74 TB	14.65 TB
WorkloadDatastore	✓ Normal	vSAN		20.74 TB	14.65 TB

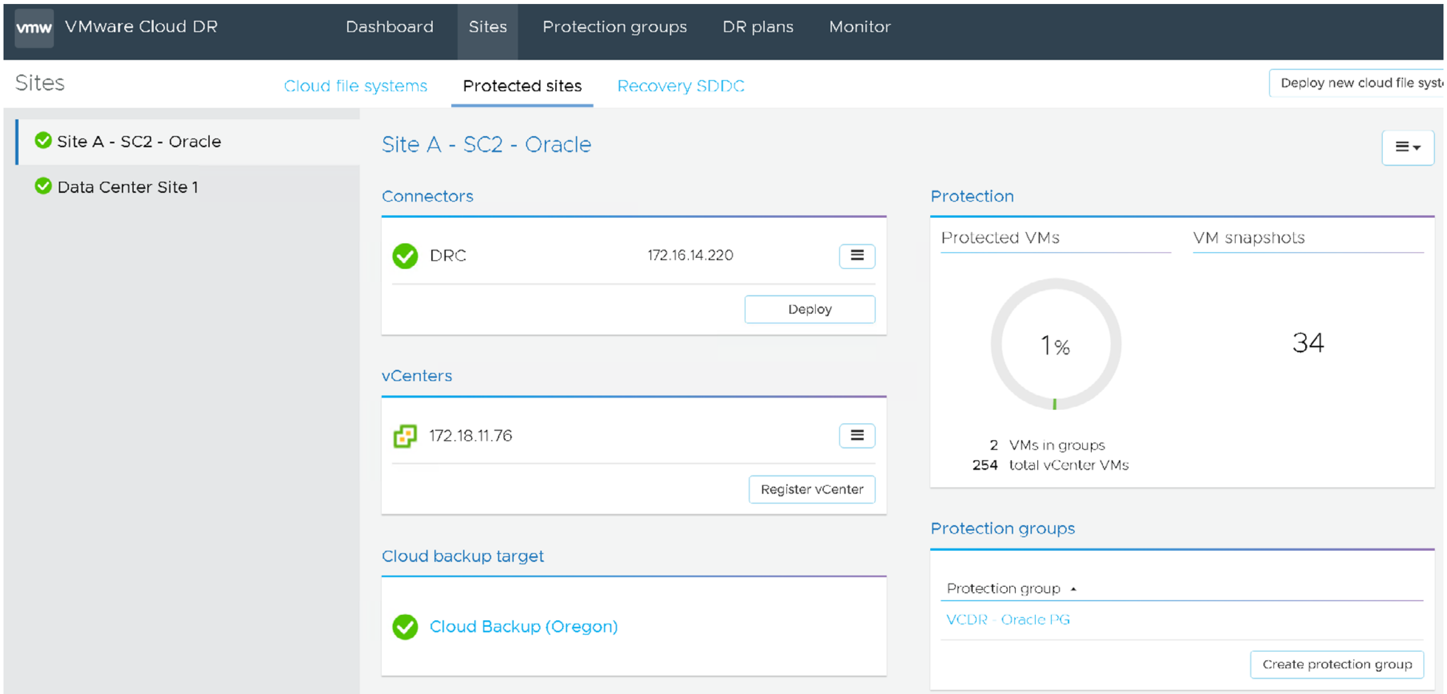
Type: NFS 3
URL: ds:///vmfs/volumes/4b1e188e-f15b516f/

Location	ds:///vmfs/volumes/4b1e188e-f15b516f/
Type	NFS 3
Hosts	2
Virtual machines	2
VM templates	0
Server	10.2.127.254
Folder	/ext_ds_01/ds01

FIGURE 125. VMware Cloud Disaster Recovery SCFS Storage

The **vsanDatastore** and **WorkloadDatastore** are part of the basic VMware Cloud on AWS storage.

The protected site **Site A - SC2 – Oracle** is as shown below:



Site A - SC2 - Oracle

Data Center Site 1

Site A - SC2 - Oracle

Connectors

DRC 172.16.14.220

vCenters

172.18.11.76

Cloud backup target

Cloud Backup (Oregon)

Protection

Protected VMs	VM snapshots
1%	34

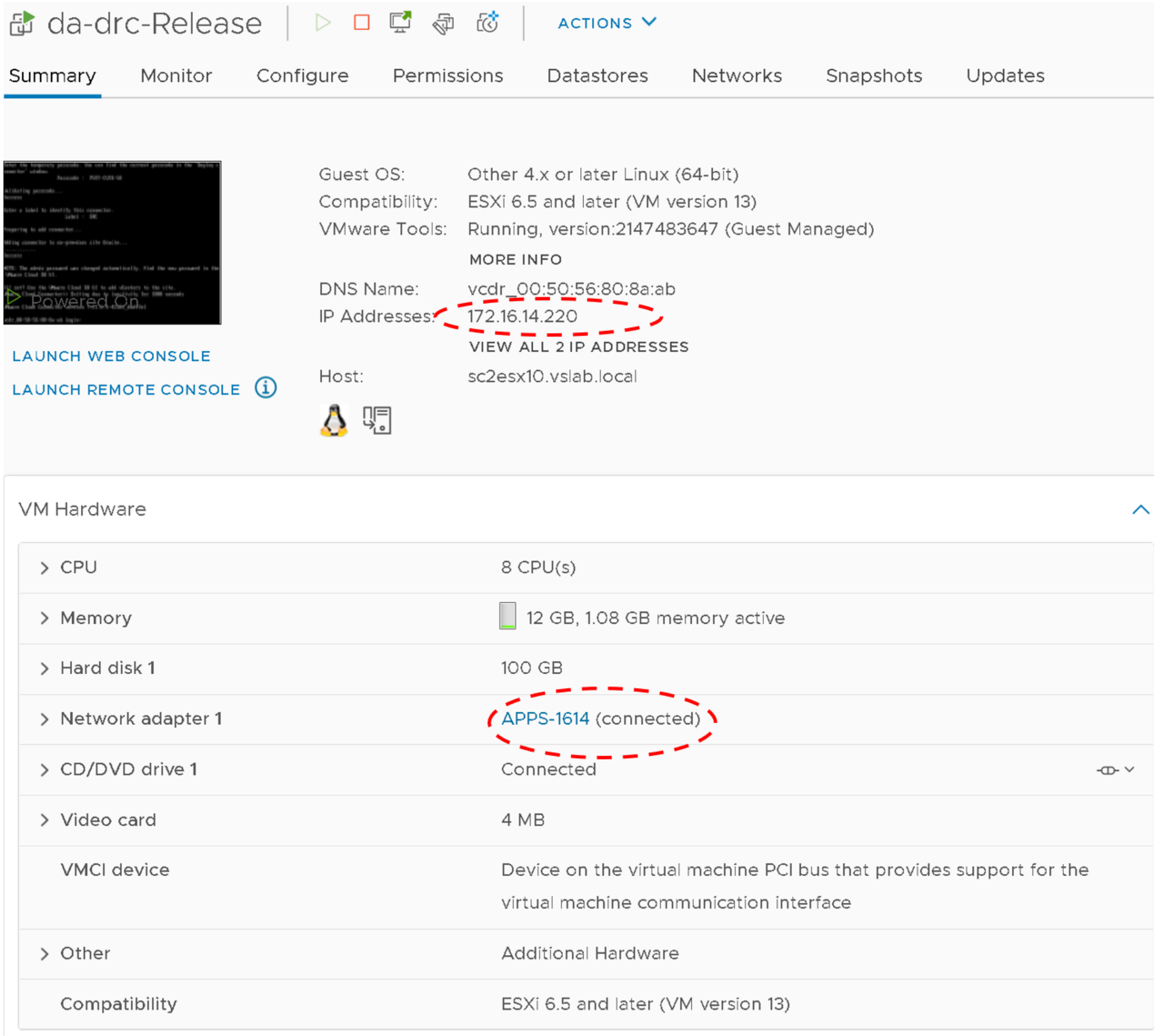
2 VMs in groups
254 total vCenter VMs

Protection groups

Protection group ▲
VCDR - Oracle PG

FIGURE 126. VMware Cloud Disaster Recovery Protected Site

The DRaaS connector appliance is deployed on protected Site A with IP address 172.16.14.220 as shown below:

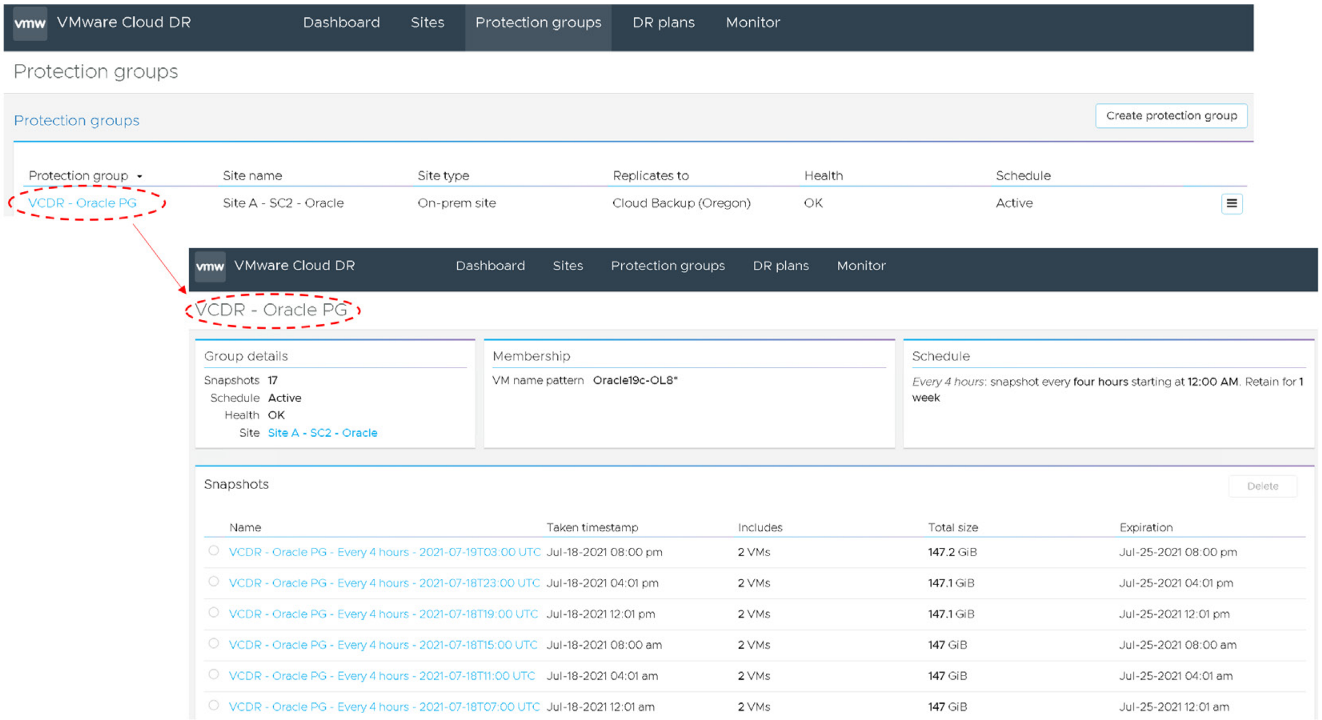


Guest OS: Other 4.x or later Linux (64-bit)
Compatibility: ESXi 6.5 and later (VM version 13)
VMware Tools: Running, version:2147483647 (Guest Managed)
DNS Name: vcdr_00:50:56:80:8a:ab
IP Addresses: 172.16.14.220
Host: sc2esx10.vslab.local

CPU	8 CPU(s)
Memory	12 GB, 1.08 GB memory active
Hard disk 1	100 GB
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Connected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 6.5 and later (VM version 13)

FIGURE 127. Site A: DRaaS Connector Appliance

The protection group **VCDR - Oracle PG** is created as shown below:



Protection groups

Protection groups

Protection group	Site name	Site type	Replicates to	Health	Schedule
VCDR - Oracle PG	Site A - SC2 - Oracle	On-prem site	Cloud Backup (Oregon)	OK	Active

VCDR - Oracle PG

Group details

Snapshots 17
Schedule Active
Health OK
Site Site A - SC2 - Oracle

Membership

VM name pattern Oracle19c-OL8*

Schedule

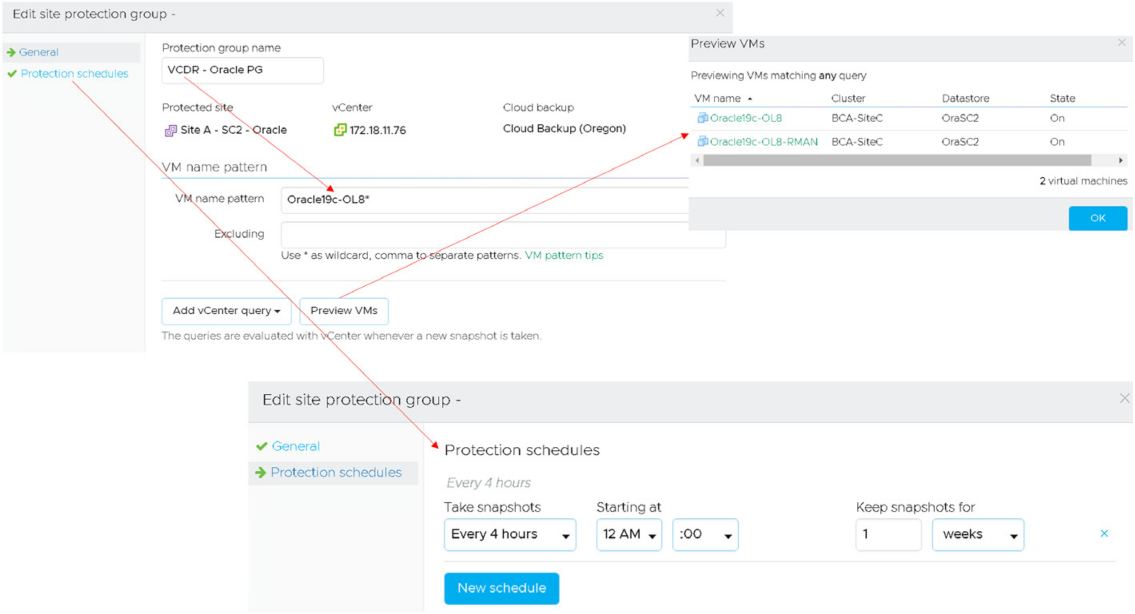
Every 4 hours: snapshot every **four hours** starting at **12:00 AM**. Retain for **1 week**

Snapshots

Name	Taken timestamp	Includes	Total size	Expiration
○ VCDR - Oracle PG - Every 4 hours - 2021-07-19T03:00 UTC	Jul-18-2021 08:00 pm	2 VMs	147.2 GiB	Jul-25-2021 08:00 pm
○ VCDR - Oracle PG - Every 4 hours - 2021-07-18T23:00 UTC	Jul-18-2021 04:01 pm	2 VMs	147.1 GiB	Jul-25-2021 04:01 pm
○ VCDR - Oracle PG - Every 4 hours - 2021-07-18T19:00 UTC	Jul-18-2021 12:01 pm	2 VMs	147.1 GiB	Jul-25-2021 12:01 pm
○ VCDR - Oracle PG - Every 4 hours - 2021-07-18T15:00 UTC	Jul-18-2021 08:00 am	2 VMs	147 GiB	Jul-25-2021 08:00 am
○ VCDR - Oracle PG - Every 4 hours - 2021-07-18T11:00 UTC	Jul-18-2021 04:01 am	2 VMs	147 GiB	Jul-25-2021 04:01 am
○ VCDR - Oracle PG - Every 4 hours - 2021-07-18T07:00 UTC	Jul-18-2021 12:01 am	2 VMs	147 GiB	Jul-25-2021 12:01 am

FIGURE 128. Site A VMware Cloud DR Protection Group

The protection group **VCDR - Oracle PG** details with VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** is as shown below:



Edit site protection group -

Protection group name: VCDR - Oracle PG

Protected site: Site A - SC2 - Oracle
vCenter: 172.18.11.76
Cloud backup: Cloud Backup (Oregon)

VM name pattern

VM name pattern: Oracle19c-OL8*
Excluding:
Use * as wildcard, comma to separate patterns. VM pattern tips

The queries are evaluated with vCenter whenever a new snapshot is taken.

Preview VMs

Previewing VMs matching **any** query

VM name	Cluster	Datastore	State
Oracle19c-OL8	BCA-SiteC	OraSC2	On
Oracle19c-OL8-RMAN	BCA-SiteC	OraSC2	On

2 virtual machines

Edit site protection group -

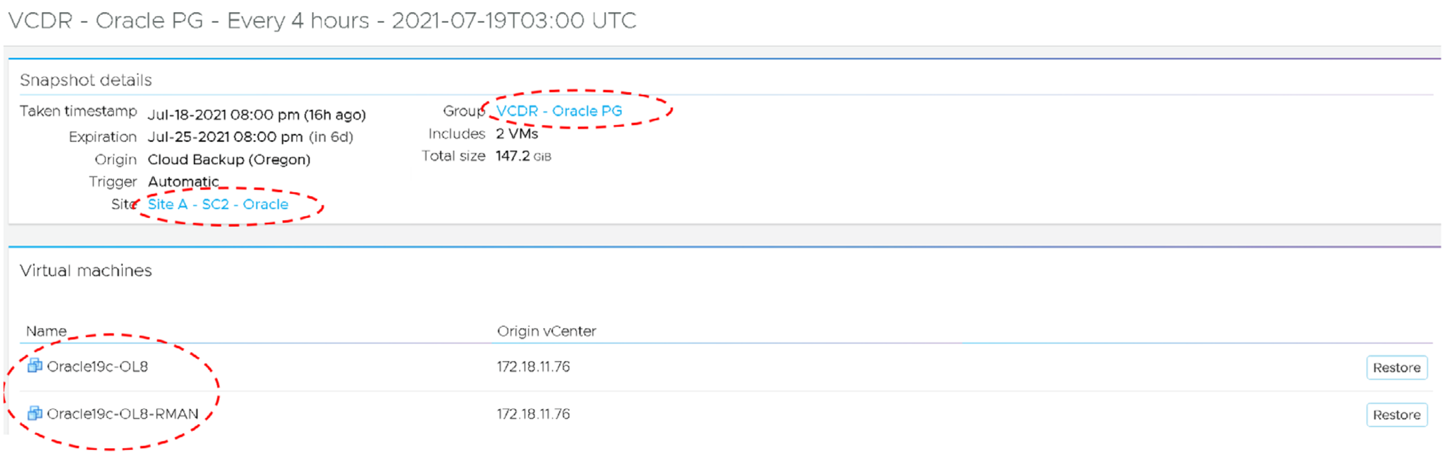
Protection schedules

Every 4 hours

Take snapshots: Every 4 hours
Starting at: 12 AM :00
Keep snapshots for: 1 weeks

FIGURE 129. SITE A: VMware Cloud DR Protection Group and Protected VMs

Details of snapshot **VCDR - Oracle PG - Every 4 hours - 2021-07-19T03:00 UTC** are as shown below for VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN**:



VCDR - Oracle PG - Every 4 hours - 2021-07-19T03:00 UTC

Snapshot details

Taken timestamp Jul-18-2021 08:00 pm (16h ago)
Expiration Jul-25-2021 08:00 pm (in 6d)
Origin Cloud Backup (Oregon)
Trigger Automatic
Site Site A - SC2 - Oracle

Group VCDR - Oracle PG
Includes 2 VMs
Total size 147.2 GiB

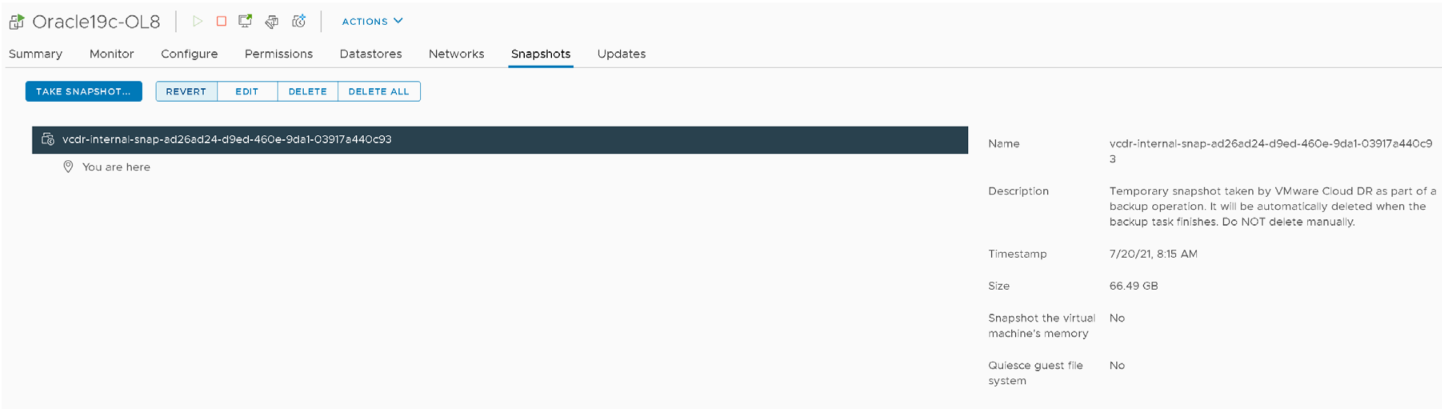
Virtual machines

Name	Origin vCenter	
Oracle19c-OL8	172.18.11.76	Restore
Oracle19c-OL8-RMAN	172.18.11.76	Restore

FIGURE 130. VMware Cloud DR Protection Group Snapshots Details

The snapshot can also be viewed on the protected site **Site A - SC2 – Oracle**. This snapshot is temporary during the protection group cycle and will be removed as soon as the changed block data has been successfully replicated to the SCFS.

The snapshot of VM **Oracle19c-OL8** is as shown below:

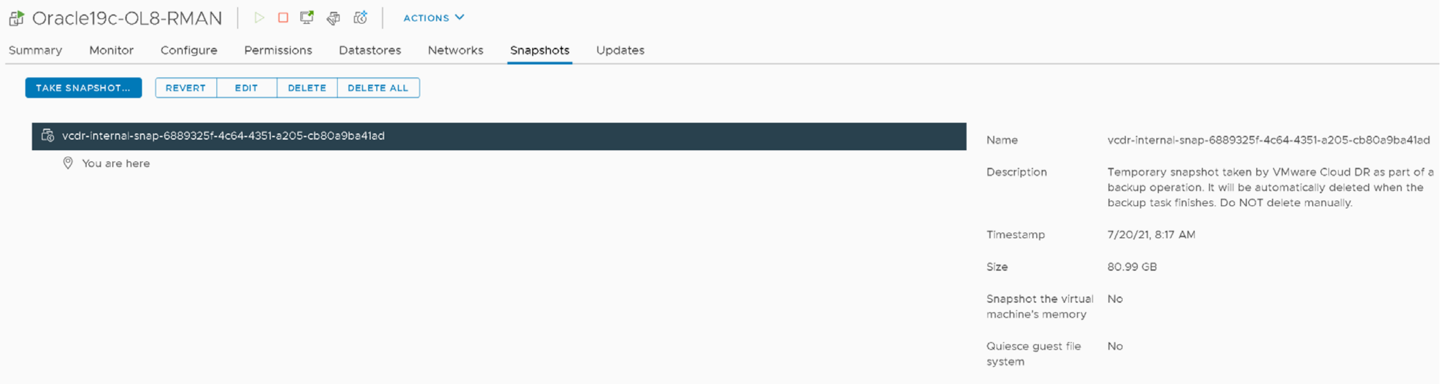


vcdr-internal-snap-ad26ad24-d9ed-460e-9da1-03917a440c93
You are here

Name vcdr-internal-snap-ad26ad24-d9ed-460e-9da1-03917a440c93
Description Temporary snapshot taken by VMware Cloud DR as part of a backup operation. It will be automatically deleted when the backup task finishes. Do NOT delete manually.
Timestamp 7/20/21, 8:15 AM
Size 66.49 GB
Snapshot the virtual machine's memory No
Quiesce guest file system No

FIGURE 131. Site A: Protected VM Oracle19c-OL8 Snapshots Details

The snapshot of VM **Oracle19c-OL8-RMAN** is as shown below:



Name	vcdr-internal-snap-6889325f-4c64-4351-a205-cb80a9ba41ad
Description	Temporary snapshot taken by VMware Cloud DR as part of a backup operation. It will be automatically deleted when the backup task finishes. Do NOT delete manually.
Timestamp	7/20/21, 8:17 AM
Size	80.99 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

FIGURE 132. Site A: Protected VM Oracle19c-OL8-RMAN Snapshots Details

The recovery SDDC **DR-SDDC** is as shown below:

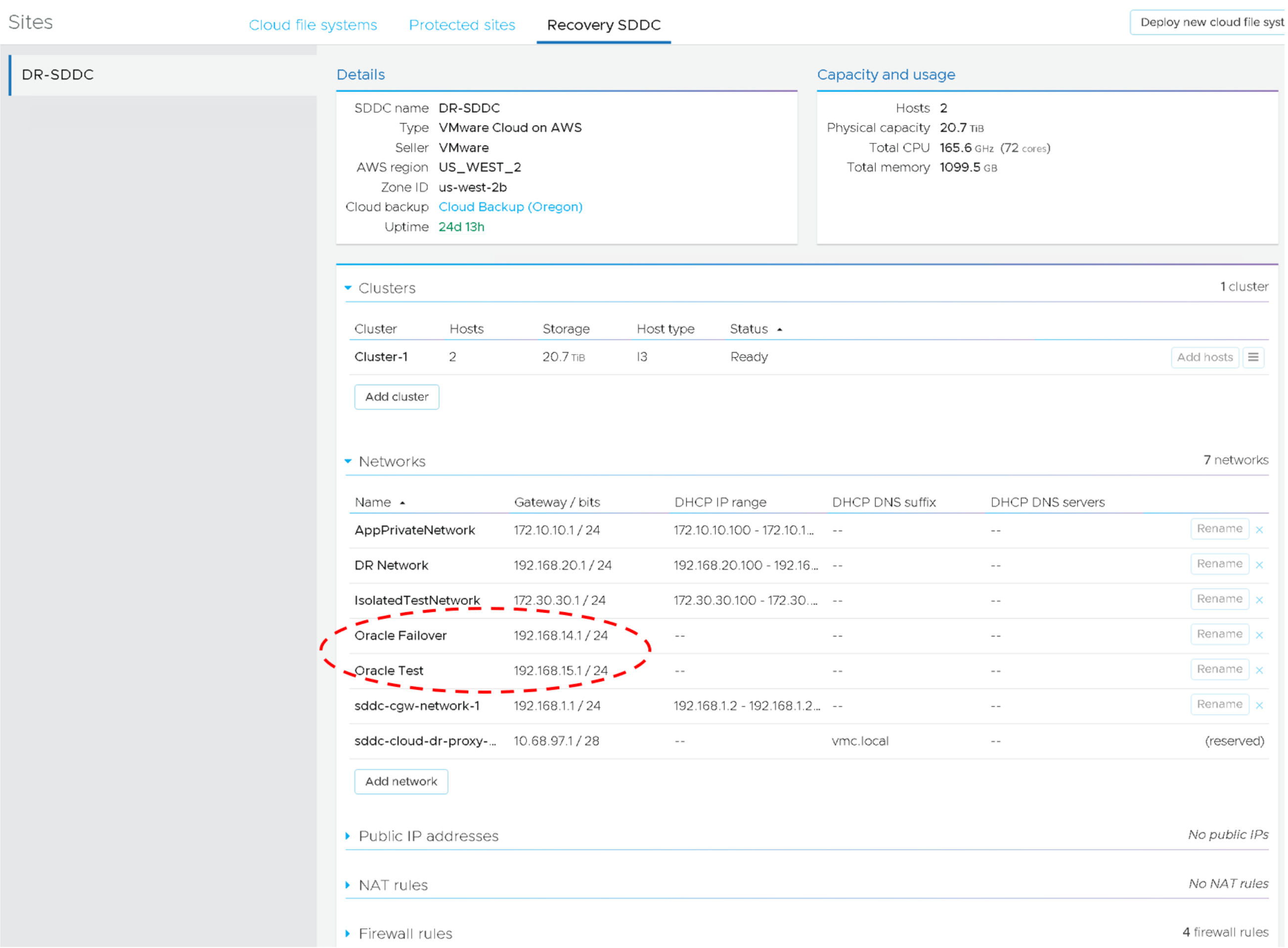
The network mapping port groups between Site A and VMware Cloud DR on VMware Cloud on AWS is as shown below:

NETWORK	SOURCE SITE	PORT GROUP	DESTINATION SITE	DESTINATION TEST NETWORK	DESTINATION RECOVERY NETWORK
Public Network	Site A	APPS-1614	VMware Cloud DR Recovery VMware Cloud on AWS	Oracle Test	Oracle Failover

TABLE 12. Network Mappings between Site A and Recovery SDDC

Two networks have been created on the recovery SDDC **DR-SDDC**:

- **Oracle Failover** with network subnet 192.168.14.1 / 24 for all **Failover** testing
- **Oracle Test** with network subset 192.168.15.1 / 24 for all **Test** testing



Sites | Cloud file systems | Protected sites | Recovery SDDC | Deploy new cloud file syst

DR-SDDC

Details

SDDC name	DR-SDDC
Type	VMware Cloud on AWS
Seller	VMware
AWS region	US_WEST_2
Zone ID	us-west-2b
Cloud backup	Cloud Backup (Oregon)
Uptime	24d 13h

Capacity and usage

Hosts	2
Physical capacity	20.7 TiB
Total CPU	165.6 GHz (72 cores)
Total memory	1099.5 GB

Clusters — 1 cluster

Cluster	Hosts	Storage	Host type	Status
Cluster-1	2	20.7 TiB	I3	Ready

Add hosts | Add cluster

Networks — 7 networks

Name	Gateway / bits	DHCP IP range	DHCP DNS suffix	DHCP DNS servers	
AppPrivateNetwork	172.10.10.1 / 24	172.10.10.100 - 172.10.1...	--	--	Rename
DR Network	192.168.20.1 / 24	192.168.20.100 - 192.16...	--	--	Rename
IsolatedTestNetwork	172.30.30.1 / 24	172.30.30.100 - 172.30....	--	--	Rename
Oracle Failover	192.168.14.1 / 24	--	--	--	Rename
Oracle Test	192.168.15.1 / 24	--	--	--	Rename
sddc-cgw-network-1	192.168.1.1 / 24	192.168.1.2 - 192.168.1.2...	--	--	Rename
sddc-cloud-dr-proxy-...	10.68.97.1 / 28	--	vmc.local	--	(reserved)

Add network

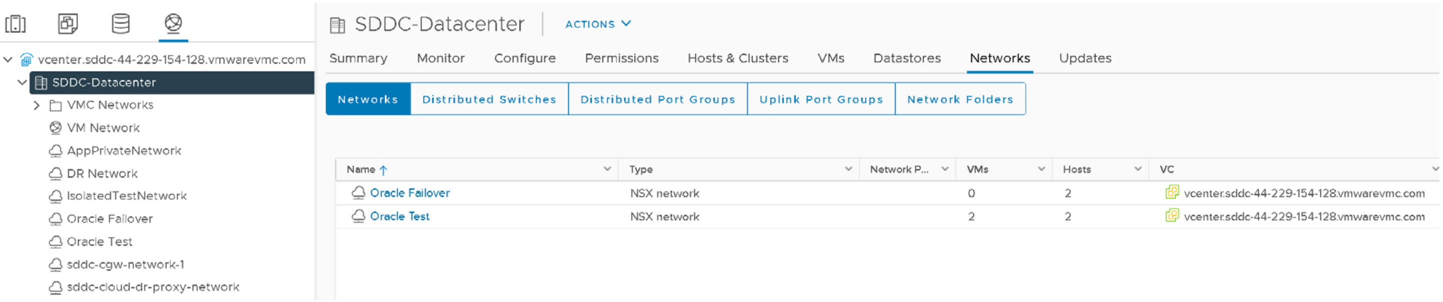
Public IP addresses — No public IPs

NAT rules — No NAT rules

Firewall rules — 4 firewall rules

FIGURE 133. VMware Cloud DR Failover and Test Network Details

The two networks on the recovery SDDC are as shown below:



vcenter.sddc-44-229-154-128.vmwarevmc.com
- SDDC-Datacenter
  - VMC Networks
  - VM Network
  - AppPrivateNetwork
  - DR Network
  - IsolatedTestNetwork
  - Oracle Failover
  - Oracle Test
  - sddc-cgw-network-1
  - sddc-cloud-dr-proxy-network

SDDC-Datacenter | ACTIONS

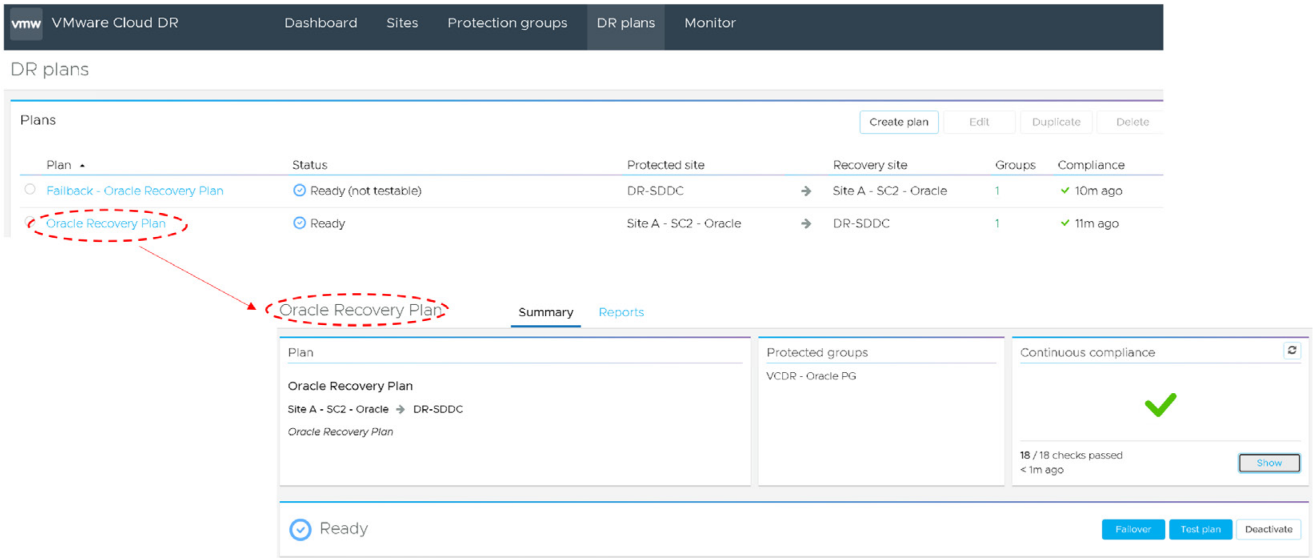
Summary | Monitor | Configure | Permissions | Hosts & Clusters | VMs | Datastores | Networks | Updates

Networks | Distributed Switches | Distributed Port Groups | Uplink Port Groups | Network Folders

Name ↑	Type	Network P...	VMs	Hosts	VC
Oracle Failover	NSX network		0	2	vcenter.sddc-44-229-154-128.vmwarevmc.com
Oracle Test	NSX network		2	2	vcenter.sddc-44-229-154-128.vmwarevmc.com

FIGURE 134. Recovery SDDC Failover and Test Network Port Group Details

The DR plan **Oracle Recovery Plan** is as shown below:



DR plans

Plans

Plan	Status	Protected site		Recovery site	Groups	Compliance
○ Failback - Oracle Recovery Plan	Ready (not testable)	DR-SDDC	→	Site A - SC2 - Oracle	1	✓ 10m ago
○ Oracle Recovery Plan	Ready	Site A - SC2 - Oracle	→	DR-SDDC	1	✓ 11m ago

Oracle Recovery Plan

Plan

Oracle Recovery Plan

Site A - SC2 - Oracle → DR-SDDC

Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

✓

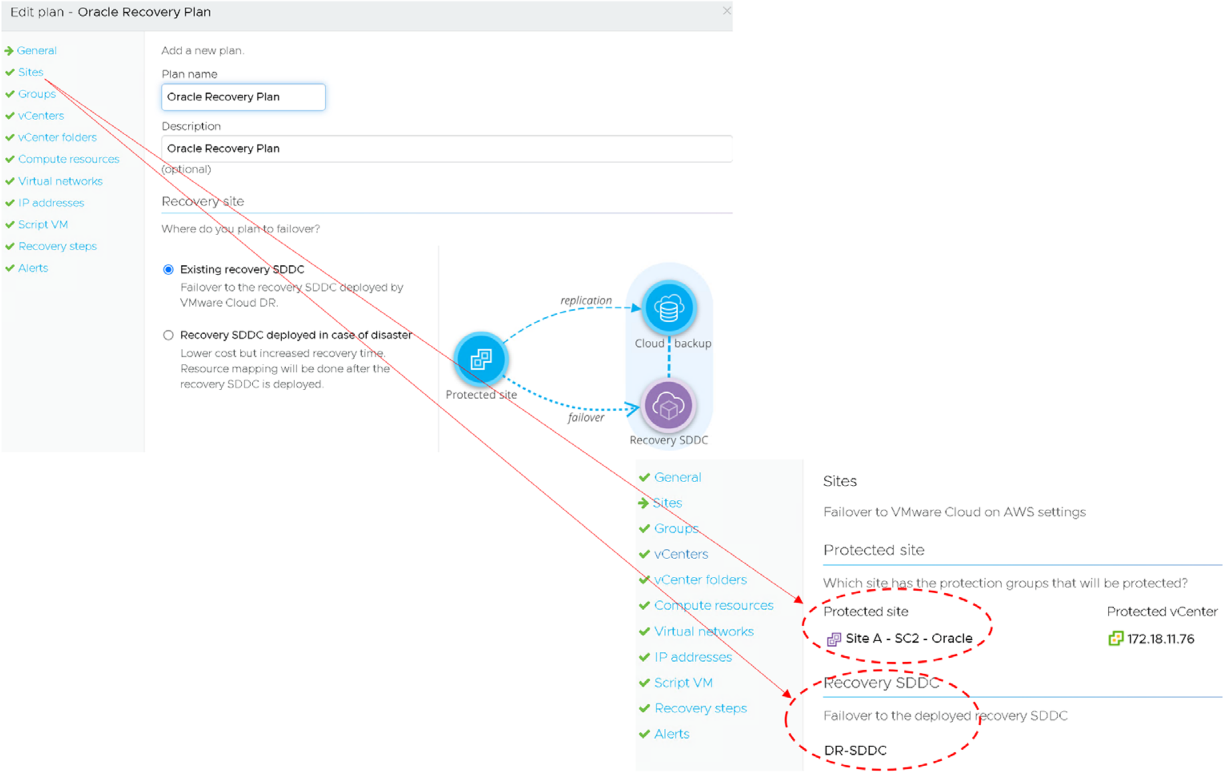
18 / 18 checks passed

< 1m ago

Ready

FIGURE 135. VMware Cloud DR Recovery Plan

Details of the DR plan **Oracle Recovery Plan** are as shown below:



Edit plan - Oracle Recovery Plan

Add a new plan.

Plan name

Oracle Recovery Plan

Description

Oracle Recovery Plan

(optional)

Recovery site

Where do you plan to failover?

● Existing recovery SDDC

Failover to the recovery SDDC deployed by VMware Cloud DR.

○ Recovery SDDC deployed in case of disaster

Lower cost but increased recovery time. Resource mapping will be done after the recovery SDDC is deployed.

Sites

Failover to VMware Cloud on AWS settings

Protected site

Which site has the protection groups that will be protected?

Protected site	Protected vCenter
Site A - SC2 - Oracle	172.18.11.76

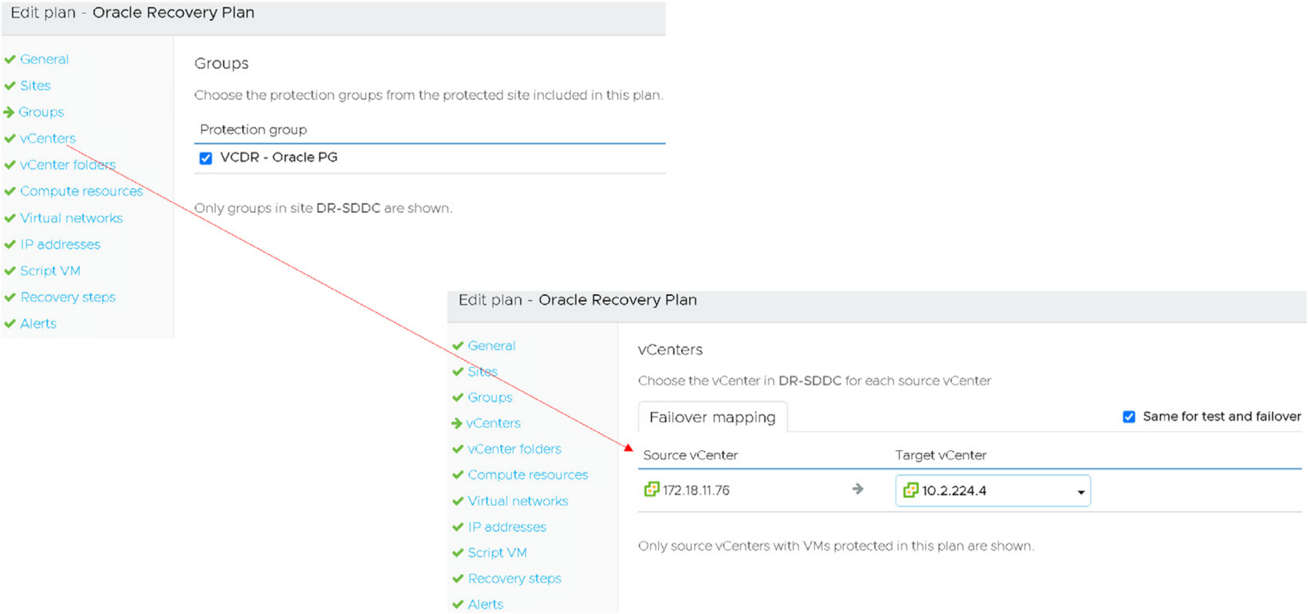
Recovery SDDC

Failover to the deployed recovery SDDC

DR-SDDC

FIGURE 136. VMware Cloud DR Recovery Plan Protected and Recovery Site

Details of the VMware Cloud DR recovery plan protection group and vCenter mappings are as shown below:



Edit plan - Oracle Recovery Plan

Groups

Choose the protection groups from the protected site included in this plan.

Protection group
☑ VCDR - Oracle PG

Only groups in site DR-SDDC are shown.

Edit plan - Oracle Recovery Plan

vCenters

Choose the vCenter in DR-SDDC for each source vCenter

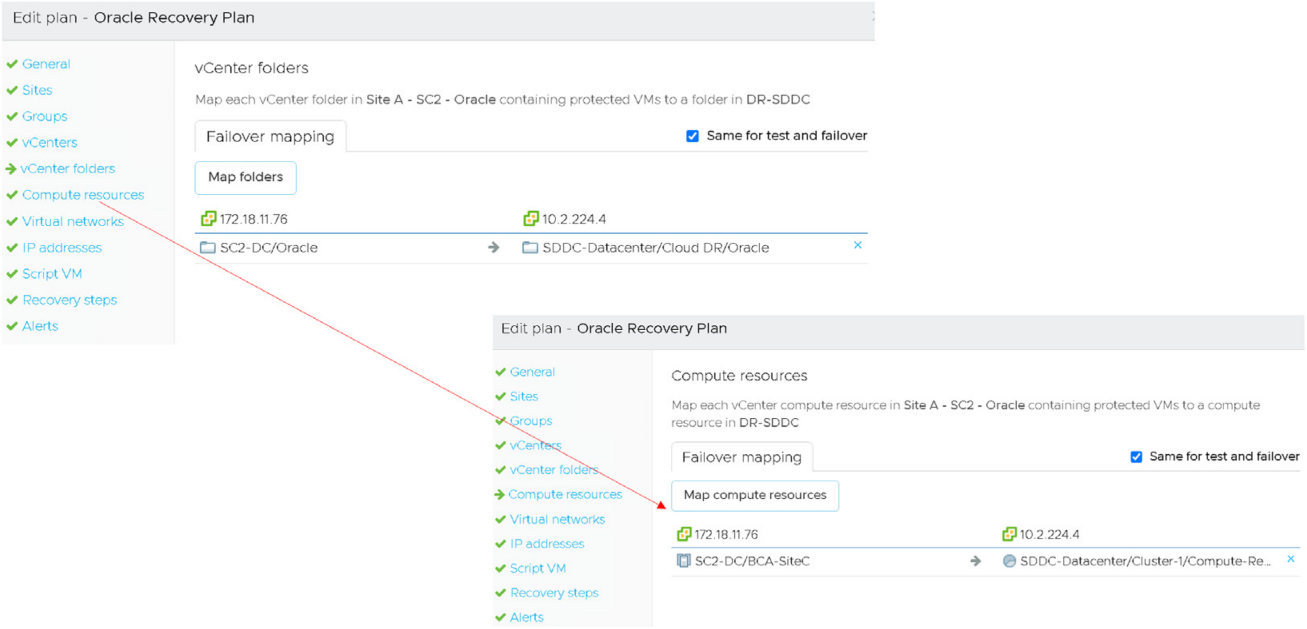
☑ Same for test and failover

Source vCenter		Target vCenter
172.18.11.76	→	10.2.224.4

Only source vCenters with VMs protected in this plan are shown.

FIGURE 137. VMware Cloud DR Recovery Plan Protection Group and vCenter Mappings

Details of the VMware Cloud DR vCenter folders and compute mappings are as shown below:



Edit plan - Oracle Recovery Plan

vCenter folders

Map each vCenter folder in Site A - SC2 - Oracle containing protected VMs to a folder in DR-SDDC

☑ Same for test and failover

172.18.11.76		10.2.224.4
SC2-DC/Oracle	→	SDDC-Datacenter/Cloud DR/Oracle

Edit plan - Oracle Recovery Plan

Compute resources

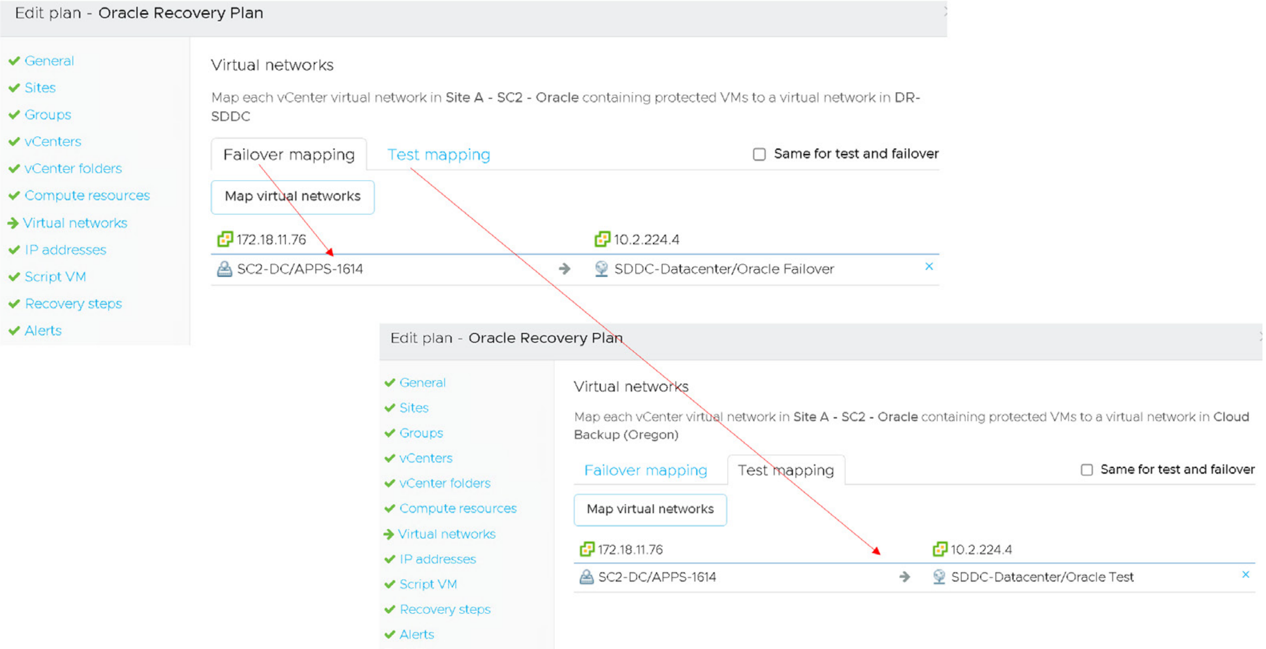
Map each vCenter compute resource in Site A - SC2 - Oracle containing protected VMs to a compute resource in DR-SDDC

☑ Same for test and failover

172.18.11.76		10.2.224.4
SC2-DC/BCA-SiteC	→	SDDC-Datacenter/Cluster-1/Compute-Re...

FIGURE 138. VMware Cloud DR Recovery vCenter Folders and Compute Mappings

Details of the VMware Cloud DR failover and test network mappings are as shown below:



Edit plan - Oracle Recovery Plan

Virtual networks

Map each vCenter virtual network in Site A - SC2 - Oracle containing protected VMs to a virtual network in DR-SDDC

172.18.11.76 → 10.2.224.4

SC2-DC/APPS-1614 → SDDC-Datacenter/Oracle Failover

Edit plan - Oracle Recovery Plan

Virtual networks

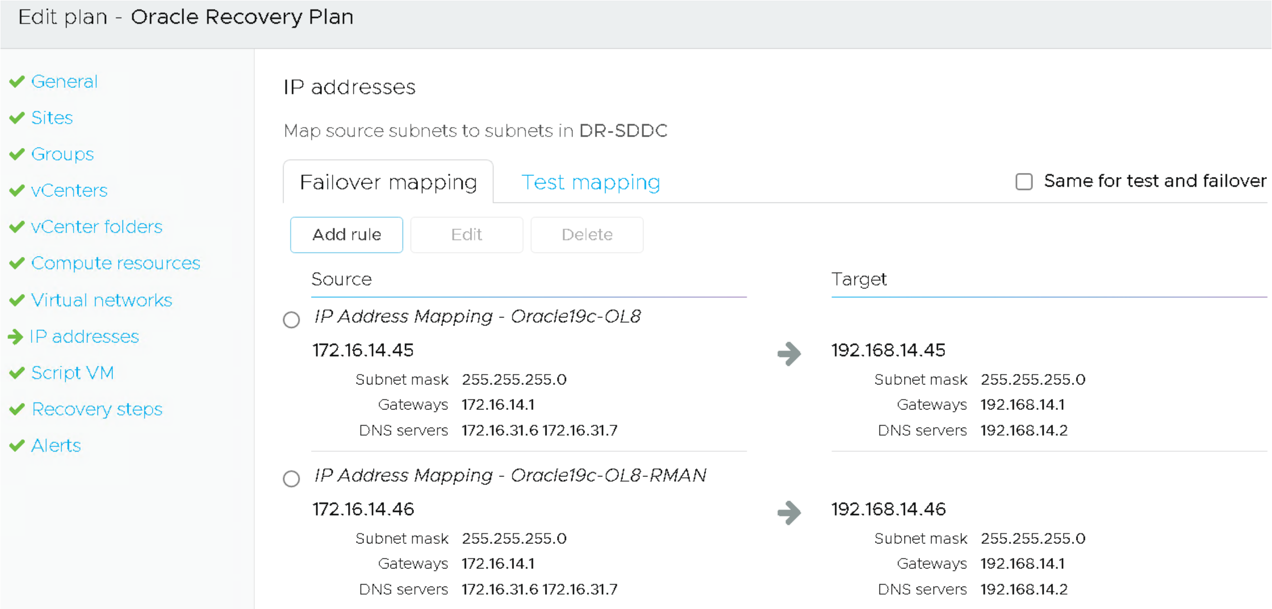
Map each vCenter virtual network in Site A - SC2 - Oracle containing protected VMs to a virtual network in Cloud Backup (Oregon)

172.18.11.76 → 10.2.224.4

SC2-DC/APPS-1614 → SDDC-Datacenter/Oracle Test

FIGURE 139. VMware Cloud DR Failover and Test Network Mappings

Details of the VMware Cloud DR failover network mappings are as shown below:



Edit plan - Oracle Recovery Plan

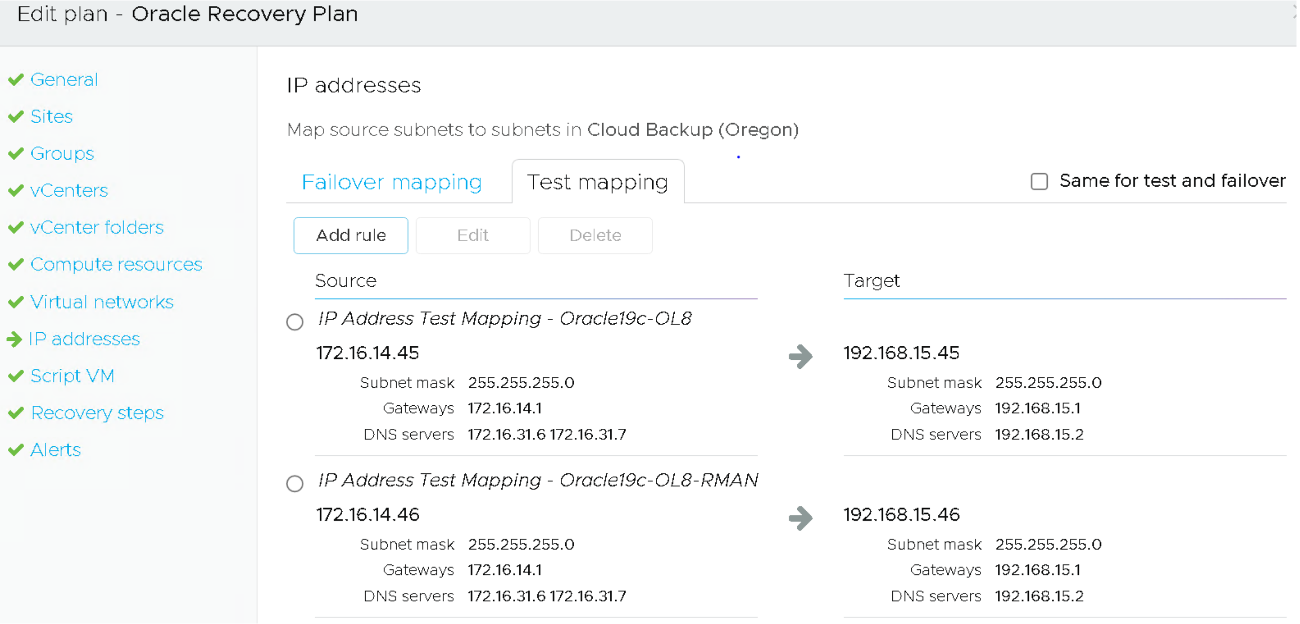
IP addresses

Map source subnets to subnets in DR-SDDC

Source		Target
○ *IP Address Mapping - Oracle19c-OL8*		
172.16.14.45	→	192.168.14.45
Subnet mask 255.255.255.0		Subnet mask 255.255.255.0
Gateways 172.16.14.1		Gateways 192.168.14.1
DNS servers 172.16.31.6 172.16.31.7		DNS servers 192.168.14.2
○ *IP Address Mapping - Oracle19c-OL8-RMAN*		
172.16.14.46	→	192.168.14.46
Subnet mask 255.255.255.0		Subnet mask 255.255.255.0
Gateways 172.16.14.1		Gateways 192.168.14.1
DNS servers 172.16.31.6 172.16.31.7		DNS servers 192.168.14.2

FIGURE 140. VMware Cloud DR Failover Network Mappings Details

Details of the VMware Cloud DR test network mappings are as shown below:



Edit plan - Oracle Recovery Plan

IP addresses

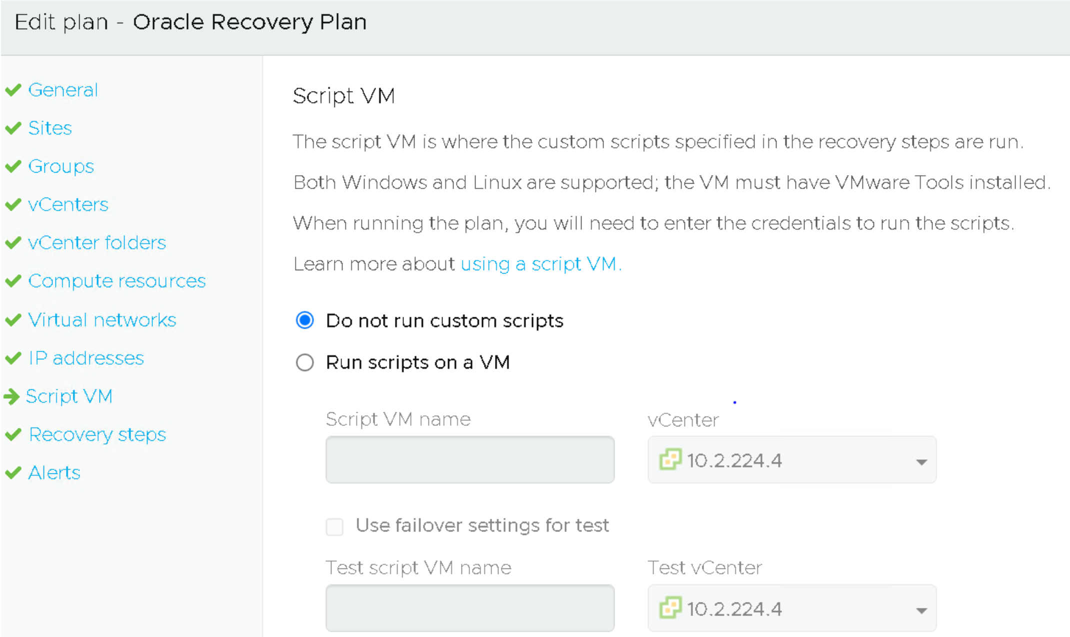
Map source subnets to subnets in Cloud Backup (Oregon)

□ Same for test and failover

Source	Target
○ *IP Address Test Mapping - Oracle19c-OL8* 172.16.14.45 Subnet mask 255.255.255.0 Gateways 172.16.14.1 DNS servers 172.16.31.6 172.16.31.7	192.168.15.45 Subnet mask 255.255.255.0 Gateways 192.168.15.1 DNS servers 192.168.15.2
○ *IP Address Test Mapping - Oracle19c-OL8-RMAN* 172.16.14.46 Subnet mask 255.255.255.0 Gateways 172.16.14.1 DNS servers 172.16.31.6 172.16.31.7	192.168.15.46 Subnet mask 255.255.255.0 Gateways 192.168.15.1 DNS servers 192.168.15.2

FIGURE 141. VMware Cloud DR Test Network Mappings Details

Details of the VMware Cloud DR recovery plan optional script are as shown below:



Edit plan - Oracle Recovery Plan

Script VM

The script VM is where the custom scripts specified in the recovery steps are run.

Both Windows and Linux are supported; the VM must have VMware Tools installed.

When running the plan, you will need to enter the credentials to run the scripts.

Learn more about using a script VM.

● Do not run custom scripts

○ Run scripts on a VM

Script VM name:

vCenter: 10.2.224.4

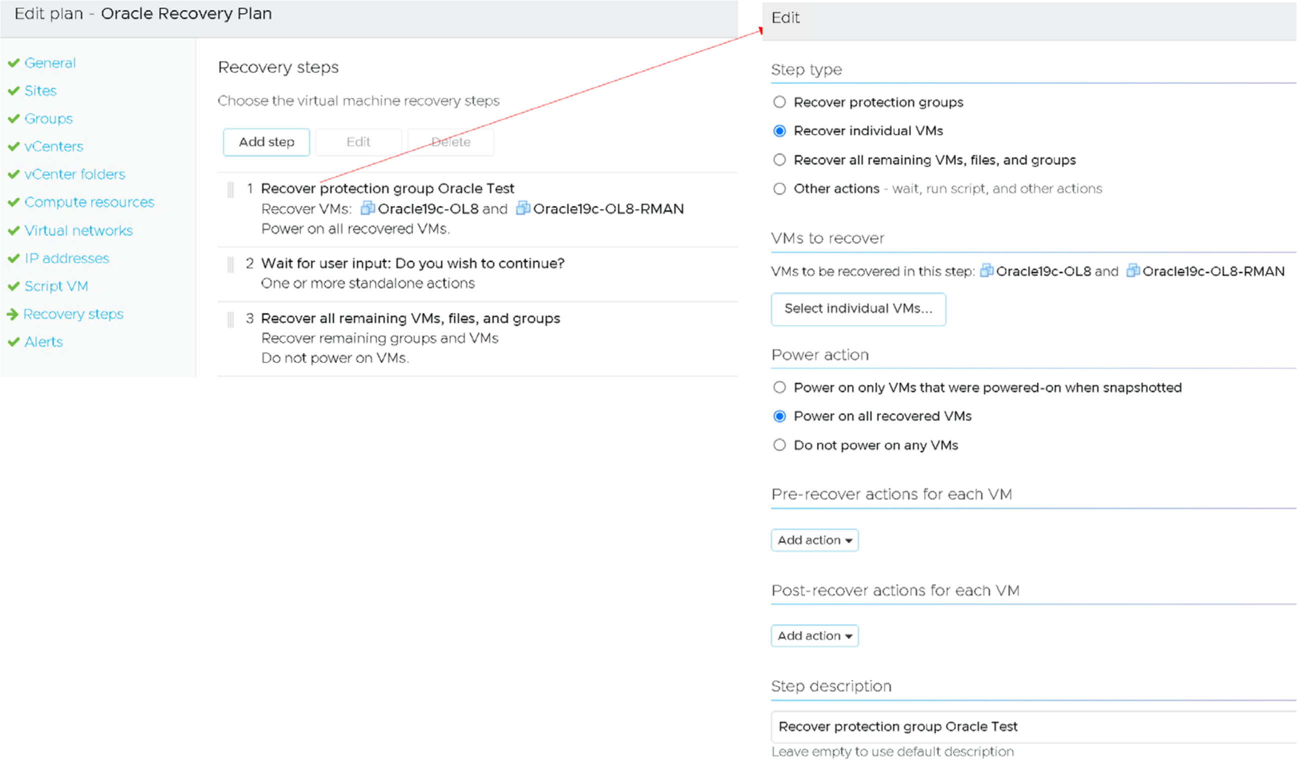
□ Use failover settings for test

Test script VM name:

Test vCenter: 10.2.224.4

FIGURE 142. VMware Cloud DR Recovery Plan Optional Script

Steps for creating the VMware Cloud DR recovery plan are continued below:



Edit plan - Oracle Recovery Plan

✓ General
✓ Sites
✓ Groups
✓ vCenters
✓ vCenter folders
✓ Compute resources
✓ Virtual networks
✓ IP addresses
✓ Script VM
→ Recovery steps
✓ Alerts

Recovery steps

Choose the virtual machine recovery steps

Add step | Edit | Delete

1 Recover protection group Oracle Test
Recover VMs: Oracle19c-OL8 and Oracle19c-OL8-RMAN
Power on all recovered VMs.

2 Wait for user input: Do you wish to continue?
One or more standalone actions

3 Recover all remaining VMs, files, and groups
Recover remaining groups and VMs
Do not power on VMs.

Edit

Step type

○ Recover protection groups
● Recover individual VMs
○ Recover all remaining VMs, files, and groups
○ Other actions - wait, run script, and other actions

VMs to recover

VMs to be recovered in this step: Oracle19c-OL8 and Oracle19c-OL8-RMAN

Select individual VMs...

Power action

○ Power on only VMs that were powered-on when snapshotted
● Power on all recovered VMs
○ Do not power on any VMs

Pre-recover actions for each VM

Add action ▾

Post-recover actions for each VM

Add action ▾

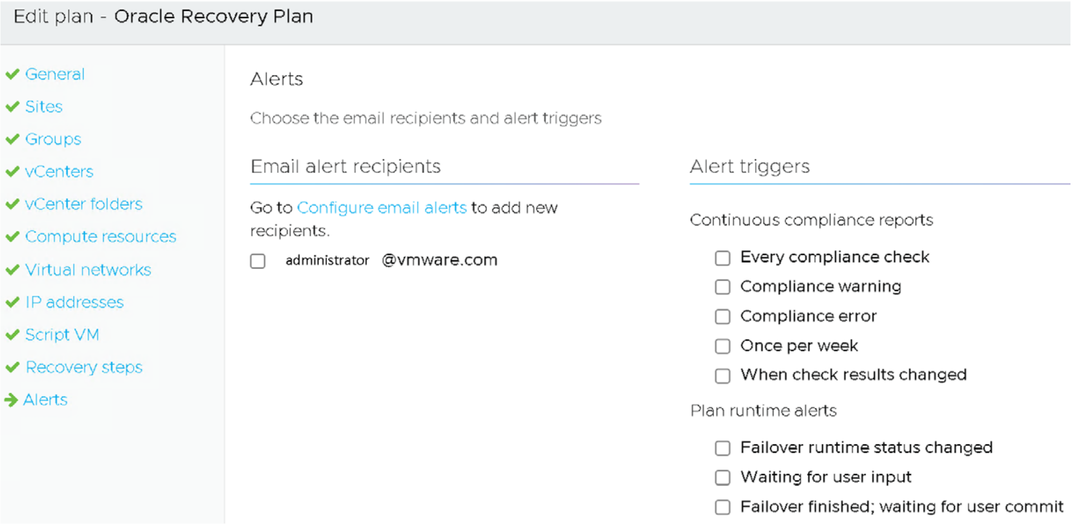
Step description

Recover protection group Oracle Test

Leave empty to use default description

FIGURE 143. VMware Cloud DR Recovery Plan Steps

Complete the VMware Cloud DR recovery plan configuration.



Edit plan - Oracle Recovery Plan

✓ General
✓ Sites
✓ Groups
✓ vCenters
✓ vCenter folders
✓ Compute resources
✓ Virtual networks
✓ IP addresses
✓ Script VM
✓ Recovery steps
→ Alerts

Alerts

Choose the email recipients and alert triggers

Email alert recipients

Go to Configure email alerts to add new recipients.

□ administrator @vmware.com

Alert triggers

Continuous compliance reports

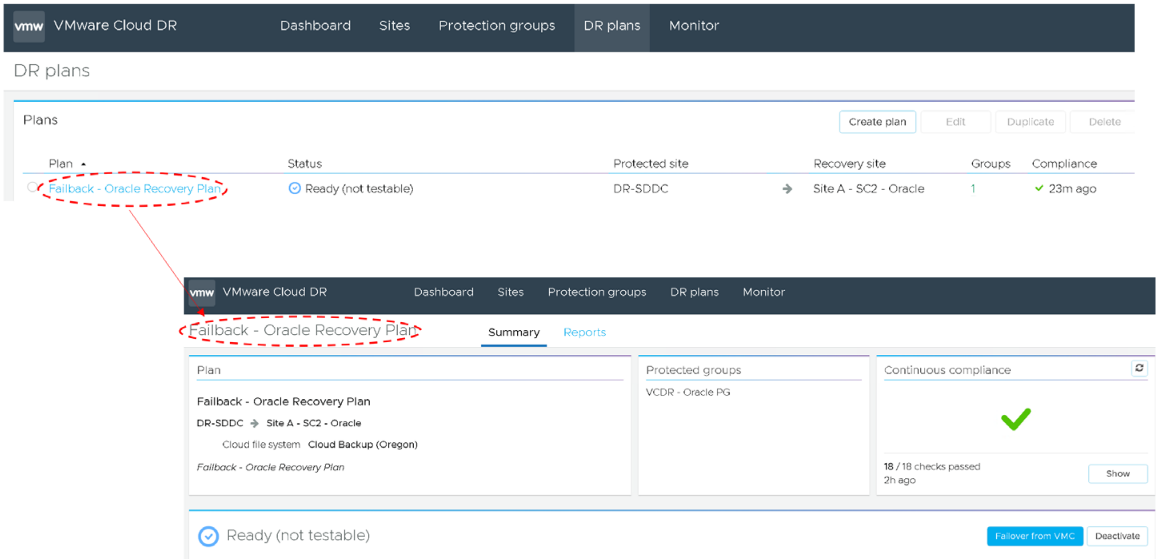
□ Every compliance check
□ Compliance warning
□ Compliance error
□ Once per week
□ When check results changed

Plan runtime alerts

□ Failover runtime status changed
□ Waiting for user input
□ Failover finished; waiting for user commit

FIGURE 144. VMware Cloud DR Recovery Plan Configure Complete

The DR plan **Failback - Oracle Recovery Plan** is as shown below:



DR plans

Plans

Plan ▲	Status	Protected site		Recovery site	Groups	Compliance
Failback - Oracle Recovery Plan	Ready (not testable)	DR-SDDC	→	Site A - SC2 - Oracle	1	✓ 23m ago

Failback - Oracle Recovery Plan

Plan

Failback - Oracle Recovery Plan

DR-SDDC → Site A - SC2 - Oracle

Cloud file system Cloud Backup (Oregon)

Failback - Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

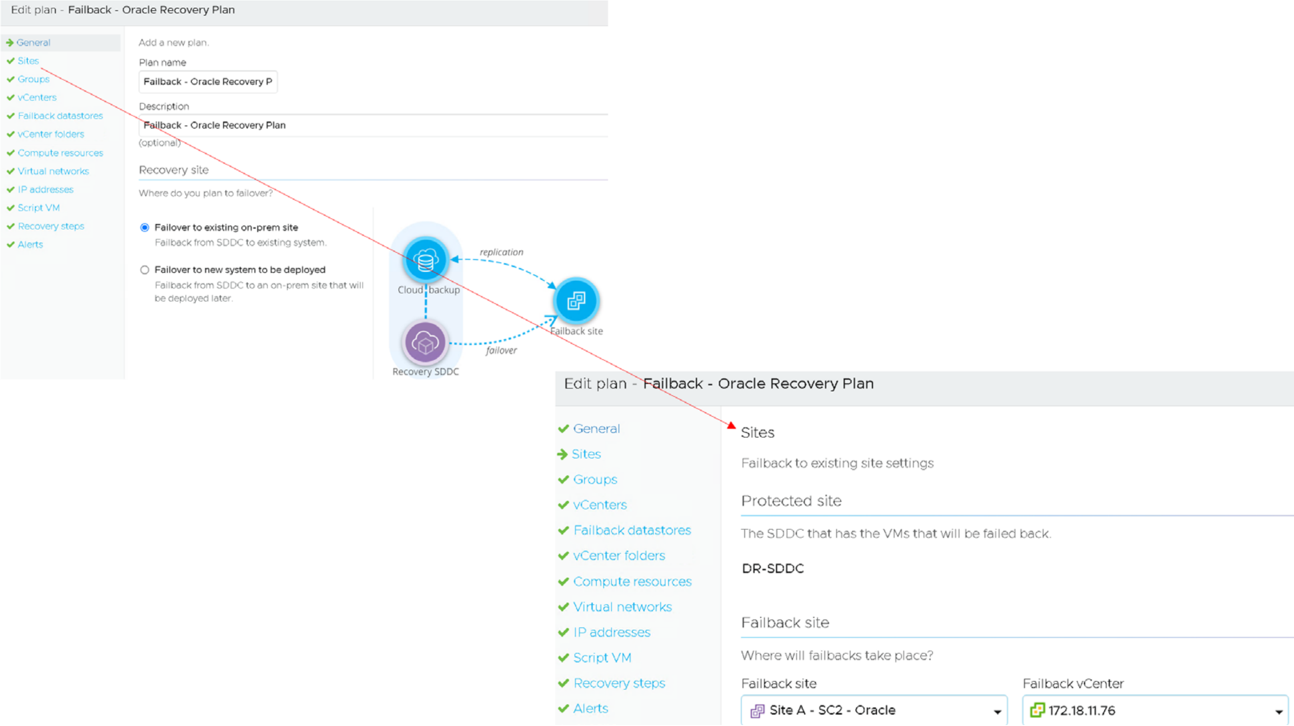
18 / 18 checks passed
2h ago

Ready (not testable)

FIGURE 145. VMware Cloud DR Failback Plan Details

Details of DR plan **Failback - Oracle Recovery Plan** are as shown below.

The details of DR plan **Failback - Oracle Recovery Plan** is simply the reverse of those for DR plan **Oracle Recovery Plan**.



Edit plan - Failback - Oracle Recovery Plan

Add a new plan.

Plan name: Failback - Oracle Recovery P

Description: Failback - Oracle Recovery Plan
(optional)

Recovery site

Where do you plan to failover?

● Failover to existing on-prem site
Failback from SDDC to existing system.

○ Failover to new system to be deployed
Failback from SDDC to an on-prem site that will be deployed later.

Edit plan - Failback - Oracle Recovery Plan

Sites

Failback to existing site settings

Protected site

The SDDC that has the VMs that will be failed back.

DR-SDDC

Failback site

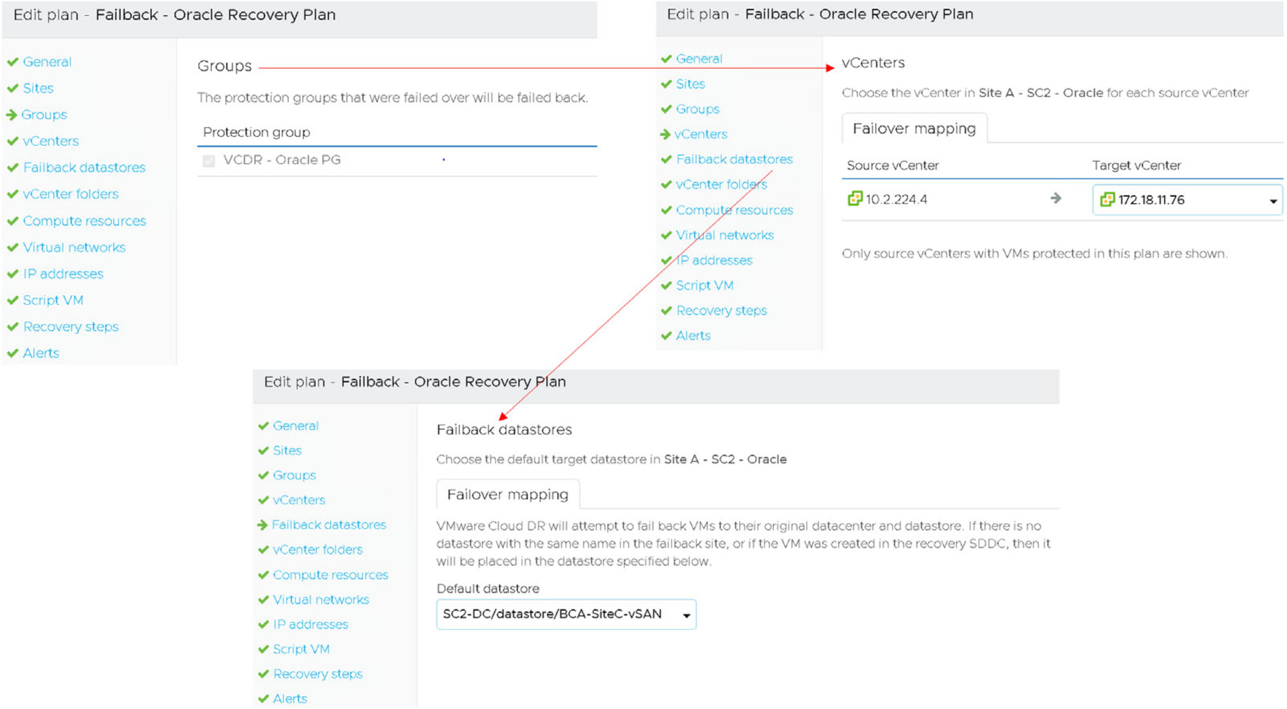
Where will failbacks take place?

Failback site: Site A - SC2 - Oracle

Failback vCenter: 172.18.11.76

FIGURE 146. VMware Cloud DR Failback Plan Protected and Failback Site

Details of the VMware Cloud DR failback plan failover and datastore mappings are as shown below:



Edit plan - **Failback - Oracle Recovery Plan**

Groups

The protection groups that were failed over will be failed back.

Protection group

☑ VCDR - Oracle PG

Edit plan - **Failback - Oracle Recovery Plan**

vCenters

Choose the vCenter in **Site A - SC2 - Oracle** for each source vCenter

Failover mapping

Source vCenter		Target vCenter
10.2.224.4	→	172.18.11.76

Only source vCenters with VMs protected in this plan are shown.

Edit plan - **Failback - Oracle Recovery Plan**

Failback datastores

Choose the default target datastore in **Site A - SC2 - Oracle**

Failover mapping

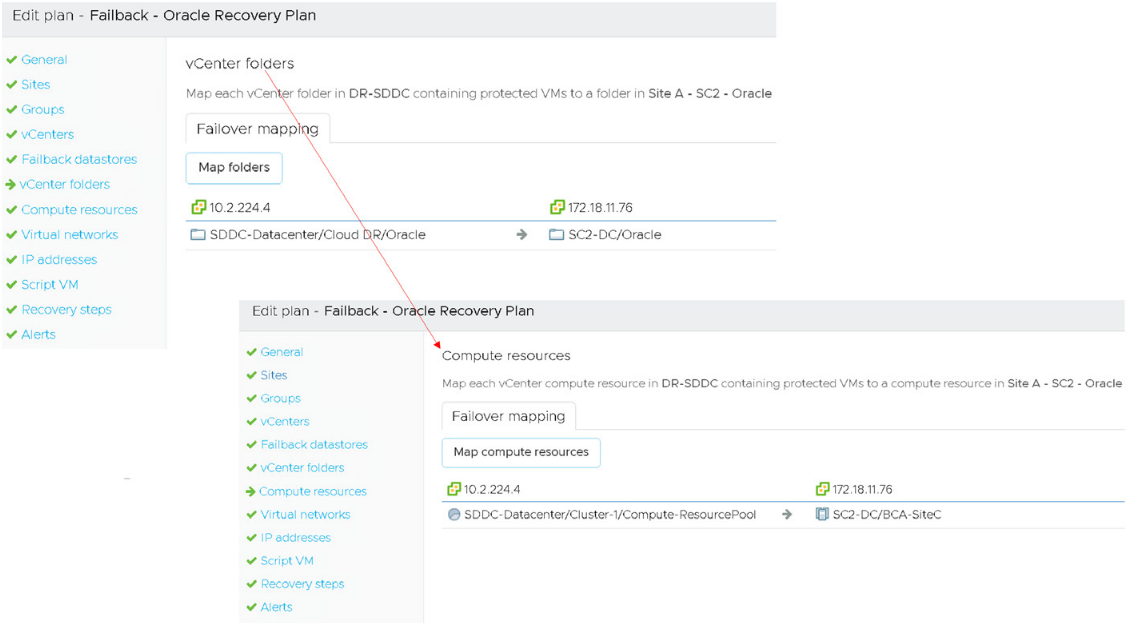
VMware Cloud DR will attempt to fail back VMs to their original datacenter and datastore. If there is no datastore with the same name in the failback site, or if the VM was created in the recovery SDDC, then it will be placed in the datastore specified below.

Default datastore

SC2-DC/datastore/BCA-SiteC-vSAN

FIGURE 147. VMware Cloud DR Failback Plan Failover and Datastore Mappings

Details of the VMware Cloud DR failback plan folder and compute mappings are as shown below:



Edit plan - **Failback - Oracle Recovery Plan**

vCenter folders

Map each vCenter folder in **DR-SDDC** containing protected VMs to a folder in **Site A - SC2 - Oracle**

Failover mapping

10.2.224.4		172.18.11.76
SDDC-Datacenter/Cloud DR/Oracle	→	SC2-DC/Oracle

Edit plan - **Failback - Oracle Recovery Plan**

Compute resources

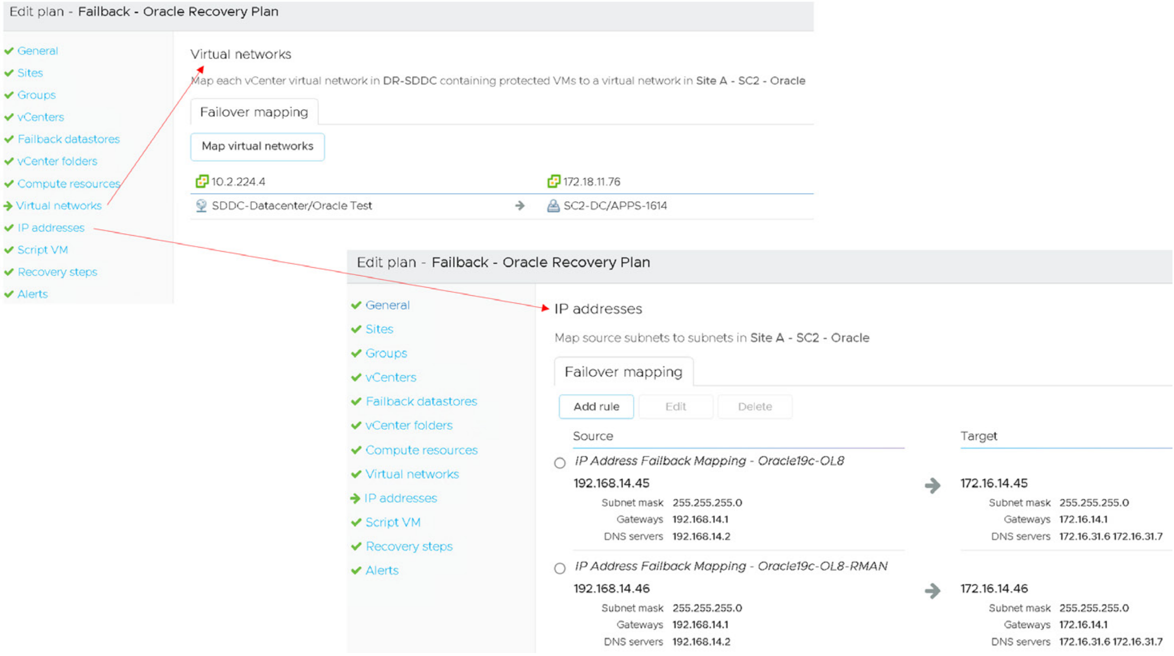
Map each vCenter compute resource in **DR-SDDC** containing protected VMs to a compute resource in **Site A - SC2 - Oracle**

Failover mapping

10.2.224.4		172.18.11.76
SDDC-Datacenter/Cluster-1/Compute-ResourcePool	→	SC2-DC/BCA-SiteC

FIGURE 148. VMware Cloud DR Failback Plan Folder and Compute Mappings

Details of the VMware Cloud DR failback network mappings are as shown below:



Edit plan - Failback - Oracle Recovery Plan

Virtual networks

Map each vCenter virtual network in DR-SDDC containing protected VMs to a virtual network in Site A - SC2 - Oracle

10.2.224.4 | 172.18.11.76
SDDC-Datacenter/Oracle Test → SC2-DC/APPS-1614

Edit plan - Failback - Oracle Recovery Plan

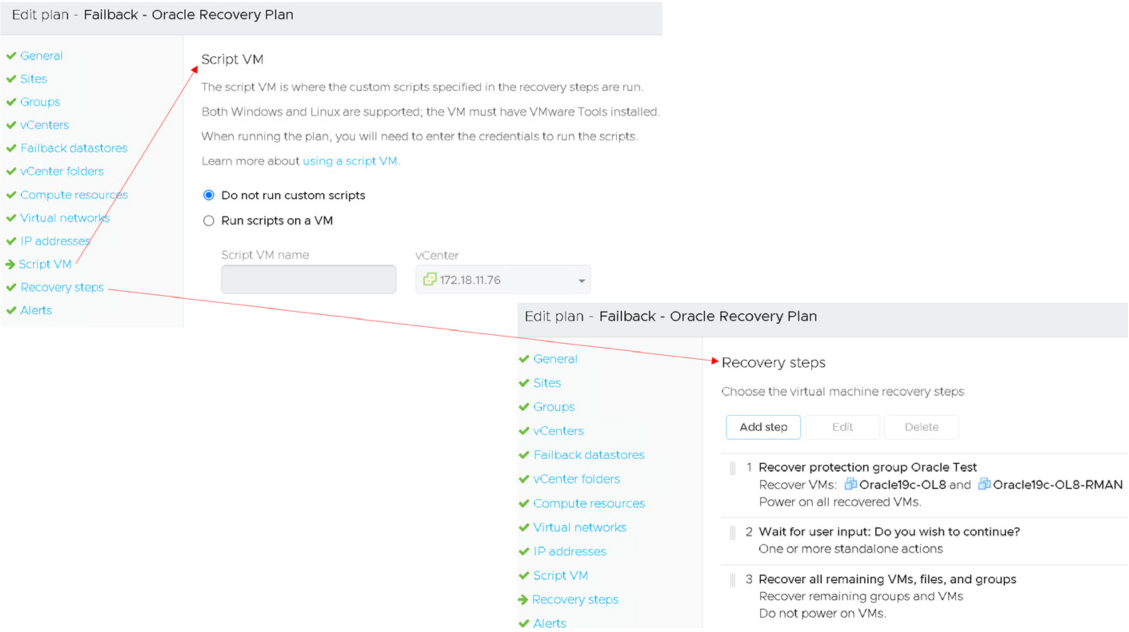
IP addresses

Map source subnets to subnets in Site A - SC2 - Oracle

Source		Target
○ *IP Address Failback Mapping - Oracle19c-OL8*		
192.168.14.45	→	172.16.14.45
Subnet mask 255.255.255.0		Subnet mask 255.255.255.0
Gateways 192.168.14.1		Gateways 172.16.14.1
DNS servers 192.168.14.2		DNS servers 172.16.31.6 172.16.31.7
○ *IP Address Failback Mapping - Oracle19c-OL8-RMAN*		
192.168.14.46	→	172.16.14.46
Subnet mask 255.255.255.0		Subnet mask 255.255.255.0
Gateways 192.168.14.1		Gateways 172.16.14.1
DNS servers 192.168.14.2		DNS servers 172.16.31.6 172.16.31.7

FIGURE 149. VMware Cloud DR Failback Network Mappings

Details of the VMware Cloud DR failback recovery plan optional script are as shown below:



Edit plan - Failback - Oracle Recovery Plan

Script VM

The script VM is where the custom scripts specified in the recovery steps are run.

Both Windows and Linux are supported; the VM must have VMware Tools installed.

When running the plan, you will need to enter the credentials to run the scripts.

Learn more about using a script VM.

● Do not run custom scripts

○ Run scripts on a VM

Script VM name:

vCenter: 172.18.11.76

Edit plan - Failback - Oracle Recovery Plan

Recovery steps

Choose the virtual machine recovery steps

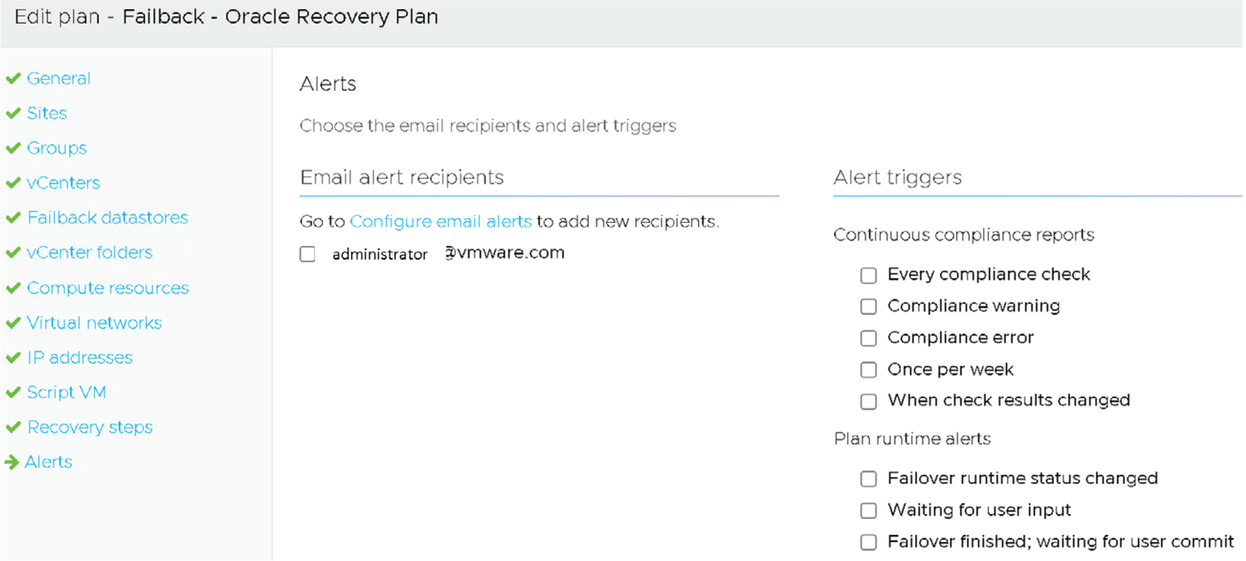
1 Recover protection group Oracle Test
Recover VMs: Oracle19c-OL8 and Oracle19c-OL8-RMAN
Power on all recovered VMs.

2 Wait for user input: Do you wish to continue?
One or more standalone actions

3 Recover all remaining VMs, files, and groups
Recover remaining groups and VMs
Do not power on VMs.

FIGURE 150. VMware Cloud DR Failback Recovery Plan Optional Script

Complete the VMware Cloud DR failback recovery plan configuration.



Edit plan - Failback - Oracle Recovery Plan

- ✓ General
- ✓ Sites
- ✓ Groups
- ✓ vCenters
- ✓ Failback datastores
- ✓ vCenter folders
- ✓ Compute resources
- ✓ Virtual networks
- ✓ IP addresses
- ✓ Script VM
- ✓ Recovery steps
- → Alerts

Alerts

Choose the email recipients and alert triggers

Email alert recipients

Go to Configure email alerts to add new recipients.

□ administrator @vmware.com

Alert triggers

Continuous compliance reports

□ Every compliance check
□ Compliance warning
□ Compliance error
□ Once per week
□ When check results changed

Plan runtime alerts

□ Failover runtime status changed
□ Waiting for user input
□ Failover finished; waiting for user commit

FIGURE 151. VMware Cloud DR Failback Recovery Plan Configuration Complete

As VMware Cloud DR uses regularly scheduled snapshots to replicate to the SCFS and VMware snapshots are not compatible with disks in multi-writer mode, VMware Cloud DR cannot replicate disks in multi-writer mode. VMware snapshots are a point-in-time (PIT) snapshot and therefore are crash-consistent.

More information regarding VMware Cloud DR components can be found in *VMware Cloud Disaster Recovery Documentation*.

Solution Validation

This solution primarily validated the business continuity and disaster recovery functionality of Oracle single-instance and Oracle RAC deployments on VMFS and vSphere Virtual Volumes storage backed by Pure x50 Storage.

Site A was chosen for all business continuity validations. Site B was chosen for on-premises disaster recovery validation and VMware Cloud on AWS was chosen for cloud-based disaster recovery validation.

Solution Test Overview

This solution validates the business continuity and disaster recovery functionality of Oracle single-instance and Oracle RAC deployments using Pure x50 Storage on-premises and in VMware clouds, at each of the three levels referenced below:

- Business Continuity
  - Application level
  - vSphere level
  - Storage level

- Disaster Recovery
  - Application level
  - vSphere level
  - Storage level

The choice of a business continuity or disaster recovery solution is dependent on application needs, SLAs, RTO, RPO and various other factors.

The focus of the solution was to ensure that for all business continuity and disaster recovery use cases, database data was always consistent.

Performance testing was not included as part of this reference architecture. Any performance data is a result of the combination of hardware configuration, software configuration, test methodology, test tool, and workload profile used in the testing.

Performance testing can be conducted by using the SLOB tool against Oracle single instance and RAC, and generating a load on the database. Oracle AWR and Linux SAR reports can be captured to compare the performance and validate the testing use cases.

Oracle Business Continuity

This section validates Oracle business continuity using Oracle application-based tools, VMware-based tools and storage-based tools for an Oracle single instance and Oracle RAC using Pure x50 Storage.

On-premises and VMware clouds may have different choices of storage offerings but the type of underlying storage (VMFS, RDM, iSCSI, NFS, vSAN, vSphere Virtual Volumes) is transparent to the Oracle layer, whether its on-premises or on VMware clouds.

Once VM disks are carved from any of these storage technologies and added to a VM, the guest operating system sees them as a regular Linux block device (/dev/sdX). The remaining steps to create ASM disks or create filesystems are the same as one would execute on physical architecture.

Application-Level Business Continuity

Recovery Manager (RMAN) is an Oracle Database client that performs backup and recovery tasks on the databases and automates administration of the backup strategies.

Other Oracle Database backup tools includes data pump, user managed backups (i.e., cold backup by shutting down the database OR hot backup by DB BEGIN/END backup commands), and database flashback.

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

On-premises

This use case focusses on leveraging the Oracle RMAN utility to back up single-instance VM **Oracle19c-OL8** and the two-node Oracle RAC **prac19c** using RMAN catalog database **rmandb**.

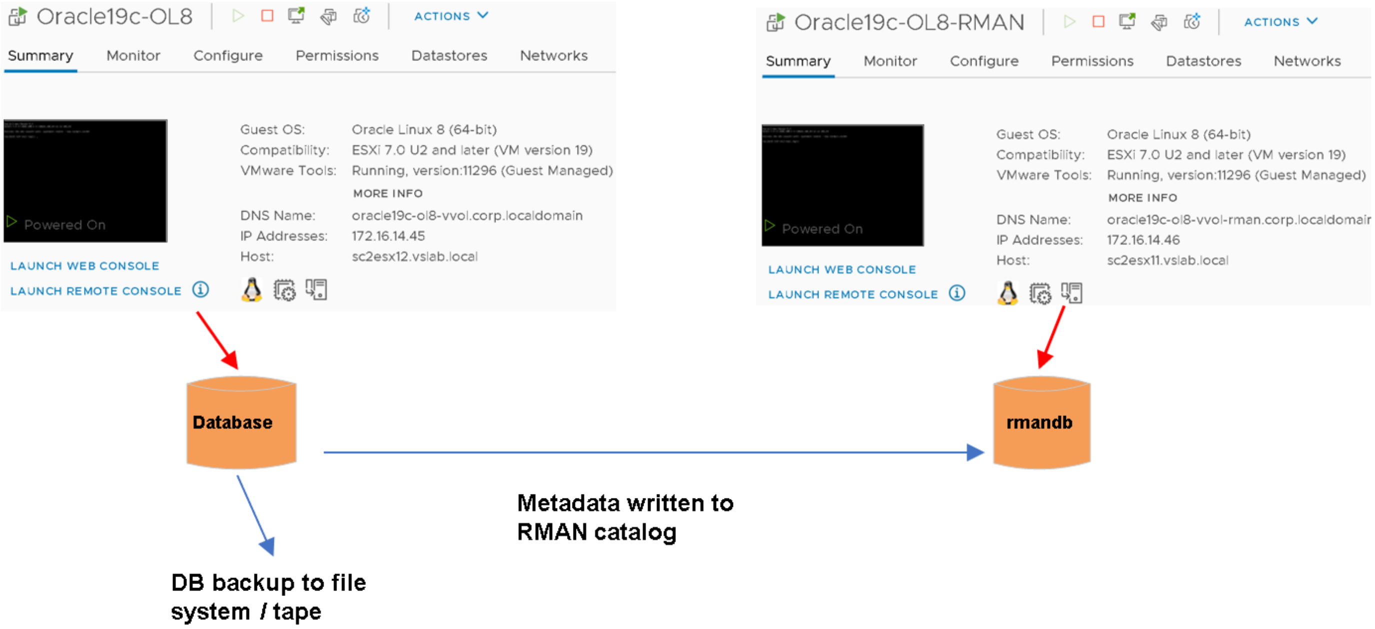
Two VMs are employed for this use case:

- Production VM **Oracle19c-OL8-VVOL**
- RMAN VM **Oracle19c-OL8-VVOL-RMAN** with RMAN catalog

RMAN utility is used to back up the database data to:

- Oracle FRA (i.e., fast recovery area), a disk location in which the database can store and manage files related to backup and recovery
- A filesystem (ext3 / ext4 / zfs / xfs) which can then be further backed up by third-party products to media
- Interact directly with media management software to write to sequential media devices such as tape libraries

Learn more about *Oracle RMAN Backup*.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol.corp.localdomain
IP Addresses: 172.16.14.45
Host: sc2esx12.vslab.local

Oracle19c-OL8-RMAN

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomair
IP Addresses: 172.16.14.46
Host: sc2esx11.vslab.local

FIGURE 152. Oracle RMAN Backup Using RMAN Catalog

Setting up RMAN backup and RMAN catalog is beyond the scope of this paper. Learn more about *Oracle RMAN*.

Using the Pure Storage Plugin and vSphere Virtual Volumes, the different use cases of Oracle RMAN utility with vSphere Virtual Volumes to back up a single instance VM and Oracle RAC cluster can be found in *Virtualizing Oracle Workloads with VMware vSphere Virtual Volumes on VMware Hybrid Cloud*.

Using the Oracle RMAN utility, the steps required to back up the two-node Oracle RAC **prac19c** using RMAN catalog database **rmandb** are the same as those employed for single-instance VM **Oracle19c-OL8-VVOL**.

More information regarding use of Oracle RMAN to backup an Oracle RAC can be found in *Real Application Clusters Administration and Deployment Guide Managing Backup and Recovery*.

VMware Clouds

The above use case, using the Oracle RMAN utility to back up the single-instance VM **Oracle19c-OL8** and the two-node Oracle RAC **prac19c** with RMAN catalog database **rmandb**, employs the same steps for all VMware clouds as well as on-premises environments

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

vSphere Level Business Continuity

VMware snapshots can be used to take a VM level point-in-time snapshot. Snapshots preserve the state and data of a VM at the time the snapshot is taken.

A VMware clone of the VM can be created from this VM snapshot, or one can simply create a VM-level clone from an existing VM without taking a VM-level snapshot.

A VMware snapshot of an Oracle VM can be taken before any database operation. The state of the VM can then be reverted back to that VM-level snapshot in case there are issues with the database operation.

Both web client and PowerCLI can be leveraged for taking a VMware snapshot and clone.

VM operations like VMware snapshots and VMware clones constructs are the same across all underlying VMware storage layers, even though there may be subtle differences in the ways some of the VM components are represented on these various storage layers.

On-premises

This use case focusses on the use of VMware snapshot and VMware Clone utility to:

- Snapshot a single instance VM **Oracle19c-OL8** for purpose of reverting to it in case of any application issue
- Clone a new single instance VM **Oracle19c-OL8-Clone** directly from VM **Oracle19c-OL8** or from a point-in-time snapshot of the single instance VM **Oracle19c-OL8**

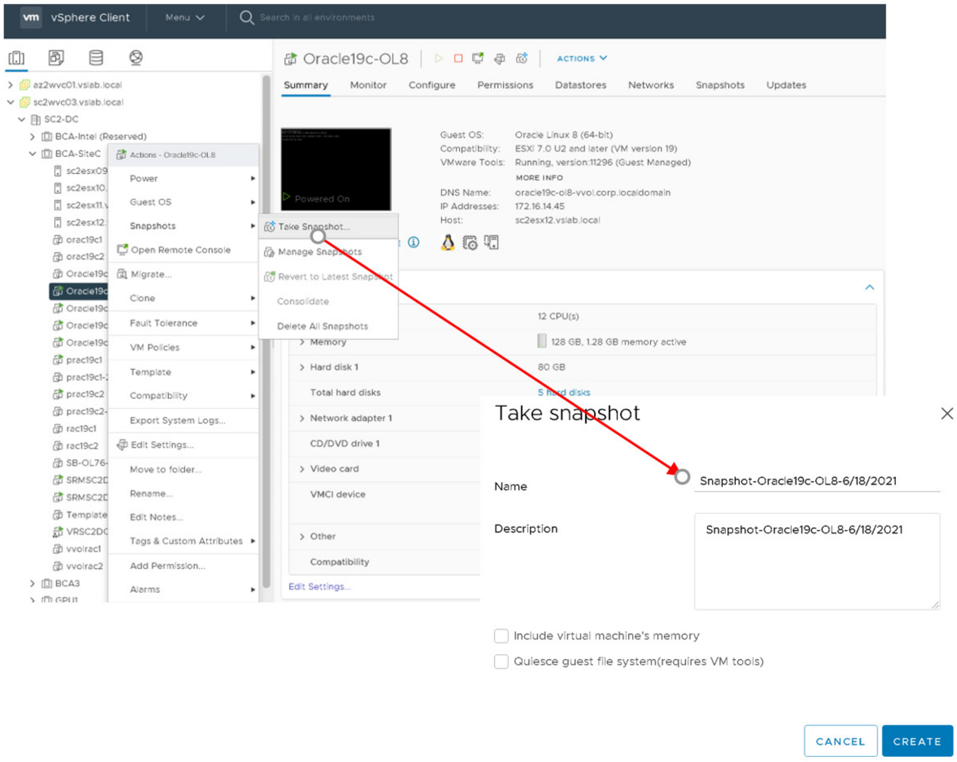
VMware Snapshot

The VM snapshot can be taken either as a:

- Crash-consistent database snapshot (without placing the database in a backup mode)
- Hot backup database snapshot by placing the database in a backup mode using **BEGIN/END Backup** commands.
- Cold backup database snapshot by shutting down the database

VMware Snapshot with Crash-Consistent Database Backup

The steps below illustrate the use of VMware Snapshot to take a crash-consistent snapshot of an Oracle single-instance database VM using the web client and reverting back to the snapshot.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol.corp.localdomain
IP Addresses: 172.16.14.45
Host: sc2esx12.vslab.local

12 CPU(s)
Memory: 128 GB, 1.28 GB memory active
Hard disk 1: 80 GB
Total hard disks: 5 hard disks

Take snapshot

Name: Snapshot-Oracle19c-OL8-6/18/2021

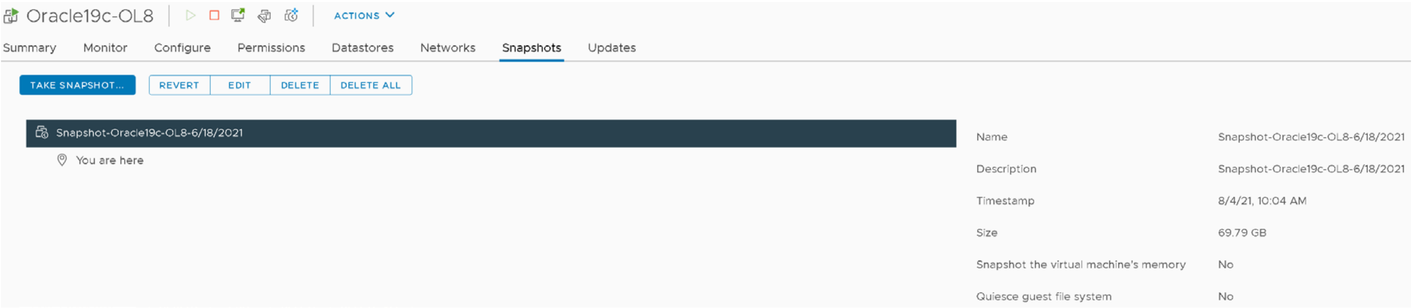
Description: Snapshot-Oracle19c-OL8-6/18/2021

☐ Include virtual machine's memory

☐ Quiesce guest file system(requires VM tools)

FIGURE 153. Steps to take VMware Snapshot of Oracle VM Oracle19c-OL8

VMware snapshot **Snapshot-Oracle19c-OL8-6/18/2021** of Oracle VM **Oracle19c-OL8** is taken successfully.



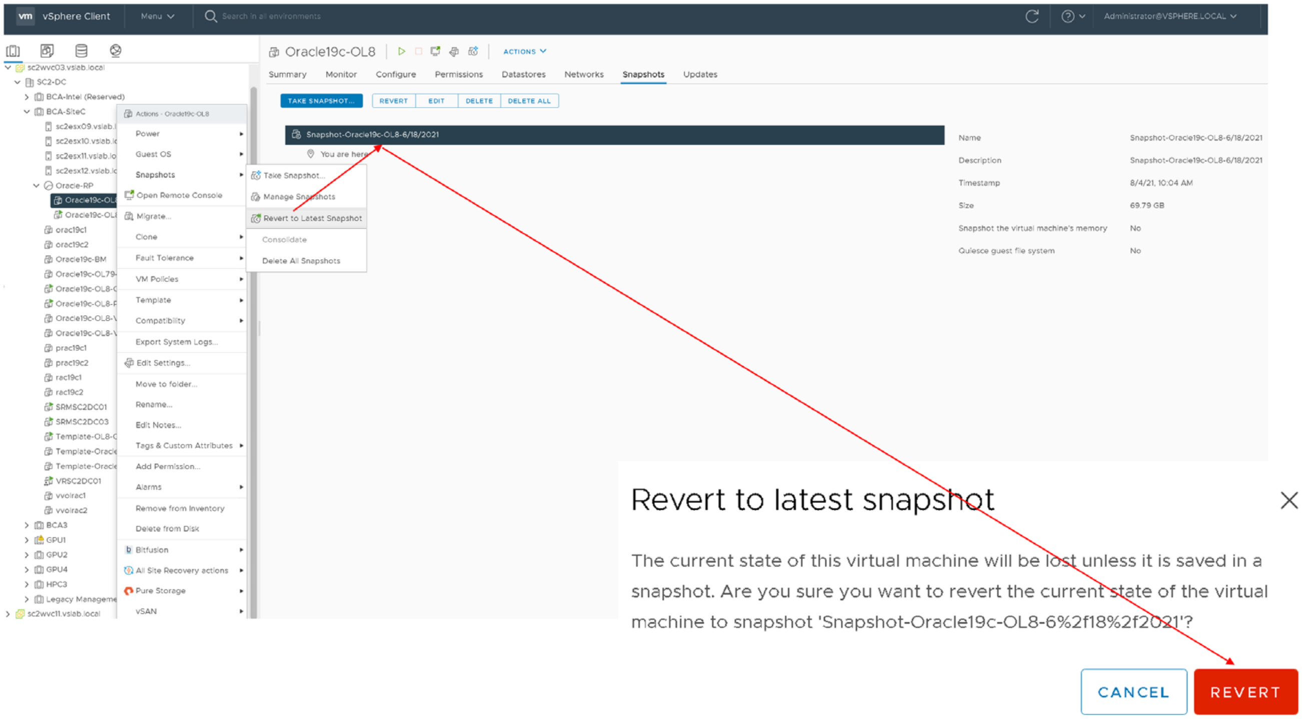
Name	Snapshot-Oracle19c-OL8-6/18/2021
Description	Snapshot-Oracle19c-OL8-6/18/2021
Timestamp	8/4/21, 10:04 AM
Size	69.79 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

FIGURE 154. VMware Snapshot Snapshot-Oracle19c-OL8-6/18/2021 of Oracle VM Oracle19c-OL8

The VM **Oracle19c-OL8** contains a point-in-time snapshot to which to revert in the event of an application issue.

To revert to the point-in-time state and data of a VM taken as part of the VM snapshot, follow the steps below.

It's recommended to shut down the database as you would normally in the VM and power off the VM.



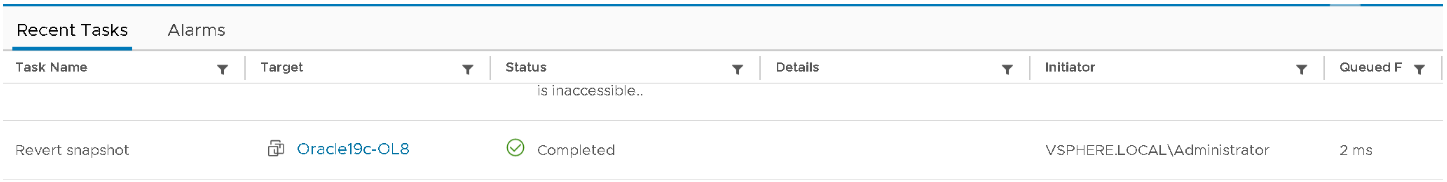
Name	Snapshot-Oracle19c-OL8-6/18/2021
Description	Snapshot-Oracle19c-OL8-6/18/2021
Timestamp	8/4/21, 10:04 AM
Size	69.79 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

Revert to latest snapshot

The current state of this virtual machine will be lost unless it is saved in a snapshot. Are you sure you want to revert the current state of the virtual machine to snapshot 'Snapshot-Oracle19c-OL8-6%2f18%2f2021'?

FIGURE 155. Steps to Revert to the VMware Snapshot Snapshot-Oracle19c-OL8-6/18/2021

The operation to revert to the snapshot is successful.

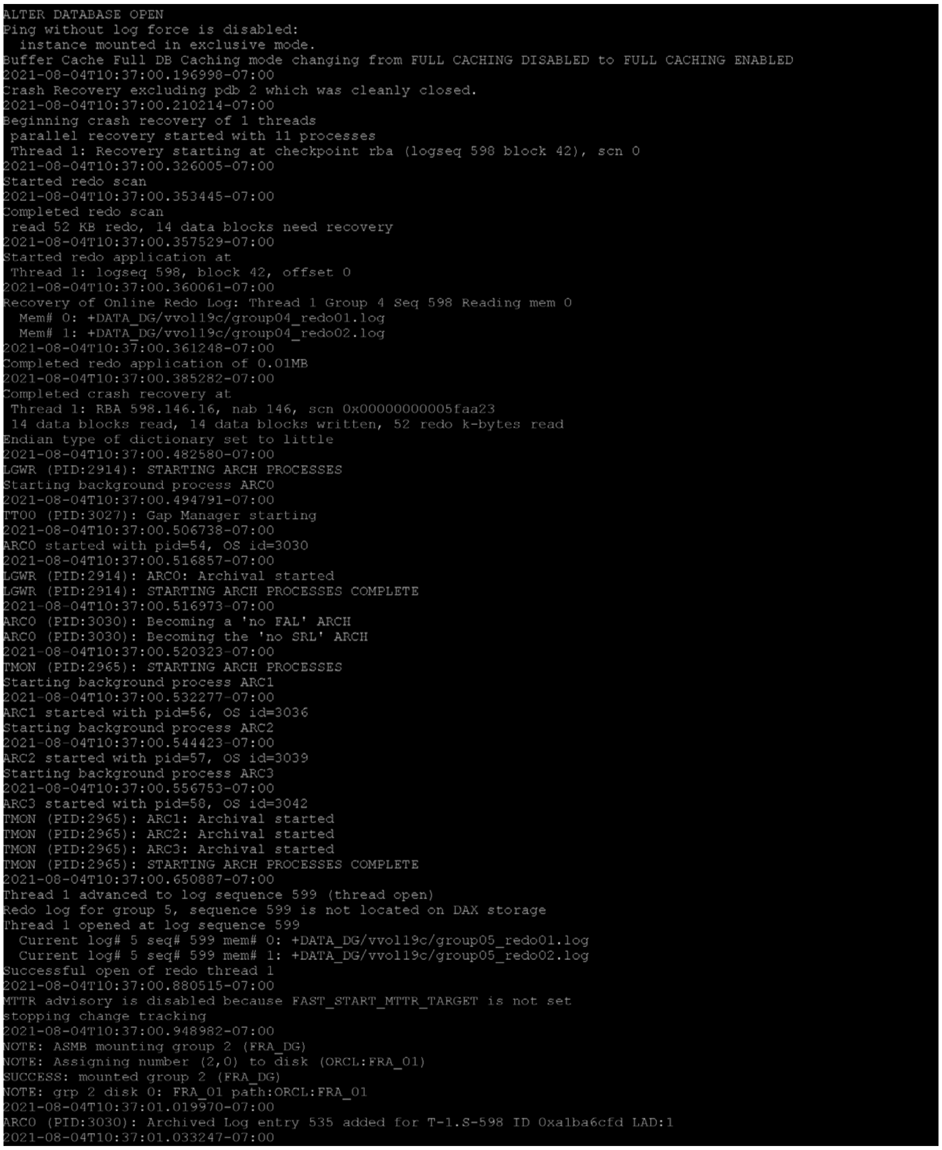


Recent Tasks | Alarms

Task Name	Target	Status	Details	Initiator	Queued F
		is inaccessible..			
Revert snapshot	Oracle19c-OL8	✓ Completed		VSPHERE.LOCAL\Administrator	2 ms

FIGURE 156. Revert Back to VMware Snapshot Successful

The Oracle VM **Oracle19c-OL8** is up with IP address 172.16.14.45 and the database **vvol19c** is up. The alert log for the database **vvol19c** shows no errors. Oracle crash recovery is performed when the database **vvol19c** starts up, which is normal and expected.



```
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
2021-08-04T10:37:00.196998-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-04T10:37:00.210214-07:00
Beginning crash recovery of 1 threads
 parallel recovery started with 11 processes
 Thread 1: Recovery starting at checkpoint rba (logseq 598 block 42), scn 0
2021-08-04T10:37:00.326005-07:00
Started redo scan
2021-08-04T10:37:00.353445-07:00
Completed redo scan
 read 52 KB redo, 14 data blocks need recovery
2021-08-04T10:37:00.357529-07:00
Started redo application at
 Thread 1: logseq 598, block 42, offset 0
2021-08-04T10:37:00.360061-07:00
Recovery of Online Redo Log: Thread 1 Group 4 Seq 598 Reading mem 0
  Mem# 0: +DATA_DG/vvol19c/group04_redo01.log
  Mem# 1: +DATA_DG/vvol19c/group04_redo02.log
2021-08-04T10:37:00.361248-07:00
Completed redo application of 0.01MB
2021-08-04T10:37:00.385282-07:00
Completed crash recovery at
 Thread 1: RBA 598.146.16, nab 146, scn 0x00000000005faa23
 14 data blocks read, 14 data blocks written, 52 redo k-bytes read
Endian type of dictionary set to little
2021-08-04T10:37:00.482580-07:00
LGWR (PID:2914): STARTING ARCH PROCESSES
Starting background process ARC0
2021-08-04T10:37:00.494791-07:00
TT00 (PID:3027): Gap Manager starting
2021-08-04T10:37:00.506738-07:00
ARC0 started with pid=54, OS id=3030
2021-08-04T10:37:00.516857-07:00
LGWR (PID:2914): ARC0: Archival started
LGWR (PID:2914): STARTING ARCH PROCESSES COMPLETE
2021-08-04T10:37:00.516973-07:00
ARC0 (PID:3030): Becoming a 'no FAL' ARCH
ARC0 (PID:3030): Becoming the 'no SRL' ARCH
2021-08-04T10:37:00.520323-07:00
TMON (PID:2965): STARTING ARCH PROCESSES
Starting background process ARC1
2021-08-04T10:37:00.532277-07:00
ARC1 started with pid=56, OS id=3036
Starting background process ARC2
2021-08-04T10:37:00.544423-07:00
ARC2 started with pid=57, OS id=3039
Starting background process ARC3
2021-08-04T10:37:00.556753-07:00
ARC3 started with pid=58, OS id=3042
TMON (PID:2965): ARC1: Archival started
TMON (PID:2965): ARC2: Archival started
TMON (PID:2965): ARC3: Archival started
TMON (PID:2965): STARTING ARCH PROCESSES COMPLETE
2021-08-04T10:37:00.650887-07:00
Thread 1 advanced to log sequence 599 (thread open)
Redo log for group 5, sequence 599 is not located on DAX storage
Thread 1 opened at log sequence 599
  Current log# 5 seq# 599 mem# 0: +DATA_DG/vvol19c/group05_redo01.log
  Current log# 5 seq# 599 mem# 1: +DATA_DG/vvol19c/group05_redo02.log
Successful open of redo thread 1
2021-08-04T10:37:00.880515-07:00
MTTR advisory is disabled because FAST_START_MTTR_TARGET is not set
stopping change tracking
2021-08-04T10:37:00.948982-07:00
NOTE: ASMB mounting group 2 (FRA_DG)
NOTE: Assigning number (2,0) to disk (ORCL:FRA_01)
SUCCESS: mounted group 2 (FRA_DG)
NOTE: grp 2 disk 0: FRA_01 path:ORCL:FRA_01
2021-08-04T10:37:01.019970-07:00
ARC0 (PID:3030): Archived Log entry 535 added for T-1.S-598 ID 0xa1ba6cfd LAD:1
2021-08-04T10:37:01.033247-07:00
```

FIGURE 157. Oracle VM Oracle19c-OL8 Alert Log details

Alternatively, the VM snapshot can also be taken using the VMware PowerCLI command.

> ***New-Snapshot -VM Oracle19c-OL8 -Name 'Snapshot-Oracle19c-OL8-6/188/2021' -Memory $false -description Oracle19c-OL8_Snap***

VMware Snapshot with Database BEGIN/END Backup Mode with Custom Quiescing Scripts

The steps below illustrate the use of VMware Snapshot of an Oracle single-instance database, by placing the database in a backup mode using **BEGIN/END Backup** commands and reverting back to the snapshot.

Putting the database in backup mode can be done either manually or automatically:

- Manual
  - Use Oracle native tools (e.g., sqlplus to place the database in a **BEGIN backup** mode).
  - Use web client or VMware PowerCLI to take a VM-level snapshot.
  - Use Oracle native tools (e.g., sqlplus to take the database out of the **BEGIN backup** mode).
- Automatic
  - Use custom quiescing scripts to run pre-freeze and post-thaw commands. VMware tools must be installed and running in the guest operating system for this feature to work correctly.

Prerequisites for custom quiescing scripts:

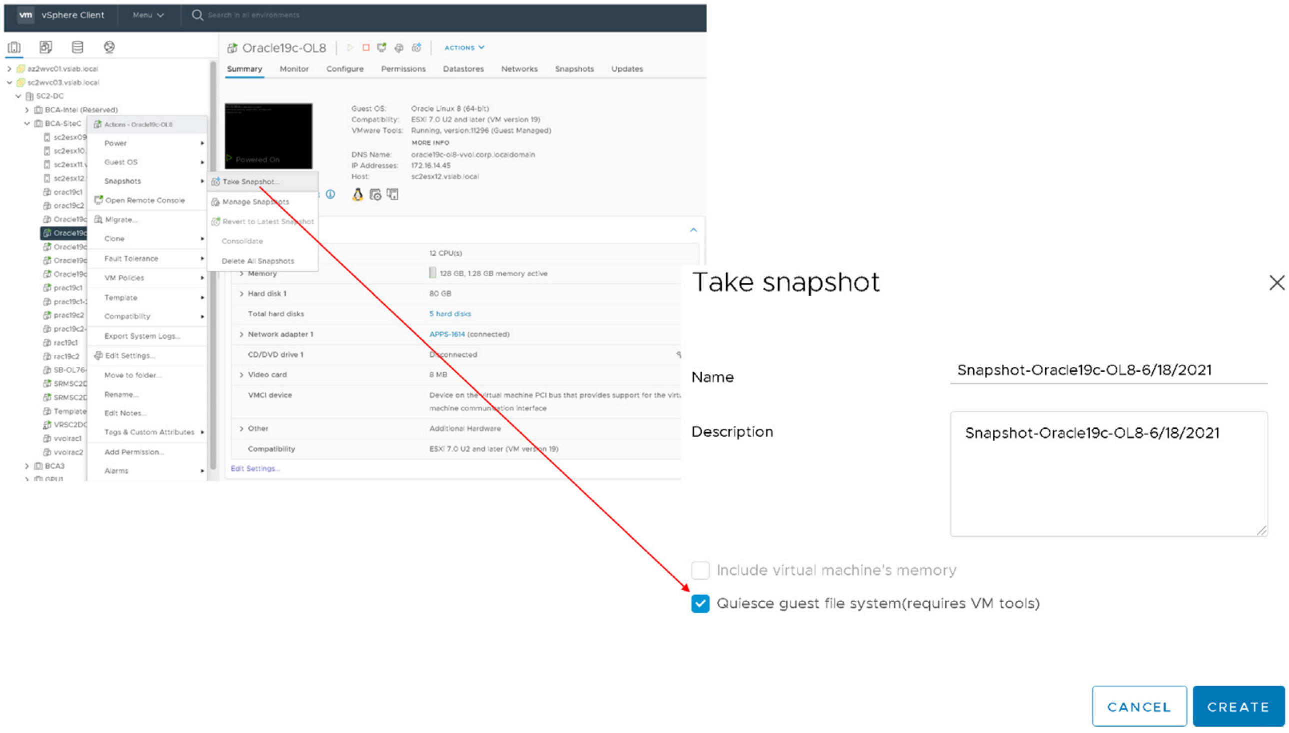
- The scripts have to be created in the /etc/vmware-tools/backupScripts.d directory on Linux VMs.
- The directory may contain one or multiple scripts that will be executed in sequence. The file names of the scripts affect the execution order (e.g., 10-application.sh, then 20-database.sh).
- Each script must be able to handle freeze, freezeFail and thaw arguments passed by the VMware tools during the different phases.
- Ensure that the scripts have correct execute permissions.

An example of a custom quiescing is shown below:

- The main script that invokes the freeze and thaw routines is created in the /etc/vmware-tools/backupScripts.d directory and has correct write permissions for the root user.
- The individual pre-freeze-script and post-thaw-script shell scripts are created under the Oracle user home directory and have correct write permissions.

Example scripts have been provided in the appendix of this document.

The steps below illustrate the use of VMware Snapshot of an Oracle single-instance database, by placing the database in a backup mode using **BEGIN/END Backup** commands and reverting to the snapshot, using Linux custom quiescing scripts.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol.corp.localdomain
IP Addresses: 172.16.14.45
Host: sc2esx12.vslab.local

12 CPU(s)
Memory: 128 GB, 1.28 GB memory active
Hard disk 1: 80 GB
Total hard disks: 5 hard disks
Network adapter 1: APPS-1614 (connected)
CD/DVD drive 1: Disconnected
Video card: 8 MB
VMCI device: Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other: Additional Hardware
Compatibility: ESXi 7.0 U2 and later (VM version 19)

Take snapshot

Name: Snapshot-Oracle19c-OL8-6/18/2021

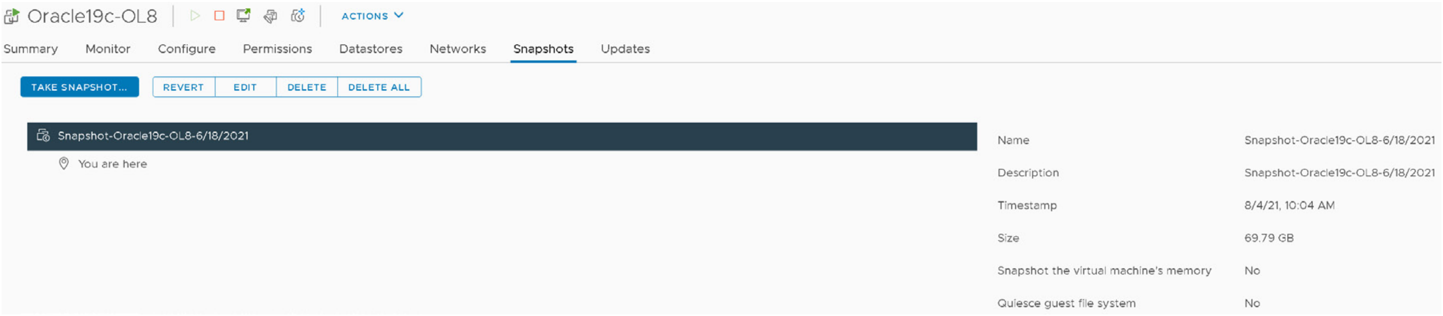
Description: Snapshot-Oracle19c-OL8-6/18/2021

☐ Include virtual machine's memory

☑ Quiesce guest file system(requires VM tools)

FIGURE 158. Steps to take VMware Snapshot of Oracle VM Oracle19c-OL8 with Quiescing

VMware snapshot **Snapshot-Oracle19c-OL8-6/18/2021** of Oracle VM **Oracle19c-OL8** with quiescing is taken successfully.

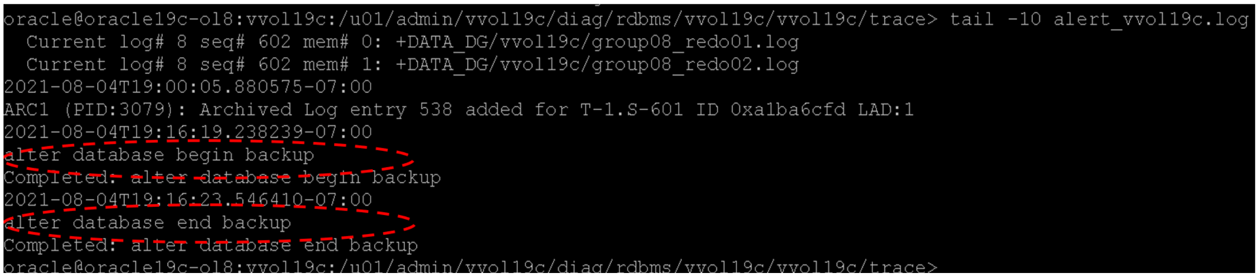


Name	Snapshot-Oracle19c-OL8-6/18/2021
Description	Snapshot-Oracle19c-OL8-6/18/2021
Timestamp	8/4/21, 10:04 AM
Size	69.79 GB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

FIGURE 159. VMware Snapshot Snapshot-Oracle19c-OL8-6/18/2021 of Oracle VM Oracle19c-OL8

The backup steps include:

- The database is placed in a **BEGIN backup** mode as part of the invocation of pre-freeze-script.
- VMware snapshot **Snapshot-Oracle19c-OL8-6/18/2021** of Oracle VM **Oracle19c-OL8** is taken successfully.
- The database is taken out of the **BEGIN backup** mode (END mode) as part of the invocation of post-thaw-script.



```
oracle@oracle19c-ol8:vvol19c:/u01/admin/vvol19c/diag/rdbms/vvol19c/vvol19c/trace> tail -10 alert_vvol19c.log
  Current log# 8 seq# 602 mem# 0: +DATA_DG/vvol19c/group08_redo01.log
  Current log# 8 seq# 602 mem# 1: +DATA_DG/vvol19c/group08_redo02.log
2021-08-04T19:00:05.880575-07:00
ARC1 (PID:3079): Archived Log entry 538 added for T-1.S-601 ID 0xa1ba6cfd LAD:1
2021-08-04T19:16:19.238239-07:00
alter database begin backup
Completed: alter database begin backup
2021-08-04T19:16:23.546410-07:00
alter database end backup
Completed: alter database end backup
oracle@oracle19c-ol8:vvol19c:/u01/admin/vvol19c/diag/rdbms/vvol19c/vvol19c/trace>
```

FIGURE 160. ALERT LOG OF DATABASE SHOWING BEGIN/END BACKUP MODES

VMware Snapshot with Cold Database Backup

The steps to take a VMware-level snapshot of an Oracle single-instance database cold by shutting down the database and then reverting back to the snapshot if needed are the same as those required for the two cases above except, in this case, the database is shutdown cold.

VMware Clone

A VMware clone of the Oracle VM can also be accomplished in one of two ways:

- Using PowerCLI command or web client to take a point-in-time VMware snapshot and cloning a VM from this snapshot using VMware PowerCLI.
  - The VMware snapshot can either use database crash-consistent method or database hot backup or database cold backup.
  - An example PowerCLI script using *vSphere API* that contains Clone_VM task and includes the ability to specify a snapshot to clone from using the **VirtualMachinecloneSpec** can be found in the *Oracle Database 12c on VMware vSAN—Day 2 Operations and Management guide*.
- Clone directly using the web client from an existing Oracle VM
  - Clone either using database crash-consistent or database hot backup or database cold backup before performing the cloning operation.
  - Using the web client to perform the VM cloning operation implicitly takes a temporary snapshot and deletes the snapshot after the cloning operation is completed.

Once the VM clone is created, the database can then be backed up to media for offshore storage and can be restored from, if needed.

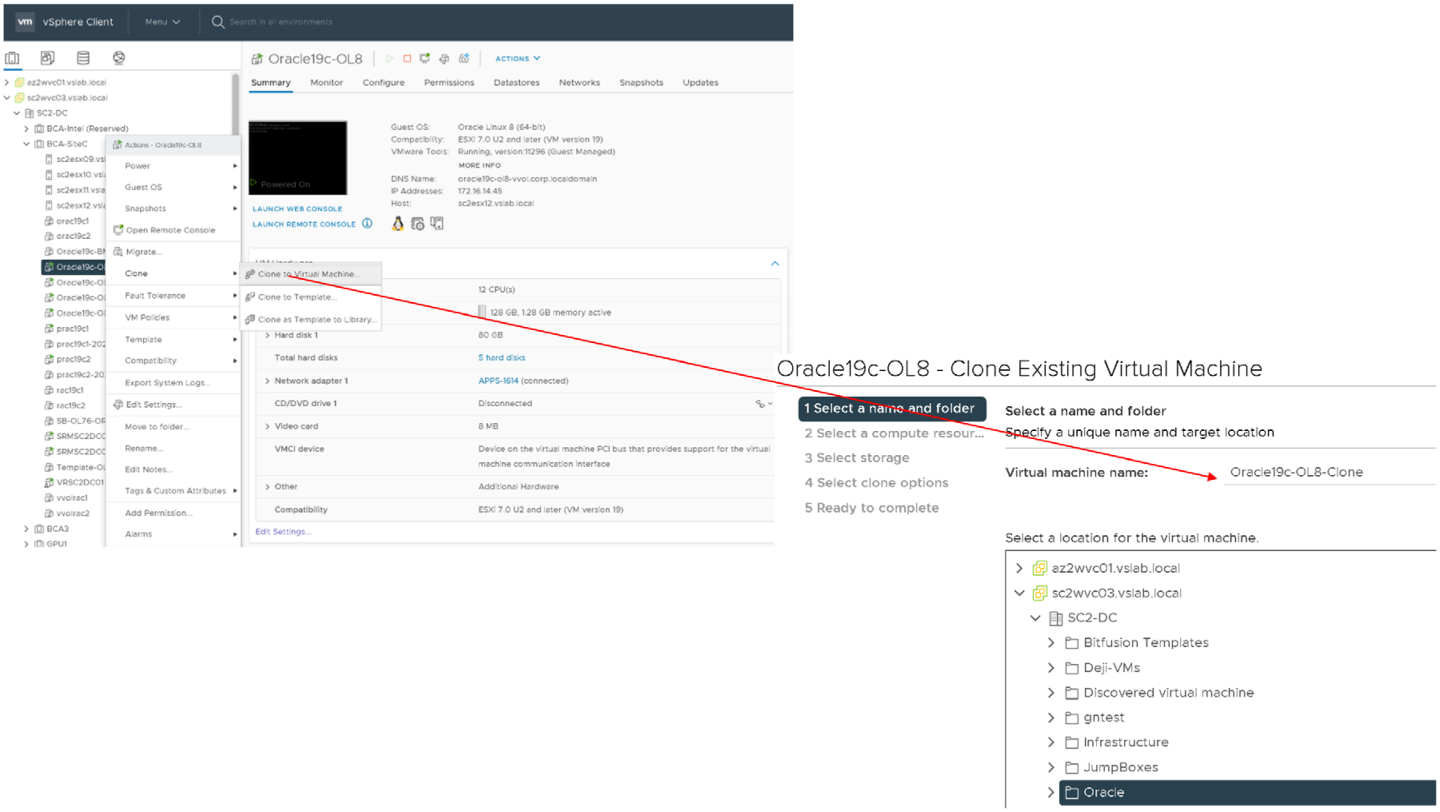
VMware **vmkfstools** command can also be used to clone VMDKs using either the snapshot of the Oracle VM or without the snapshot. The steps to clone Oracle VM VMDKs from a VM-level snapshot using VMware **vmkfstools** command can be found in the *Oracle Database 12c on VMware vSAN—Day 2 Operations and Management guide*.

Using VMware Snapshot, vSphere Virtual Volumes and Pure Storage Plugin, a VM-level or a VMDK-level snapshot can also be taken of the Oracle single-instance VM. The steps to achieve this can be found in the *Virtualizing Oracle Workloads with VMware vSphere Virtual Volumes on VMware Hybrid Cloud guide*.

The steps for taking a VMware snapshot and clone are the same as those employed for any underlying VMware storage.

In case of snapshot and clone of an Oracle VM using crash-consistent database snapshot, Oracle crash recovery is performed when the database starts up, which is normal and expected. If and when placing the database in backup mode, database recovery would need to be performed using archivelog, which is normal and expected.

The steps below illustrate the use of VMware Clone to clone a new Oracle VM directly from an existing Oracle VM, using database crash-consistent method from the web client.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol.corp.localdomain
IP Addresses: 172.16.14.45
Host: sc2esx12.vslab.local

12 CPU(s)
128 GB, 1.28 GB memory active
Hard disk 1: 80 GB
Total hard disks: 5 hard disks
Network adapter 1: APPS-1614 (connected)
CD/DVD drive 1: Disconnected
Video card: 8 MB
VMCI device: Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other: Additional Hardware
Compatibility: ESXi 7.0 U2 and later (VM version 19)

Oracle19c-OL8 - Clone Existing Virtual Machine

1 Select a name and folder
2 Select a compute resour...
3 Select storage
4 Select clone options
5 Ready to complete

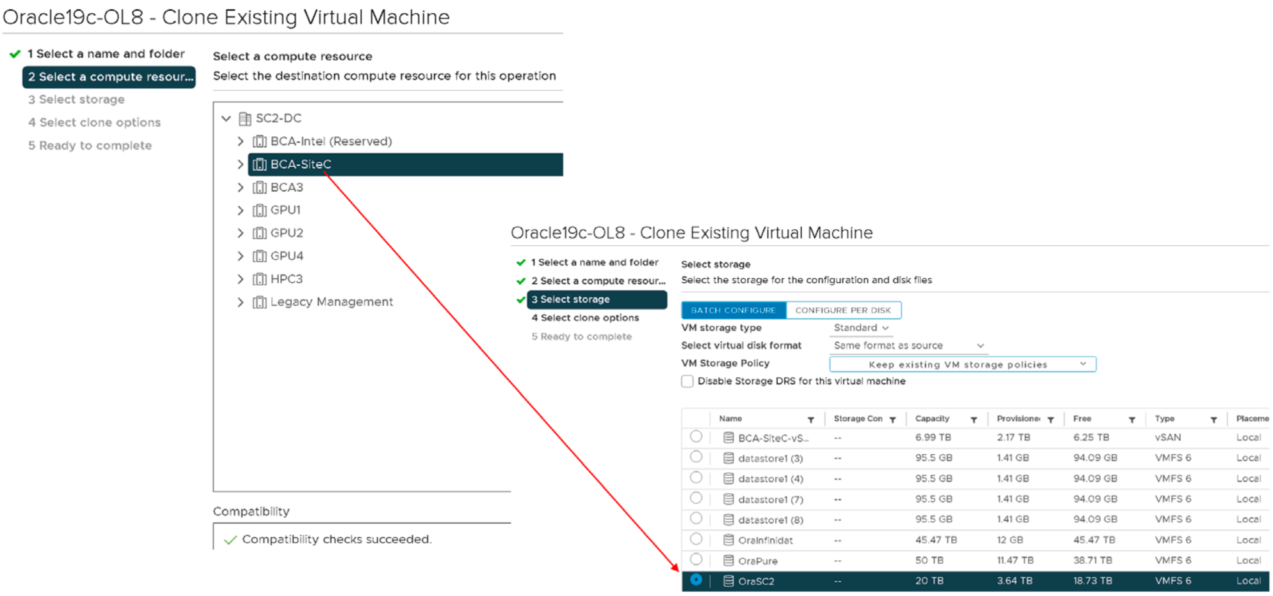
Select a name and folder
Specify a unique name and target location

Virtual machine name: Oracle19c-OL8-Clone

Select a location for the virtual machine.

FIGURE 161. VMware Clone of Oracle VM Oracle19c-OL8

Select the target compute cluster and datastore for Oracle VM **Oracle19c-OL8-clone**.



Oracle19c-OL8 - Clone Existing Virtual Machine

- ✓ 1 Select a name and folder
- 2 Select a compute resour...
- 3 Select storage
- 4 Select clone options
- 5 Ready to complete

Select a compute resource

Select the destination compute resource for this operation

- SC2-DC
  - BCA-Intel (Reserved)
  - BCA-SiteC
  - BCA3
  - GPU1
  - GPU2
  - GPU4
  - HPC3
  - Legacy Management

Compatibility

✓ Compatibility checks succeeded.

Oracle19c-OL8 - Clone Existing Virtual Machine

- ✓ 1 Select a name and folder
- ✓ 2 Select a compute resour...
- ✓ 3 Select storage
- 4 Select clone options
- 5 Ready to complete

Select storage

Select the storage for the configuration and disk files

BATCH CONFIGURE | CONFIGURE PER DISK

VM storage type: Standard

Select virtual disk format: Same format as source

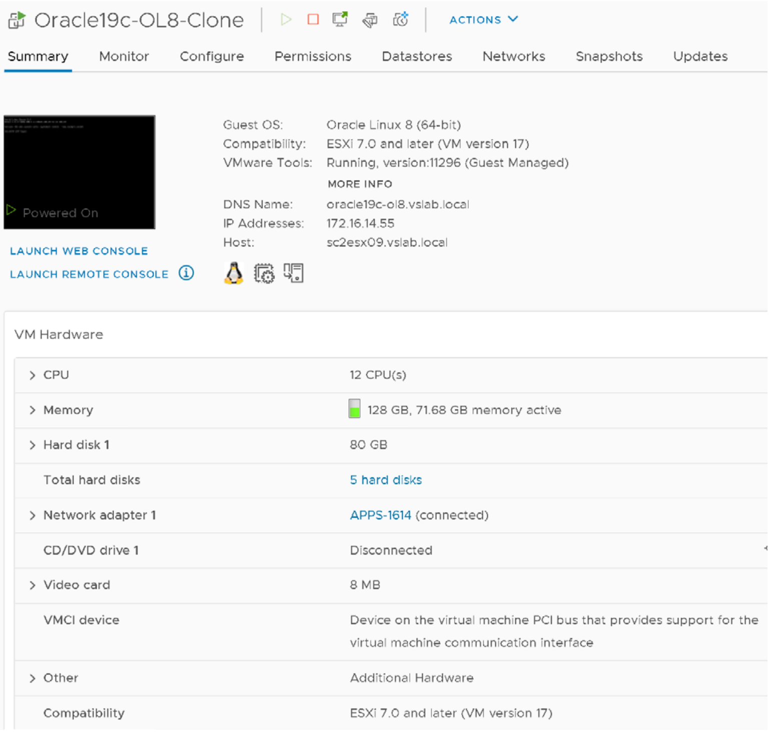
VM Storage Policy: Keep existing VM storage policies

☐ Disable Storage DRS for this virtual machine

	Name	Storage Con	Capacity	Provisione	Free	Type	Placeme
○	BCA-SiteC-vS...	--	6.99 TB	2.17 TB	6.25 TB	vSAN	Local
○	datastore1 (3)	--	95.5 GB	1.41 GB	94.09 GB	VMFS 6	Local
○	datastore1 (4)	--	95.5 GB	1.41 GB	94.09 GB	VMFS 6	Local
○	datastore1 (7)	--	95.5 GB	1.41 GB	94.09 GB	VMFS 6	Local
○	datastore1 (8)	--	95.5 GB	1.41 GB	94.09 GB	VMFS 6	Local
○	OraInfinidat	--	45.47 TB	12 GB	45.47 TB	VMFS 6	Local
○	OraPure	--	50 TB	11.47 TB	38.71 TB	VMFS 6	Local
●	OraSC2	--	20 TB	3.64 TB	18.73 TB	VMFS 6	Local

FIGURE 162. VMware Clone of Oracle VM Oracle19c-OL8 Pick Compute and Datastore

The Oracle VM **Oracle19c-OL8-clone** is up with IP address 172.16.14.55 and the copy of the database **vvol19c** is up.



Oracle19c-OL8-Clone

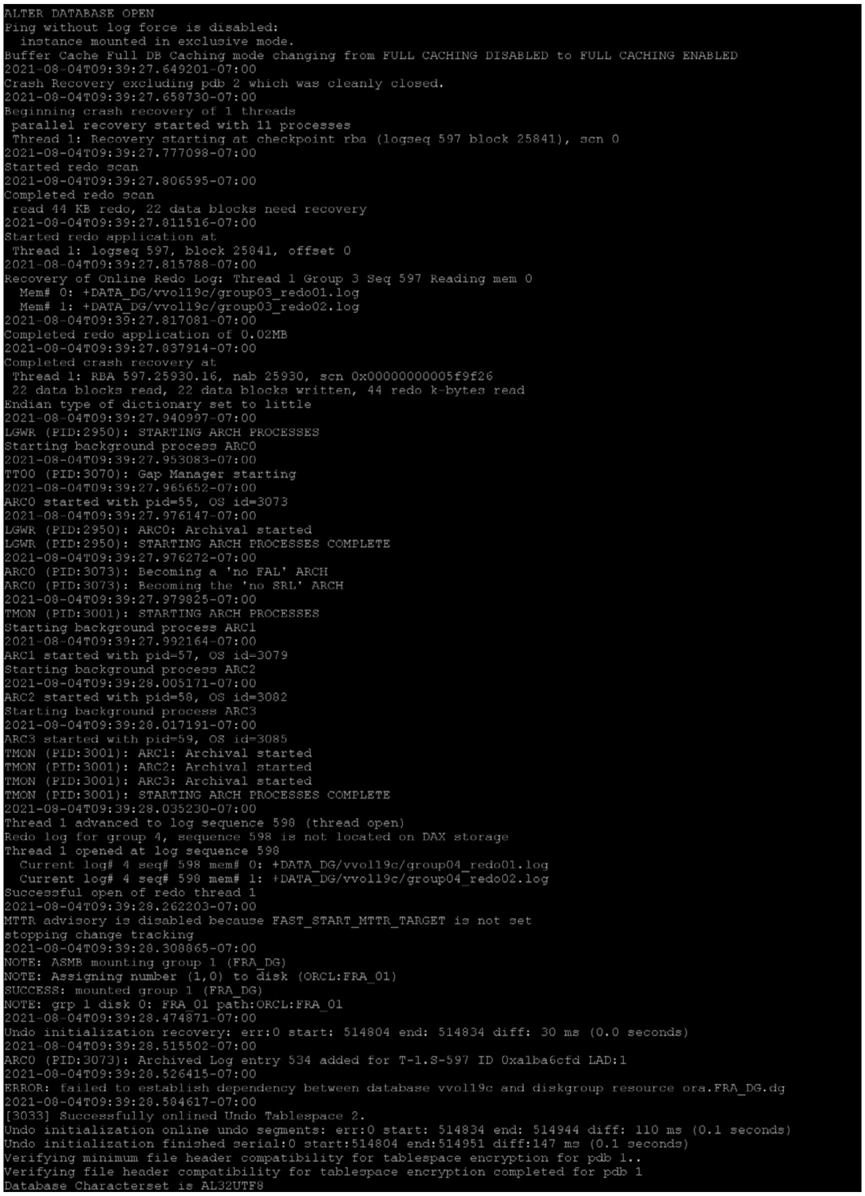
Guest OS:	Oracle Linux 8 (64-bit)
Compatibility:	ESXi 7.0 and later (VM version 17)
VMware Tools:	Running, version:11296 (Guest Managed)
DNS Name:	oracle19c-ol8.vslab.local
IP Addresses:	172.16.14.55
Host:	sc2esx09.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 71.68 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 163. Oracle VM Oracle19c-OL8-Clone Details

The alert log for the database copy **vvol19c** shows no errors. Oracle crash recovery is performed when the database copy **vvol19c** starts up, which is normal and expected.



```
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
2021-08-04T09:39:27.649201-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-08-04T09:39:27.658730-07:00
Beginning crash recovery of 1 threads
 parallel recovery started with 11 processes
 Thread 1: Recovery starting at checkpoint rba (logseq 597 block 25841), scn 0
2021-08-04T09:39:27.777098-07:00
Started redo scan
2021-08-04T09:39:27.806595-07:00
Completed redo scan
 read 44 KB redo, 22 data blocks need recovery
2021-08-04T09:39:27.811516-07:00
Started redo application at
 Thread 1: logseq 597, block 25841, offset 0
2021-08-04T09:39:27.815788-07:00
Recovery of Online Redo Log: Thread 1 Group 3 Seq 597 Reading mem 0
  Mem# 0: +DATA_DG/vvol19c/group03_redo01.log
  Mem# 1: +DATA_DG/vvol19c/group03_redo02.log
2021-08-04T09:39:27.817081-07:00
Completed redo application of 0.02MB
2021-08-04T09:39:27.837914-07:00
Completed crash recovery at
 Thread 1: RBA 597.25930.16, nab 25930, scn 0x00000000005f9f26
 22 data blocks read, 22 data blocks written, 44 redo k-bytes read
Endian type of dictionary set to little
2021-08-04T09:39:27.940997-07:00
LGWR (PID:2950): STARTING ARCH PROCESSES
Starting background process ARC0
2021-08-04T09:39:27.953083-07:00
TT00 (PID:3070): Gap Manager starting
2021-08-04T09:39:27.965652-07:00
ARC0 started with pid=55, OS id=3073
2021-08-04T09:39:27.976147-07:00
LGWR (PID:2950): ARC0: Archival started
LGWR (PID:2950): STARTING ARCH PROCESSES COMPLETE
2021-08-04T09:39:27.976272-07:00
ARC0 (PID:3073): Becoming a 'no FAL' ARCH
ARC0 (PID:3073): Becoming the 'no SRL' ARCH
2021-08-04T09:39:27.979825-07:00
TMON (PID:3001): STARTING ARCH PROCESSES
Starting background process ARC1
2021-08-04T09:39:27.992164-07:00
ARC1 started with pid=57, OS id=3079
Starting background process ARC2
2021-08-04T09:39:28.005171-07:00
ARC2 started with pid=58, OS id=3082
Starting background process ARC3
2021-08-04T09:39:28.017191-07:00
ARC3 started with pid=59, OS id=3085
TMON (PID:3001): ARC1: Archival started
TMON (PID:3001): ARC2: Archival started
TMON (PID:3001): ARC3: Archival started
TMON (PID:3001): STARTING ARCH PROCESSES COMPLETE
2021-08-04T09:39:28.035230-07:00
Thread 1 advanced to log sequence 598 (thread open)
Redo log for group 4, sequence 598 is not located on DAX storage
Thread 1 opened at log sequence 598
  Current log# 4 seq# 598 mem# 0: +DATA_DG/vvol19c/group04_redo01.log
  Current log# 4 seq# 598 mem# 1: +DATA_DG/vvol19c/group04_redo02.log
Successful open of redo thread 1
2021-08-04T09:39:28.262203-07:00
MTTR advisory is disabled because FAST_START_MTTR_TARGET is not set
stopping change tracking
2021-08-04T09:39:28.308865-07:00
NOTE: ASMB mounting group 1 (FRA_DG)
NOTE: Assigning number (1,0) to disk (ORCL:FRA_01)
SUCCESS: mounted group 1 (FRA_DG)
NOTE: grp 1 disk 0: FRA_01 path:ORCL:FRA_01
2021-08-04T09:39:28.474871-07:00
Undo initialization recovery: err:0 start: 514804 end: 514834 diff: 30 ms (0.0 seconds)
2021-08-04T09:39:28.515502-07:00
ARC0 (PID:3073): Archived Log entry 534 added for T-1.S-597 ID 0xa1ba6cfd LAD:1
2021-08-04T09:39:28.526415-07:00
ERROR: failed to establish dependency between database vvol19c and diskgroup resource ora.FRA_DG.dg
2021-08-04T09:39:28.584617-07:00
[3033] Successfully onlined Undo Tablespace 2.
Undo initialization online undo segments: err:0 start: 514834 end: 514944 diff: 110 ms (0.1 seconds)
Undo initialization finished serial:0 start:514804 end:514951 diff:147 ms (0.1 seconds)
Verifying minimum file header compatibility for tablespace encryption for pdb 1..
Verifying file header compatibility for tablespace encryption completed for pdb 1
Database Characterset is AL32UTF8
```

FIGURE 164. Oracle VM Oracle19c-OL8-Clone Alert Log Details

In case of Oracle RAC, a current restriction of the multi-writer attribute as documented in *KB 1034165* is VMware snapshots and cloning of multi-writer VMDKs are not supported. Currently, the VMware snapshot and cloning utility cannot be used with Oracle RAC to snapshot or clone RAC VMs with multi-writer VMDKs.

For an Oracle RAC cluster, independent-persistent disk mode is not required to enable multi-writer for shared VMDKs. However, default-dependent disk mode causes a *cannot snapshot shared disk* error when a VM-level snapshot is taken of an Oracle RAC VM. Use of independent-persistent disk mode allows taking a snapshot of the non-shared disk or disks (e.g., OS, Oracle binaries, standalone file system), while the shared disk(s) are backed up separately via a storage-level snapshot mechanism (e.g., vVOL-level backup of the shared VMDKs or LUN-level backup of shared VMDKs).

In the case of an Oracle RAC cluster, the snapshot process occurs in two steps:

- VM-level snapshot for non-shared VMDKs with disk mode set to **Dependent** for all RAC VMs
- Application-level (e.g., Oracle RMAN) for the RAC database OR storage-based snapshot for shared RAC VMDKs with disk mode set to **Independent-Persistent** from any RAC VM

More information on backing up Oracle RAC using VMware vVols Storage level can be found in the *Virtualizing Oracle Workloads with VMware vSphere Virtual Volumes on VMware Hybrid Cloud guide*.

VMware Clouds

The above use case of employs VMware Snapshot and Clone utilities to snapshot or clone the single-instance VM **Oracle19c-OL8** using the web client or VMware PowerCLI command, following the same steps for all VMware Cloud-supported storage as well as on-premises storage.

VMware **vmkfstools** command capability is not available on VMware clouds, as this command requires access to the ESXi hosts. VMware Cloud is a managed service and does not provide direct access to the ESXi hosts.

Native storage-based snapshot and cloning capability is not available on most VMware clouds as most VMware clouds are managed services and do not provide direct access to the storage layer.

Current restrictions of the multi-writer attribute, disallowing VMware snapshots or cloning as documented in *KB 1034165*, applies to VMware Cloud as well.

Storage Level Business Continuity

Storage-based snapshots can be used to take a storage LUN-level point-in-time snapshot. A storage clone can then be provisioned from the LUN-level snapshot.

Storage-based snapshots and clones of a VMware datastore are at a storage LUN level, so the granularity of operation is at the storage LUN level and will not provide VM-level granularity.

A storage-based snapshot can be taken before any database operation and if the state of the database has to be reverted back to the snapshot, the state of the storage LUN will be reverted back to the snapshot time. This affects the state of all the VMs on that storage LUN.

Storage-based cloning can also be done by cloning a storage LUN from the storage-based snapshot. The steps to mount a clone of a VMFS datastore with resignaturing can be found in *Mount a VMFS Datastore Copy guide*.

On the other hand, storage-based snapshots and clones of a VM on vSphere Virtual Volumes is at a vVOL level, so the granularity of operation is likewise at the vVOL level.

As noted in *Supported Backup, Restore and Recovery Operations using Third Party Snapshot Technologies* (Oracle Doc ID 604683.1), third-party storage vendor snapshots must conform to the following requirements:

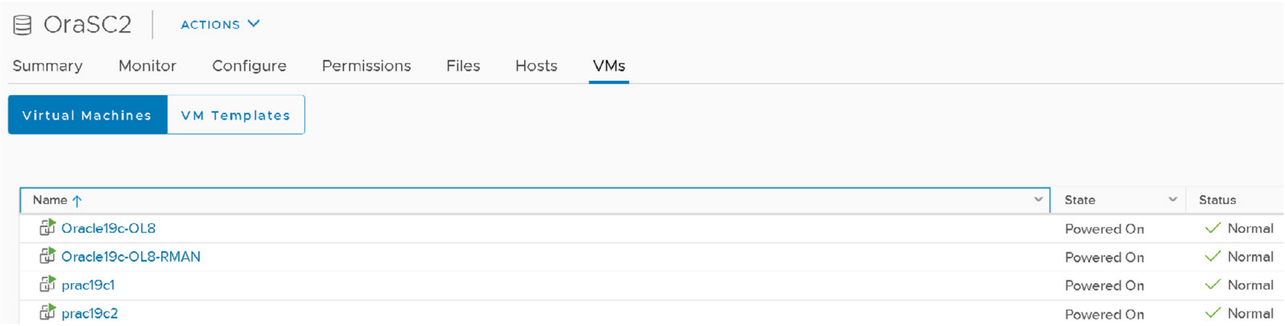
- Integrated with Oracle's recommended restore and recovery operations above
- Database crash-consistent at the point of the snapshot
- Write-ordering is preserved for each file within a snapshot

On-premises Using vSphere VMFS Storage

This use case focusses on employing storage-based snapshot and cloning to take a storage LUN-level point-in-time snapshot and clone a new storage LUN from the LUN-level snapshot. The storage LUN would then be resignatured before using that as a copy of the original ESXI datastore.

A copy of the original VM **Oracle19c-OL8** would be brought up as VM **Oracle19c-OL8-Copy** and database contents can be copied from VM **Oracle19c-OL8-Copy** to original VM **Oracle19c-OL8** in the event any database level restores are needed.

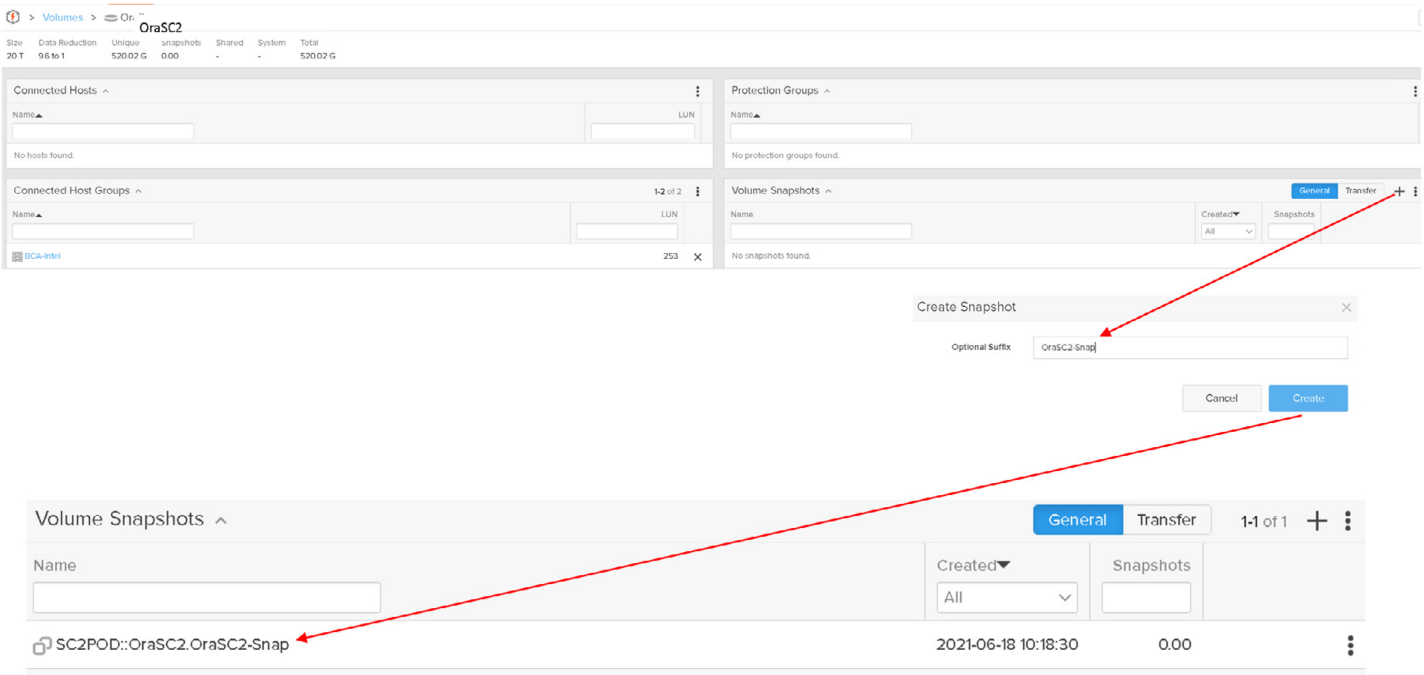
The VMFS datastore **OraSC2** houses two single-instance VMs and one Oracle RAC as shown below:



Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

FIGURE 165. VMware VMFS Datastore with Single-Instance and Oracle RAC VMs

Use the Pure Storage GUI to take a storage-based snapshot of the LUN **OraSC2** called **OraSC2-Snap**. A storage-based clone **ORASC2-Copy** is taken from the storage snapshot **OraSC2-Snap**. Delete the storage snapshot after the clone **ORASC2-Copy** is created.



Size	Data Reduction	Unique	Snapshots	Shared	System	Total
20 T	9.6 to 1	520.02 G	0.00	-	-	520.02 G

No hosts found.

No protection groups found.

Name	LUN
BCA-Intel	253

No snapshots found.

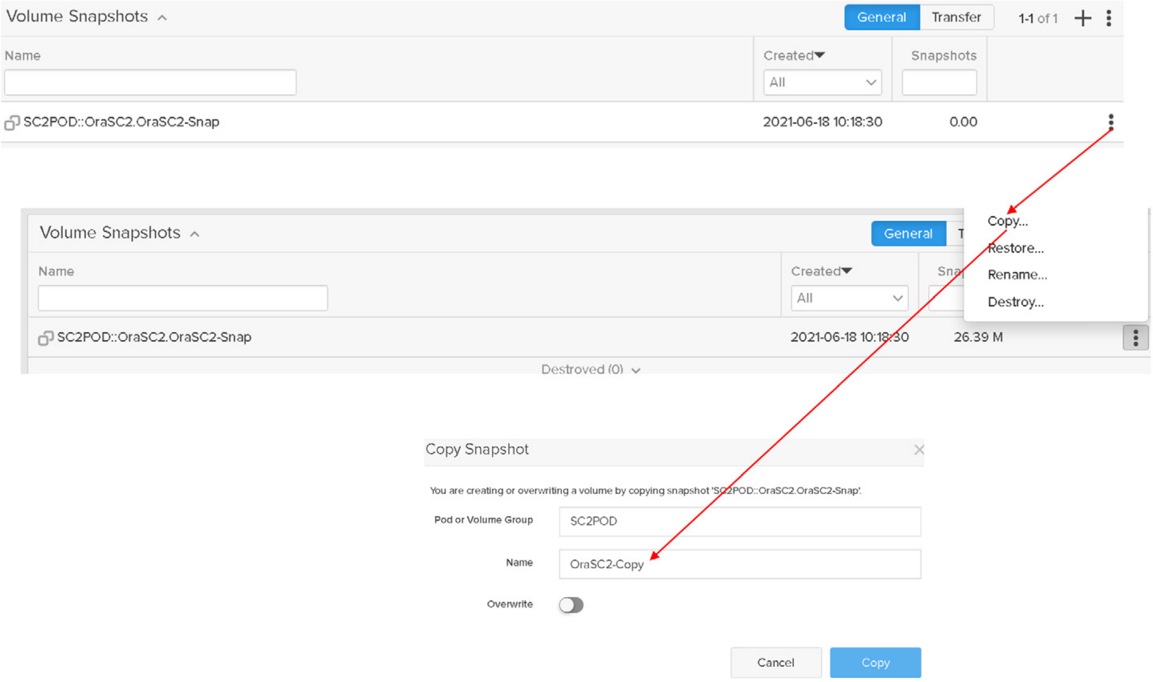
Optional Suffix: OraSC2-Snap

Volume Snapshots — 1-1 of 1

Name	Created	Snapshots
SC2POD::OraSC2.OraSC2-Snap	2021-06-18 10:18:30	0.00

FIGURE 166. Create Storage Level Snapshot

From the storage-based snapshot **OraSC2-Snap**, create storage clone **ORASC2-Copy**.



Name	Created	Snapshots
SC2POD::OraSC2.OraSC2-Snap	2021-06-18 10:18:30	0.00
SC2POD::OraSC2.OraSC2-Snap	2021-06-18 10:18:30	26.39 M

Copy Snapshot

You are creating or overwriting a volume by copying snapshot 'SC2POD::OraSC2.OraSC2-Snap'.

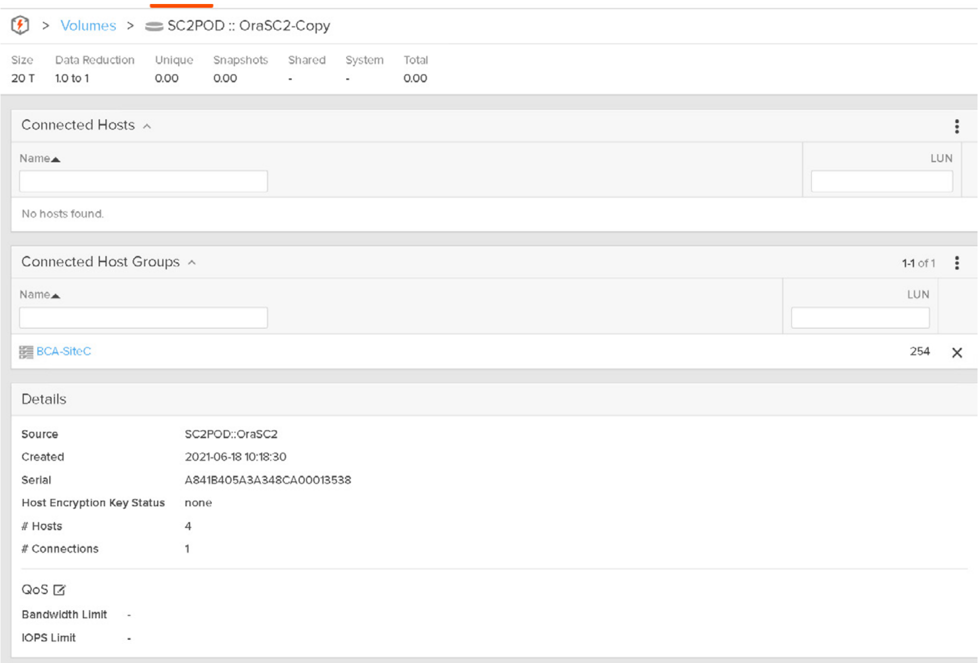
Pod or Volume Group: SC2POD

Name: OraSC2-Copy

Overwrite: ○

FIGURE 167. Create Storage-Based Clone from Storage-Level Snapshot

The clone **ORASC2-Copy** is attached to the ESXi host which is currently hosting the Oracle VM **Oracle19c-OL8**.



> Volumes > SC2POD :: OraSC2-Copy

Size	Data Reduction	Unique	Snapshots	Shared	System	Total
20 T	1.0 to 1	0.00	0.00	-	-	0.00

Connected Hosts

Name	LUN
No hosts found.	

Connected Host Groups

Name	LUN
BCA-SiteC	254

Details

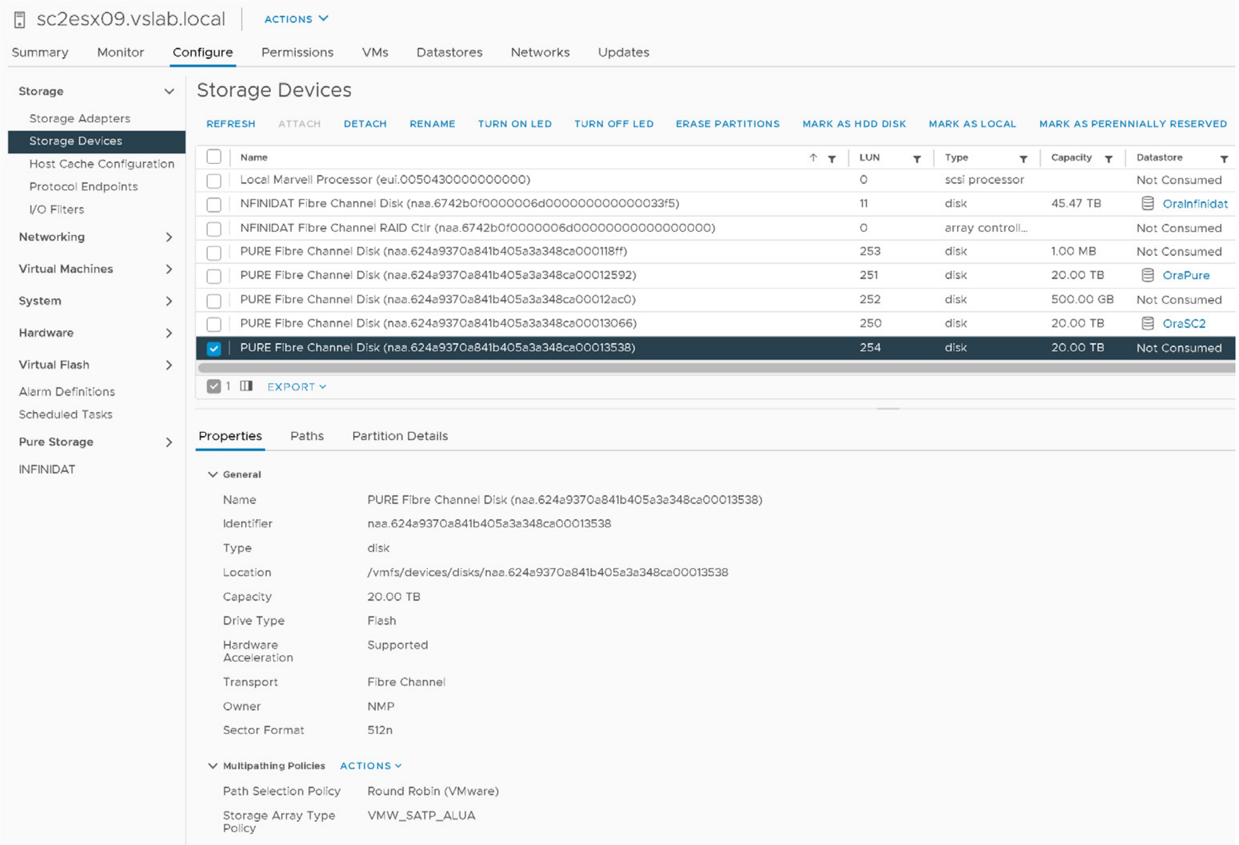
Source	SC2POD::OraSC2
Created	2021-06-18 10:18:30
Serial	A841B405A3A348CA00013538
Host Encryption Key Status	none
# Hosts	4
# Connections	1

QoS

Bandwidth Limit	-
IOPS Limit	-

FIGURE 168. Attach Storage-Based Clone to ESXi Host Group

Rescan the ESXi host's storage via the web client to see the new LUN.



Storage Devices

	Name	LUN	Type	Capacity	Datastore
□	Local Marvell Processor (eui.0050430000000000)	0	scsi processor		Not Consumed
□	NFINIDAT Fibre Channel Disk (naa.6742b0f0000006d000000000000033f5)	11	disk	45.47 TB	OraInfinidat
□	NFINIDAT Fibre Channel RAID Ctlr (naa.6742b0f0000006d0000000000000000)	0	array controll...		Not Consumed
□	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca000118ff)	253	disk	1.00 MB	Not Consumed
□	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00012592)	251	disk	20.00 TB	OraPure
□	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00012ac0)	252	disk	500.00 GB	Not Consumed
□	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00013066)	250	disk	20.00 TB	OraSC2
☑	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00013538)	254	disk	20.00 TB	Not Consumed

☑ 1

General

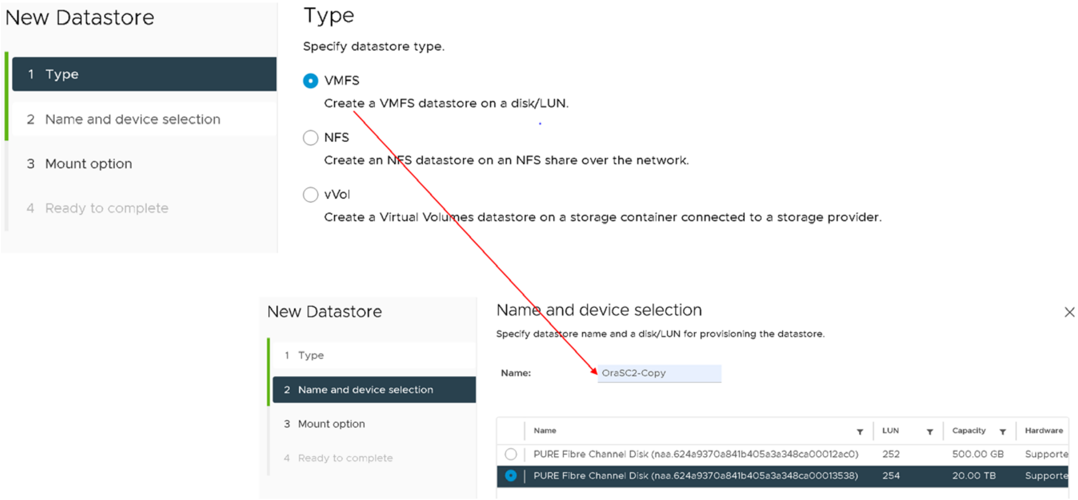
Name	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00013538)
Identifier	naa.624a9370a841b405a3a348ca00013538
Type	disk
Location	/vmfs/devices/disks/naa.624a9370a841b405a3a348ca00013538
Capacity	20.00 TB
Drive Type	Flash
Hardware Acceleration	Supported
Transport	Fibre Channel
Owner	NMP
Sector Format	512n

Multipathing Policies ACTIONS

Path Selection Policy	Round Robin (VMware)
Storage Array Type Policy	VMW_SATP_ALUA

FIGURE 169. New Storage LUN on ESXi Server

The steps to create a new datastore **OraSC2-Copy** with resignaturing are as shown below:



Type

Specify datastore type.

● VMFS

Create a VMFS datastore on a disk/LUN.

○ NFS

Create an NFS datastore on an NFS share over the network.

○ vVol

Create a Virtual Volumes datastore on a storage container connected to a storage provider.

Name and device selection

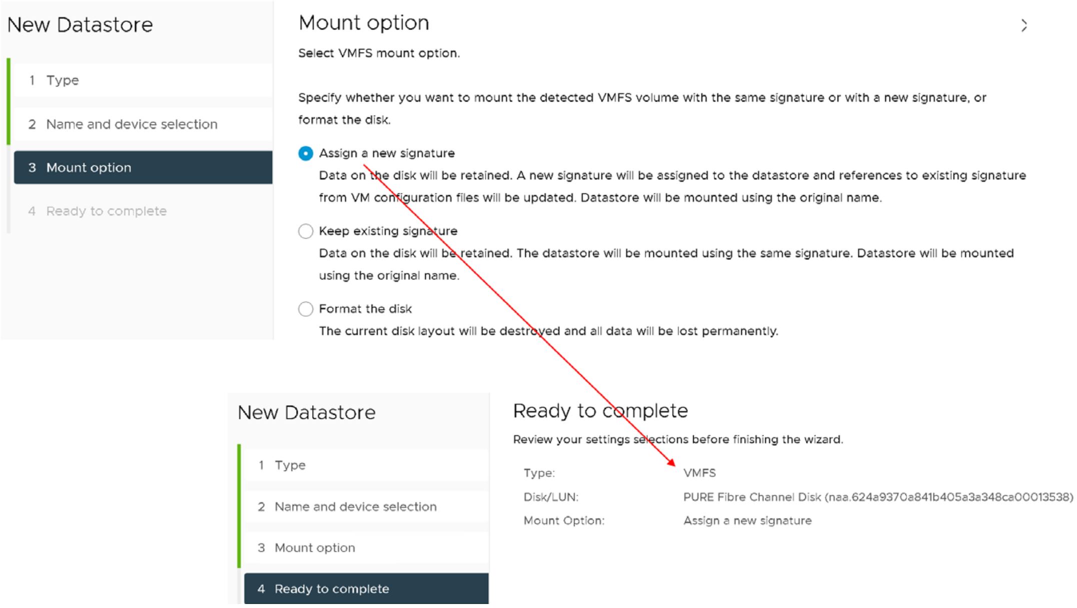
Specify datastore name and a disk/LUN for provisioning the datastore.

Name: OraSC2-Copy

	Name	LUN	Capacity	Hardware
○	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00012ac0)	252	500.00 GB	Supporte
●	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00013538)	254	20.00 TB	Supporte

FIGURE 170. New VMFS Datastore

Resignature the new datastore **OraSC2-Copy**.



New Datastore

1 Type
2 Name and device selection
3 Mount option
4 Ready to complete

Mount option

Select VMFS mount option.

Specify whether you want to mount the detected VMFS volume with the same signature or with a new signature, or format the disk.

● Assign a new signature
Data on the disk will be retained. A new signature will be assigned to the datastore and references to existing signature from VM configuration files will be updated. Datastore will be mounted using the original name.

○ Keep existing signature
Data on the disk will be retained. The datastore will be mounted using the same signature. Datastore will be mounted using the original name.

○ Format the disk
The current disk layout will be destroyed and all data will be lost permanently.

New Datastore

1 Type
2 Name and device selection
3 Mount option
4 Ready to complete

Ready to complete

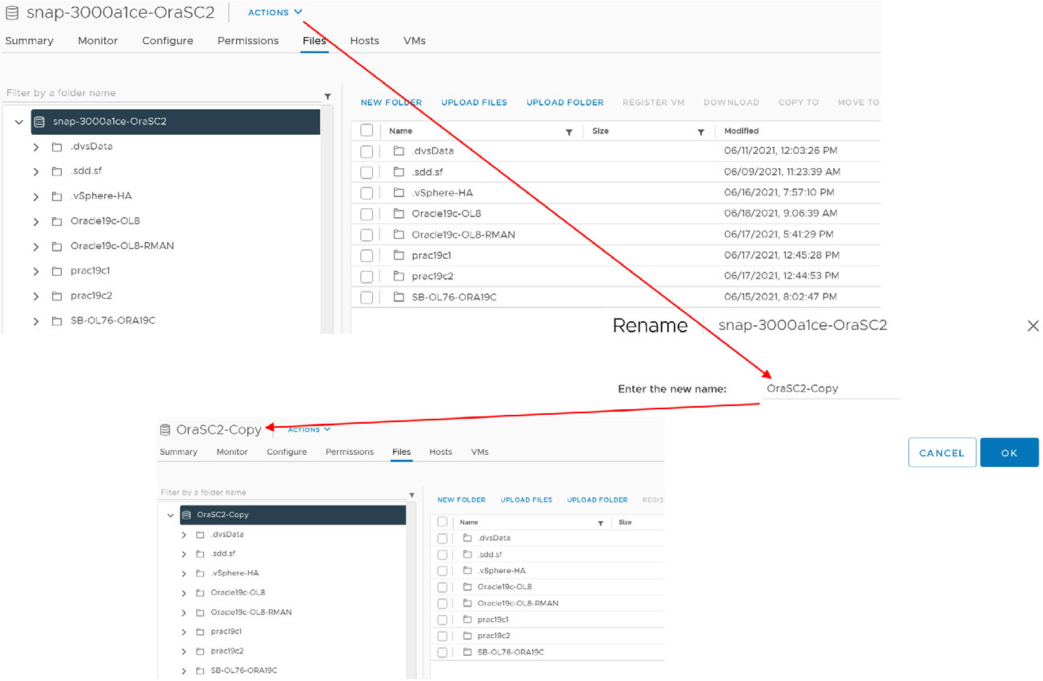
Review your settings selections before finishing the wizard.

Type:	VMFS
Disk/LUN:	PURE Fibre Channel Disk (naa.624a9370a841b405a3a348ca00013538)
Mount Option:	Assign a new signature

FIGURE 171. Resignature VMFS Datastore and Complete

The new datastore on cloned volumes is created with a cryptic name, not the one we provided to the wizard.

Right-click on the name to rename it to a user-friendly name.



snap-3000a1ce-OraSC2

Name	Size	Modified
.dvsData		06/11/2021, 12:03:26 PM
.sdd.sf		06/09/2021, 11:23:39 AM
.vSphere-HA		06/16/2021, 7:57:10 PM
Oracle19c-OL8		06/18/2021, 9:06:39 AM
Oracle19c-OL8-RMAN		06/17/2021, 5:41:29 PM
prac19c1		06/17/2021, 12:45:28 PM
prac19c2		06/17/2021, 12:44:53 PM
SB-OL76-ORA19C		06/15/2021, 8:02:47 PM

Rename snap-3000a1ce-OraSC2

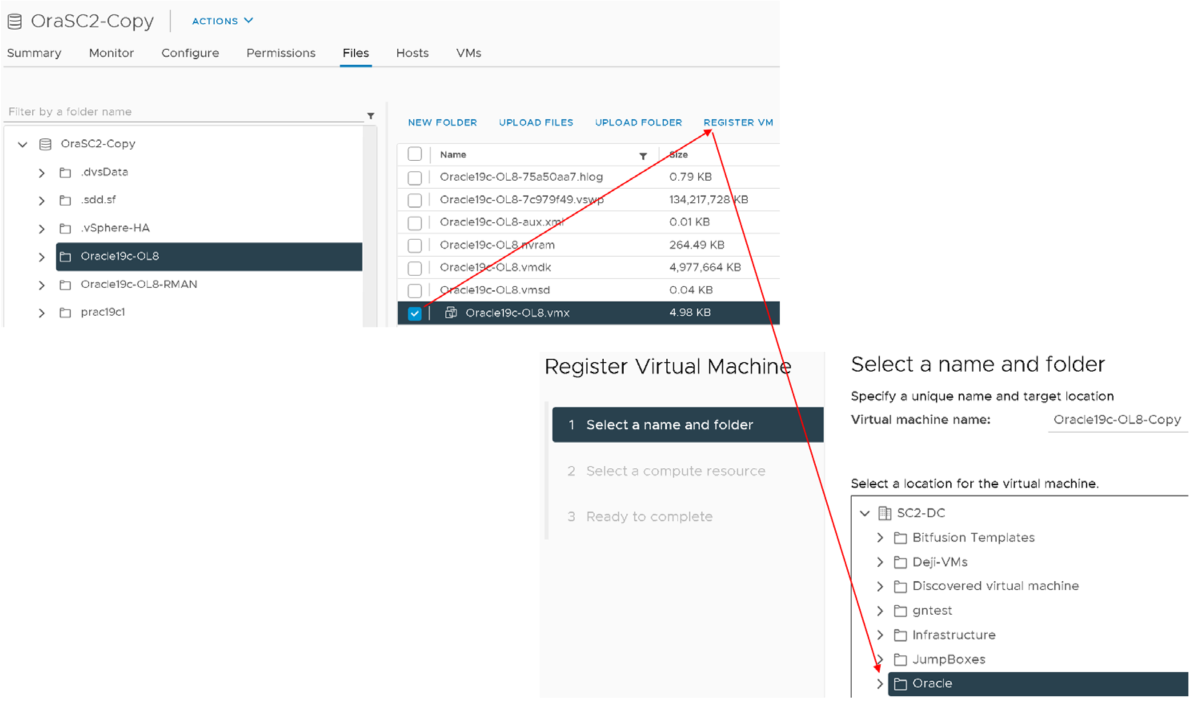
Enter the new name: OraSC2-Copy

OraSC2-Copy

Name	Size
.dvsData	
.sdd.sf	
.vSphere-HA	
Oracle19c-OL8	
Oracle19c-OL8-RMAN	
prac19c1	
prac19c2	
SB-OL76-ORA19C	

FIGURE 172. Rename VMFS Datastore

Register the Oracle VM **Oracle19c-OL8** on the datastore copy **OraSC2-Copy** as **Oracle19c-OL8-Copy**.



	Name	Size
□	Oracle19c-OL8-75a50aa7.hlog	0.79 KB
□	Oracle19c-OL8-7c979f49.vswp	134,217,728 KB
□	Oracle19c-OL8-aux.xml	0.01 KB
□	Oracle19c-OL8.nvram	264.49 KB
□	Oracle19c-OL8.vmdk	4,977,664 KB
□	Oracle19c-OL8.vmsd	0.04 KB
☑	Oracle19c-OL8.vmx	4.98 KB

Register Virtual Machine

1 Select a name and folder

2 Select a compute resource

3 Ready to complete

Select a name and folder

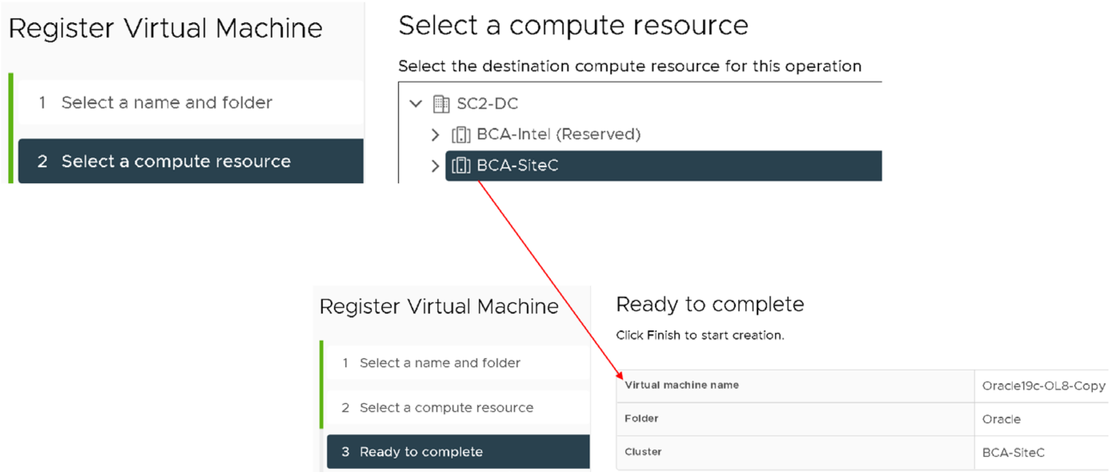
Specify a unique name and target location

Virtual machine name: Oracle19c-OL8-Copy

Select a location for the virtual machine.

FIGURE 173. Register VM Oracle19c-OL8-Copy

Select the target compute resources and datastore for Oracle VM **Oracle19c-OL8-Copy**.


Register Virtual Machine

1 Select a name and folder

2 Select a compute resource

Select a compute resource

Select the destination compute resource for this operation

Register Virtual Machine

1 Select a name and folder

2 Select a compute resource

3 Ready to complete

Ready to complete

Click Finish to start creation.

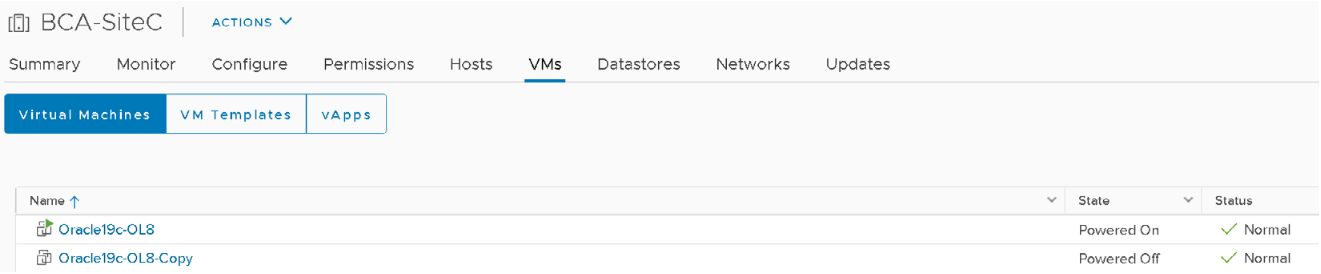
Virtual machine name	Oracle19c-OL8-Copy
Folder	Oracle
Cluster	BCA-SiteC

FIGURE 174. VM Oracle19c-OL8-Copy Compute Resource and Complete

A copy of the original Oracle VM **Oracle19c-OL8** is brought up as VM **Oracle19c-OL8-Copy**. Assign a new IP address to the VM **Oracle19c-OL8-Copy**. The VM **Oracle19c-OL8-Copy** database has the same name as in the original Oracle VM **Oracle19c-OL8**.

Oracle crash recovery is performed when the database starts up, which is normal and expected.

Perform database operations to restore the database contents as required.



Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-Copy	Powered Off	✓ Normal

FIGURE 175. VM Oracle19c-OL8-Copy

When the database restore operation is completed, the VM copy **Oracle19c-OL8-Copy** can be shut down and unregistered from VM. The datastore copy **OraSC2-Copy** can be then unmounted using the web client. Using the Pure Storage GUI, the storage LUN **OraSC2-Copy** can then be deleted.

Similar steps can be followed in the case of Oracle VM **Oracle19c-OL8-RMAN**, bringing up a copy of the VM **Oracle19c-OL8-RMAN-Copy**.

The steps above for performing storage-based snapshots and cloning of Oracle VM **Oracle19c-OL8** can be used for Oracle RAC **prac19c** VMs as well. These can be found in the **Oracle Backup of RAC** section in *Virtualizing Oracle Workloads with VMware vSphere Virtual Volumes on VMware Hybrid Cloud guide*.

Similar steps for performing storage-based backup/restore of Oracle VM **Oracle19c-OL8** on a VMFS datastore can be found in *Cloning an Oracle Database on VMware VMFS guide*.

On-premises Using vSphere Virtual Volumes Storage

As mentioned, storage-based snapshots and clones of a VMFS datastore are at a storage LUN level, so the granularity of operation is also at the storage LUN level.

In case of vVOLs datastores, granularity of operation can occur at a VM or VMDK level using vSphere Virtual Volumes

- A traditional VM-level snapshot using the web client
- A VMDK-level snapshot using the Pure Storage Plugin

Details for use of vSphere Virtual Volumes and Pure Storage Plugin with Oracle VM backup and restores can be found in the *Virtualizing Oracle Workloads with VMware vSphere Virtual Volumes on VMware Hybrid Cloud guide*.

VMware Clouds

Native storage-based snapshot and cloning capability is not available on most VMware clouds as most VMware clouds are managed services and do not provide direct access to the storage layer.

To enable additional storage capacity in VMware Cloud on AWS, the ability to attach external NFS cloud-managed storage to a VMware Cloud SDDC through a managed service provider is offered as well (e.g., Faction Cloud Control Volumes). Learn more about *Faction Managed VMware Cloud*.

This solution architecture does not focus on third-party provided storage solutions.

Oracle Disaster Recovery

This section validates Oracle disaster recovery using Oracle application-based tools, VMware-based tools and storage-based tools for Oracle single-instance and Oracle RAC using Pure x50 Storage.

On-premises and VMware clouds may have different choices of storage offerings but the type of underlying storage (VMFS, RDM, iSCSI, NFS, vSAN, vSphere Virtual Volumes) is transparent to the Oracle layer, whether its on-premises or on VMware clouds.

Once VM disks are carved from any of these storage technologies and added to a VM, the guest operating system sees them as a regular Linux block device (/dev/sdX). The remaining steps to create ASM disks or filesystems are the same as those one would employ on physical architecture.

Application-Level Disaster Recovery

Oracle Data Guard is an Oracle Database tool that provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases, enabling production Oracle databases to survive disasters and data corruptions.

Other Oracle Database DR tools include Oracle GoldenGate. Other third-party DR tools are also available.

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

On-premises

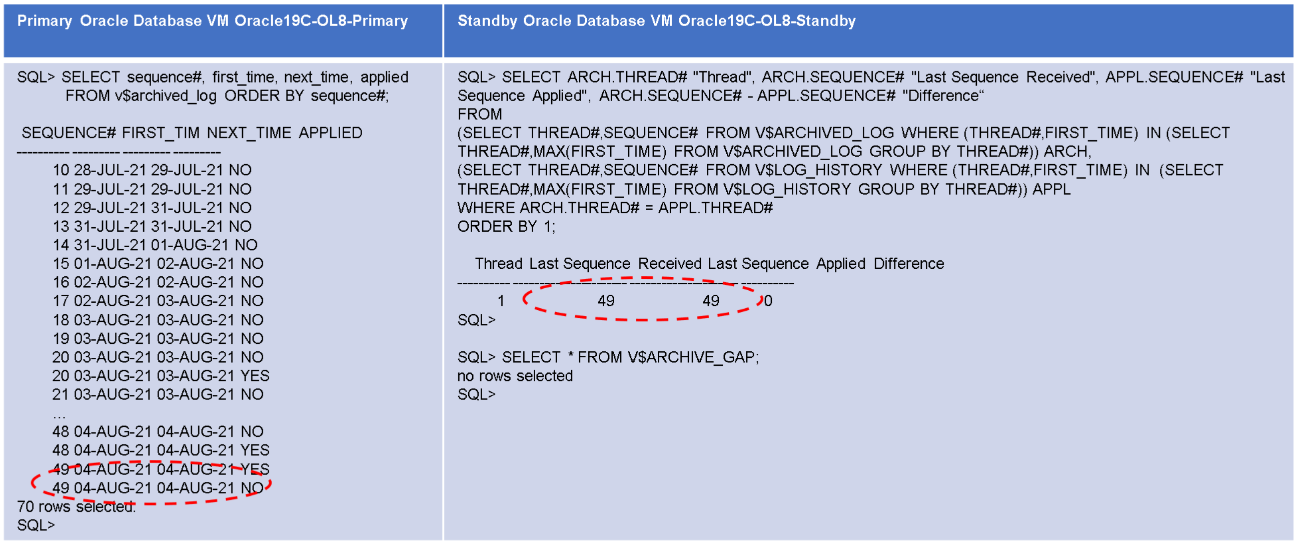
This use case focusses at a high level on the use of Oracle Data Guard to provide disaster recovery to the single-instance primary VM **Oracle19c-OL8** on Site A, using the physical standby VM **Oracle19c-OL8-DG** on **Site B**.

Two VMs are employed for this use case:

- Primary 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 172.16.14.51 on Site B

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

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



Primary Oracle Database VM Oracle19C-OL8-Primary

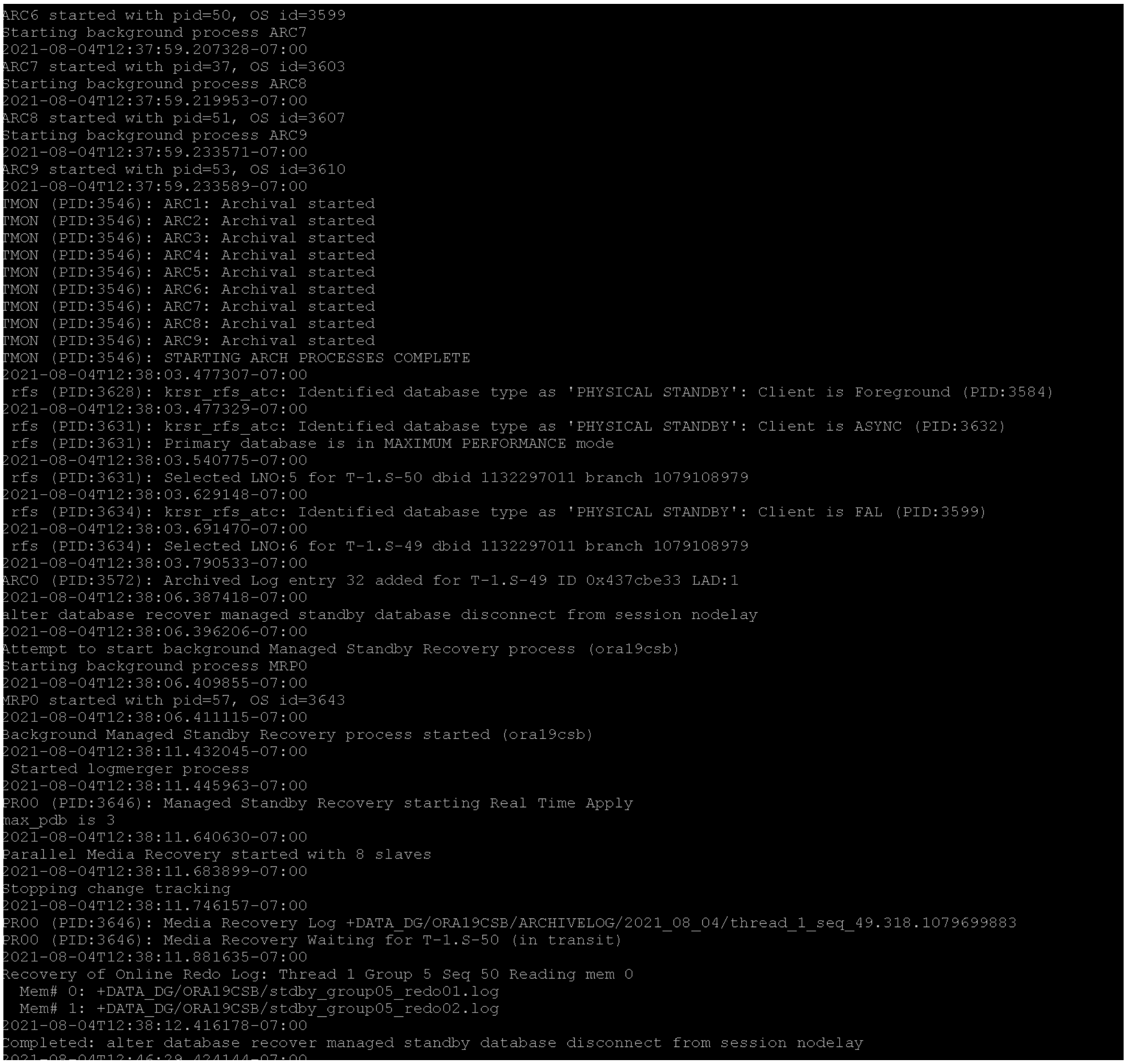
```
SQL> SELECT sequence#, first_time, next_time, applied
        FROM v$archived_log ORDER BY sequence#;

 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>
```

Standby Oracle Database VM Oracle19C-OL8-Standby

```
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 176. Primary and Standby Oracle Database Status

The standby Oracle VM **Oracle19c-OL8-Standby** alert log for the database **ora19c** shows no errors and shows the redo log application if and when it is generated on the primary database.



```
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
2021-08-04T12:46:29.424144-07:00
```

FIGURE 177. Alert log for Standby Oracle Database

The steps for setting up Oracle Data Guard for an Oracle RAC cluster **prac19c** are similar to a single instance with certain subtleties. More information can be found in the *Oracle Data Guard and Oracle Real Application Clusters guide*.

Oracle Data Guard role transitions switchover and failover are the same when applied to physical architecture. Learn more about *role transitions*.

Using VMware Site Recovery Manager Workflow for Oracle Data Guard Role Transition

Oracle Data Guard facilitates the redo transport in a physical Data Guard setup. A database operates in one of the following mutually exclusive roles: primary or standby.

Oracle Data Guard enables you to change these roles dynamically by using SQL statements, or by using either of the Oracle Data Guard broker's interfaces.

Oracle Data Guard supports the following role transitions:

- **Switchover** – Allows the primary database to switch roles with one of its standby databases. There is no data loss during a switchover. After a switchover, each database continues to participate in the Oracle Data Guard configuration with its new role.
- **Failover** – Changes a standby database to the primary role in response to a primary database failure. If the primary database was not operating in either maximum protection mode or maximum availability mode before the failure, some data loss may occur. If Flashback database is enabled on the primary database, it can be reinstated as a standby for the new primary database once the reason for the failure is corrected.

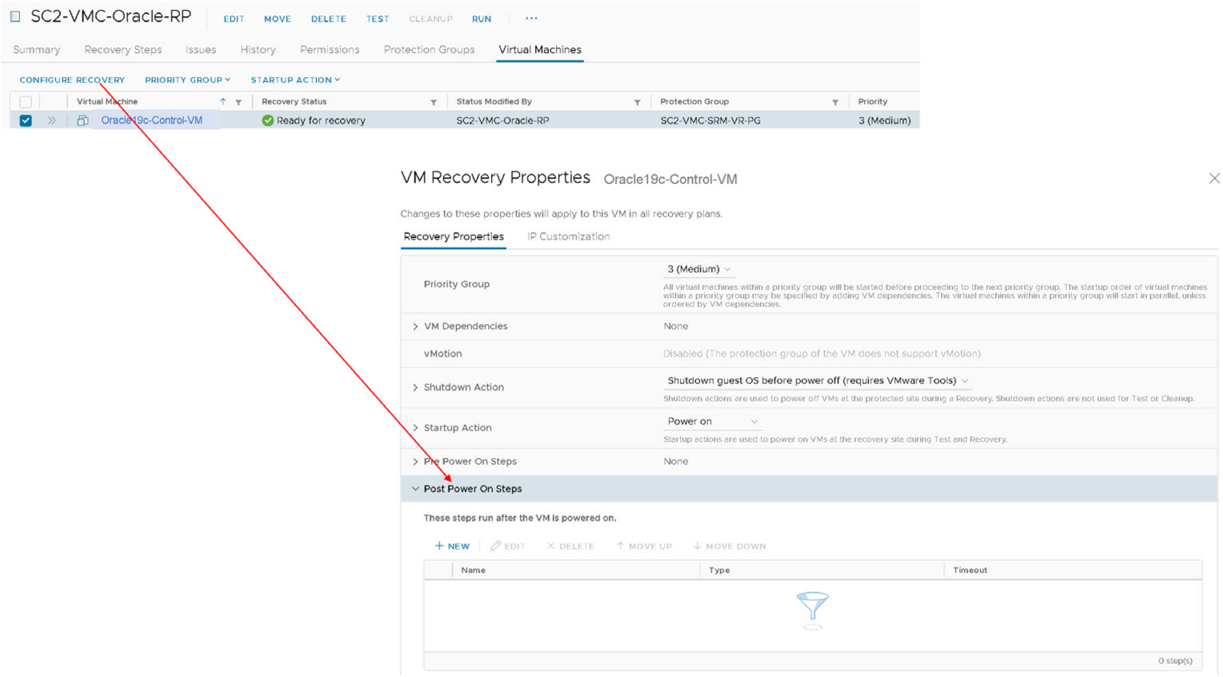
Learn more about *role transitions*.

VMware Site Recovery Manager is a business continuity and disaster recovery solution that helps you plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.

A use case could be to combine the workflow capability of VMware Site Recovery Manager to assist with the role transitioning of Oracle Data Guard environments in case of testing a DR scenario or in event of an actual DR.

For example, as part of configuring the recovery plan **SC2-VMC-Oracle-RP**

- One could configure the recovery of a control VM **Oracle19c-Control-VM**
- Control VM **Oracle19c-Control-VM** can have a power-on step with a shell script embedded which is executed once the control VM **Oracle19c-Control-VM** is fully powered up
- The post power-on shell script can run a command on the local control VM or any VM it can ssh to, for example, run a shell script residing locally on standby VM **Oracle19c-OL8-Standby** to perform the database role transition to failover to a standby database.



☐		Virtual Machine	Recovery Status	Status Modified By	Protection Group	Priority
☑	»	Oracle19c-Control-VM	✓ Ready for recovery	SC2-VMC-Oracle-RP	SC2-VMC-SRM-VR-PG	3 (Medium)

VM Recovery Properties Oracle19c-Control-VM

Changes to these properties will apply to this VM in all recovery plans.

Priority Group	3 (Medium) All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual machines within a priority group may be specified by adding VM dependencies. The virtual machines within a priority group will start in parallel, unless ordered by VM dependencies.
> VM Dependencies	None
vMotion	Disabled (The protection group of the VM does not support vMotion)
> Shutdown Action	Shutdown guest OS before power off (requires VMware Tools) Shutdown actions are used to power off VMs at the protected site during a Recovery. Shutdown actions are not used for Test or Cleanup.
> Startup Action	Power on Startup actions are used to power on VMs at the recovery site during Test and Recovery.
> Pre Power On Steps	None
⌄ Post Power On Steps	

These steps run after the VM is powered on.

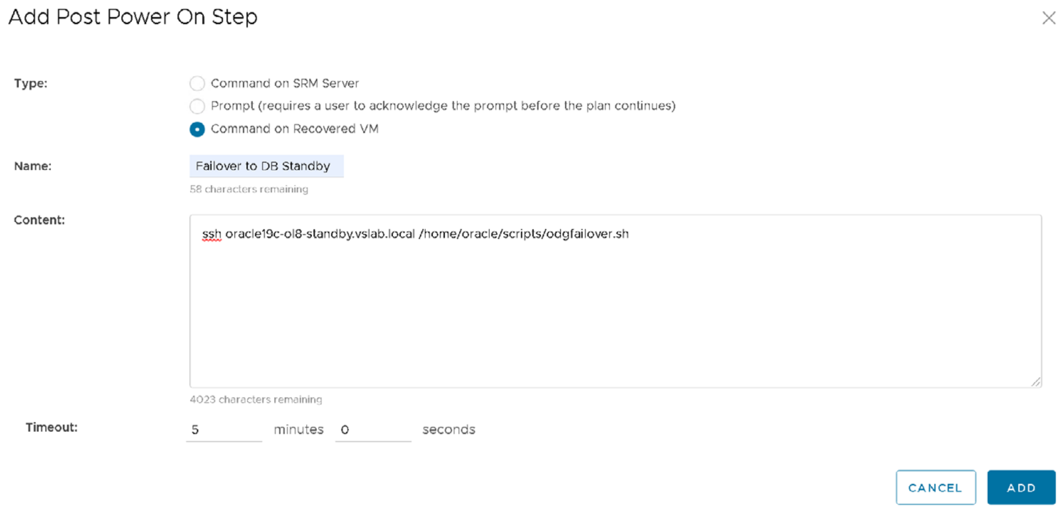
Name	Type	Timeout

0 step(s)

FIGURE 178. Recovery Plan with Post Power-On Configuration

The steps to add the post power-on step to VM **Oracle19c-Control-VM** is as shown below.

The post power-on step contains a call out to a shell script, residing locally on standby VM **Oracle19c-OL8-Standby**. This shell script could then perform the database role transition to failover to a standby database.



Add Post Power On Step

Type:
○ Command on SRM Server
○ Prompt (requires a user to acknowledge the prompt before the plan continues)
● Command on Recovered VM

Name: Failover to DB Standby
58 characters remaining

Content:

```
ssh oracle19c-ol8-standby.vslab.local /home/oracle/scripts/odgfailover.sh
```

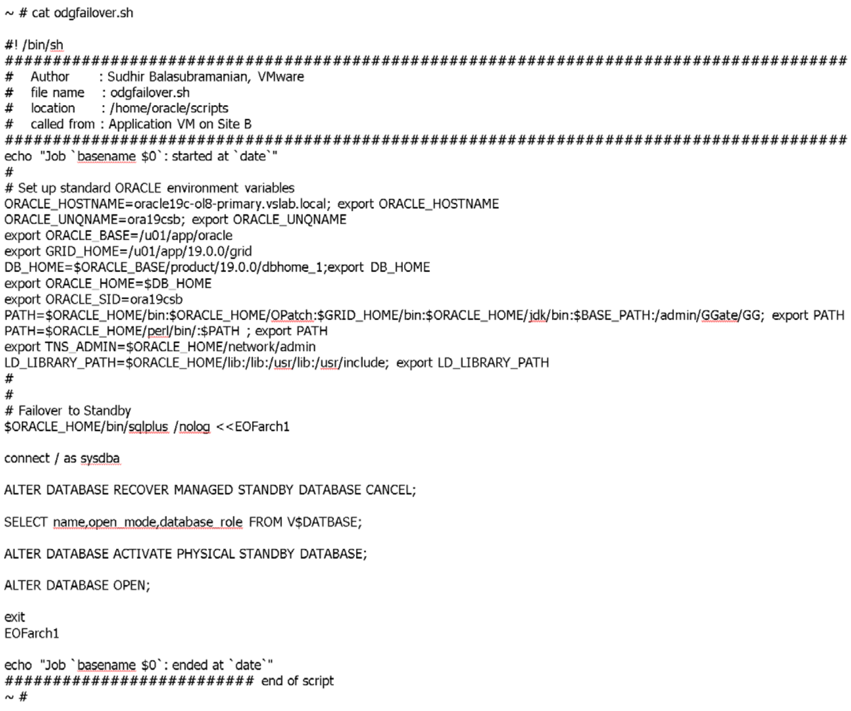
4023 characters remaining

Timeout: 5 minutes 0 seconds

FIGURE 179. Post Power-On Step with Embedded Shell Script

For example, the invocation command could be **ssh oracle19c-ol8-standby.vslab.local /home/oracle/scripts/odgfailover.sh**.

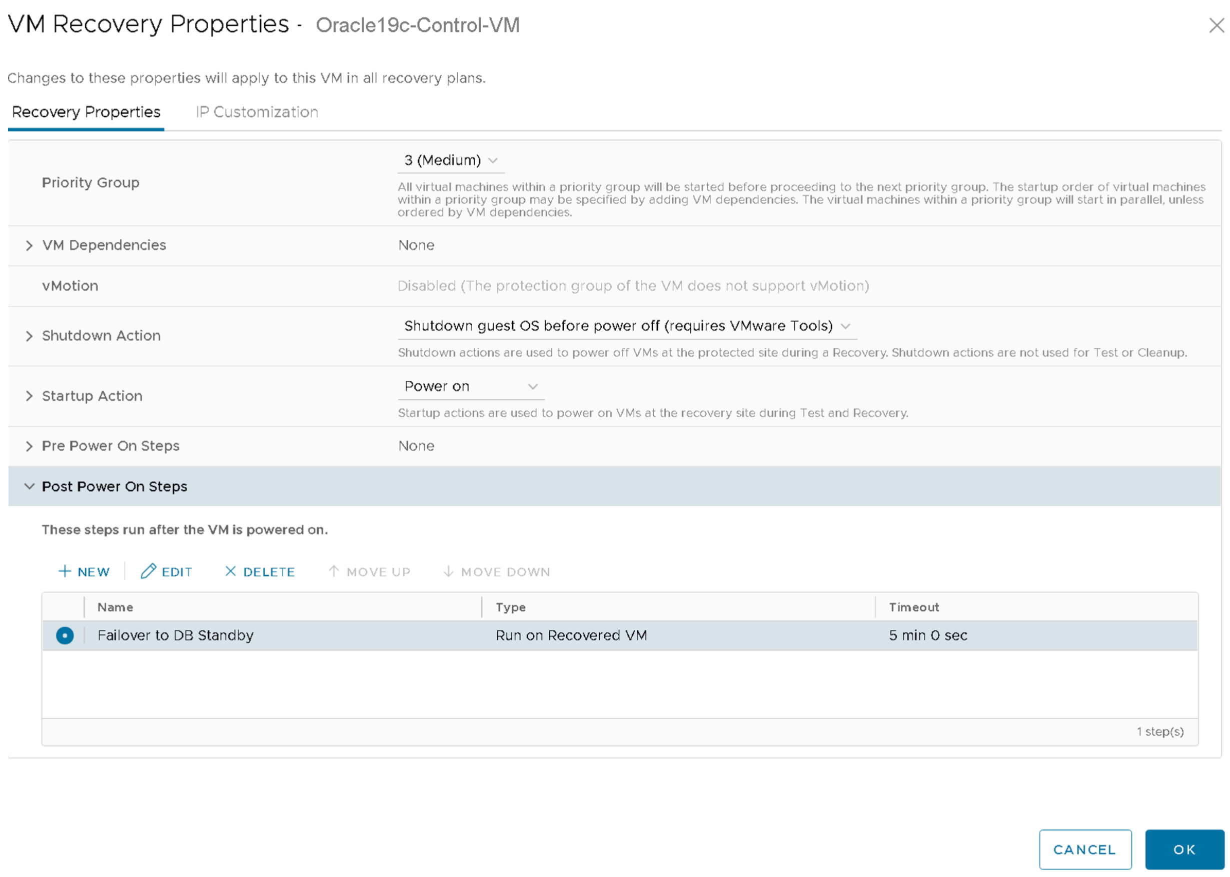
Example of a shell script that could be invoked to perform database role transition to failover to a standby database is as shown below:



```
~ # cat odgfailover.sh

#! /bin/sh
########################################################################################
#    Author       : Sudhir Balasubramanian, VMware
#    file name    : odgfailover.sh
#    location     : /home/oracle/scripts
#    called from : Application VM on Site B
########################################################################################
echo  "Job `basename $0`: started at `date`"
#
# Set up standard ORACLE environment variables
ORACLE_HOSTNAME=oracle19c-ol8-primary.vslab.local; export ORACLE_HOSTNAME
ORACLE_UNQNAME=ora19csb; export ORACLE_UNQNAME
export ORACLE_BASE=/u01/app/oracle
export GRID_HOME=/u01/app/19.0.0/grid
DB_HOME=$ORACLE_BASE/product/19.0.0/dbhome_1;export DB_HOME
export ORACLE_HOME=$DB_HOME
export ORACLE_SID=ora19csb
PATH=$ORACLE_HOME/bin:$ORACLE_HOME/OPatch:$GRID_HOME/bin:$ORACLE_HOME/jdk/bin:$BASE_PATH:/admin/GGate/GG;  export PATH
PATH=$ORACLE_HOME/perl/bin/:$PATH  ; export PATH
export TNS_ADMIN=$ORACLE_HOME/network/admin
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib:/usr/include;  export LD_LIBRARY_PATH
#
#
# Failover  to Standby
$ORACLE_HOME/bin/sqlplus /nolog <<EOFarch1

connect / as sysdba

ALTER DATABASE RECOVER MANAGED STANDBY DATABASE CANCEL;

SELECT name,open_mode,database_role FROM V$DATBASE;

ALTER DATABASE ACTIVATE PHYSICAL STANDBY DATABASE;

ALTER DATABASE OPEN;

exit
EOFarch1

echo  "Job `basename $0`: ended at `date`"
##########################  end of script
~ #
```

FIGURE 180. Example of a Post Power-On Shell Script

More details on post power-on steps are shown below:



VM Recovery Properties - Oracle19c-Control-VM

Changes to these properties will apply to this VM in all recovery plans.

Priority Group: 3 (Medium)

All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual machines within a priority group may be specified by adding VM dependencies. The virtual machines within a priority group will start in parallel, unless ordered by VM dependencies.

VM Dependencies: None

vMotion: Disabled (The protection group of the VM does not support vMotion)

Shutdown Action: Shutdown guest OS before power off (requires VMware Tools)

Shutdown actions are used to power off VMs at the protected site during a Recovery. Shutdown actions are not used for Test or Cleanup.

Startup Action: Power on

Startup actions are used to power on VMs at the recovery site during Test and Recovery.

Pre Power On Steps: None

Post Power On Steps

These steps run after the VM is powered on.

	Name	Type	Timeout
●	Failover to DB Standby	Run on Recovered VM	5 min 0 sec

1 step(s)

FIGURE 181. Post Power-On Process Configuration Details

The above use case is appropriate in the event there are a number of standby databases with role transitions to manage. One could combine the workflow capability of VMware Site Recovery Manager to assist with role transitioning of Oracle Data Guard environments in a testing DR scenario or in event of an actual DR.

The above use case is relevant for both on-premises and VMware clouds.

VMware Clouds

The above use case employing Oracle Data Guard to provide disaster recovery to the single-instance VM **Oracle19c-OL8-Primary** using the standby VM **Oracle19c-OL8-Standby** is accomplished with the same steps across all VMware clouds and on-premises environments.

On VMware Cloud on AWS, one could use two SDDC clusters deployed on two different availability zones (AZ), setting up the single-instance VM **Oracle19c-OL8-Primary** on AZ1 and standby VM **Oracle19c-OL8-Standby** on AZ2, thereby providing Oracle Data Guard services between the two AZs.

vSphere Level Disaster Recovery

VMware Site Recovery Manager with VMware vSphere Replication can provide disaster recovery to Oracle VMs from on-premises Site A to Site B **OR** from on-premises Site A or Site B to any VMware Cloud.

In a typical Site Recovery Manager installation, the protected site provides business-critical datacenter services. The recovery site is an alternative infrastructure to which Site Recovery Manager can migrate these services.

vSphere Replication replicates at the VM level. This process occurs independently of the storage layer as mentioned earlier, whether the VMDK resides on a NFS, VMFS, vSAN or a vVOL datastore.

As mentioned earlier, **Write-order fidelity is guaranteed with vSphere Replication on the disks or VMDKs that comprise a VM**. However, consistency cannot be guaranteed across multiple VMs. vSphere Replication supports replicating VMs on local, attached, Virtual SAN, FC, iSCSI, or NFS storage. vSphere Replication cannot replicate VMs that are part of an MSCS cluster. vSphere Replication cannot replicate disks in multi-writer mode.

More information regarding VMware Site Recovery Manager and VMware vSphere Replication can be found in *VMware Site Recovery Manager Installation and Configuration* and *VMware vSphere Replication*.

On-premises

This use case focusses on the utilization of VMware Site Recovery Manager with VMware vSphere Replication to provide disaster recovery to Oracle single-instance VM **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** across on-premises sites A and B.

The steps to configure vSphere Replication for Oracle VM **Oracle19c-OL8** are as shown below. These steps are the same for Oracle VM **Oracle19c-OL8-RMAN**.

This use cases provisions the Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** on a VMFS datastore and holds true for NFS, VMFS, vSAN or vVOL datastores. vSphere Replication operates at a VMDK level completely independent from the underlying datastore storage characteristics.

Oracle RAC uses the multi-writer attribute to share VMDKs as part of the RAC cluster. The multi-writer attribute is documented in *KB 1034165*. Currently, vSphere Replication 8.4 cannot replicate VMs that share VMDK files. This limitation is referenced in *VMware vSphere Replication 8.4 Release Notes*.

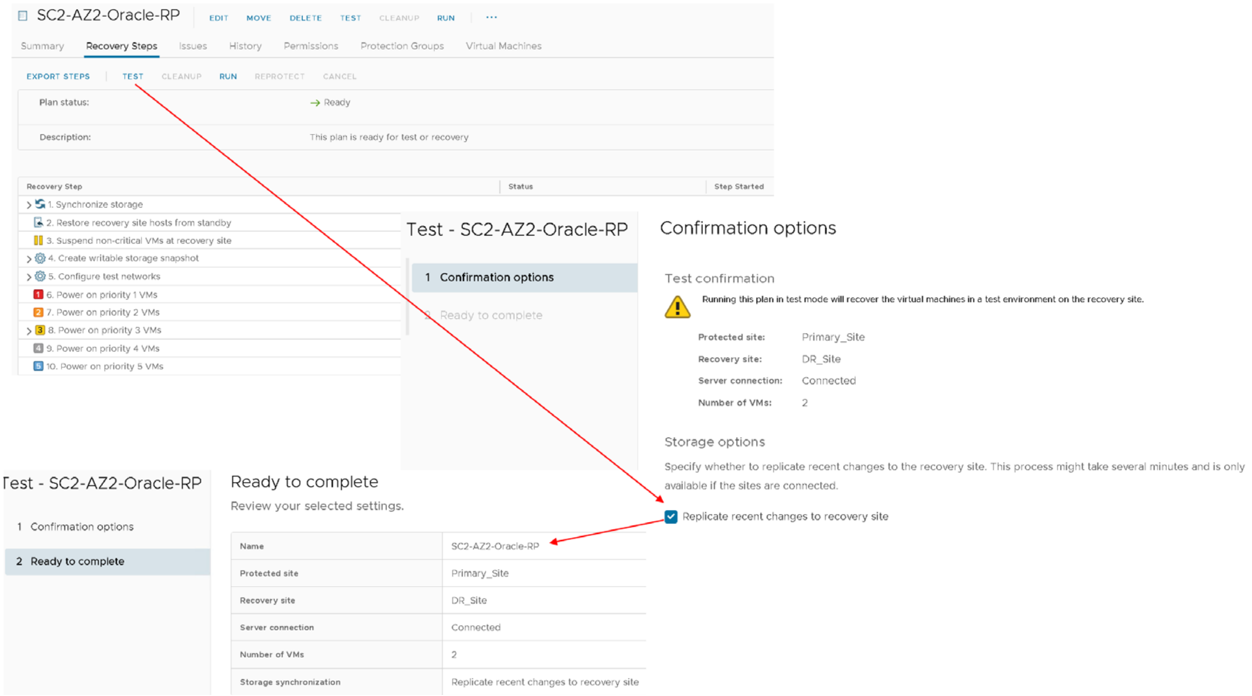
Test Recovery Plan

The recovery plan can be tested before being used for planned migration or for disaster recovery. Testing a recovery plan will ensure the primary VM on the protected site is still replicating with the replica VM disk files on the recovery site. The vSphere Replication server creates redo logs on the VM disk files on the recovery site, so that synchronization can continue normally. During a recovery plan test, there is no impact or disruption to the protected VMs, replication or RPO.

The VMs on the recovery site are run on a test network and on a temporary snapshot of replicated data at the recovery site. No operations are disrupted at the protected site. A snapshot is created on the recovery site of all the disk files of the VMs in the recovery plan.

When running a recovery plan test, recent changes can be replicated to simulate a planned migration, or not replicated to simulate a disaster.

Steps to test the recovery plan **SC2-AZ2-Oracle-RP** are as shown below:



Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby		
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
5. Configure test networks		
6. Power on priority 1 VMs		
7. Power on priority 2 VMs		
8. Power on priority 3 VMs		
9. Power on priority 4 VMs		
10. Power on priority 5 VMs		

Test - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Test confirmation

Running this plan in test mode will recover the virtual machines in a test environment on the recovery site.

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	2

Storage options

Specify whether to replicate recent changes to the recovery site. This process might take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

Test - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

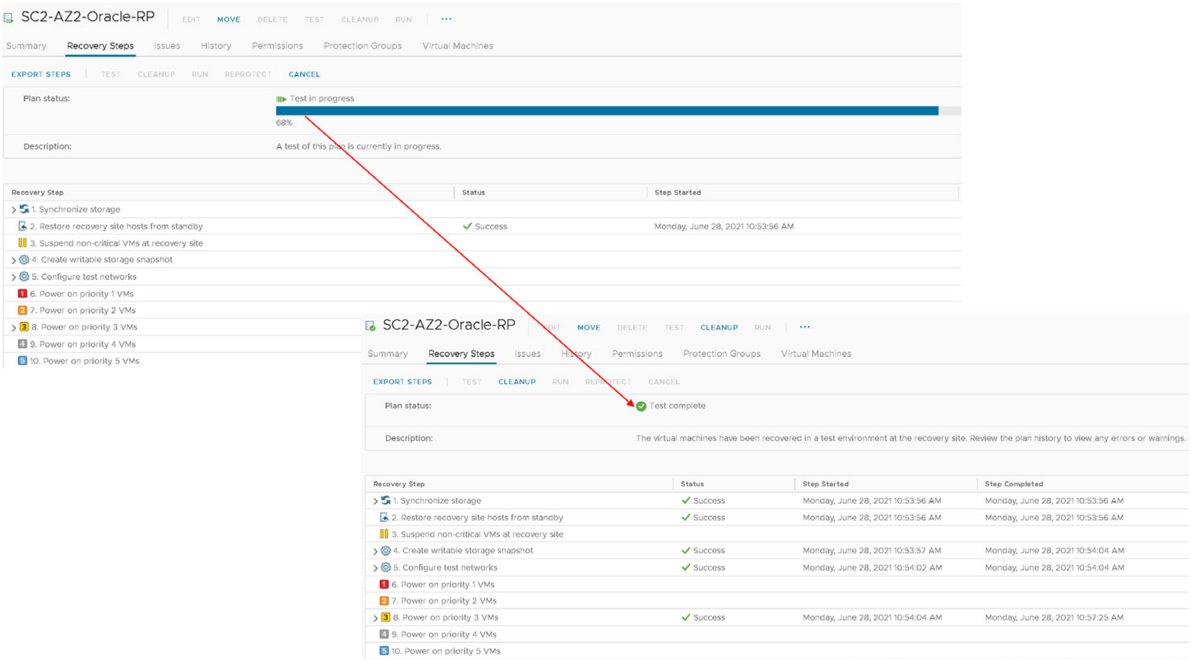
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	2
Storage synchronization	Replicate recent changes to recovery site

FIGURE 182. Test Recovery Plan SC2-AZ2-Oracle-RP

The test of the recovery plan completes successfully.



Plan status: Test in progress

68%

Description: A test of this plan is currently in progress.

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby	✓ Success	Monday, June 28, 2021 10:53:56 AM
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
5. Configure test networks		
6. Power on priority 1 VMs		
7. Power on priority 2 VMs		
8. Power on priority 3 VMs		
9. Power on priority 4 VMs		
10. Power on priority 5 VMs		

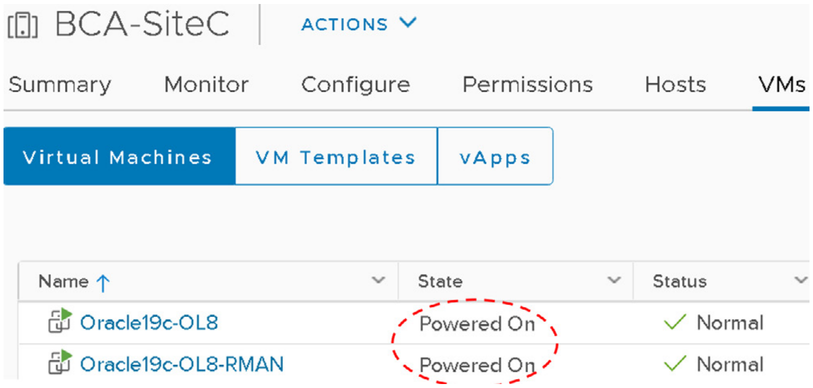
Plan status: ✓ Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Monday, June 28, 2021 10:53:56 AM	Monday, June 28, 2021 10:53:56 AM
2. Restore recovery site hosts from standby	✓ Success	Monday, June 28, 2021 10:53:56 AM	Monday, June 28, 2021 10:53:56 AM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Monday, June 28, 2021 10:53:57 AM	Monday, June 28, 2021 10:54:04 AM
5. Configure test networks	✓ Success	Monday, June 28, 2021 10:54:02 AM	Monday, June 28, 2021 10:54:04 AM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Monday, June 28, 2021 10:54:04 AM	Monday, June 28, 2021 10:57:25 AM
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

FIGURE 183. Test Recovery Plan SC2-AZ2-Oracle-RP Completion

VMs on Protected Site A are still powered on.

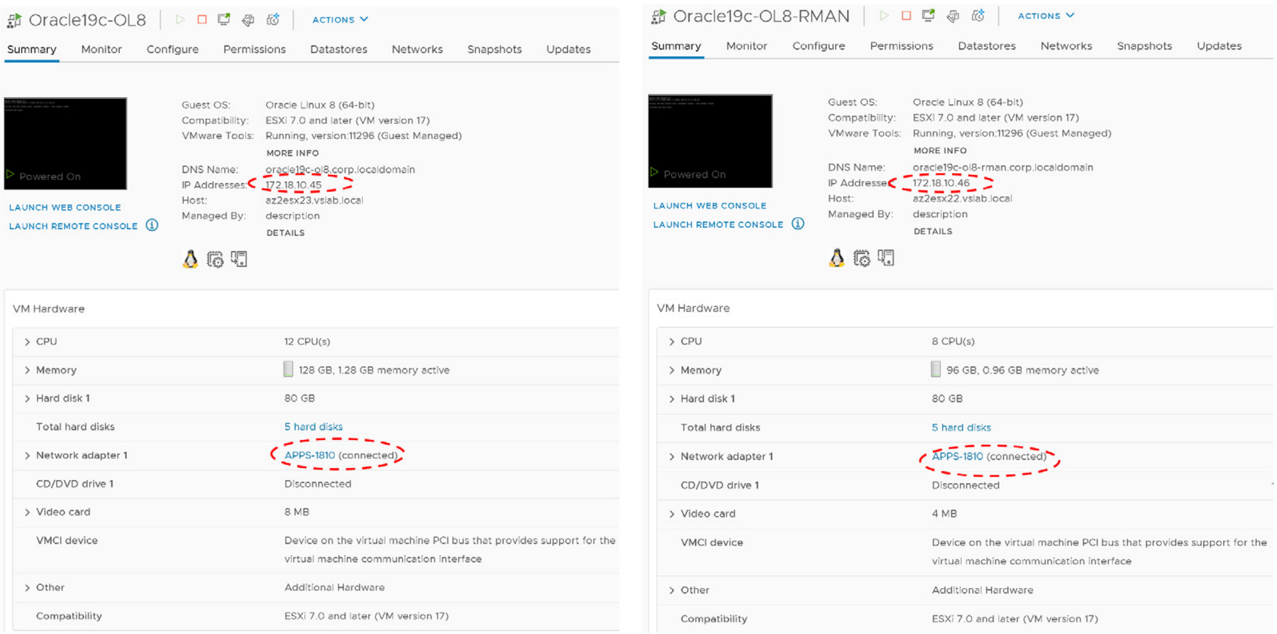


BCA-SiteC | ACTIONS

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal

FIGURE 184. Test Recovery Plan VM Details

Oracle VM **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** on Recovery Site B are powered on with the IP addressing scheme set per network mappings to test network **APPS-1810**.



Oracle19c-OL8 | ACTIONS

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.corp.localdomain
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local
Managed By: description

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Oracle19c-OL8-RMAN | ACTIONS

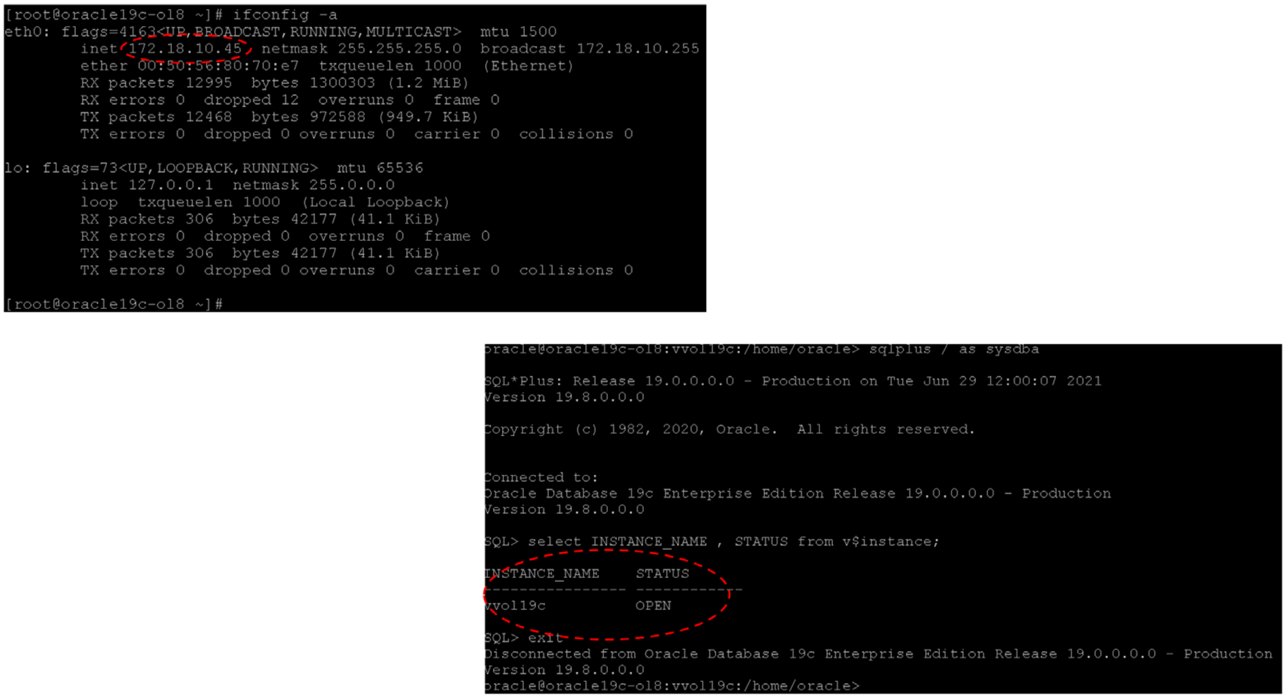
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.corp.localdomain
IP Addresse 172.18.10.46
Host: az2esx22.vslab.local
Managed By: description

VM Hardware

CPU	8 CPU(s)
Memory	96 GB, 0.96 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 185. Test Recovery Plan VM Networking Details

The Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database **vvol19c** is up.

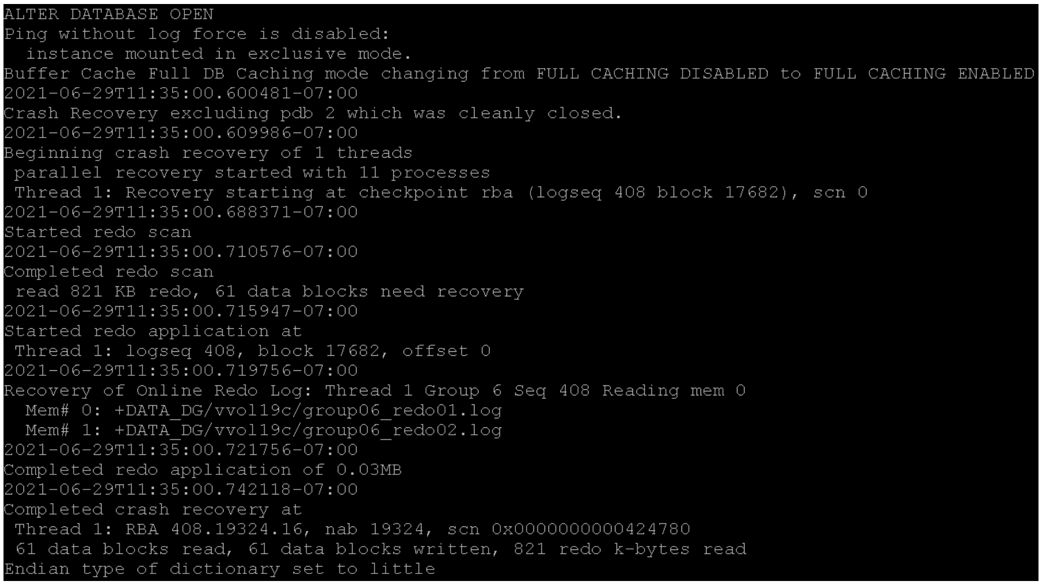


```
[root@oracle19c-ol8 ~]# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.10.45  netmask 255.255.255.0  broadcast 172.18.10.255
        ether 00:50:56:80:70:e7  txqueuelen 1000  (Ethernet)
        RX packets 12995  bytes 1300303 (1.2 MiB)
        RX errors 0  dropped 12  overruns 0  frame 0
        TX packets 12468  bytes 972588 (949.7 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 306  bytes 42177 (41.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 306  bytes 42177 (41.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@oracle19c-ol8 ~]#
```

```
oracle@oracle19c-ol8:vvol19c:/home/oracle> sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Jun 29 12:00:07 2021
Version 19.8.0.0.0

Copyright (c) 1982, 2020, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL> select INSTANCE_NAME , STATUS from v$instance;

INSTANCE_NAME    STATUS
---------------- ------------
vvol19c          OPEN

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0
oracle@oracle19c-ol8:vvol19c:/home/oracle>
```

FIGURE 186. VM Oracl19c-OL8 Networking and Database Details

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



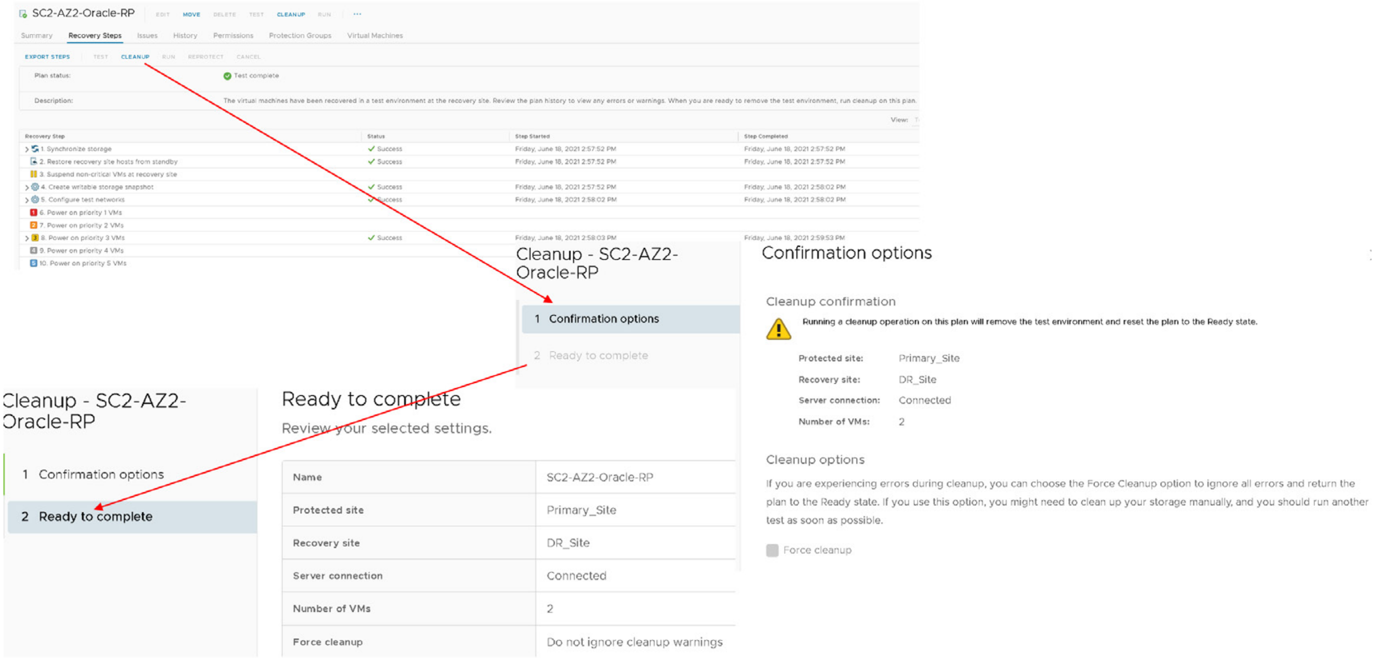
```
ALTER DATABASE OPEN
Ping without log force is disabled:
  instance mounted in exclusive mode.
Buffer Cache Full DB Caching mode changing from FULL CACHING DISABLED to FULL CACHING ENABLED
2021-06-29T11:35:00.600481-07:00
Crash Recovery excluding pdb 2 which was cleanly closed.
2021-06-29T11:35:00.609986-07:00
Beginning crash recovery of 1 threads
 parallel recovery started with 11 processes
 Thread 1: Recovery starting at checkpoint rba (logseq 408 block 17682), scn 0
2021-06-29T11:35:00.688371-07:00
Started redo scan
2021-06-29T11:35:00.710576-07:00
Completed redo scan
 read 821 KB redo, 61 data blocks need recovery
2021-06-29T11:35:00.715947-07:00
Started redo application at
 Thread 1: logseq 408, block 17682, offset 0
2021-06-29T11:35:00.719756-07:00
Recovery of Online Redo Log: Thread 1 Group 6 Seq 408 Reading mem 0
  Mem# 0: +DATA_DG/vvol19c/group06_redo01.log
  Mem# 1: +DATA_DG/vvol19c/group06_redo02.log
2021-06-29T11:35:00.721756-07:00
Completed redo application of 0.03MB
2021-06-29T11:35:00.742118-07:00
Completed crash recovery at
 Thread 1: RBA 408.19324.16, nab 19324, scn 0x0000000000424780
 61 data blocks read, 61 data blocks written, 821 redo k-bytes read
Endian type of dictionary set to little
```

FIGURE 187. VM Oracl19c-OL8 Database Alert Log Details

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

As mentioned earlier, **write-order fidelity is guaranteed with vSphere Replication on the disks or VMDKs that comprise a VM**.

At the successful completion of the test recovery, perform the cleanup of the test recovery as shown below. As part of the cleanup after running a test, the vSphere Replication server removes the redo logs from the disks on the recovery site and discards the changes.



SC2-AZ2-Oracle-RP
EDIT MOVE DELETE TEST CLEANUP RUN ...
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS TEST CLEANUP RUN REPROTECT CANCEL

Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Friday, June 18, 2021 2:57:52 PM	Friday, June 18, 2021 2:57:52 PM
2. Restore recovery site hosts from standby	✓ Success	Friday, June 18, 2021 2:57:52 PM	Friday, June 18, 2021 2:57:52 PM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Friday, June 18, 2021 2:57:52 PM	Friday, June 18, 2021 2:58:02 PM
5. Configure test networks	✓ Success	Friday, June 18, 2021 2:58:02 PM	Friday, June 18, 2021 2:58:02 PM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Friday, June 18, 2021 2:58:03 PM	Friday, June 18, 2021 2:59:53 PM
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

Cleanup - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Cleanup confirmation

Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	2

Cleanup options

If you are experiencing errors during cleanup, you can choose the Force Cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you might need to clean up your storage manually, and you should run another test as soon as possible.

□ Force cleanup

Cleanup - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

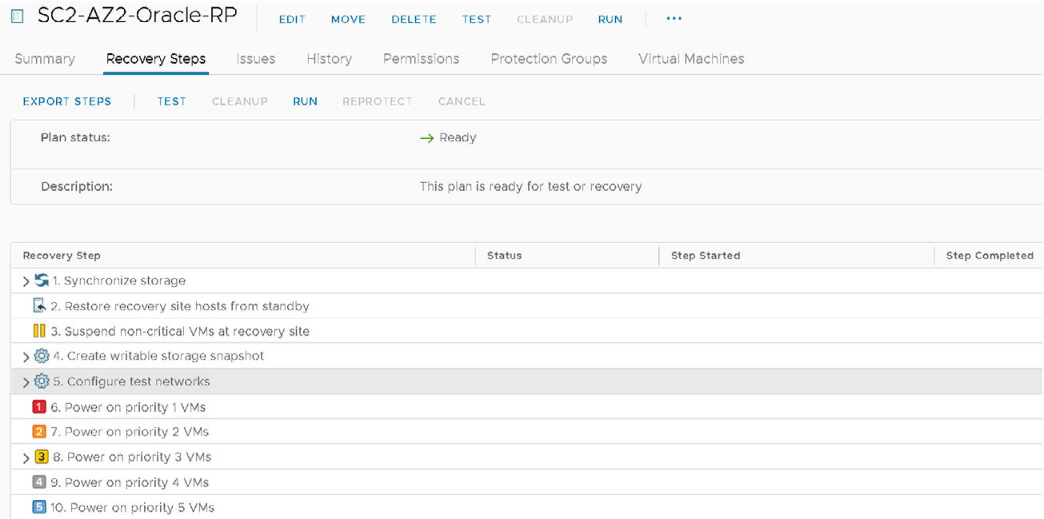
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

FIGURE 188. Cleanup Test Recovery Plan SC2-AZ2-Oracle-RP

The cleanup of test recovery is successful.



SC2-AZ2-Oracle-RP
EDIT MOVE DELETE TEST CLEANUP RUN ...
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS TEST CLEANUP RUN REPROTECT CANCEL

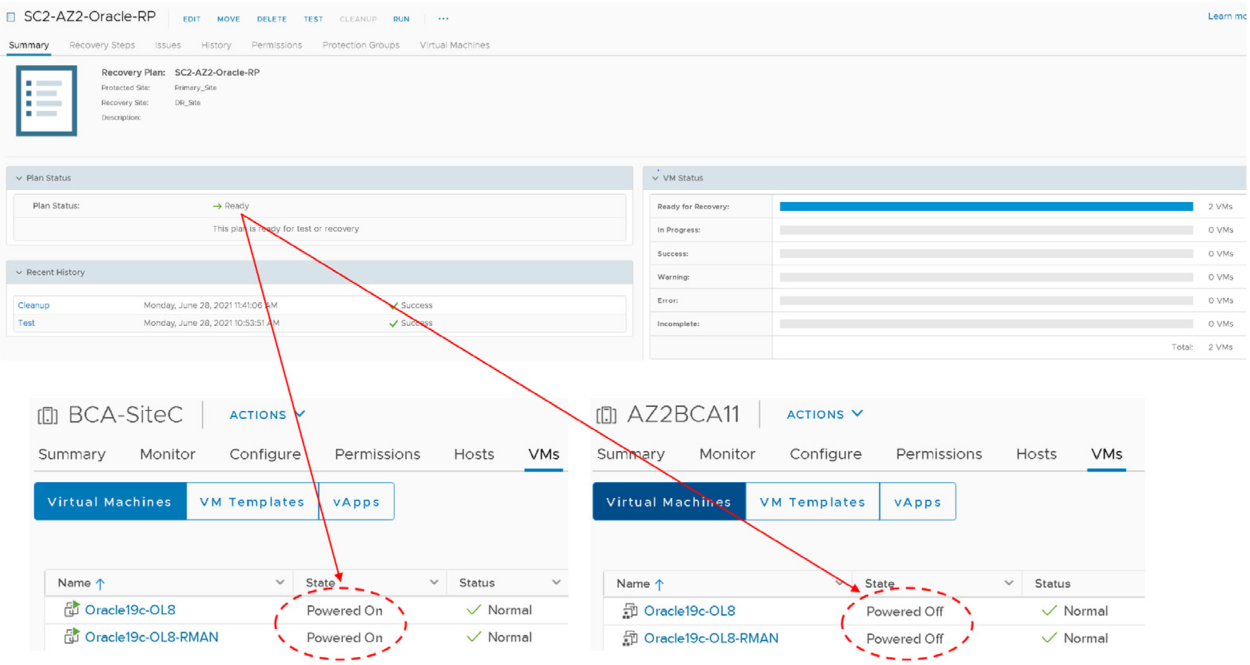
Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage			
2. Restore recovery site hosts from standby			
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot			
5. Configure test networks			
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs			
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

FIGURE 189. Steps to Cleanup Test Recovery Plan SC2-AZ2-Oracle-RP

VMs on Protected Site A are still powered on. We can see the placeholder VMs on recovery Site B are powered off.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Cleanup	Monday, June 28, 2021 11:41:06 AM	✓ Success
Test	Monday, June 28, 2021 10:53:51 AM	✓ Success

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

BCA-SiteC

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal

AZ2BCA11

Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal

FIGURE 190. Cleanup Test Recovery Plan SC2-AZ2-Oracle-RP Successful

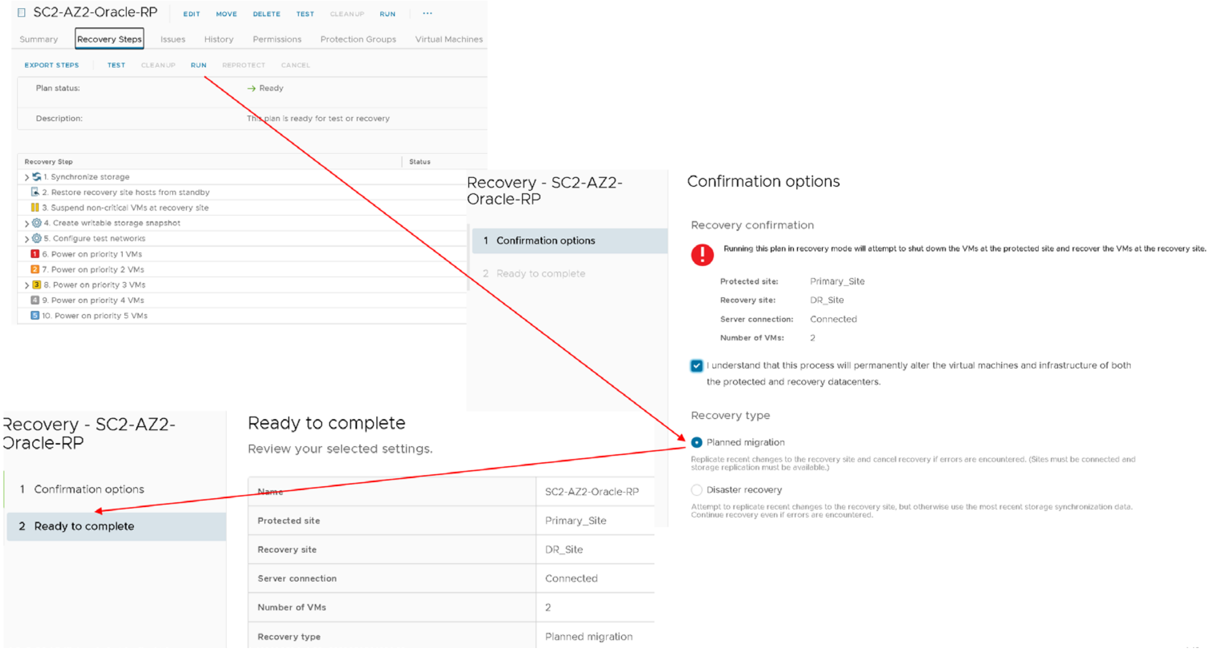
More information regarding testing a recovery plan can be found in the *VMware Site Recovery Manager guide*.

Run Recovery Plan for Planned Migration

Performing a planned migration or disaster recovery by running a recovery plan will result in VM migration from the protected site to the recovery site. If the protected site suffers an unforeseen event that might result in data loss, the recovery plan can also be run under unplanned circumstances.

Planned migration – During a planned migration, Site Recovery Manager synchronizes the VM data on the recovery site with the VMs on the protected site. Site Recovery Manager attempts to shut down the protected VMs gracefully and performs a final synchronization to prevent data loss, then powers on the VMs on the recovery site. If errors occur during a planned migration, the plan stops so that the errors can be resolved, and the plan rerun.

Steps to run a planned migration of recovery plan **SC2-AZ2-Oracle-RP** are as shown below:



Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status
1. Synchronize storage	
2. Restore recovery site hosts from standby	
3. Suspend non-critical VMs at recovery site	
4. Create writable storage snapshot	
5. Configure test networks	
6. Power on priority 1 VMs	
7. Power on priority 2 VMs	
8. Power on priority 3 VMs	
9. Power on priority 4 VMs	
10. Power on priority 5 VMs	

Recovery - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	2

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

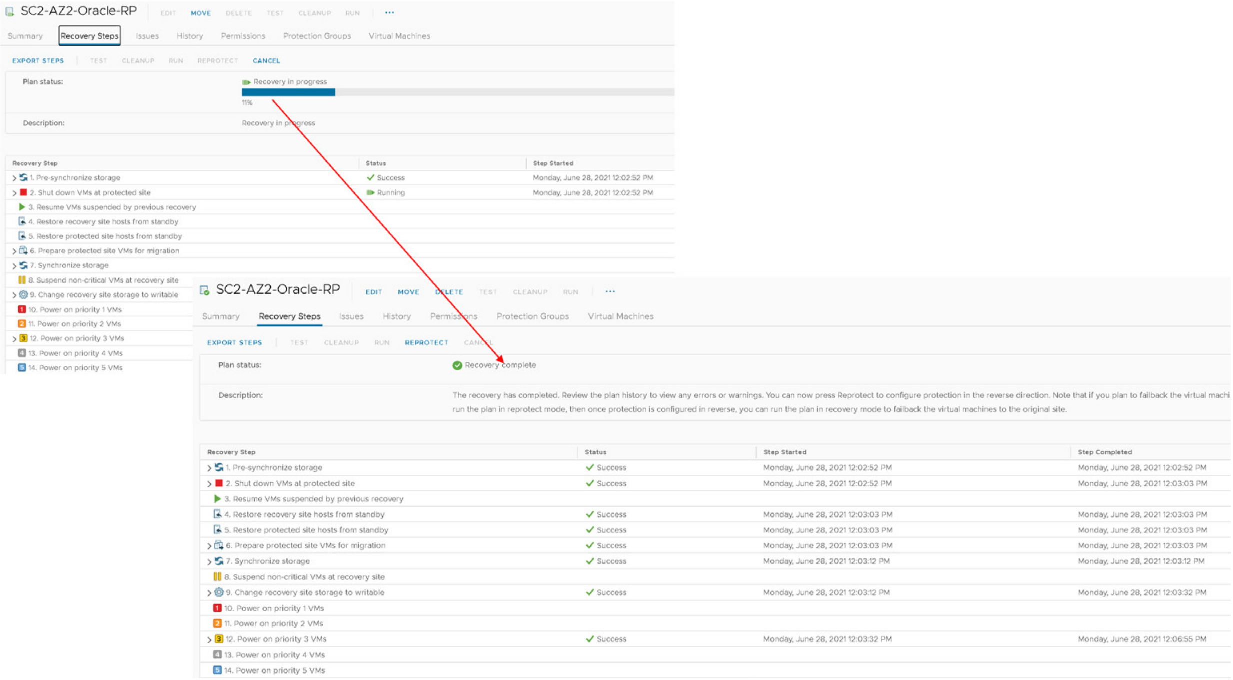
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	2
Recovery type	Planned migration

FIGURE 191. Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP

Planned migration of recovery plan **SC2-AZ2-Oracle-RP** completes successfully.



Plan status: Recovery in progress 11%

Description: Recovery in progress

Recovery Step	Status	Step Started
1. Pre-synchronize storage	✓ Success	Monday, June 28, 2021 12:02:52 PM
2. Shut down VMs at protected site	Running	Monday, June 28, 2021 12:02:52 PM
3. Resume VMs suspended by previous recovery		
4. Restore recovery site hosts from standby		
5. Restore protected site hosts from standby		
6. Prepare protected site VMs for migration		
7. Synchronize storage		
8. Suspend non-critical VMs at recovery site		
9. Change recovery site storage to writable		
10. Power on priority 1 VMs		
11. Power on priority 2 VMs		
12. Power on priority 3 VMs		
13. Power on priority 4 VMs		
14. Power on priority 5 VMs		

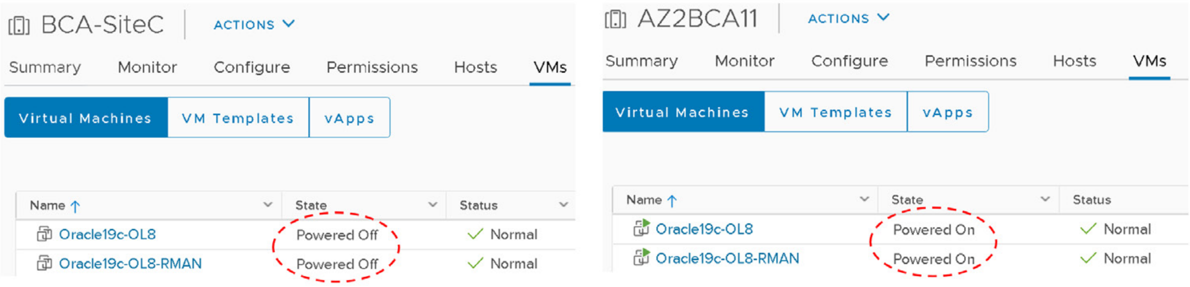
Plan status: ✓ Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machi run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✓ Success	Monday, June 28, 2021 12:02:52 PM	Monday, June 28, 2021 12:02:52 PM
2. Shut down VMs at protected site	✓ Success	Monday, June 28, 2021 12:02:52 PM	Monday, June 28, 2021 12:03:03 PM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Monday, June 28, 2021 12:03:03 PM	Monday, June 28, 2021 12:03:03 PM
5. Restore protected site hosts from standby	✓ Success	Monday, June 28, 2021 12:03:03 PM	Monday, June 28, 2021 12:03:03 PM
6. Prepare protected site VMs for migration	✓ Success	Monday, June 28, 2021 12:03:03 PM	Monday, June 28, 2021 12:03:03 PM
7. Synchronize storage	✓ Success	Monday, June 28, 2021 12:03:12 PM	Monday, June 28, 2021 12:03:12 PM
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✓ Success	Monday, June 28, 2021 12:03:12 PM	Monday, June 28, 2021 12:03:32 PM
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
12. Power on priority 3 VMs	✓ Success	Monday, June 28, 2021 12:03:32 PM	Monday, June 28, 2021 12:06:55 PM
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

FIGURE 192. Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP in Process

Planned migration of recovery plan **SC2-AZ2-Oracle-RP** is successful. Protected Site A VMs are powered off and Recovery Site B VMs are powered on.



BCA-SiteC

Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal

AZ2BCA11

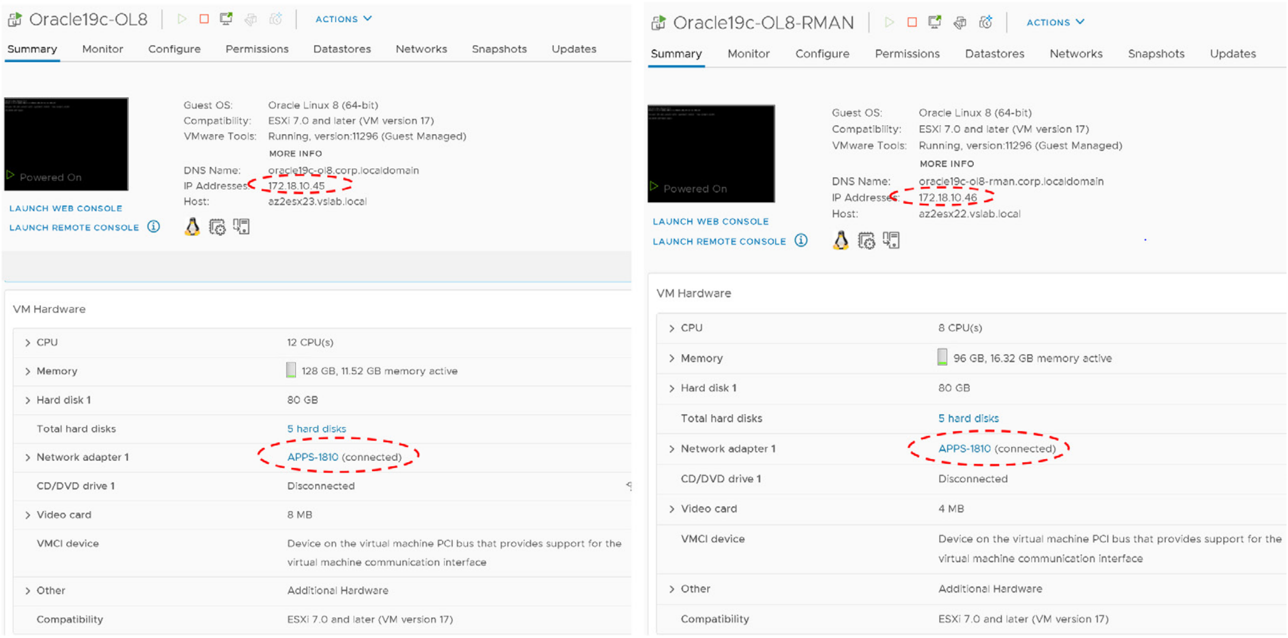
Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal

FIGURE 193. Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP VM Status

Recovery Site B Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined per network mappings to recovery network **APPS-1810**.

As in the case of testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database vvol19c is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected. The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

As mentioned earlier, **write-order fidelity is guaranteed with vSphere Replication on the disks or VMDKs that comprise a VM**.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.corp.localdomain
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local

VM Hardware

> CPU	12 CPU(s)
> Memory	128 GB, 11.52 GB memory active
> Hard disk 1	80 GB
Total hard disks	5 hard disks
> Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
> Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
> Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Oracle19c-OL8-RMAN

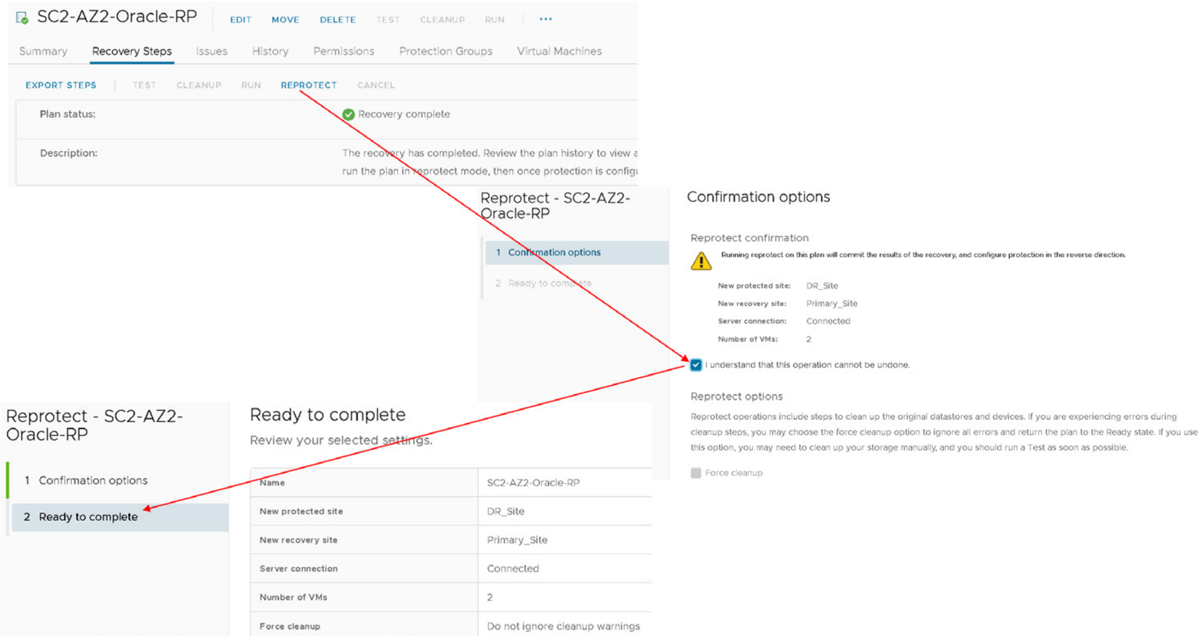
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx22.vslab.local

VM Hardware

> CPU	8 CPU(s)
> Memory	96 GB, 16.32 GB memory active
> Hard disk 1	80 GB
Total hard disks	5 hard disks
> Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
> Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
> Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 194. After Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP VM Networking

At the successful completion of the planned migration, run **Reprotect** to protect Site B, which is now the new protected site.



SC2-AZ2-Oracle-RP

EDIT MOVE DELETE TEST CLEANUP RUN ···
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS | TEST CLEANUP RUN REPROTECT CANCEL

Plan status: Recovery complete

Description: The recovery has completed. Review the plan history to view a
run the plan in reprotect mode, then once protection is configu

Reprotect - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: DR_Site

New recovery site: Primary_Site

Server connection: Connected

Number of VMs: 2

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

☐ Force cleanup

Reprotect - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

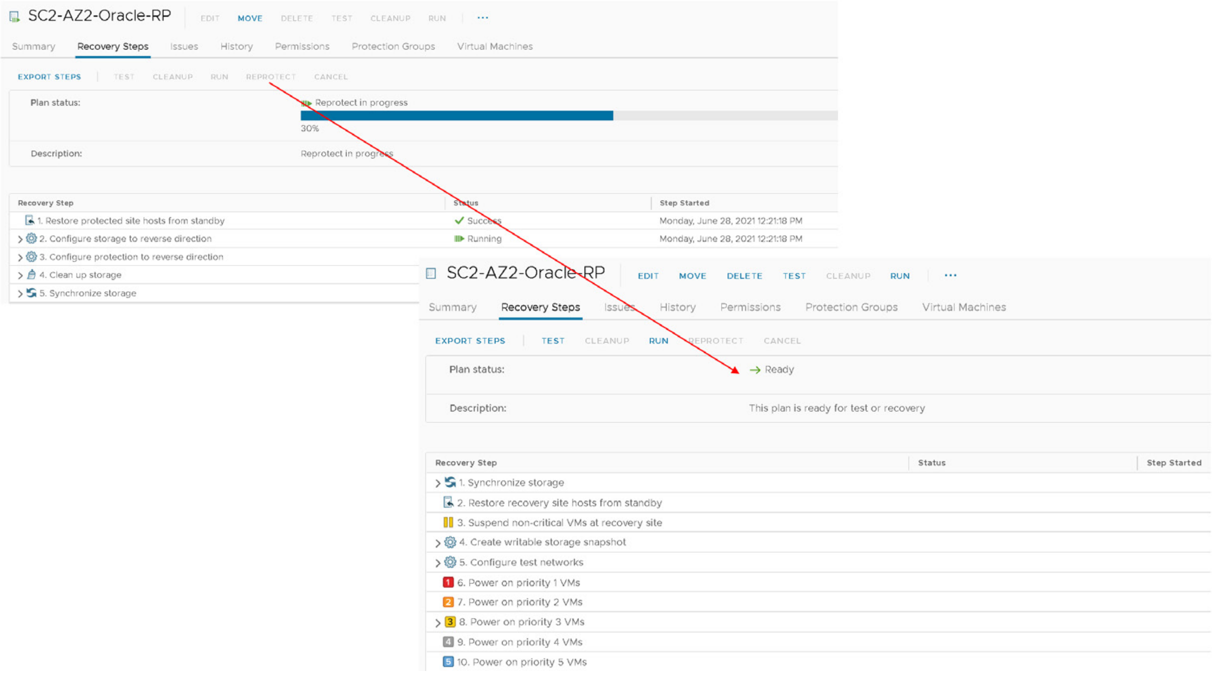
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
New protected site	DR_Site
New recovery site	Primary_Site
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

FIGURE 195. Reprotect VMs after Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP

Reprotection of VMs after planned migration of recovery plan **SC2-AZ2-Oracle-RP** is as shown below:



SC2-AZ2-Oracle-RP

EDIT MOVE DELETE TEST CLEANUP RUN ···
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS | TEST CLEANUP RUN REPROTECT CANCEL

Plan status: Reprotect in progress

30%

Description: Reprotect in progress

Recovery Step	Status	Step Started
1. Restore protected site hosts from standby	✓ Success	Monday, June 28, 2021 12:21:18 PM
2. Configure storage to reverse direction	Running	Monday, June 28, 2021 12:21:18 PM
3. Configure protection to reverse direction		
4. Clean up storage		
5. Synchronize storage		

SC2-AZ2-Oracle-RP

EDIT MOVE DELETE TEST CLEANUP RUN ···
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS | TEST CLEANUP RUN REPROTECT CANCEL

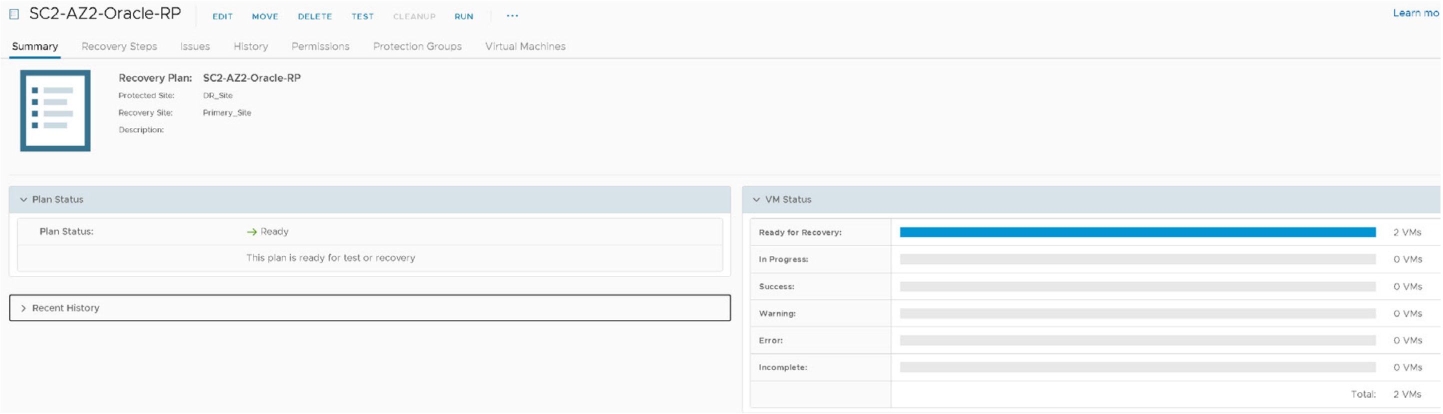
Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby		
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
5. Configure test networks		
6. Power on priority 1 VMs		
7. Power on priority 2 VMs		
8. Power on priority 3 VMs		
9. Power on priority 4 VMs		
10. Power on priority 5 VMs		

FIGURE 196. Reprotection of VMs after Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP in Progress

The reprotect step to protect the Site B is successful. Now the new protected site is Site B and the DR site is Site A.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Plan Status

Plan Status: → Ready

This plan is ready for test or recovery

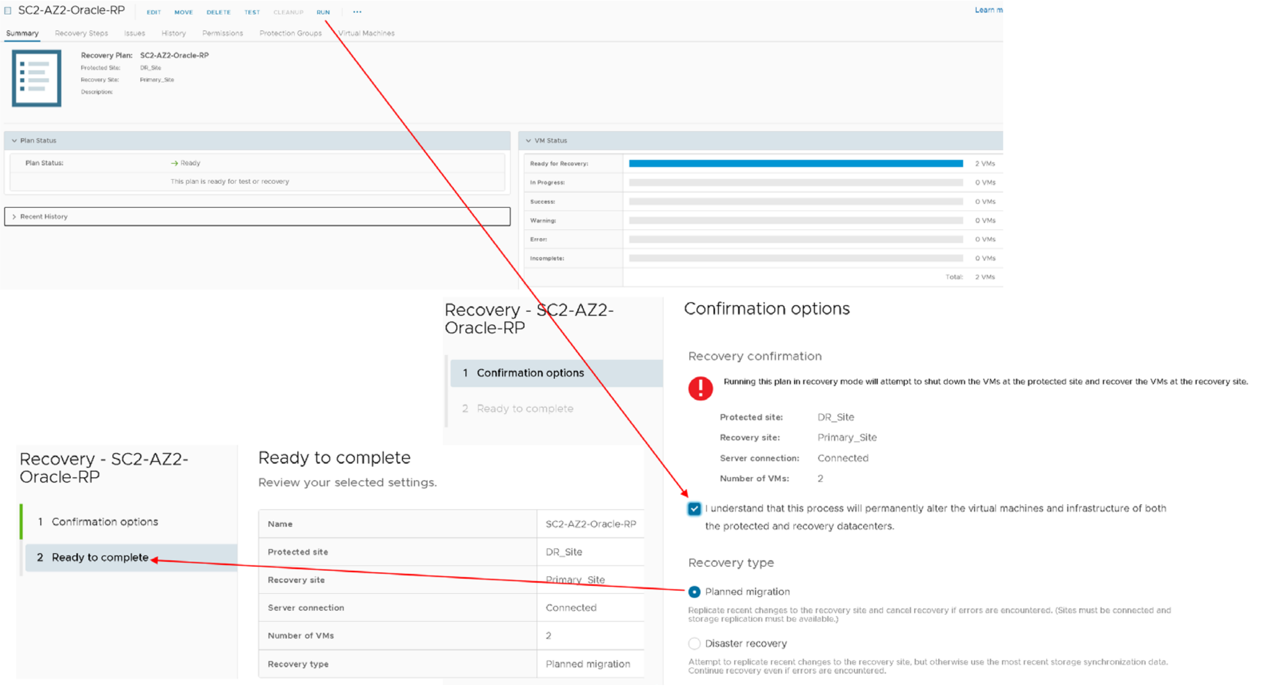
Recent History

VM Status

Ready for Recovery:		2 VMs
In Progress:		0 VMs
Success:		0 VMs
Warning:		0 VMs
Error:		0 VMs
Incomplete:		0 VMs
	Total:	2 VMs

FIGURE 197. Reprotection of VMs after Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP Successful

Run another planned migration to switch the protected site from Site B back to Site A.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Plan Status

Plan Status: → Ready

This plan is ready for test or recovery

Recent History

VM Status

Ready for Recovery:		2 VMs
In Progress:		0 VMs
Success:		0 VMs
Warning:		0 VMs
Error:		0 VMs
Incomplete:		0 VMs
	Total:	2 VMs

Recovery - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: DR_Site
Recovery site: Primary_Site
Server connection: Connected
Number of VMs: 2

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

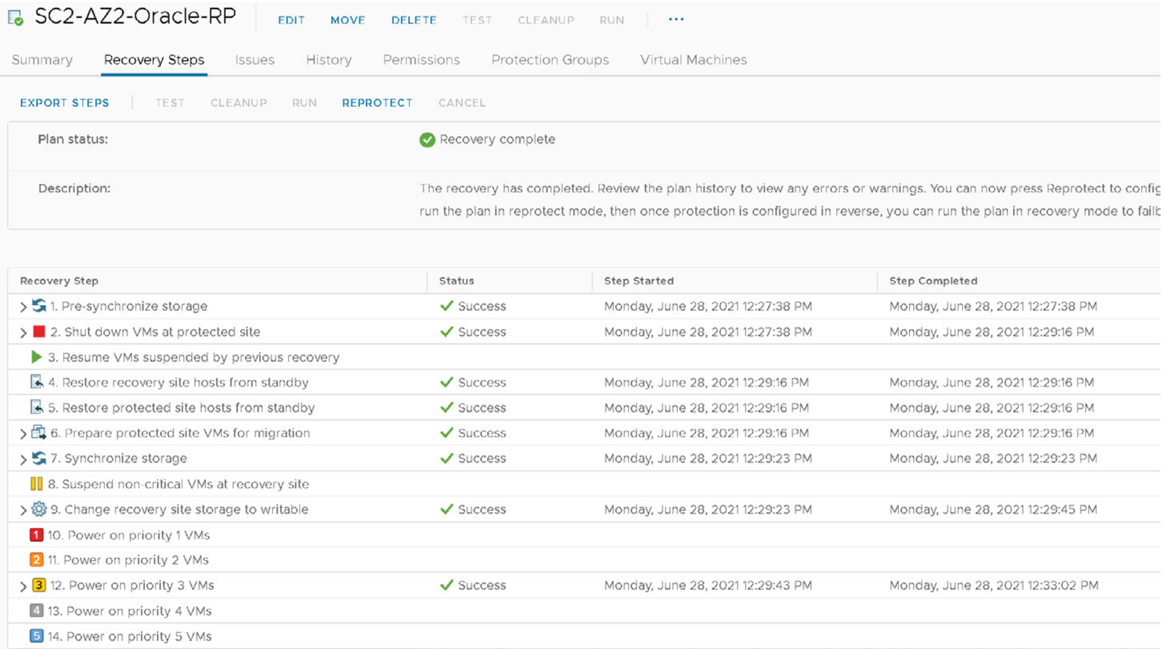
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
Protected site	DR_Site
Recovery site	Primary_Site
Server connection	Connected
Number of VMs	2
Recovery type	Planned migration

FIGURE 198. Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP from Site B to Site A

The planned migration from Site B to Site A is successful.



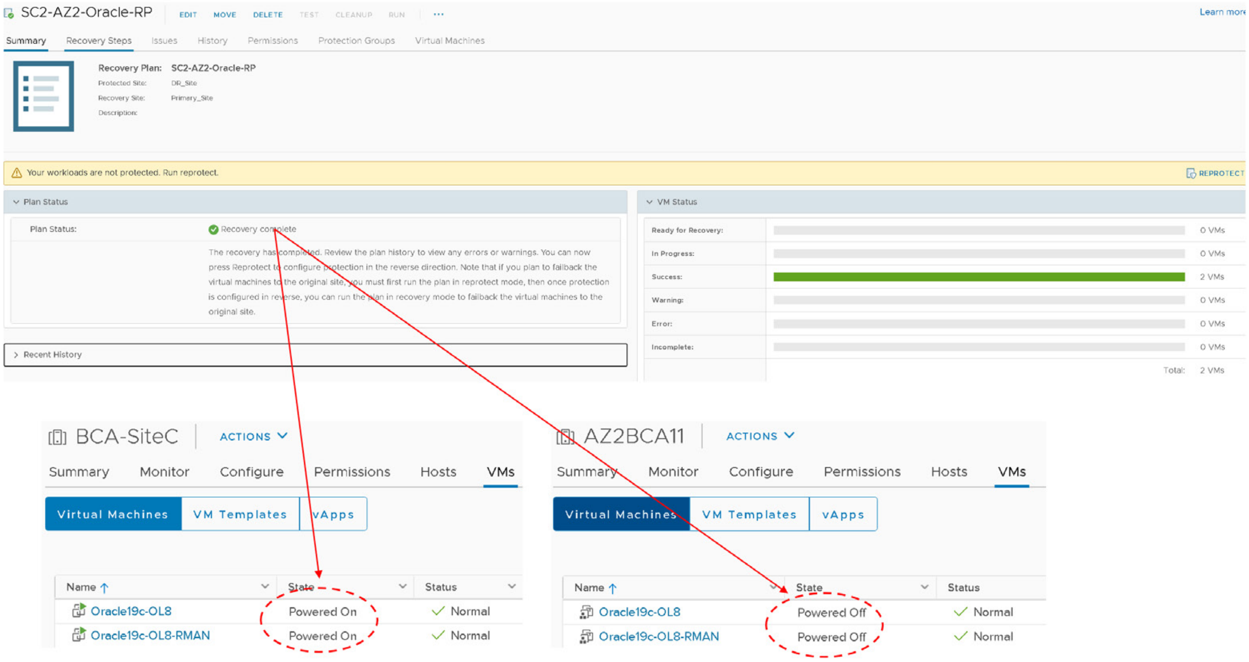
Plan status: ✓ Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to config
run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failb

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✓ Success	Monday, June 28, 2021 12:27:38 PM	Monday, June 28, 2021 12:27:38 PM
2. Shut down VMs at protected site	✓ Success	Monday, June 28, 2021 12:27:38 PM	Monday, June 28, 2021 12:29:16 PM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Monday, June 28, 2021 12:29:16 PM	Monday, June 28, 2021 12:29:16 PM
5. Restore protected site hosts from standby	✓ Success	Monday, June 28, 2021 12:29:16 PM	Monday, June 28, 2021 12:29:16 PM
6. Prepare protected site VMs for migration	✓ Success	Monday, June 28, 2021 12:29:16 PM	Monday, June 28, 2021 12:29:16 PM
7. Synchronize storage	✓ Success	Monday, June 28, 2021 12:29:23 PM	Monday, June 28, 2021 12:29:23 PM
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✓ Success	Monday, June 28, 2021 12:29:23 PM	Monday, June 28, 2021 12:29:45 PM
1 10. Power on priority 1 VMs			
2 11. Power on priority 2 VMs			
3 12. Power on priority 3 VMs	✓ Success	Monday, June 28, 2021 12:29:43 PM	Monday, June 28, 2021 12:33:02 PM
4 13. Power on priority 4 VMs			
5 14. Power on priority 5 VMs			

FIGURE 199. Planned Migration of Recovery Plan SC2-AZ2-Oracle-RP from Site B to Site A steps

VMs on Protected Site A vVOL datastore **OraVVOL** are powered back on and we see the VMs on Recovery Site B are powered off.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: ✓ Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	2 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

BCA-SiteC

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal

AZ2BCA11

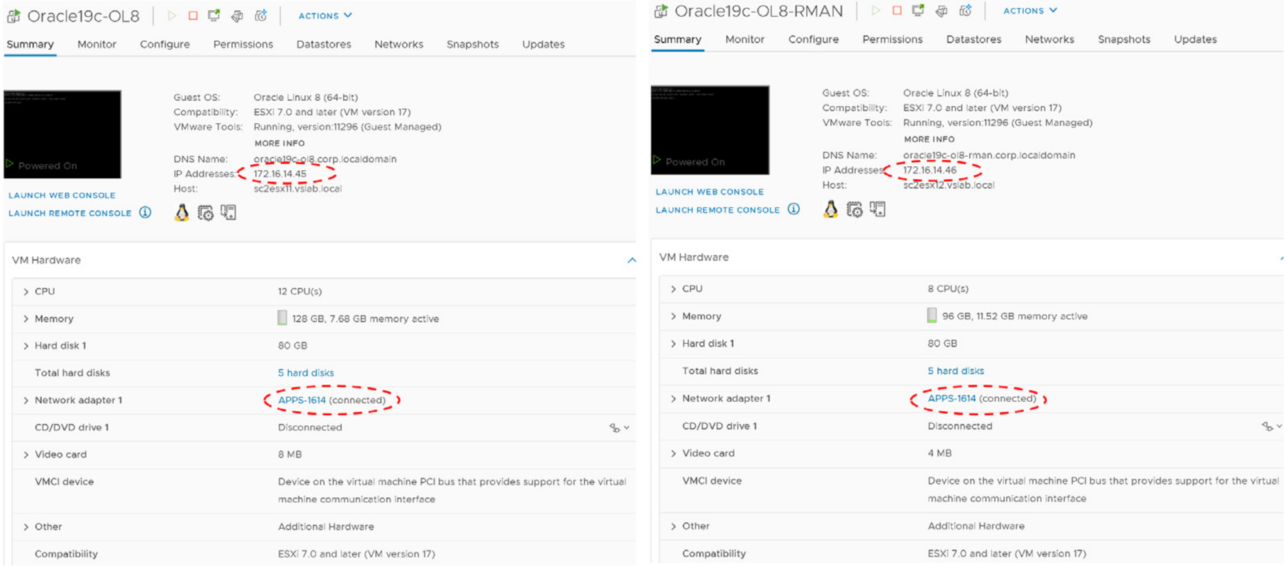
Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal

FIGURE 200. VM Status after Planed Migration from Site B to Site A

Site A Oracle VM **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined per network mappings to primary network **APPS-1614**.

As in the case of testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.16.14.45 and the database vvol19c is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.16.14.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.corp.localdomain
IP Addresses: 172.16.14.45
Host: sc2esx11.vslab.local

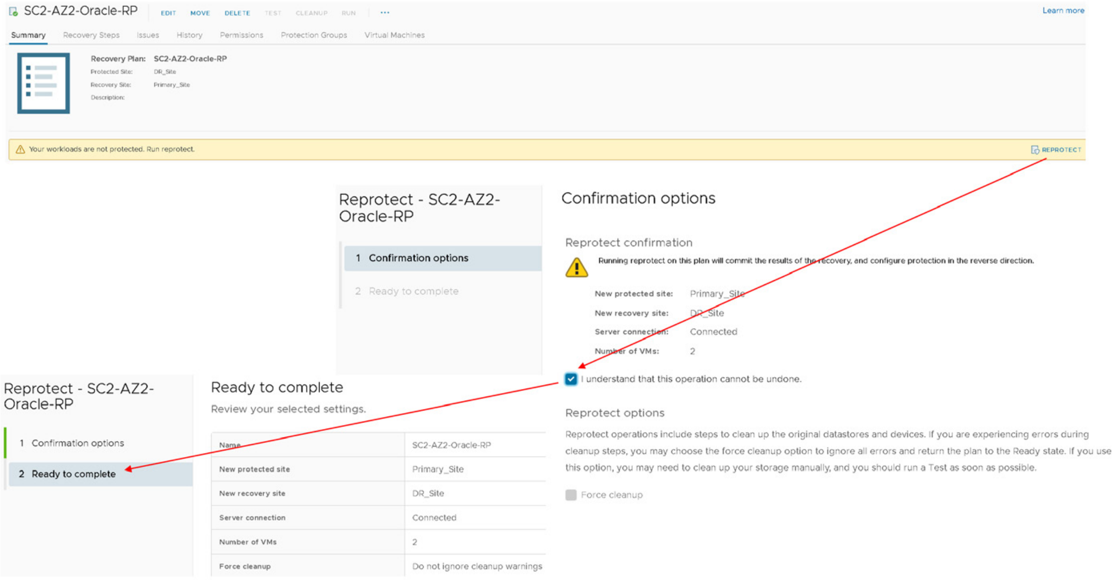
CPU	12 CPU(s)
Memory	128 GB, 7.68 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.corp.localdomain
IP Addresses: 172.16.14.46
Host: sc2esx12.vslab.local

CPU	8 CPU(s)
Memory	96 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 201. VM Networking Details after Planed Migration from Site B to Site A

Run **Reprotect** to reprotect the VMs on the Protected Site A.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Your workloads are not protected. Run reprotect.

Reprotect - SC2-AZ2-Oracle-RP

1 Confirmation options
2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: Primary_Site
New recovery site: DR_Site
Server connection: Connected
Number of VMs: 2

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-RP

1 Confirmation options
2 Ready to complete

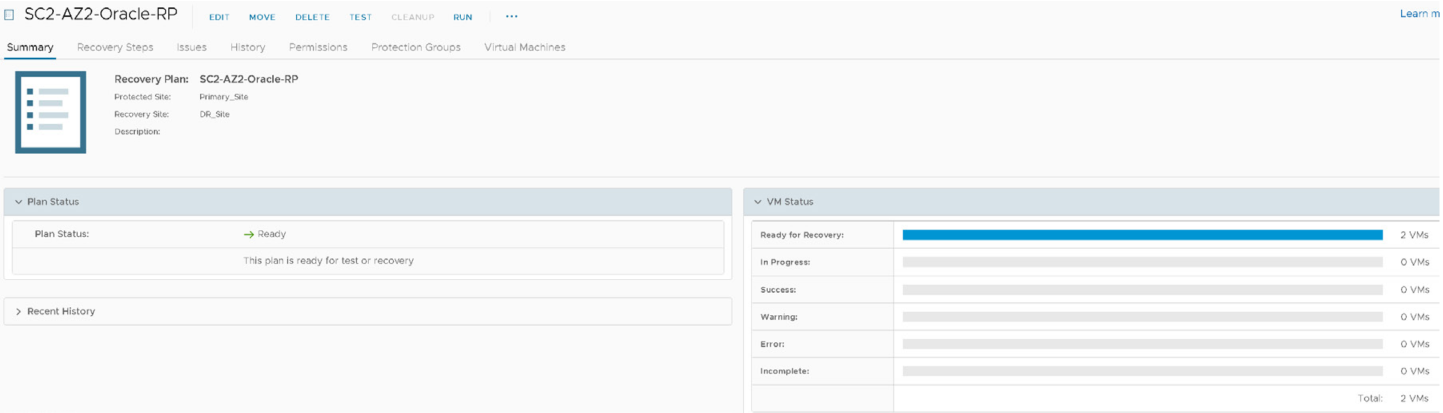
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
New protected site	Primary_Site
New recovery site	DR_Site
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

FIGURE 202. Reprotect Site A VMs After Failback

Reprotection of Protected Site A vVOL VMs successful.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

FIGURE 203. Reprotect Site A VMs After Failback Successful

More information regarding running a planned migration can be found in the *VMware Site Recovery Manager guide*.

Run Recovery Plan for Disaster Recovery

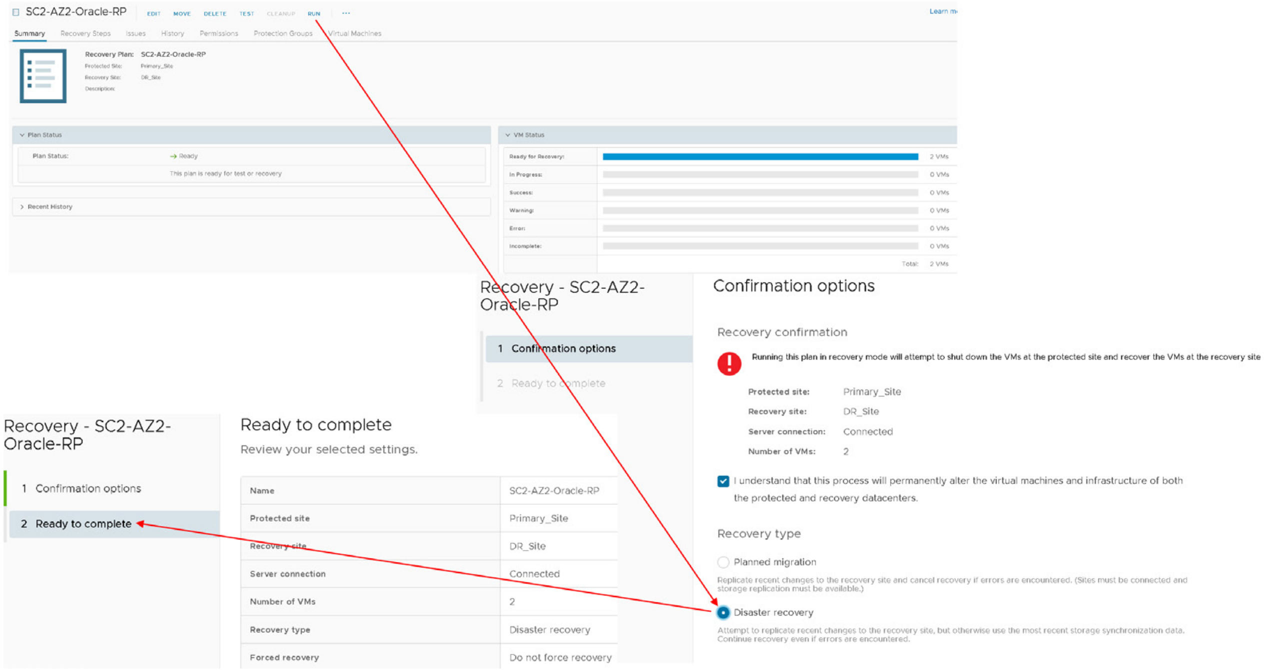
Disaster Recovery – During a disaster recovery, Site Recovery Manager first attempts a storage synchronization. If it succeeds, Site Recovery Manager uses the synchronized storage state to recover VMs on the recovery site to their most recent available state, according to the recovery point objective (RPO) that you set when you configure replication.

When you run a recovery plan to perform a disaster recovery, Site Recovery Manager attempts to shut down the VMs on the protected site. If Site Recovery Manager cannot shut down the VMs, Site Recovery Manager still powers on the copies at the recovery site.

In case the protected site comes back online after disaster recovery, the recovery plan goes into an inconsistent state, where production VMs are running on both sites, known as a split-brain scenario. Site Recovery Manager detects this state, and you can run the plan again to power off the VMs on the protected site. The recovery plan then returns to a consistent state, and you can run reprotect.

If Site Recovery Manager detects that a datastore on the protected site is in all paths down (APD) state and is preventing a VM from shutting down, Site Recovery Manager waits for a period before attempting to shut down the VM again. The APD state is usually transient, so by waiting for a datastore in the APD state to come back online, Site Recovery Manager can gracefully shut down the protected VMs on that datastore.

Steps to run a disaster recovery scenario of recovery plan **SC2-AZ2-Oracle-RP** are as shown below:



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Ready for Recovery:		2 VMs
In Progress:		0 VMs
Success:		0 VMs
Warning:		0 VMs
Error:		0 VMs
Incomplete:		0 VMs
	Total:	2 VMs

Recovery - SC2-AZ2-Oracle-RP
1 Confirmation options
2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	2

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

○ Planned migration
Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

● Disaster recovery
Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

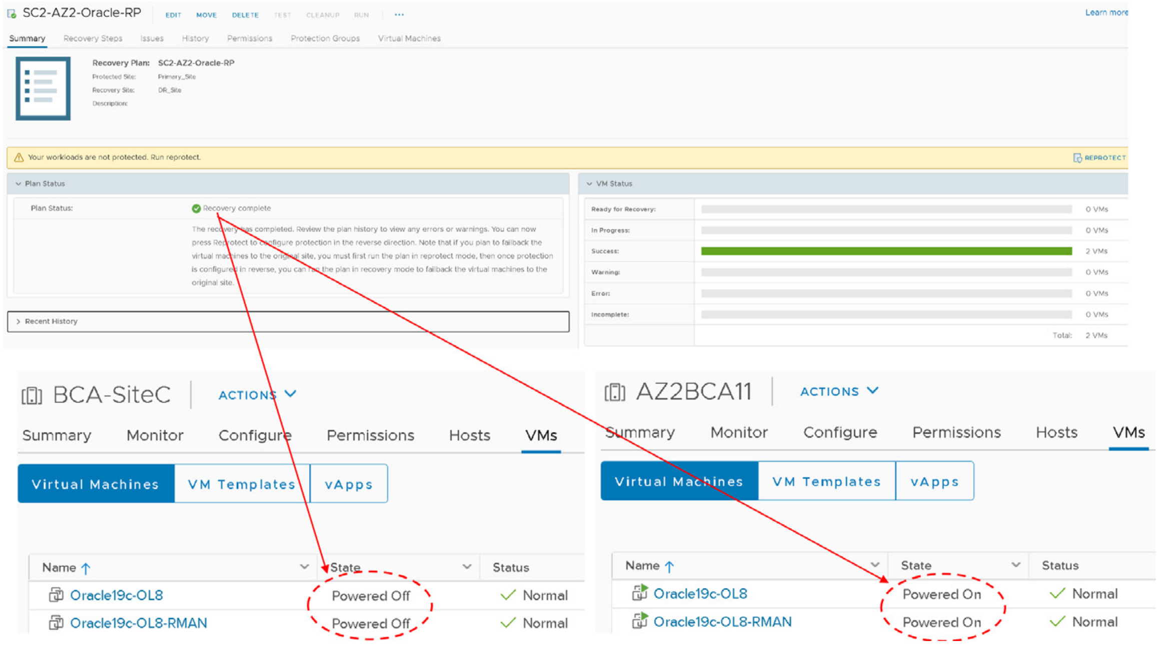
Recovery - SC2-AZ2-Oracle-RP
1 Confirmation options
2 Ready to complete

Ready to complete
Review your selected settings.

Name	SC2-AZ2-Oracle-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	2
Recovery type	Disaster recovery
Forced recovery	Do not force recovery

FIGURE 204. Disaster Recovery Use Case for Recovery Plan SC2-AZ2-Oracle-RP

Disaster recovery of recovery plan **SC2-AZ2-Oracle-RP** is successful. Protected Site A VMs are powered off and Recovery Site B VMs are powered on.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete
The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to fallback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to fallback the virtual machines to the original site.

Ready for Recovery:		0 VMs
In Progress:		0 VMs
Success:		2 VMs
Warning:		0 VMs
Error:		0 VMs
Incomplete:		0 VMs
	Total:	2 VMs

BCA-SiteC

Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal

AZ2BCA11

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal

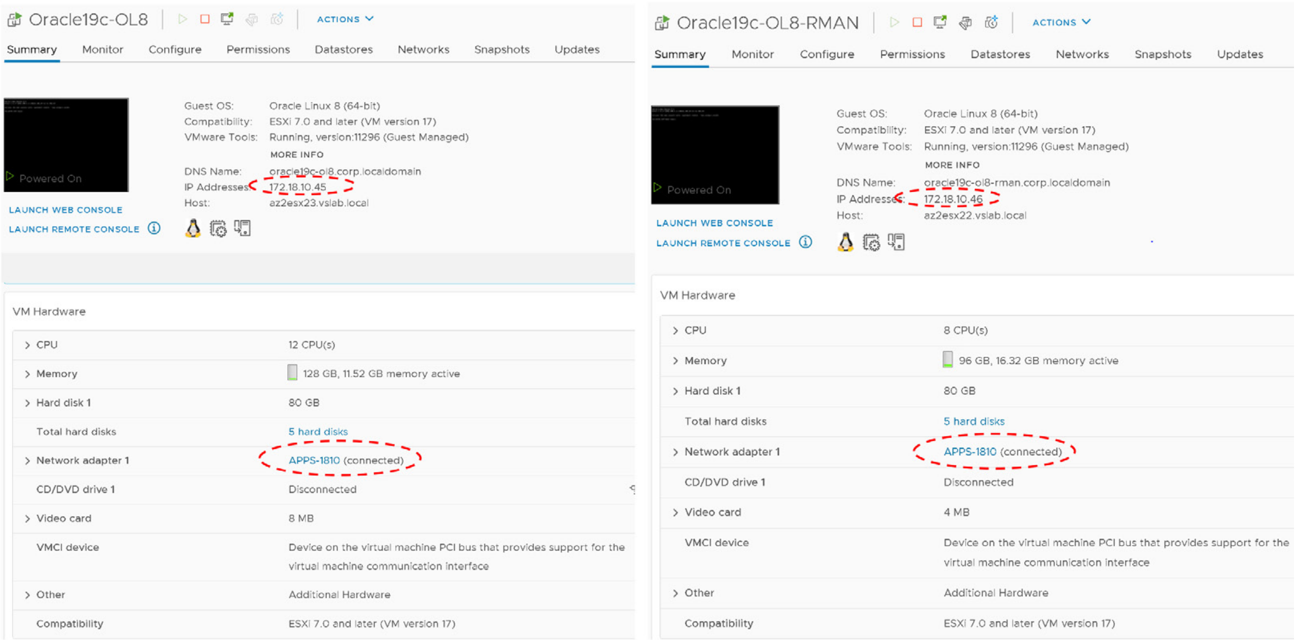
FIGURE 205. VM's Status after Disaster Recovery Run of Recovery Plan SC2-AZ2-Oracle-RP

Recovery Site B Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined per network mappings to recovery network **APPS-1810**.

As in the case of testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database vvol19c is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

As mentioned earlier, **write-order fidelity is guaranteed with vSphere Replication on the disks or VMDKs that comprise a VM**.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.corp.localdomain
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx22.vslab.local

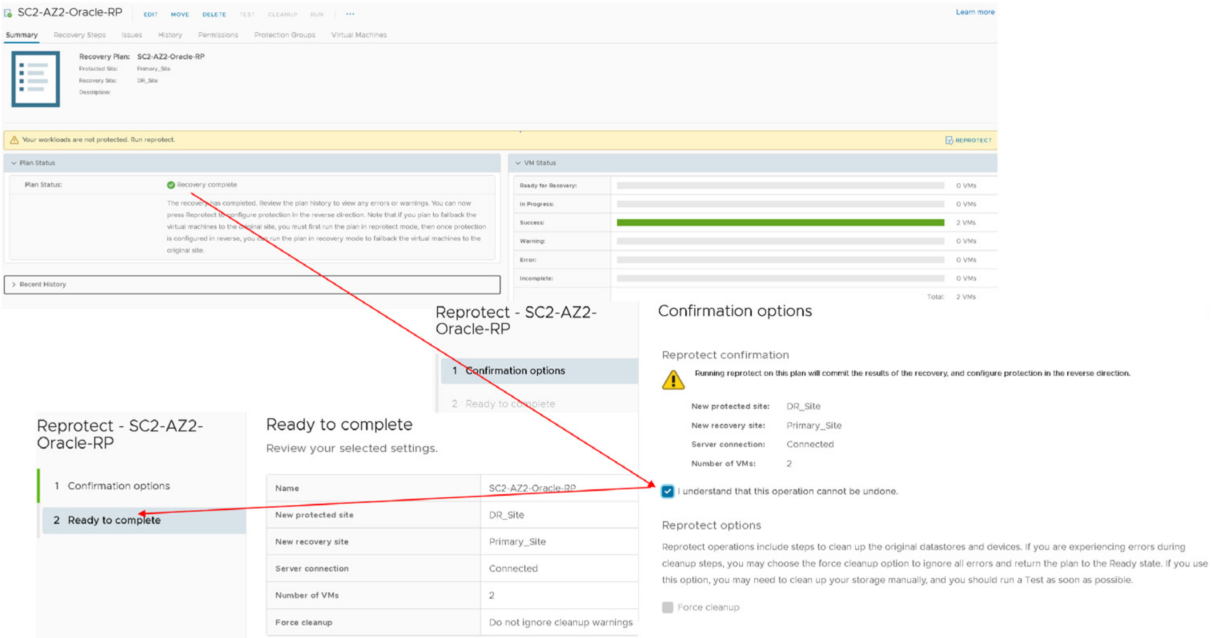
VM Hardware

CPU	8 CPU(s)
Memory	96 GB, 16.32 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 206. VM's Networking Status After Disaster Recovery Run of Recovery Plan SC2-AZ2-Oracle-RP

In event of real disaster, Site A may not be available. This use case is a DR exercise, so Site A is available in this instance.

After the successful completion of the disaster recovery exercise and ensuring that Site A is back operationally, run **Reprotect** to protect Site B, which is now the new protected site.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	2 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

Reprotect - SC2-AZ2-Oracle-RP

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: DR_Site
New recovery site: Primary_Site
Server connection: Connected
Number of VMs: 2

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-RP

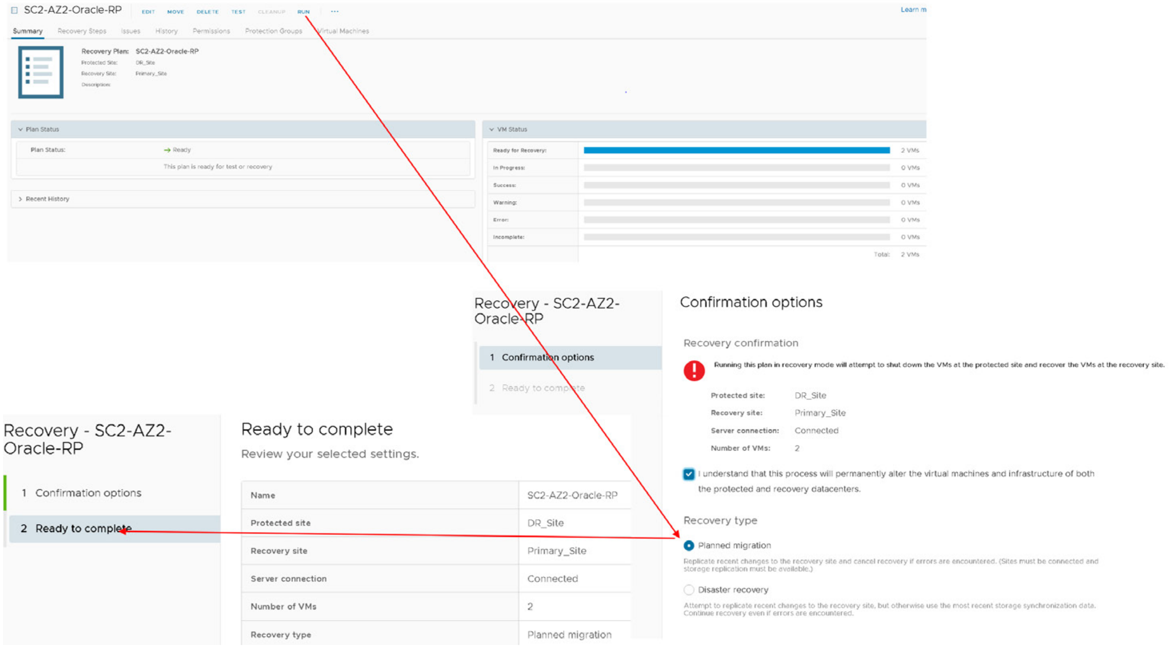
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
New protected site	DR_Site
New recovery site	Primary_Site
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

FIGURE 207. Reprotect Site B VMs

Run a planned migration to switch the protected site from Site B back to Site A.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Plan Status: Ready

This plan is ready for test or recovery

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

Recovery - SC2-AZ2-Oracle-RP

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: DR_Site
Recovery site: Primary_Site
Server connection: Connected
Number of VMs: 2

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-RP

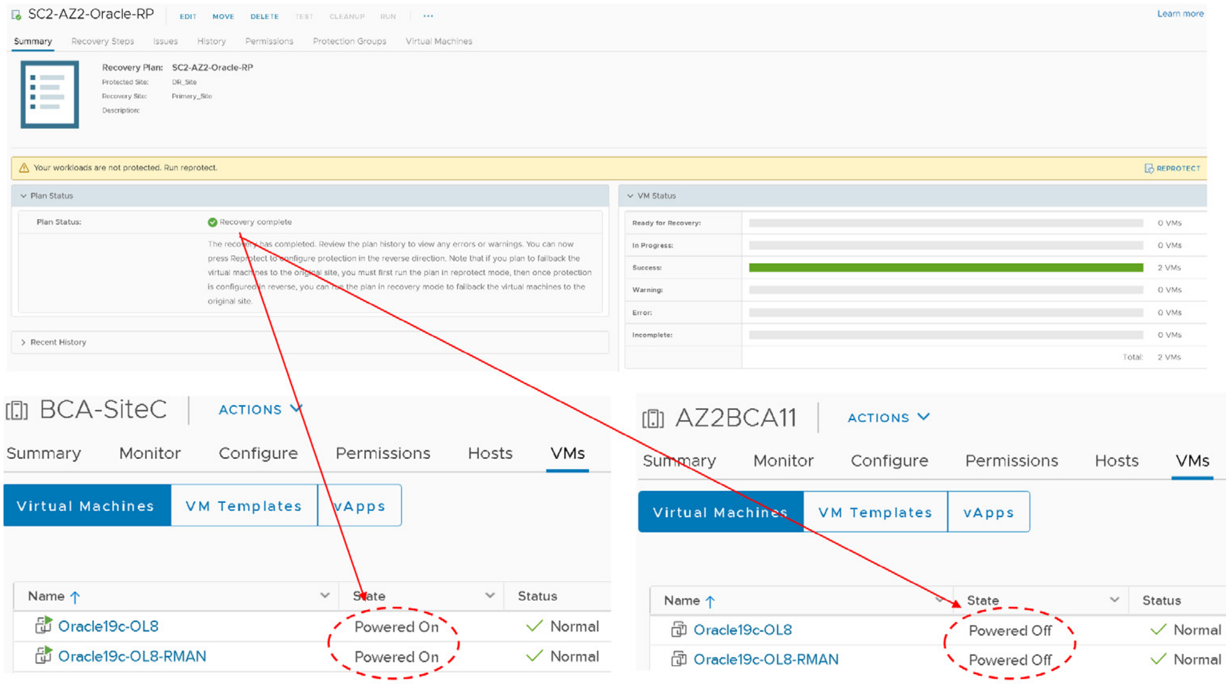
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
Protected site	DR_Site
Recovery site	Primary_Site
Server connection	Connected
Number of VMs	2
Recovery type	Planned migration

FIGURE 208. Planned Migration from Site B to Site A

Planned migration from Site B to Site A is successful. VMs on Protected Site A are powered back on and we see that VMs on Recovery Site B powered off.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	2 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

BCA-SiteC

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal

AZ2BCA11

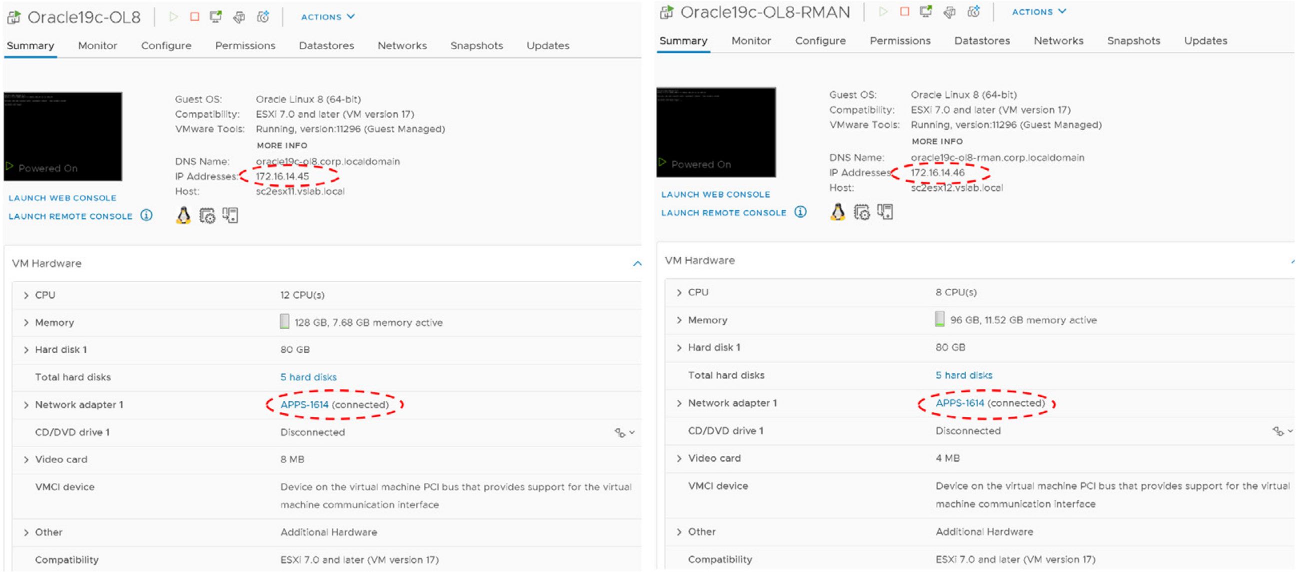
Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal

FIGURE 209. Planned Migration from Site B to Site A Successful

Site A Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined per network mappings to primary network **APPS-1614**.

As in the case of testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.16.14.45 and the database vvol19c is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.16.14.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.



Guest OS:	Oracle Linux 8 (64-bit)
Compatibility:	ESXi 7.0 and later (VM version 17)
VMware Tools:	Running, version:11296 (Guest Managed)
DNS Name:	oracle19c-ol8.corp.localdomain
IP Addresses:	172.16.14.45
Host:	sc2esx11.vslab.local

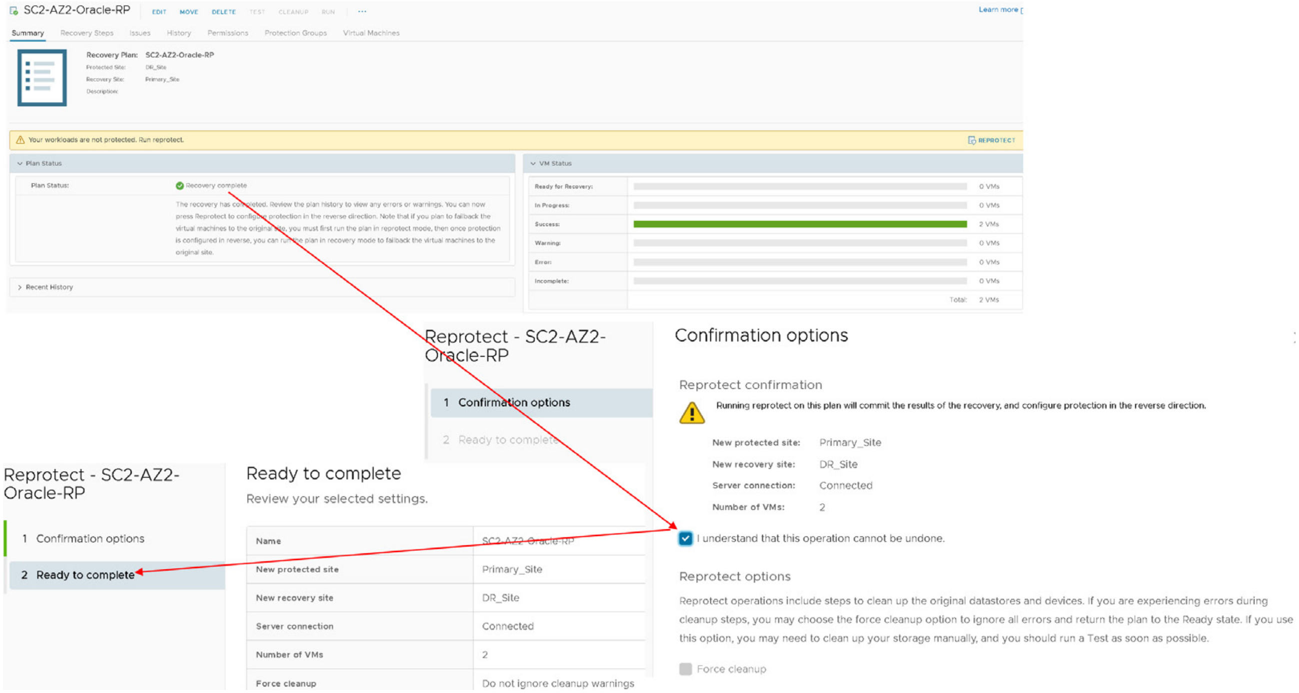
VM Hardware	
CPU	12 CPU(s)
Memory	128 GB, 7.68 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS:	Oracle Linux 8 (64-bit)
Compatibility:	ESXi 7.0 and later (VM version 17)
VMware Tools:	Running, version:11296 (Guest Managed)
DNS Name:	oracle19c-ol8-rman.corp.localdomain
IP Addresses:	172.16.14.46
Host:	sc2esx12.vslab.local

VM Hardware	
CPU	8 CPU(s)
Memory	96 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 210. VM Networking Status after Planned Migration from Site B to Site A Successful

Run **Reprotect** to reprotect the VMs on the Protected Site A.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

VM Status	
Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	2 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

Reprotect - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site:	Primary_Site
New recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	2

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-RP

1 Confirmation options

2 Ready to complete

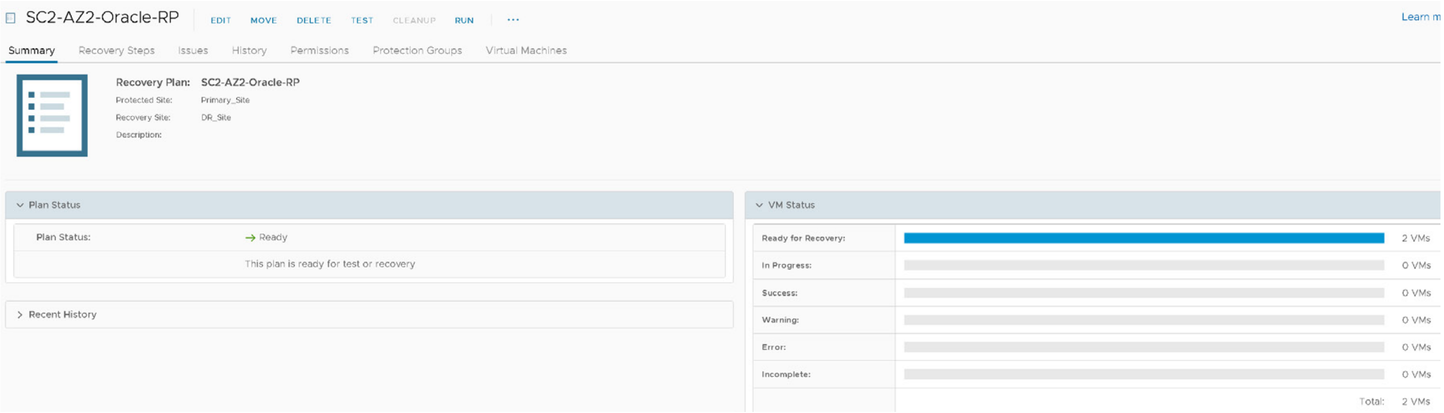
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-RP
New protected site	Primary_Site
New recovery site	DR_Site
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

FIGURE 211. Reprotect VM on Site A

Reprotection of Protected Site A VMs is successful.



Recovery Plan: SC2-AZ2-Oracle-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

FIGURE 212. Reprotect VM on Site A Successful

More information regarding the disaster recovery steps of a recovery plan can be found in the *VMware Site Recovery Manager guide*.

VMware Clouds

Site Recovery Manager along with vSphere Replication can be used to provide disaster recovery services from on-premises VMware environment to all other VMware multi-clouds including VMware Cloud on Dell EMC, Google Cloud VMware Engine (GCVE), Azure VMware Solutions (AVS), and Oracle Cloud VMware Solution (OCVS).

VMware site recovery brings VMware enterprise-class SDDC disaster recovery-as-a-service to the AWS Cloud.

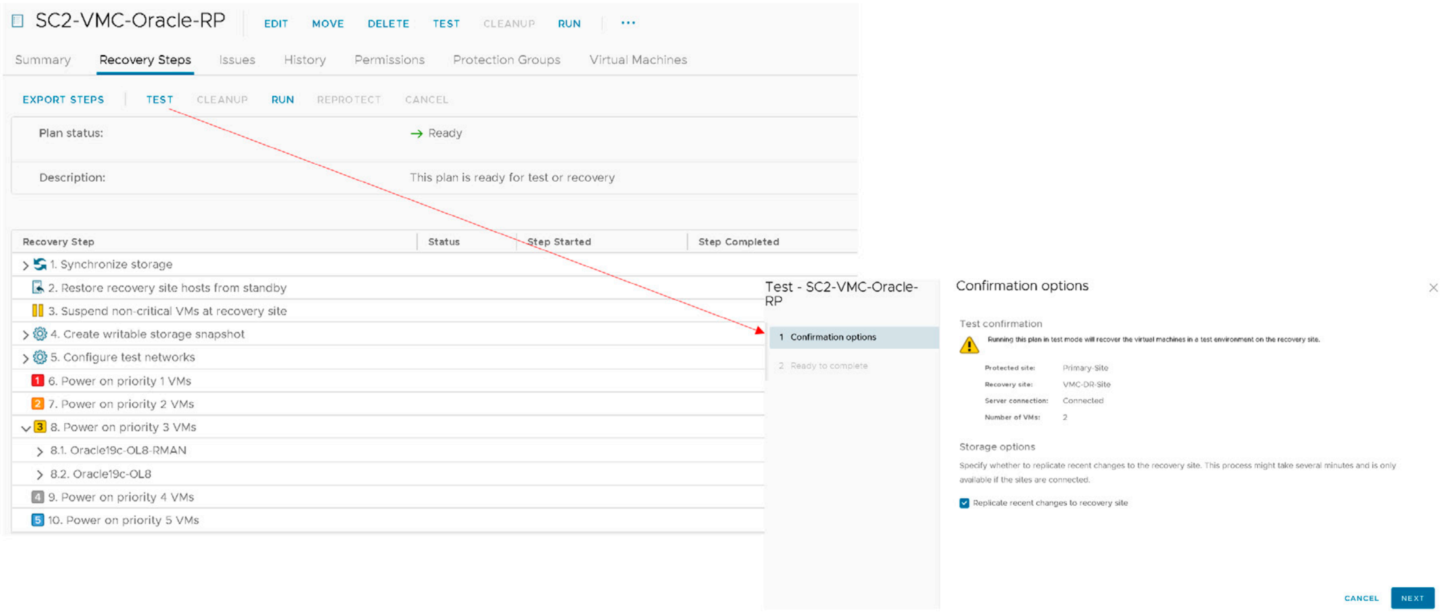
This use case focusses on utilizing VMware site recovery to provide disaster recovery to Oracle single-instance VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** from on-premises Site A to VMware Cloud on AWS.

For on-premises, this use cases provisions the Oracle VMs Oracle19c-OL8 and **Oracle19c-OL8-RMAN** on a VMFS datastore, and applies as well to NFS, VMFS, vSAN or vVOL datastores. vSphere Replication operates at a VMDK level, completely independent of underlying datastore storage characteristics.

The underlying storage in VMware Cloud on AWS and other VMware Cloud offerings is VMware hyperconverged storage (vSAN).

Test Recovery Plan

Steps to test the recovery plan **SC2-VMC-Oracle-RP** are as shown below:



Plan status: Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage			
2. Restore recovery site hosts from standby			
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot			
5. Configure test networks			
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs			
8.1. Oracle19c-OL8-RMAN			
8.2. Oracle19c-OL8			
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

Confirmation options

Test confirmation

Running this plan in test mode will recover the virtual machines in a test environment on the recovery site.

Protected site: Primary-Site
Recovery site: VMC-DR-Site
Server connection: Connected
Number of VMs: 2

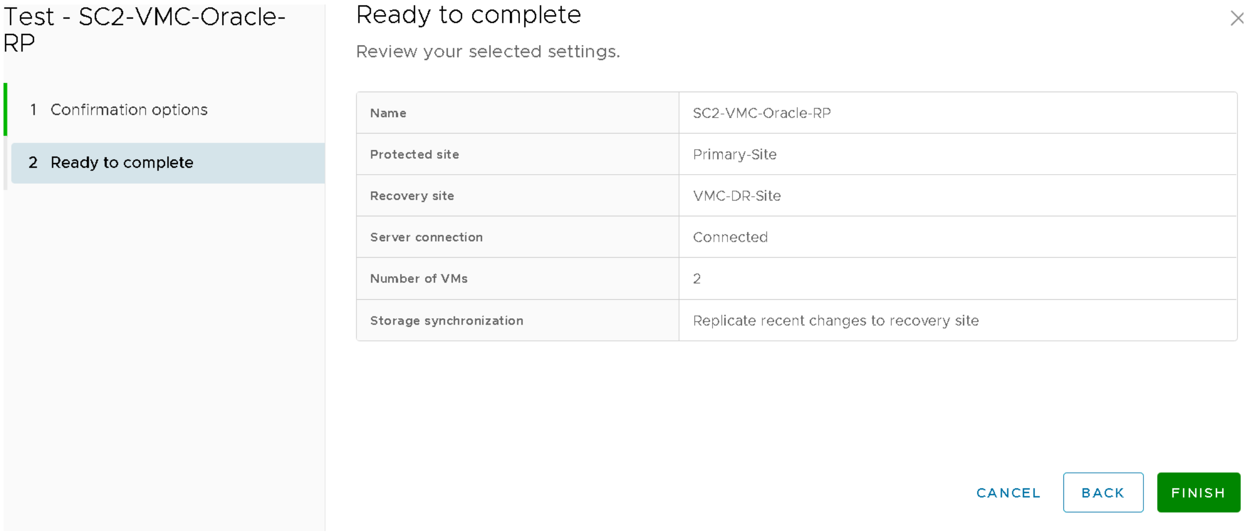
Storage options

Specify whether to replicate recent changes to the recovery site. This process might take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

FIGURE 213. Start Test Recovery Plan SC2-VMC-Oracle-RP

Confirmation of test recovery plan **SC2-VMC-Oracle-RP** is as shown below:



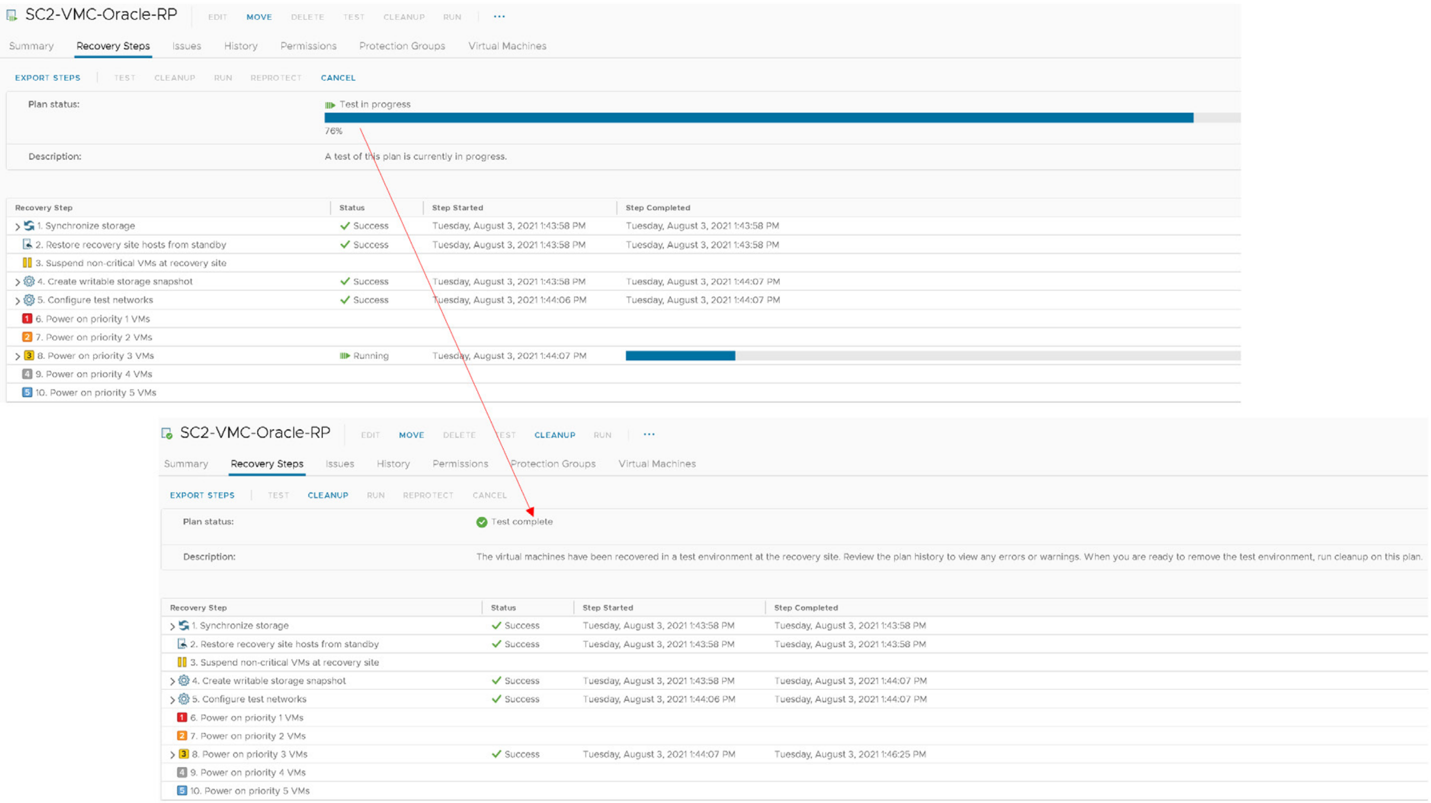
Ready to complete

Review your selected settings.

Name	SC2-VMC-Oracle-RP
Protected site	Primary-Site
Recovery site	VMC-DR-Site
Server connection	Connected
Number of VMs	2
Storage synchronization	Replicate recent changes to recovery site

FIGURE 214. Test Recovery Plan SC2-VMC-Oracle-RP Confirmation

The test of the recovery plan completes successfully.



SC2-VMC-Oracle-RP
EDIT MOVE DELETE TEST CLEANUP RUN ···
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS TEST CLEANUP RUN REPROTECT CANCEL

Plan status: Test in progress

76%

Description: A test of this plan is currently in progress.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:43:58 PM
2. Restore recovery site hosts from standby	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:43:58 PM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:44:07 PM
5. Configure test networks	✓ Success	Tuesday, August 3, 2021 1:44:06 PM	Tuesday, August 3, 2021 1:44:07 PM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	Running	Tuesday, August 3, 2021 1:44:07 PM	
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

SC2-VMC-Oracle-RP
EDIT MOVE DELETE TEST CLEANUP RUN ···
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS TEST CLEANUP RUN REPROTECT CANCEL

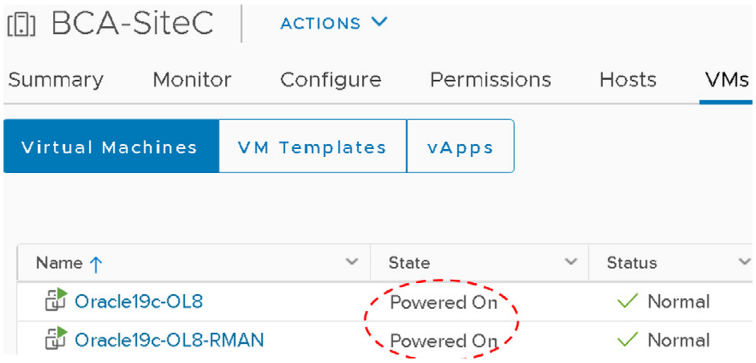
Plan status: ✓ Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:43:58 PM
2. Restore recovery site hosts from standby	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:43:58 PM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:44:07 PM
5. Configure test networks	✓ Success	Tuesday, August 3, 2021 1:44:06 PM	Tuesday, August 3, 2021 1:44:07 PM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Tuesday, August 3, 2021 1:44:07 PM	Tuesday, August 3, 2021 1:46:25 PM
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

FIGURE 215. Test Recovery Plan SC2-VMC-Oracle-RP Successful

VMs on Protected Site A are still powered on.

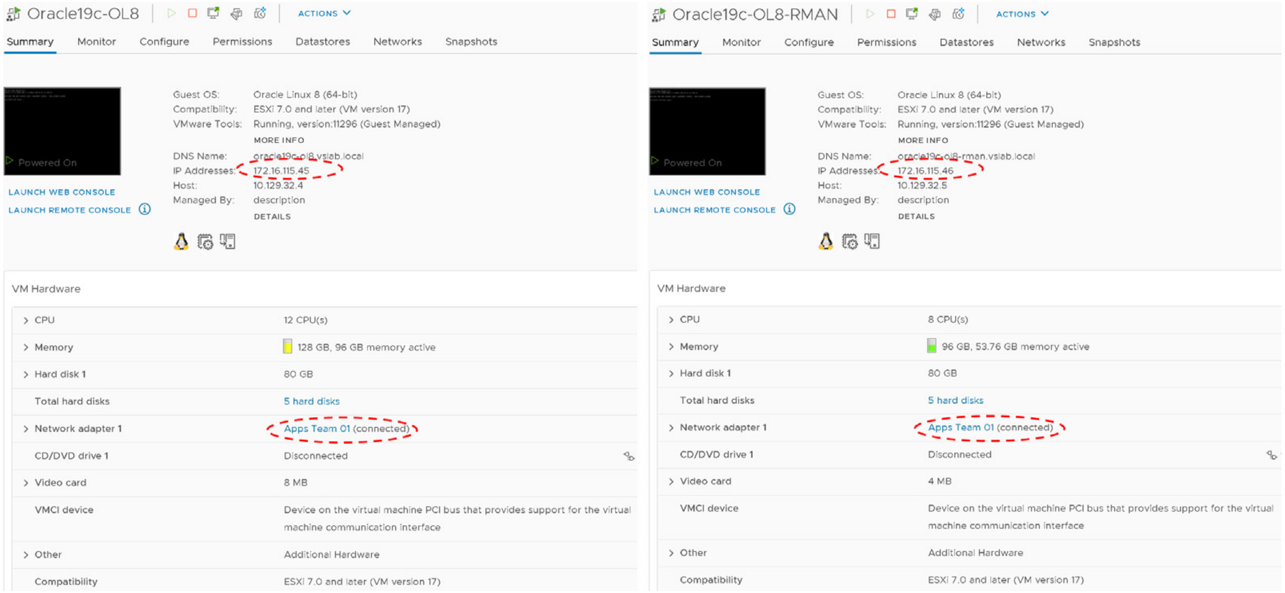


BCA-SiteC
ACTIONS
Summary Monitor Configure Permissions Hosts VMs
Virtual Machines VM Templates vApps

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal

FIGURE 216. Site A VM Details

Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** on recovery VMware Cloud on AWS are powered on with the IP addressing scheme set per network mappings to test network **Apps Team 01**.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.16.115.45
Host: 10.129.32.4
Managed By: description

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 96 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	Apps Team 01 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Oracle19c-OL8-RMAN

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.vslab.local
IP Addresses: 172.16.115.46
Host: 10.129.32.5
Managed By: description

VM Hardware

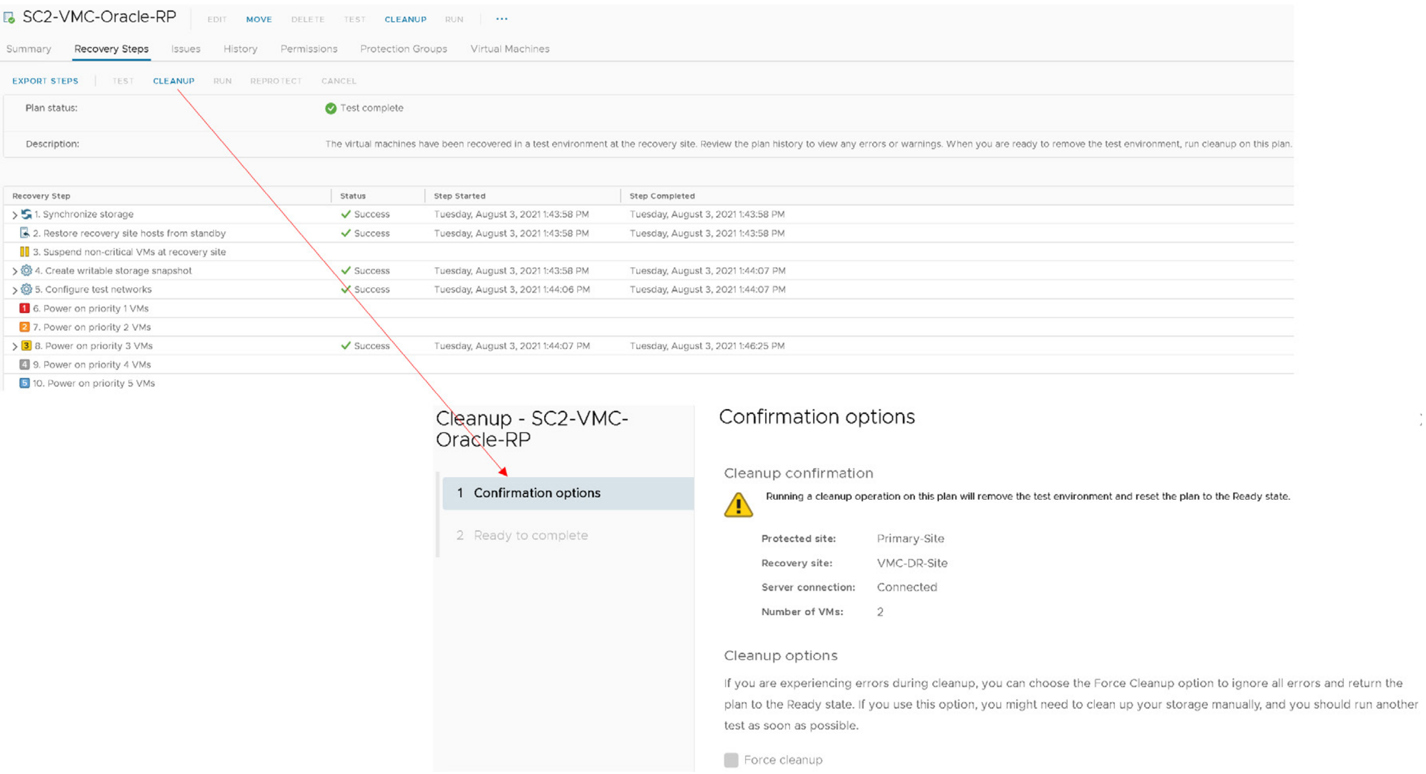
CPU	8 CPU(s)
Memory	96 GB, 53.76 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	Apps Team 01 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 217. Test Recovery Plan VM Networking Details

The Oracle VM **Oracle19c-OL8** is up with IP address 172.16.115.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.16.115.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

As mentioned earlier, **write-order fidelity is guaranteed with vSphere Replication on the disks or VMDKs that comprise a VM**. At the successful completion of the test recovery, perform the cleanup of the test recovery as shown below. As part of the cleanup after running a test, the vSphere Replication server removes the redo logs from the disks on the recovery site and discards the changes.



Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:43:58 PM
2. Restore recovery site hosts from standby	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:43:58 PM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Tuesday, August 3, 2021 1:43:58 PM	Tuesday, August 3, 2021 1:44:07 PM
5. Configure test networks	✓ Success	Tuesday, August 3, 2021 1:44:06 PM	Tuesday, August 3, 2021 1:44:07 PM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Tuesday, August 3, 2021 1:44:07 PM	Tuesday, August 3, 2021 1:46:25 PM
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

Cleanup - SC2-VMC-Oracle-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Cleanup confirmation

Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.

Protected site:	Primary-Site
Recovery site:	VMC-DR-Site
Server connection:	Connected
Number of VMs:	2

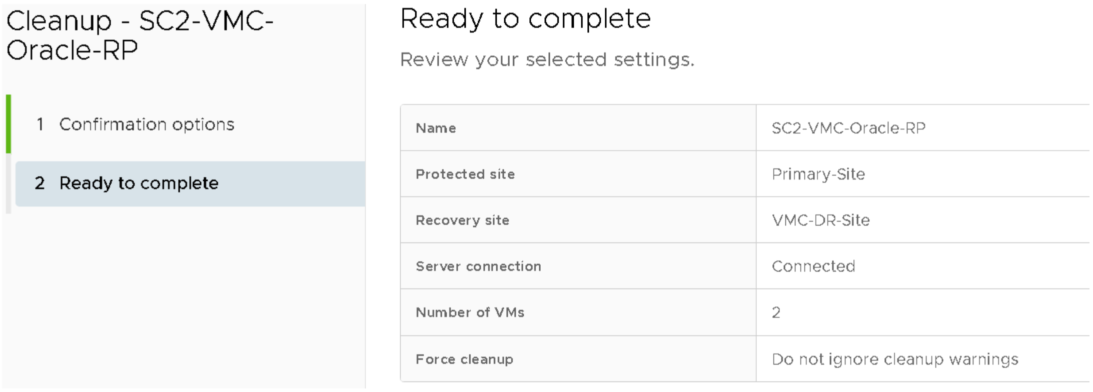
Cleanup options

If you are experiencing errors during cleanup, you can choose the Force Cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you might need to clean up your storage manually, and you should run another test as soon as possible.

□ Force cleanup

FIGURE 218. Start Cleanup Test Recovery Plan SC2-VMC-Oracle-RP

Confirmation of cleanup of test recovery plan **SC2-VMC-Oracle-RP** is as shown below:



Cleanup - SC2-VMC-Oracle-RP

1 Confirmation options

2 Ready to complete

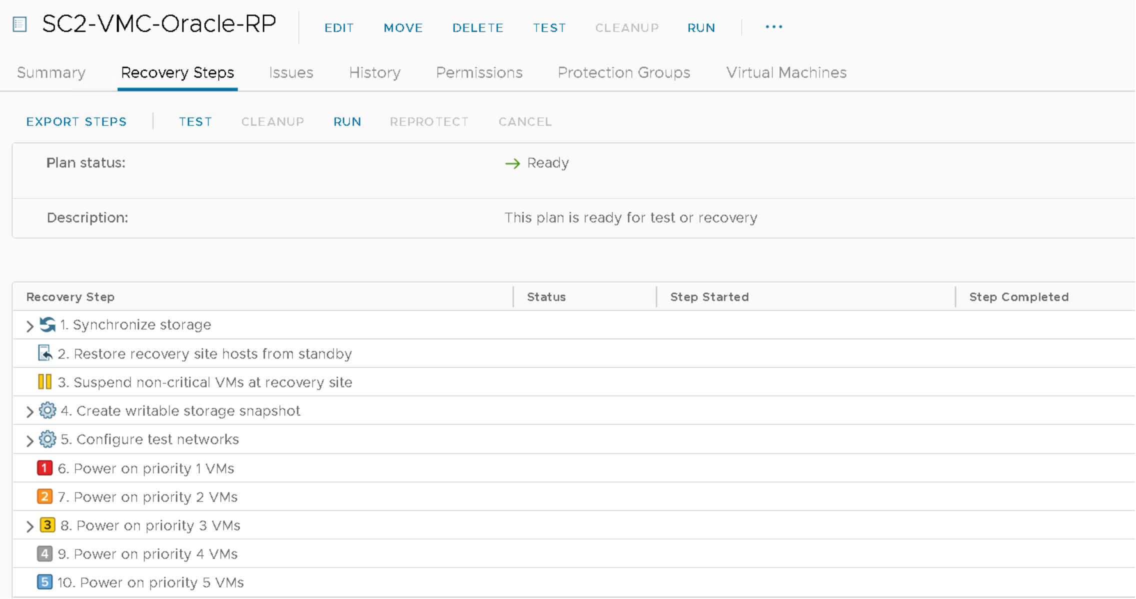
Ready to complete

Review your selected settings.

Name	SC2-VMC-Oracle-RP
Protected site	Primary-Site
Recovery site	VMC-DR-Site
Server connection	Connected
Number of VMs	2
Force cleanup	Do not ignore cleanup warnings

FIGURE 219. Cleanup Test Recovery Plan SC2-VMC-Oracle-RP Confirmation

The cleanup of the test recovery is successful.



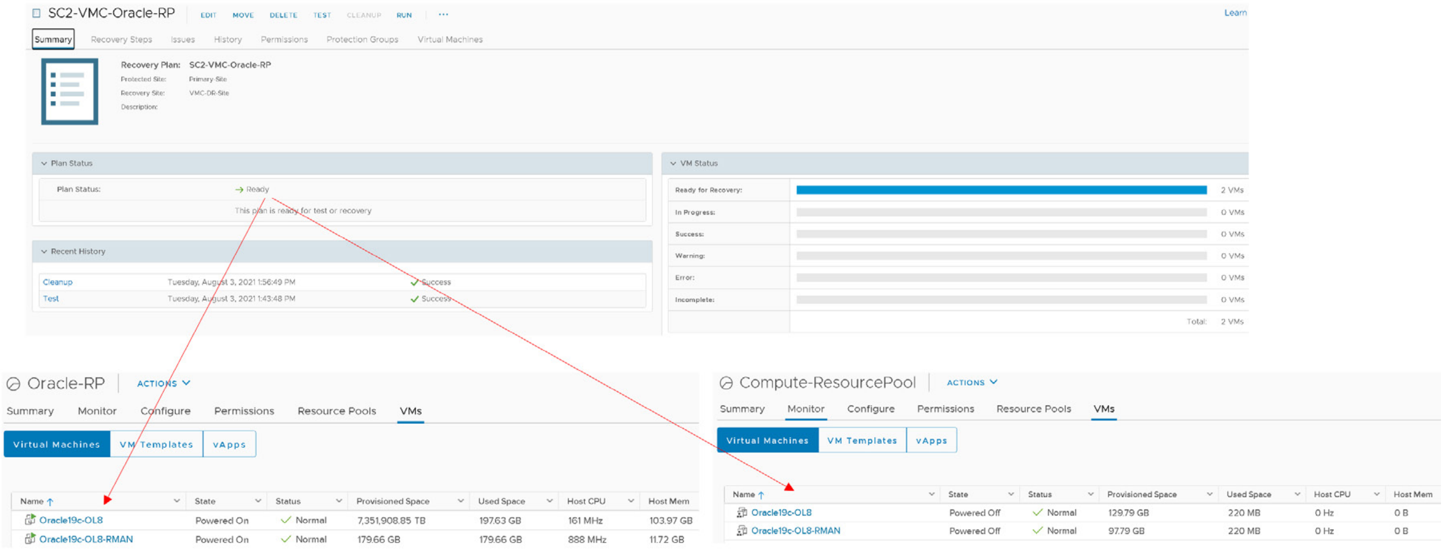
Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage			
2. Restore recovery site hosts from standby			
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot			
5. Configure test networks			
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs			
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

FIGURE 220. Steps to Cleanup Test Recovery Plan SC2-AZ2-Oracle-RP

The VMs on Protected Site A are still powered on. We can see the placeholder VMs on recovery site VMware Cloud on AWS are powered off.



Recovery Plan: SC2-VMC-Oracle-RP
Protected Site: Primary-Site
Recovery Site: VMC-DR-Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Cleanup	Tuesday, August 3, 2021 1:56:49 PM	✓ Success
Test	Tuesday, August 3, 2021 1:43:48 PM	✓ Success

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
Oracle19c-OL8	Powered On	✓ Normal	7,351,908.85 TB	197.63 GB	161 MHz	103.97 GB
Oracle19c-OL8-RMAN	Powered On	✓ Normal	179.66 GB	179.66 GB	888 MHz	11.72 GB

Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
Oracle19c-OL8	Powered Off	✓ Normal	129.79 GB	220 MB	0 Hz	0 B
Oracle19c-OL8-RMAN	Powered Off	✓ Normal	97.79 GB	220 MB	0 Hz	0 B

FIGURE 221. Cleanup Test Recovery Plan SC2-VMC-Oracle-RP Successful

More information regarding the testing recovery plan can be found in the *VMware Site Recovery Manager guide*.

The steps to run the recovery plan for planned migration and the recovery plan for disaster recovery are the same as those employed in on-premises use cases.

VMware Cloud Disaster Recovery

VMware Cloud Disaster Recovery is a VMware on-demand disaster recovery service that is delivered as an easy-to-use SaaS solution, offering cloud economics to help keep disaster recovery costs under control.

VMware Cloud Disaster Recovery can provide disaster recovery to Oracle workloads from on-premises Site A to VMware Cloud on AWS.

VMware Cloud Disaster Recovery uses regularly scheduled snapshots to replicate to the SCFS. VMware snapshots are point-in-time (PIT) snapshots and are therefore crash-consistent. Write-order fidelity is guaranteed for all VMDKs of the VM as a result.

VMware snapshots are not compatible with disks in multi-writer mode and VMware Cloud Disaster Recovery cannot replicate disks in multi-writer mode. Learn more about *VMware Cloud DR and shared disks*.

This use case focusses on the utilization of VMware Cloud Disaster Recovery to provide disaster recovery to two Oracle single-instance VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** from on-premises Site A to VMware Cloud on AWS.

As VMware Cloud DR uses regularly scheduled snapshots to replicate to the SCFS and VMware snapshots are not compatible with disks in multi-writer mode, VMware Cloud DR cannot replicate disks in multi-writer mode. VMware snapshots are a point-in-time snapshot and are therefore crash-consistent.

Failover DR Plan

A DR plan includes a set of recovery steps that capture ordering constraints and action-sequencing instructions for DR operations, which occur when you run the plan.

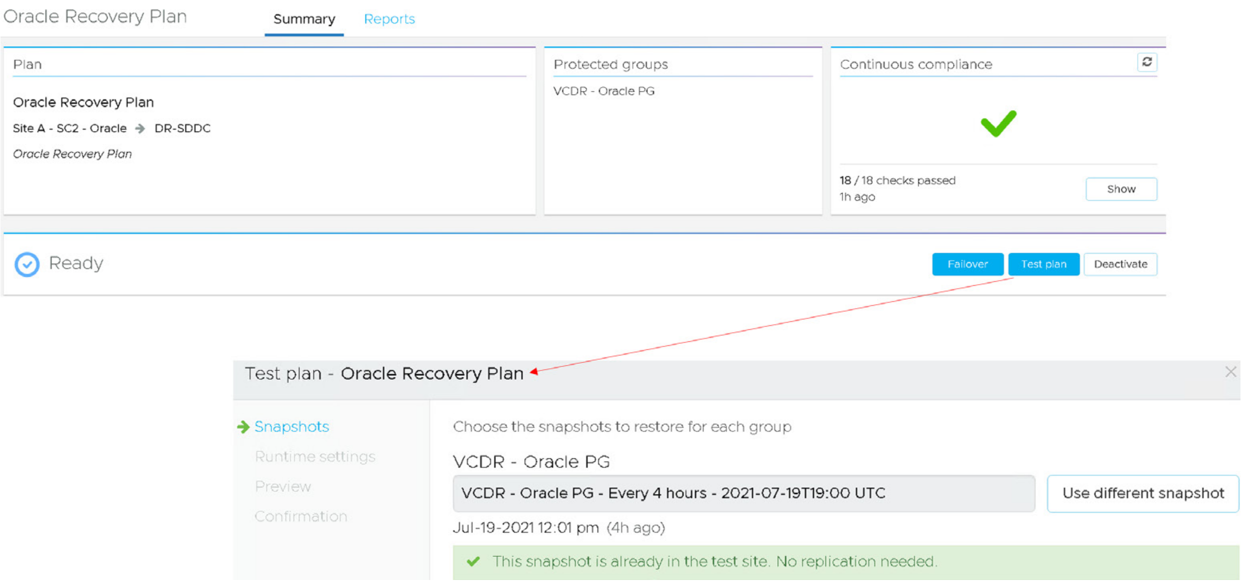
A failover DR plan can run after a real-life disaster event, or as a test failover before a real disaster occurs. You can run a failover plan in the following ways:

- **Failover** – A failover operation is run following a disaster event when the source site is no longer available. The failover operation orchestrates on the destination site based on previously replicated snapshots. When failing over to a VMware Cloud on AWS SDDC, VMs that belong to the protection groups defined in your DR plan are recovered to the vCenter in a recovery SDDC.
- **Test failover** – A test failover operation is similar to regular failover operation, but runs in the context of its own test execution environment. Another difference is that by default, a test failover stops on the first failure, whereas a regular failover continues to run, even after failures. You can override all default behaviors by custom options prior to starting the failover operation. With a test failover, you have the option to clean up the test plan.

Learn more about *How a Failover DR Plan Runs*.

Running a Test Failover of the DR Plan

Steps to test the failover DR plan **Oracle Recovery Plan** are as shown below:



Oracle Recovery Plan — Summary | Reports

Plan: Oracle Recovery Plan
Site A - SC2 - Oracle → DR-SDDC
Oracle Recovery Plan

Protected groups: VCDR - Oracle PG

Continuous compliance: 18 / 18 checks passed, 1h ago

Ready

Test plan - Oracle Recovery Plan

Choose the snapshots to restore for each group

VCDR - Oracle PG

VCDR - Oracle PG - Every 4 hours - 2021-07-19T19:00 UTC

Jul-19-2021 12:01 pm (4h ago)

This snapshot is already in the test site. No replication needed.

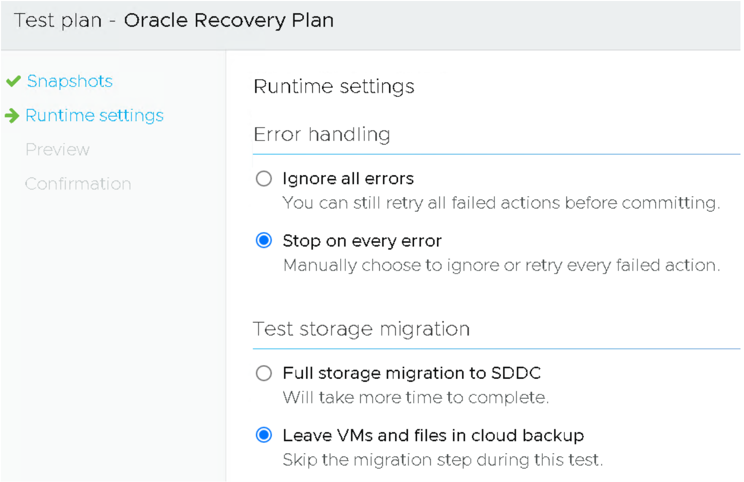
FIGURE 222. Test Failover DR Plan

Test failover operations give you the option of performing a full storage vMotion from the staging datastore to the SDDC datastore to emulate a real failover—or to leave VMs on the staging datastore to cut down on the failover time (preview feature)—and to allow you to test and debug your failover faster.

We can select the storage to migrate VMs to during the failover:

- Full storage migration to SDDC. Select this option to migrate all VMs to vSAN storage on the SDDC. The failover operation requires more time, but this option is optimal for those VMs that need lower latency and higher I/O.
- Leave VMs and files on the cloud file system. Use the cloud backup SCFS as highly available storage and run recovered VMs directly from the cloud file system. If you select this, failover is faster and there is no dependency on SDDC hosts for storage capacity. With this option, the SDDC can be substantially smaller in size because VMs are kept on the cloud file system datastore, eliminating the vSAN storage capacity constraints. This configuration can be more cost-effective.

With this more cost-effective preview feature, the SDDC can be substantially smaller in size because VMs are kept on the cloud file system datastore, eliminating vSAN storage capacity constraints, which can incur costs.



Test plan - **Oracle Recovery Plan**

Runtime settings

Error handling

○ Ignore all errors
You can still retry all failed actions before committing.

● Stop on every error
Manually choose to ignore or retry every failed action.

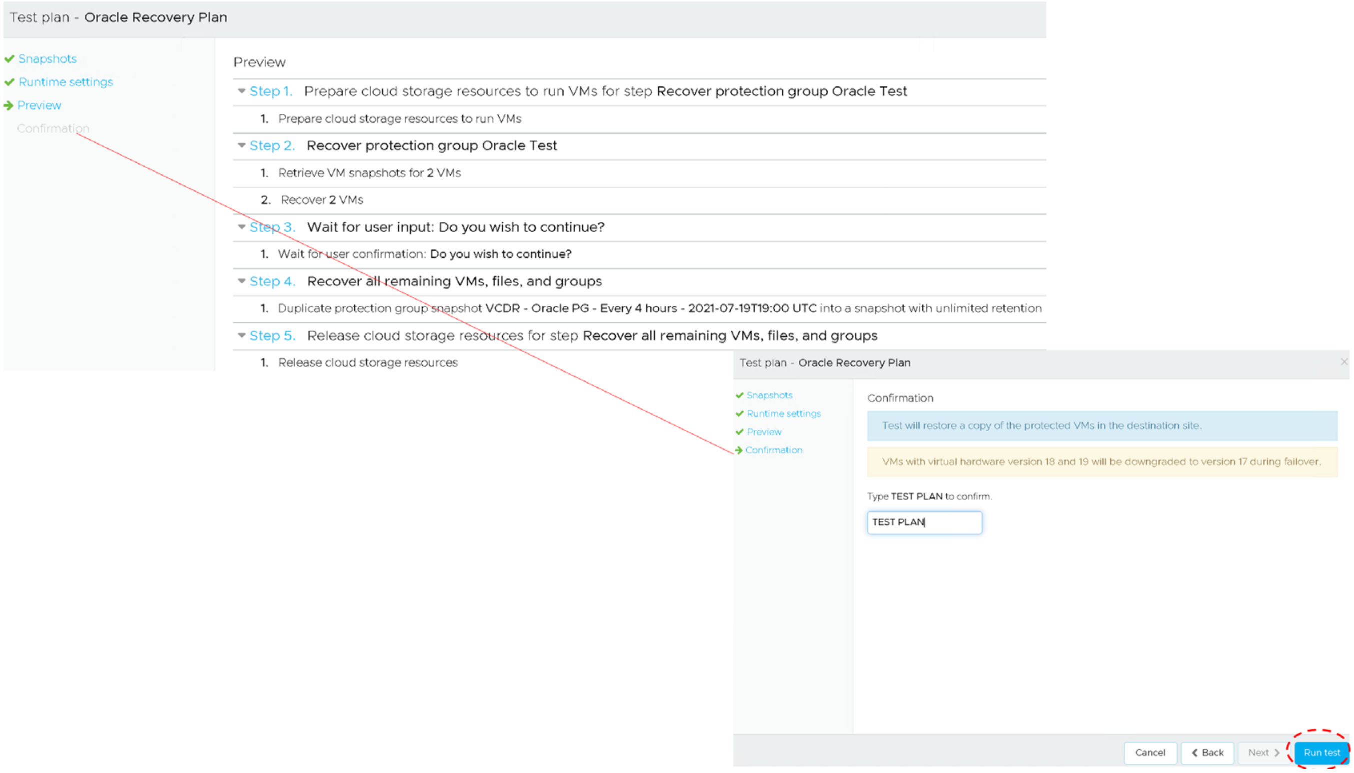
Test storage migration

○ Full storage migration to SDDC
Will take more time to complete.

● Leave VMs and files in cloud backup
Skip the migration step during this test.

FIGURE 223. Test Failover DR Plan Options

Confirmation of the test failover DR plan is as shown below:



Test plan - **Oracle Recovery Plan**

Preview

- Step 1. Prepare cloud storage resources to run VMs for step **Recover protection group Oracle Test**
  1. Prepare cloud storage resources to run VMs
- Step 2. **Recover protection group Oracle Test**
  1. Retrieve VM snapshots for 2 VMs
  2. Recover 2 VMs
- Step 3. **Wait for user input: Do you wish to continue?**
  1. Wait for user confirmation: **Do you wish to continue?**
- Step 4. **Recover all remaining VMs, files, and groups**
  1. Duplicate protection group snapshot **VCDR - Oracle PG - Every 4 hours - 2021-07-19T19:00 UTC** into a snapshot with unlimited retention
- Step 5. Release cloud storage resources for step **Recover all remaining VMs, files, and groups**
  1. Release cloud storage resources

Test plan - **Oracle Recovery Plan**

Confirmation

Test will restore a copy of the protected VMs in the destination site.

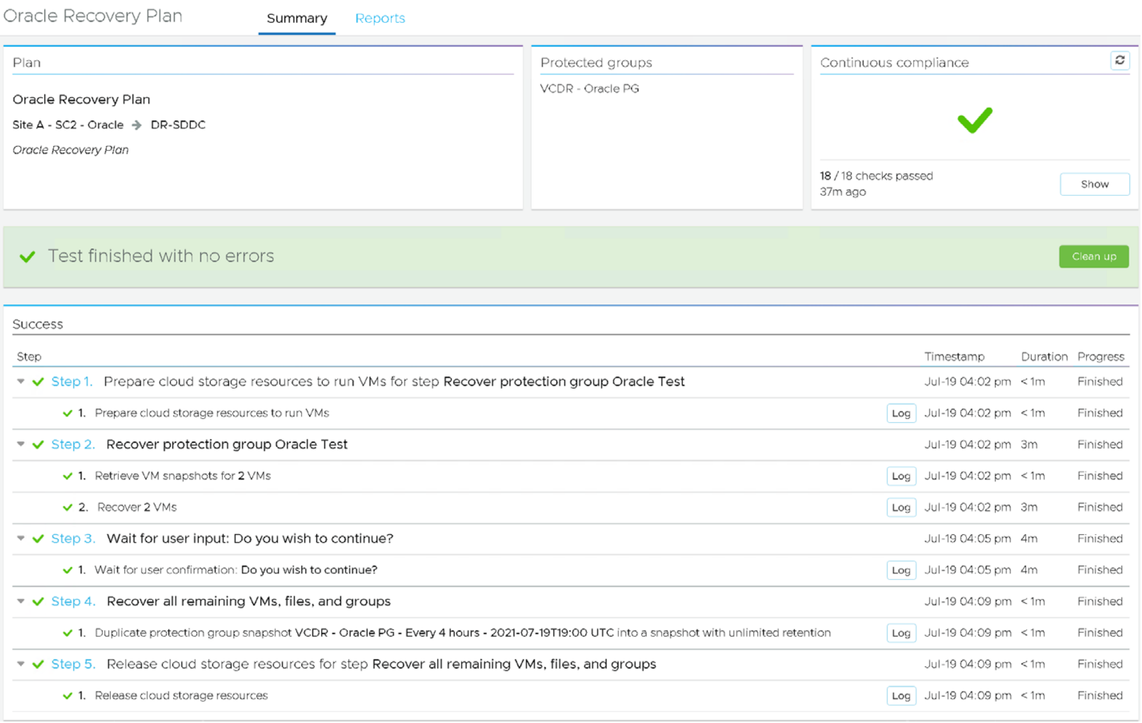
VMs with virtual hardware version 18 and 19 will be downgraded to version 17 during failover.

Type **TEST PLAN** to confirm.

TEST PLAN

FIGURE 224. Confirm Test Failover DR Plan Run

The test failover is run when the **Run Test** button is clicked.



Oracle Recovery Plan

Plan

Oracle Recovery Plan
Site A - SC2 - Oracle → DR-SDDC
Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

18 / 18 checks passed
37m ago

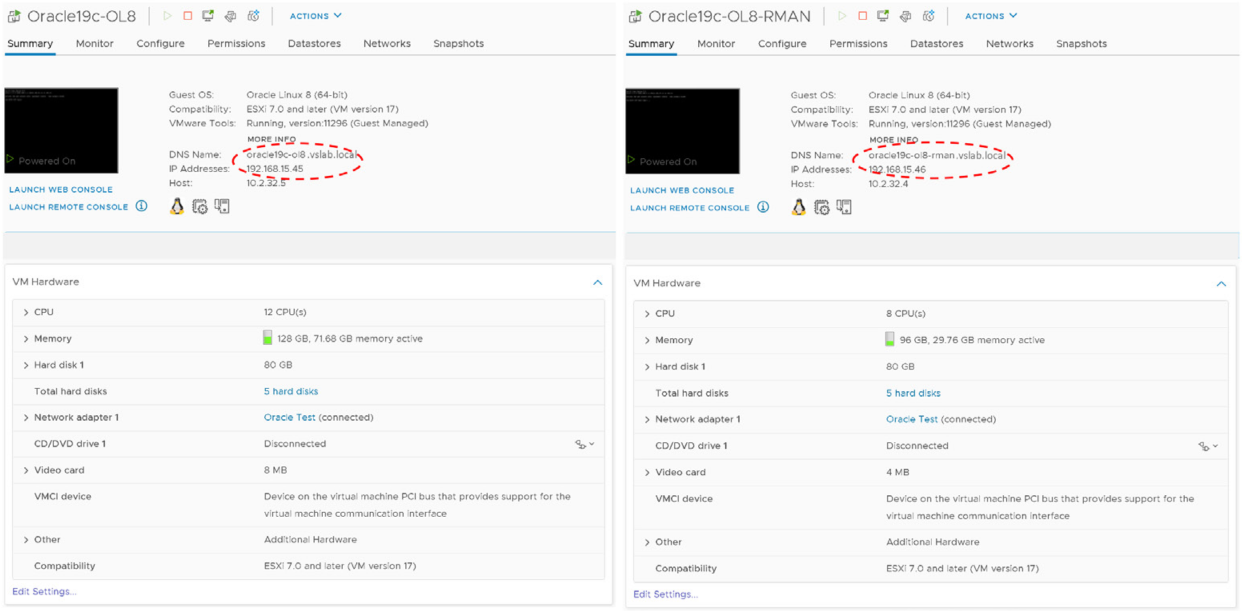
✓ Test finished with no errors

Success

Step		Timestamp	Duration	Progress
✓ Step 1. Prepare cloud storage resources to run VMs for step **Recover protection group Oracle Test**		Jul-19 04:02 pm	< 1m	Finished
✓ 1. Prepare cloud storage resources to run VMs	Log	Jul-19 04:02 pm	< 1m	Finished
✓ Step 2. Recover protection group Oracle Test		Jul-19 04:02 pm	3m	Finished
✓ 1. Retrieve VM snapshots for **2** VMs	Log	Jul-19 04:02 pm	< 1m	Finished
✓ 2. Recover **2** VMs	Log	Jul-19 04:02 pm	3m	Finished
✓ Step 3. Wait for user input: Do you wish to continue?		Jul-19 04:05 pm	4m	Finished
✓ 1. Wait for user confirmation: **Do you wish to continue?**	Log	Jul-19 04:05 pm	4m	Finished
✓ Step 4. Recover all remaining VMs, files, and groups		Jul-19 04:09 pm	< 1m	Finished
✓ 1. Duplicate protection group snapshot **VCDR - Oracle PG - Every 4 hours - 2021-07-19T19:00 UTC** into a snapshot with unlimited retention	Log	Jul-19 04:09 pm	< 1m	Finished
✓ Step 5. Release cloud storage resources for step **Recover all remaining VMs, files, and groups**		Jul-19 04:09 pm	< 1m	Finished
✓ 1. Release cloud storage resources	Log	Jul-19 04:09 pm	< 1m	Finished

FIGURE 225. Test Failover DR Plan Completed Successfully

The test completed with no errors.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 192.168.15.45
Host: 10.2.32.5

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 71.68 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	Oracle Test (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.vslab.local
IP Addresses: 192.168.15.46
Host: 10.2.32.4

VM Hardware

CPU	8 CPU(s)
Memory	96 GB, 29.76 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	Oracle Test (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

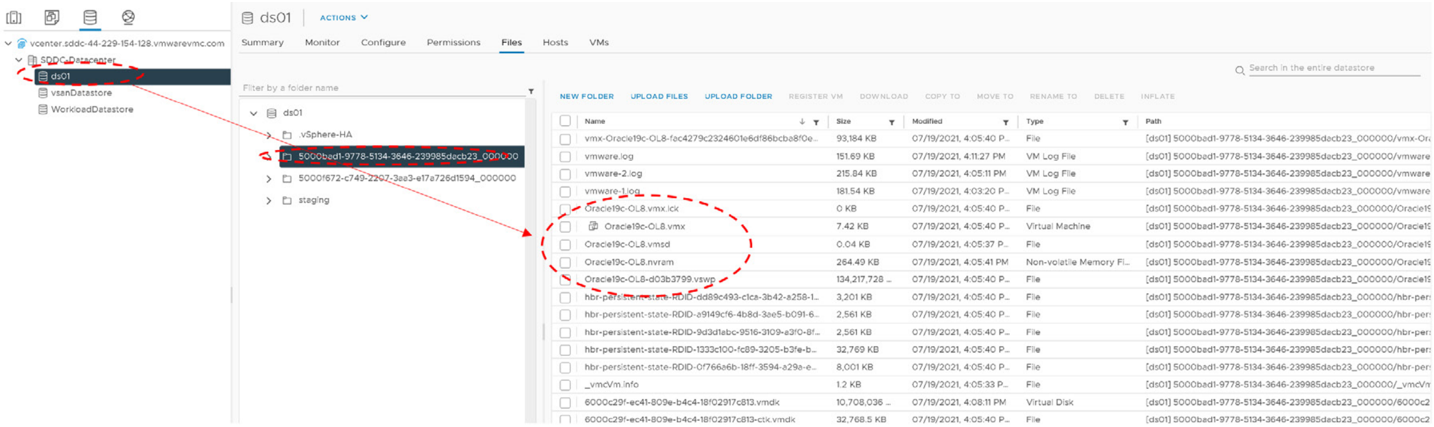
FIGURE 226. VM Networking Status After Test Failover DR Plan

The Oracle VM **Oracle19c-OL8** is up with IP address 192.168.15.45 and the database vvol19c is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 192.168.15.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

VMware Cloud Disaster Recovery uses regularly scheduled snapshots to replicate to the SCFS. VMware snapshots are point-in-time (PIT) snapshots and are therefore crash-consistent. Write-order fidelity is guaranteed for all VMDKs of the VM as a result.

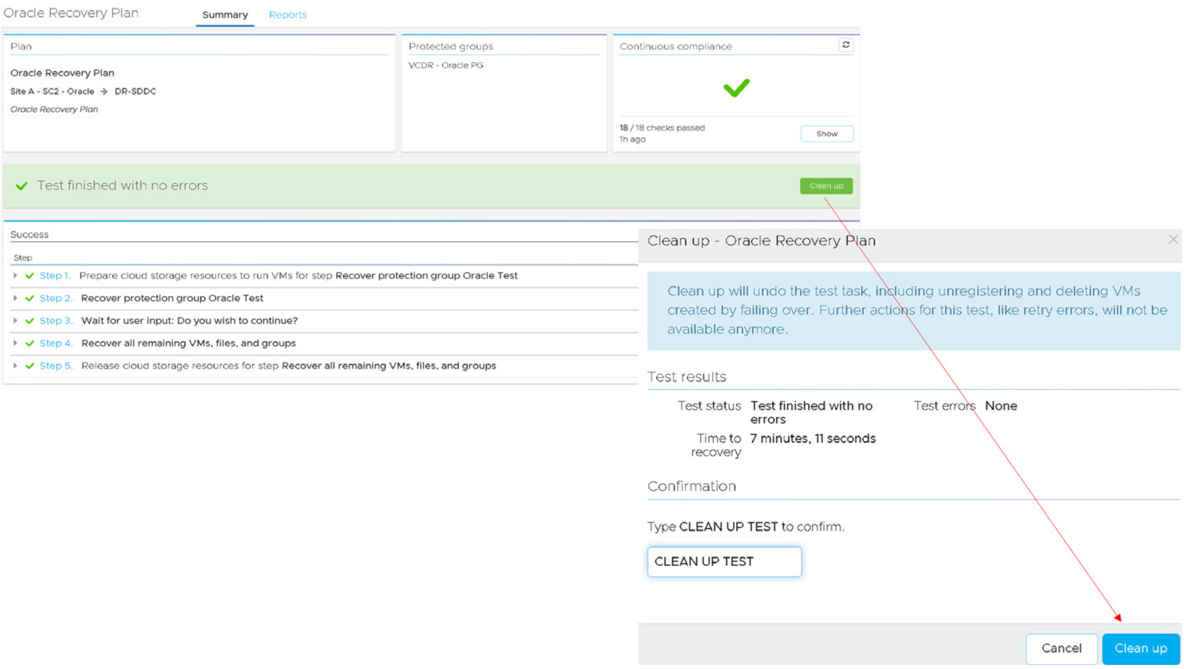
Navigating the files folders on datastore **ds1** shows VM **Oracle19c-OL8** is present. The VM **Oracle19c-OL8-RMAN** is present on another folder on the same datastore.



Name	Size	Modified	Type	Path
vmx-Oracle19c-OL8-fac4279c2324601e6df86bcba8f0e...	93,184 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/vmx-Ora
vmware.log	151.69 KB	07/19/2021, 4:11:27 PM	VM Log File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/vmware
vmware-2.log	215.84 KB	07/19/2021, 4:05:11 PM	VM Log File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/vmware
vmware-1.log	181.54 KB	07/19/2021, 4:03:20 P...	VM Log File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/vmware
Oracle19c-OL8.vmx.lck	0 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/Oracle19
Oracle19c-OL8.vmx	7.42 KB	07/19/2021, 4:05:40 P...	Virtual Machine	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/Oracle19
Oracle19c-OL8.vmsd	0.04 KB	07/19/2021, 4:05:37 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/Oracle19
Oracle19c-OL8.nvram	264.49 KB	07/19/2021, 4:05:41 PM	Non-volatile Memory Fi...	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/Oracle19
Oracle19c-OL8-d03b3799.vswp	134,217,728 ...	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/Oracle19
hbr-persistent-state-RDID-dd89c493-c1ca-3b42-a258-1...	3,201 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/hbr-pers
hbr-persistent-state-RDID-a9149cf6-4b8d-3ae5-b091-6...	2,561 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/hbr-pers
hbr-persistent-state-RDID-9d3d1abc-9516-3109-a3f0-8f...	2,561 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/hbr-pers
hbr-persistent-state-RDID-1333c100-fc89-3205-b3fe-b...	32,769 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/hbr-pers
hbr-persistent-state-RDID-0f766a6b-18ff-3594-a29a-e...	8,001 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/hbr-pers
_vmcVm.info	1.2 KB	07/19/2021, 4:05:33 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/_vmcVm
6000c29f-ec41-809e-b4c4-18f02917c813.vmdk	10,708,036 ...	07/19/2021, 4:08:11 PM	Virtual Disk	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/6000c2
6000c29f-ec41-809e-b4c4-18f02917c813-ctk.vmdk	32,768.5 KB	07/19/2021, 4:05:40 P...	File	[ds01] 5000bad1-9778-5134-3646-239985dacb23_000000/6000c2

FIGURE 227. VM Oracle19c-OL8 VMDK Details

Run a cleanup of the test failover run.



Plan

Oracle Recovery Plan
Site A - SC2 - Oracle → DR-SDDC
Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

✓

18 / 18 checks passed
1h ago

✓ Test finished with no errors

Success

Step

- ✓ Step 1. Prepare cloud storage resources to run VMs for step **Recover protection group Oracle Test**
- ✓ Step 2. Recover protection group Oracle Test
- ✓ Step 3. Wait for user input: Do you wish to continue?
- ✓ Step 4. Recover all remaining VMs, files, and groups
- ✓ Step 5. Release cloud storage resources for step **Recover all remaining VMs, files, and groups**

Clean up - Oracle Recovery Plan

Clean up will undo the test task, including unregistering and deleting VMs created by failing over. Further actions for this test, like retry errors, will not be available anymore.

Test results

Test status: Test finished with no errors
Test errors: None
Time to recovery: 7 minutes, 11 seconds

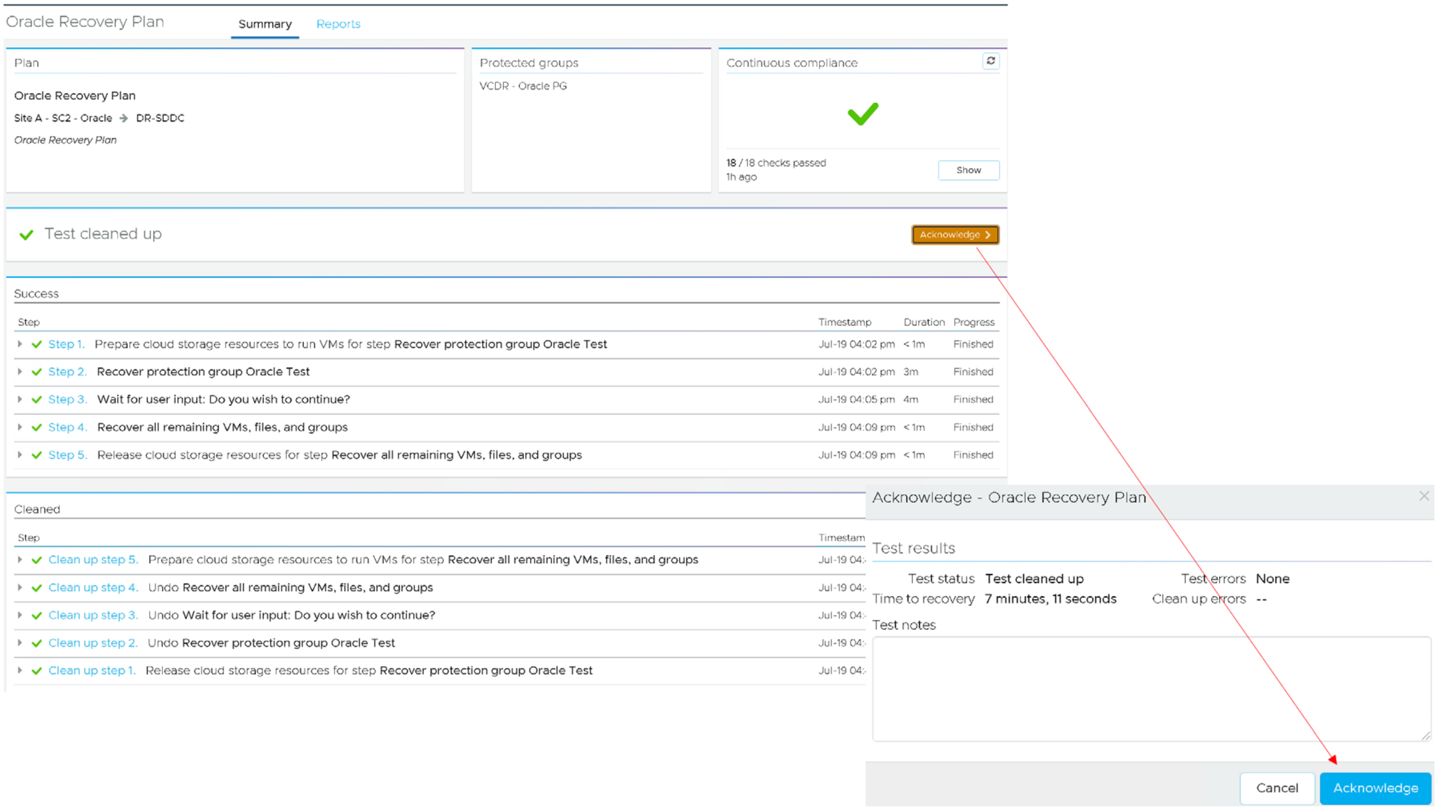
Confirmation

Type **CLEAN UP TEST** to confirm.

CLEAN UP TEST

FIGURE 228. Cleanup of DR Plan

Cleanup of the DR Plan completes successfully.



Plan

Oracle Recovery Plan
Site A - SC2 - Oracle → DR-SDDC
Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

18 / 18 checks passed
1h ago

✓ Test cleaned up

Success

Step	Timestamp	Duration	Progress
✓ Step 1. Prepare cloud storage resources to run VMs for step **Recover protection group Oracle Test**	Jul-19 04:02 pm	< 1m	Finished
✓ Step 2. **Recover protection group Oracle Test**	Jul-19 04:02 pm	3m	Finished
✓ Step 3. **Wait for user input: Do you wish to continue?**	Jul-19 04:05 pm	4m	Finished
✓ Step 4. **Recover all remaining VMs, files, and groups**	Jul-19 04:09 pm	< 1m	Finished
✓ Step 5. Release cloud storage resources for step **Recover all remaining VMs, files, and groups**	Jul-19 04:09 pm	< 1m	Finished

Cleaned

Step	Timestam
✓ Clean up step 5. Prepare cloud storage resources to run VMs for step **Recover all remaining VMs, files, and groups**	Jul-19 04:
✓ Clean up step 4. Undo **Recover all remaining VMs, files, and groups**	Jul-19 04:
✓ Clean up step 3. Undo **Wait for user input: Do you wish to continue?**	Jul-19 04:
✓ Clean up step 2. Undo **Recover protection group Oracle Test**	Jul-19 04:
✓ Clean up step 1. Release cloud storage resources for step **Recover protection group Oracle Test**	Jul-19 04:

Acknowledge - Oracle Recovery Plan

Test results

Test status	Test cleaned up	Test errors	None
Time to recovery	7 minutes, 11 seconds	Clean up errors	--

Test notes

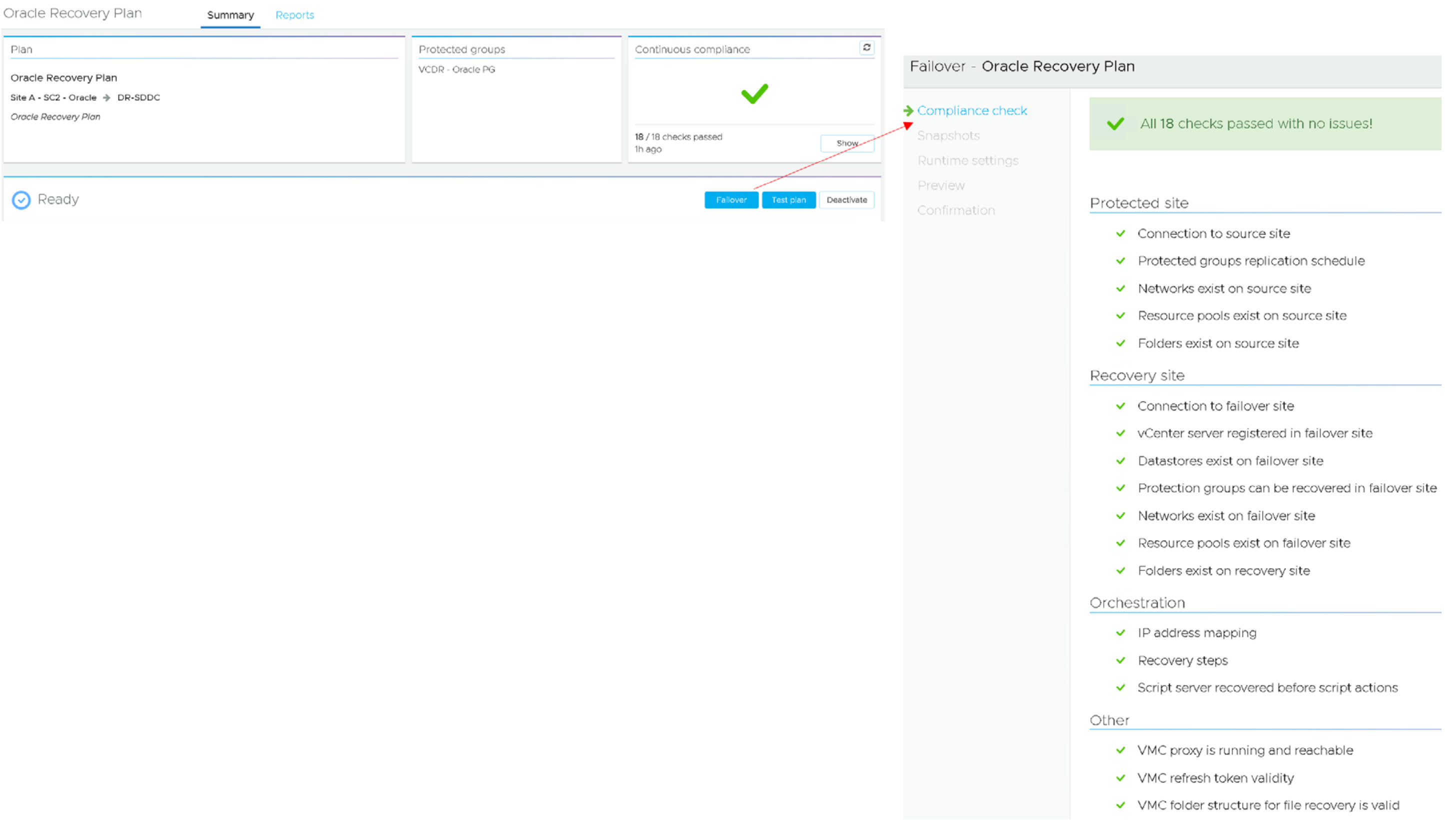
FIGURE 229. Cleanup of DR Plan Completed Successfully

Learn more about *Running a Test Failover*.

Running a Failover of the DR Plan

A failover operation is run following a disaster event when the source site is no longer available.

Steps to run the failover DR plan **Oracle Recovery Plan** are as shown below. In this use case, we simulated an actual DR event, even though the protected site was available.



Oracle Recovery Plan

Summary Reports

Plan

Oracle Recovery Plan

Site A - SC2 - Oracle → DR-SDDC

Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

18 / 18 checks passed

1h ago

Show

Ready

Failover Test plan Deactivate

Failover - Oracle Recovery Plan

→ Compliance check

Snapshots

Runtime settings

Preview

Confirmation

✓ All 18 checks passed with no issues!

Protected site

- ✓ Connection to source site
- ✓ Protected groups replication schedule
- ✓ Networks exist on source site
- ✓ Resource pools exist on source site
- ✓ Folders exist on source site

Recovery site

- ✓ Connection to failover site
- ✓ vCenter server registered in failover site
- ✓ Datastores exist on failover site
- ✓ Protection groups can be recovered in failover site
- ✓ Networks exist on failover site
- ✓ Resource pools exist on failover site
- ✓ Folders exist on recovery site

Orchestration

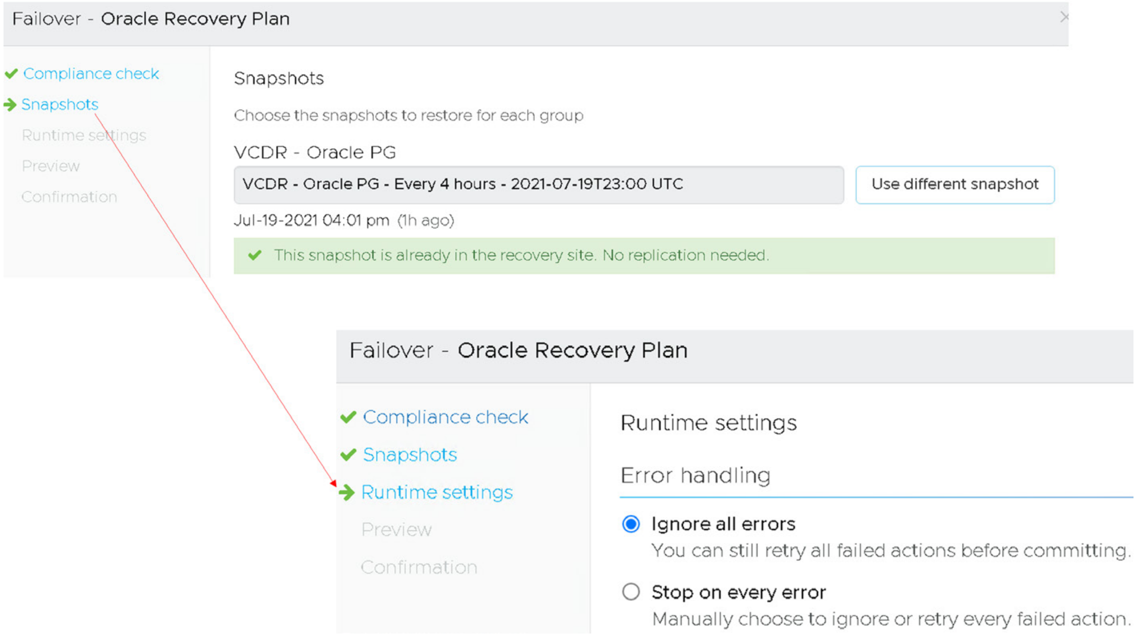
- ✓ IP address mapping
- ✓ Recovery steps
- ✓ Script server recovered before script actions

Other

- ✓ VMC proxy is running and reachable
- ✓ VMC refresh token validity
- ✓ VMC folder structure for file recovery is valid

FIGURE 230. Start Failover of DR Plan

The failover plan options are as shown below:



Failover - Oracle Recovery Plan

- ✓ Compliance check
- ➔ Snapshots
- Runtime settings
- Preview
- Confirmation

Snapshots

Choose the snapshots to restore for each group

VCDR - Oracle PG

VCDR - Oracle PG - Every 4 hours - 2021-07-19T23:00 UTC

Jul-19-2021 04:01 pm (1h ago)

✓ This snapshot is already in the recovery site. No replication needed.

Failover - Oracle Recovery Plan

- ✓ Compliance check
- ✓ Snapshots
- ➔ Runtime settings
- Preview
- Confirmation

Runtime settings

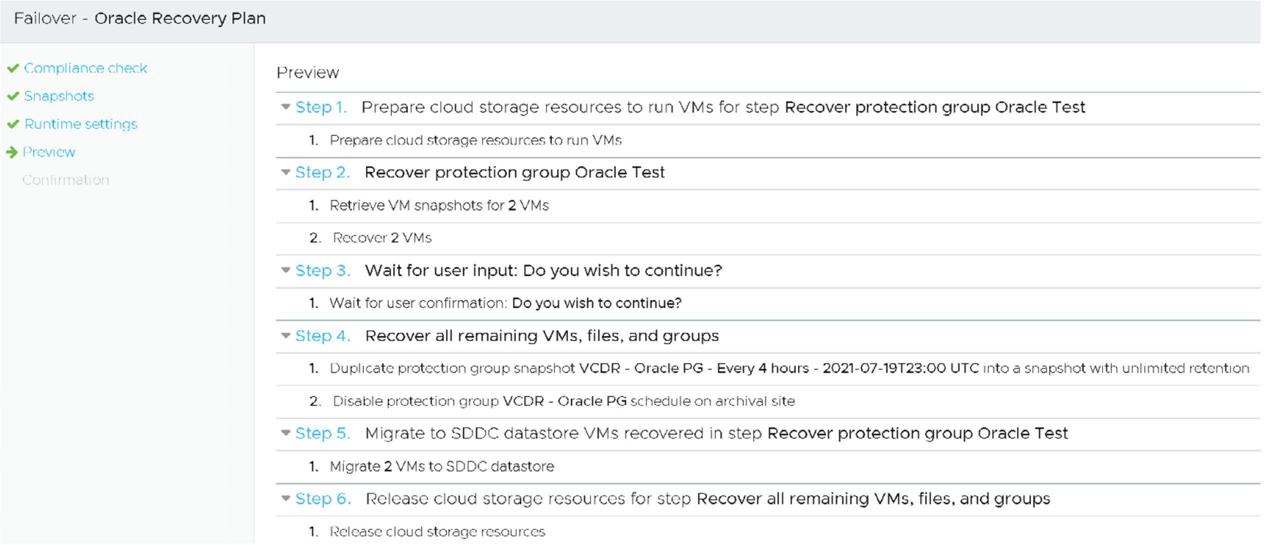
Error handling

● Ignore all errors
You can still retry all failed actions before committing.

○ Stop on every error
Manually choose to ignore or retry every failed action.

FIGURE 231. Failover of DR Plan Options

The default is **full storage migration to SDDC**. This use case is a simulation of an actual DR event, even though this was a planned DR event.



Failover - Oracle Recovery Plan

- ✓ Compliance check
- ✓ Snapshots
- ✓ Runtime settings
- ➔ Preview
- Confirmation

Preview

Step 1. Prepare cloud storage resources to run VMs for step Recover protection group Oracle Test

1. Prepare cloud storage resources to run VMs

Step 2. Recover protection group Oracle Test

1. Retrieve VM snapshots for 2 VMs
2. Recover 2 VMs

Step 3. Wait for user input: Do you wish to continue?

1. Wait for user confirmation: Do you wish to continue?

Step 4. Recover all remaining VMs, files, and groups

1. Duplicate protection group snapshot VCDR - Oracle PG - Every 4 hours - 2021-07-19T23:00 UTC into a snapshot with unlimited retention
2. Disable protection group VCDR - Oracle PG schedule on archival site

Step 5. Migrate to SDDC datastore VMs recovered in step Recover protection group Oracle Test

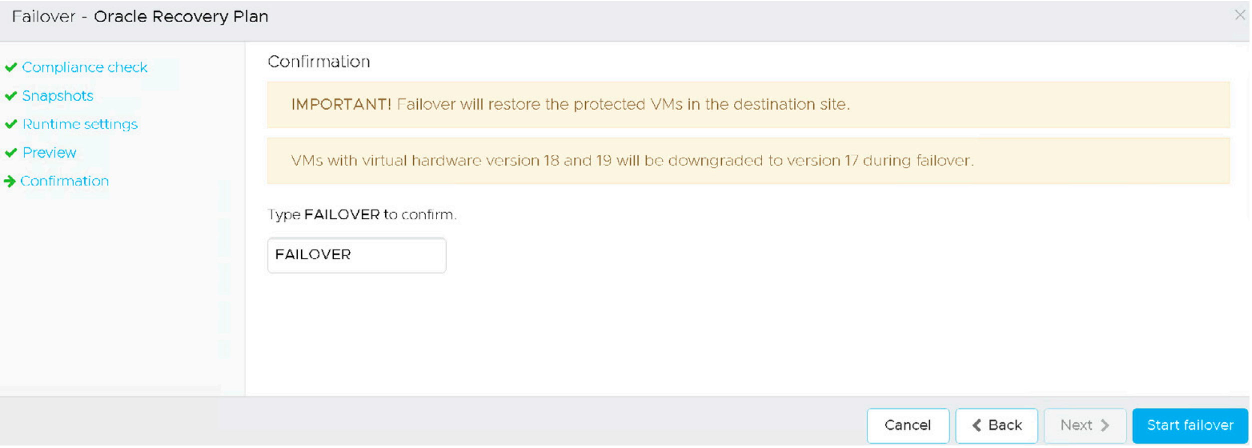
1. Migrate 2 VMs to SDDC datastore

Step 6. Release cloud storage resources for step Recover all remaining VMs, files, and groups

1. Release cloud storage resources

FIGURE 232. Failover of DR Plan Steps

Confirmation of the failover DR plan is as shown below:



Failover - Oracle Recovery Plan

- ✓ Compliance check
- ✓ Snapshots
- ✓ Runtime settings
- ✓ Preview
- → Confirmation

Confirmation

IMPORTANT! Failover will restore the protected VMs in the destination site.

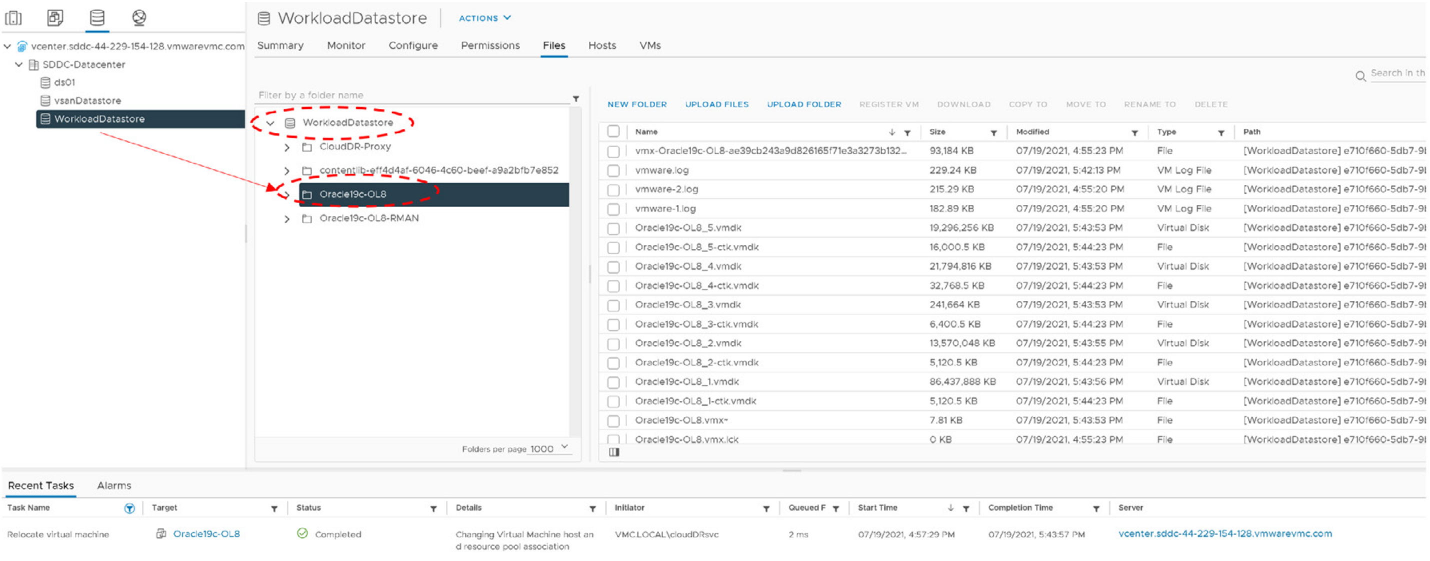
VMs with virtual hardware version 18 and 19 will be downgraded to version 17 during failover.

Type FAILOVER to confirm.

FAILOVER

FIGURE 233. Confirmation of Failover of DR Plan

We can see that VMs **Oracle19c-OL8** and **Oracle19c-OL8-=RMAN** have been successfully migrated via vSphere Storage vMotion to the vSAN workload datastore.

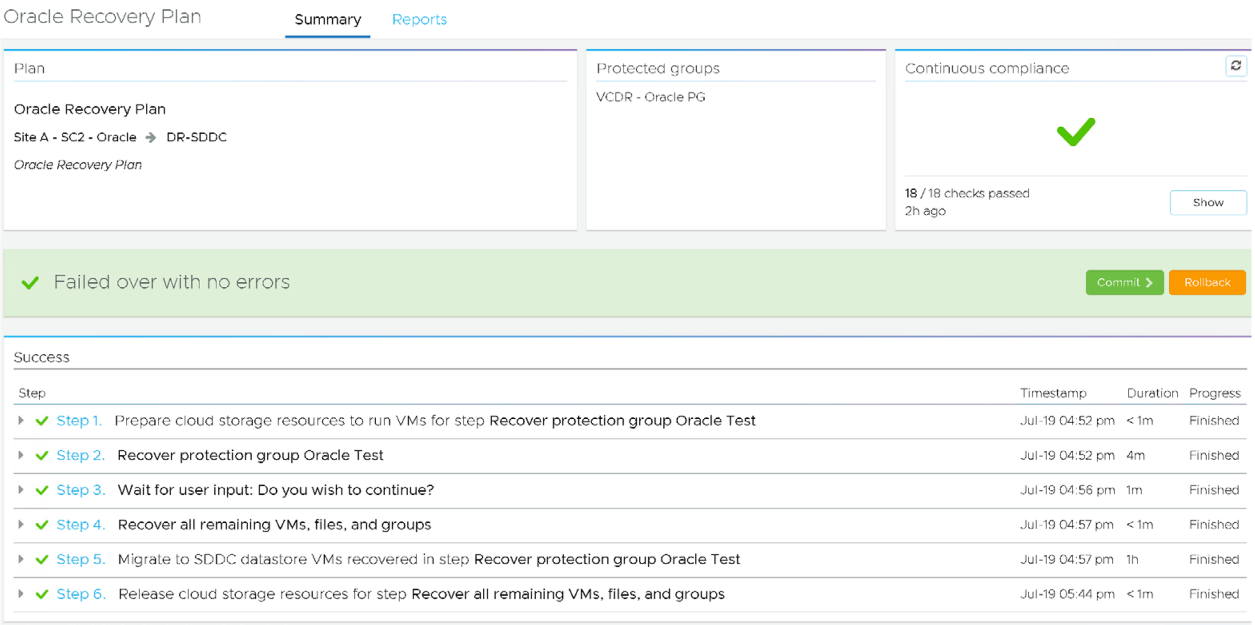


Name	Size	Modified	Type	Path
vmx-Oracle19c-OL8-ae39cb243a9d826165f71e3a3273b132...	93,184 KB	07/19/2021, 4:55:23 PM	File	[WorkloadDatastore] e710f660-5db7-9I
vmware.log	229.24 KB	07/19/2021, 5:42:13 PM	VM Log File	[WorkloadDatastore] e710f660-5db7-9I
vmware-2.log	215.29 KB	07/19/2021, 4:55:20 PM	VM Log File	[WorkloadDatastore] e710f660-5db7-9I
vmware-1.log	182.89 KB	07/19/2021, 4:55:20 PM	VM Log File	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_5.vmdk	19,296,256 KB	07/19/2021, 5:43:53 PM	Virtual Disk	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_5-ctk.vmdk	16,000.5 KB	07/19/2021, 5:44:23 PM	File	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_4.vmdk	21,794,816 KB	07/19/2021, 5:43:53 PM	Virtual Disk	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_4-ctk.vmdk	32,768.5 KB	07/19/2021, 5:44:23 PM	File	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_3.vmdk	241,664 KB	07/19/2021, 5:43:53 PM	Virtual Disk	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_3-ctk.vmdk	6,400.5 KB	07/19/2021, 5:44:23 PM	File	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_2.vmdk	13,570,048 KB	07/19/2021, 5:43:55 PM	Virtual Disk	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_2-ctk.vmdk	5,120.5 KB	07/19/2021, 5:44:23 PM	File	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_1.vmdk	86,437,888 KB	07/19/2021, 5:43:56 PM	Virtual Disk	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8_1-ctk.vmdk	5,120.5 KB	07/19/2021, 5:44:23 PM	File	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8.vmx~	7.81 KB	07/19/2021, 5:43:53 PM	File	[WorkloadDatastore] e710f660-5db7-9I
Oracle19c-OL8.vmx.lck	0 KB	07/19/2021, 4:55:23 PM	File	[WorkloadDatastore] e710f660-5db7-9I

Task Name	Target	Status	Details	Initiator	Queued F	Start Time	Completion Time	Server
Relocate virtual machine	Oracle19c-OL8	✓ Completed	Changing Virtual Machine host and resource pool association	VMC.LOCAL\cloudDRsvc	2 ms	07/19/2021, 4:57:29 PM	07/19/2021, 5:43:57 PM	vcenter.sddc-44-229-154-128.vmwarevmc.com

FIGURE 234. VM Oracle19c-OL8 VMDK Details

The failover of the DR plan completed successfully.



Oracle Recovery Plan — Summary | Reports

Plan

Oracle Recovery Plan

Site A - SC2 - Oracle → DR-SDDC

Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

✓

18 / 18 checks passed

2h ago

Show

✓ Failed over with no errors

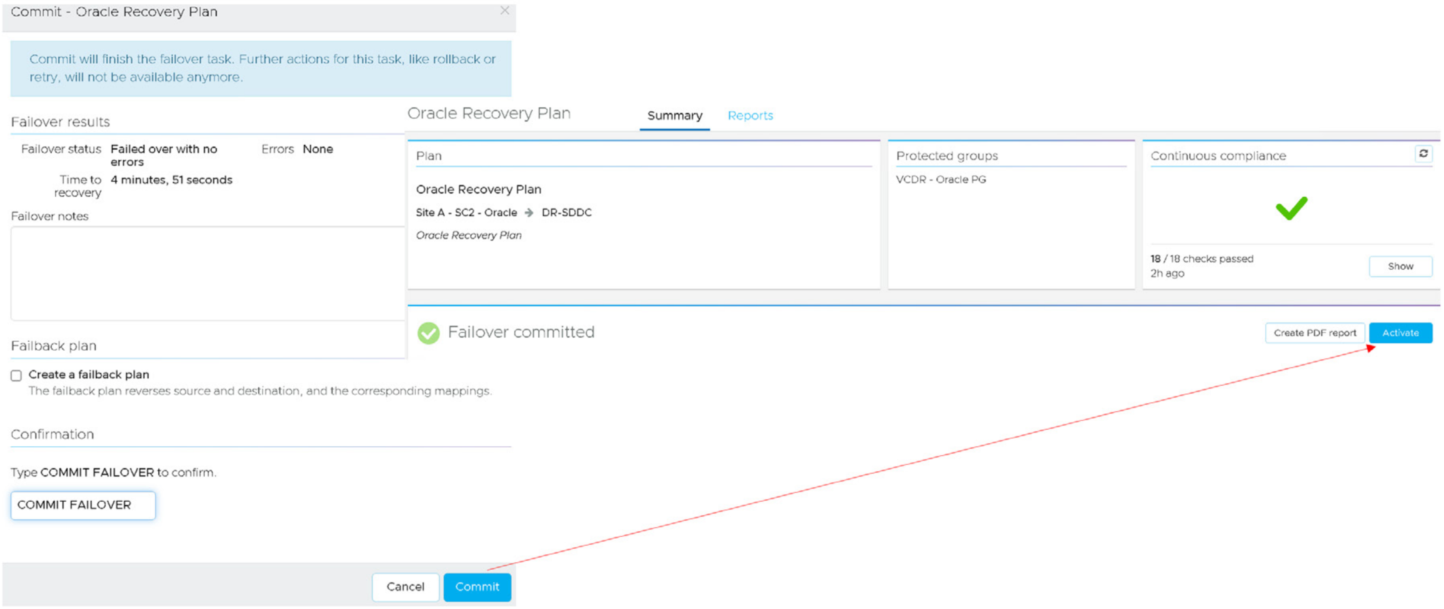
Commit › Rollback

Success

Step		Timestamp	Duration	Progress
✓ Step 1.	Prepare cloud storage resources to run VMs for step **Recover protection group Oracle Test**	Jul-19 04:52 pm	< 1m	Finished
✓ Step 2.	Recover protection group Oracle Test	Jul-19 04:52 pm	4m	Finished
✓ Step 3.	Wait for user input: Do you wish to continue?	Jul-19 04:56 pm	1m	Finished
✓ Step 4.	Recover all remaining VMs, files, and groups	Jul-19 04:57 pm	< 1m	Finished
✓ Step 5.	Migrate to SDDC datastore VMs recovered in step **Recover protection group Oracle Test**	Jul-19 04:57 pm	1h	Finished
✓ Step 6.	Release cloud storage resources for step **Recover all remaining VMs, files, and groups**	Jul-19 05:44 pm	< 1m	Finished

FIGURE 235. Failover of DR Plan Completed Successfully

After a failover finishes, commit the plan to make the effects permanent. When you commit a completed failover plan, the plan transitions to the failover committed state. Commit a failover with extra caution. Until you explicitly commit the failover operation, it can still be rolled back (even following a successful completion). But after commit, there is no rollback.



Commit - Oracle Recovery Plan

Commit will finish the failover task. Further actions for this task, like rollback or retry, will not be available anymore.

Failover results

Failover status: Failed over with no errors

Errors: None

Time to recovery: 4 minutes, 51 seconds

Failover notes

Failback plan

□ Create a failback plan

The failback plan reverses source and destination, and the corresponding mappings.

Confirmation

Type **COMMIT FAILOVER** to confirm.

COMMIT FAILOVER

Cancel | Commit

Oracle Recovery Plan — Summary | Reports

Plan

Oracle Recovery Plan

Site A - SC2 - Oracle → DR-SDDC

Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

✓

18 / 18 checks passed

2h ago

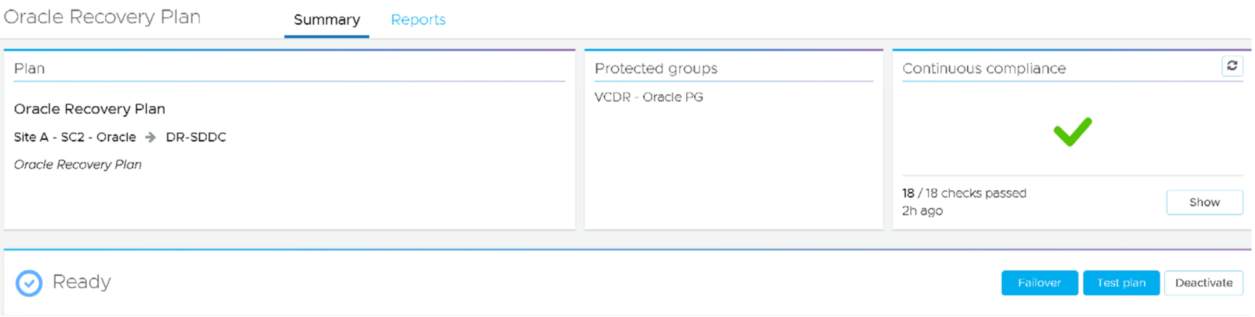
Show

✓ Failover committed

Create PDF report | Activate

FIGURE 236. Commit Failover of DR Plan

In event of a real DR, the plan should be deactivated so that any further compliance checks will not run and error out. In this case, the recovery plan was left activated as the failover DR was a simulated exercise.



Plan

Oracle Recovery Plan
Site A - SC2 - Oracle → DR-SDDC
Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

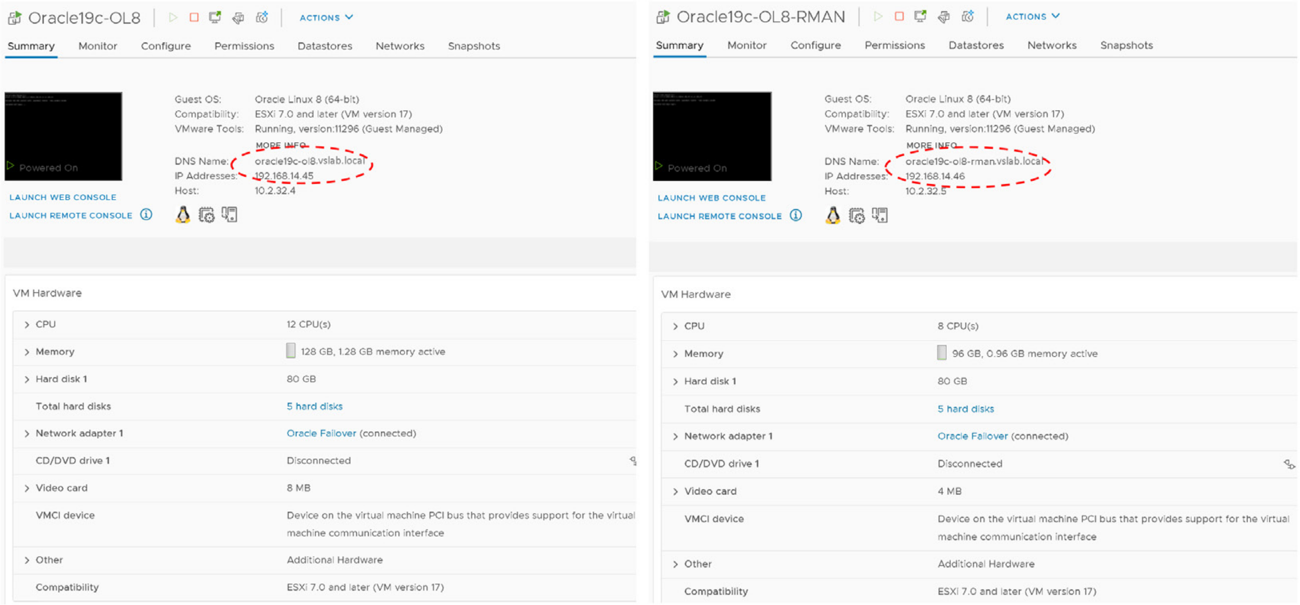
Continuous compliance

18 / 18 checks passed
2h ago

Ready

FIGURE 237. Recovery DR Plan Status

The Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are recovered on the DR site as show below:



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 192.168.14.45
Host: 10.2.32.4

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	Oracle Failover (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.vslab.local
IP Addresses: 192.168.14.46
Host: 10.2.32.5

VM Hardware

CPU	8 CPU(s)
Memory	96 GB, 0.96 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	Oracle Failover (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 238. VM Oracle19c-OL8 and Oracle19c-OL8-RMAN Status

The Oracle VM **Oracle19c-OL8** is up with IP address 192.168.14.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 192.168.14.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

Learn more about *Running a Failover DR Plan*.

Failback DR Plan

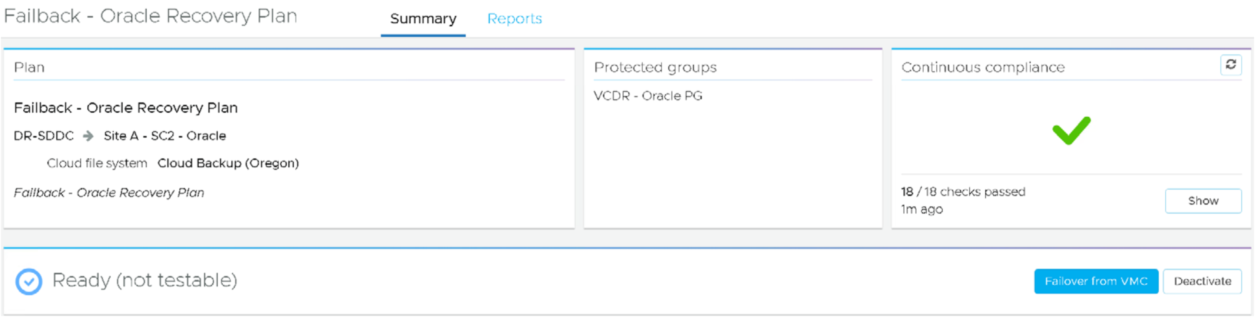
Once the protected site is made available after a disaster event, the steps to run the failback DR plan **Failback-Oracle Recovery Plan** can be employed as shown below.

You can run a DR plan to failback from a VMware Cloud on AWS SDDC to a protected vSphere site. Failback from an SDDC returns only changed data. There is no rehydration, and the data remains in its native compressed and deduplicated form.

Learn more about *Running a Failback DR Plan*.

As mentioned in the previous section, the failover of the DR plan **Oracle Recovery Plan** was actually a simulated one, so Protected Site A was still available. In this case, power the Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** down before proceeding.

The failback DR plan is as shown below:



Failback - Oracle Recovery Plan

Plan

Failback - Oracle Recovery Plan

DR-SDDC → Site A - SC2 - Oracle

Cloud file system Cloud Backup (Oregon)

Failback - Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

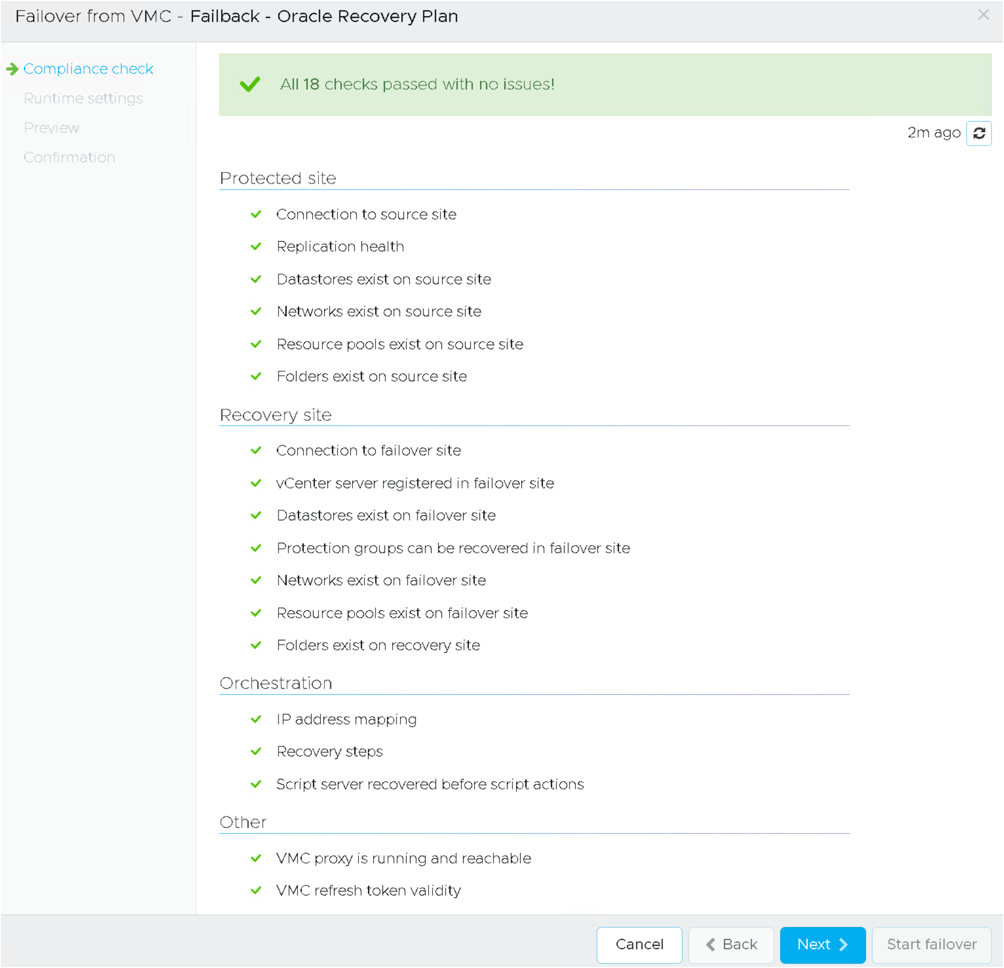
Continuous compliance

18 / 18 checks passed
1m ago

Ready (not testable)

FIGURE 239. Failback DR Plan

The failback DR plan steps pass all validation checks as shown below:



Failover from VMC - Failback - Oracle Recovery Plan

✓ All 18 checks passed with no issues!

2m ago

Protected site

- ✓ Connection to source site
- ✓ Replication health
- ✓ Datastores exist on source site
- ✓ Networks exist on source site
- ✓ Resource pools exist on source site
- ✓ Folders exist on source site

Recovery site

- ✓ Connection to failover site
- ✓ vCenter server registered in failover site
- ✓ Datastores exist on failover site
- ✓ Protection groups can be recovered in failover site
- ✓ Networks exist on failover site
- ✓ Resource pools exist on failover site
- ✓ Folders exist on recovery site

Orchestration

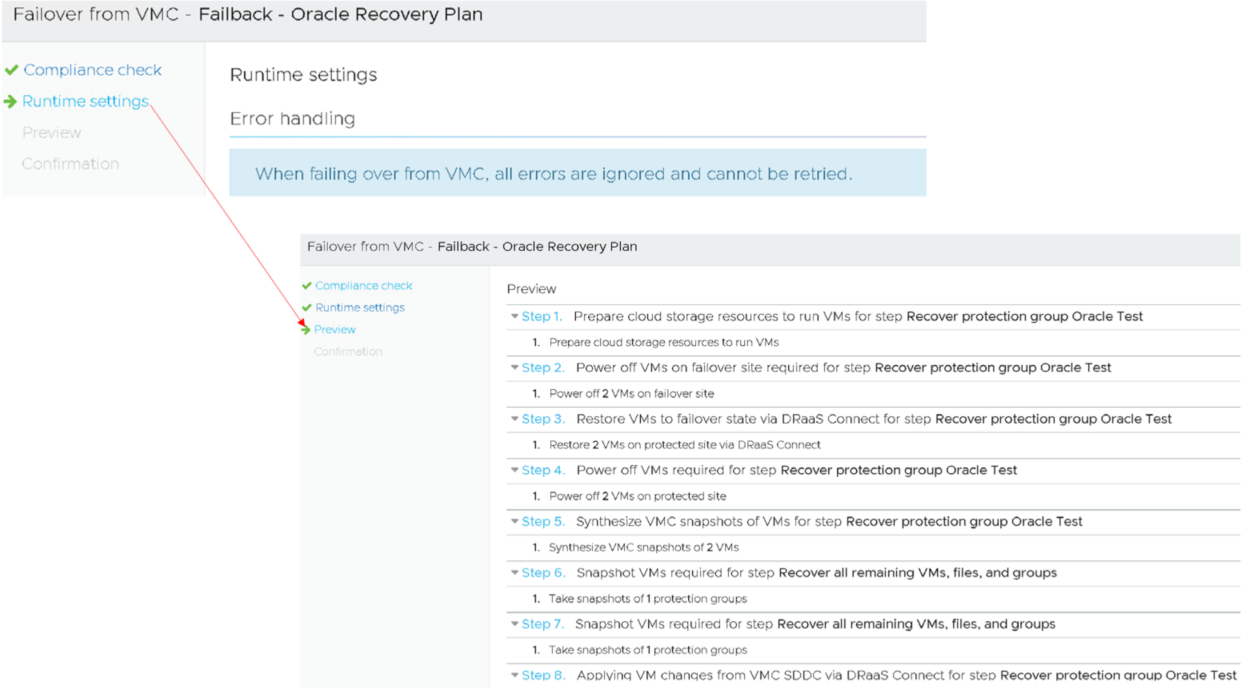
- ✓ IP address mapping
- ✓ Recovery steps
- ✓ Script server recovered before script actions

Other

- ✓ VMC proxy is running and reachable
- ✓ VMC refresh token validity

FIGURE 240. Failback DR Plan Steps

Steps of the failback DR plan are continued below:



Failover from VMC - **Failback - Oracle Recovery Plan**

Runtime settings

Error handling

When failing over from VMC, all errors are ignored and cannot be retried.

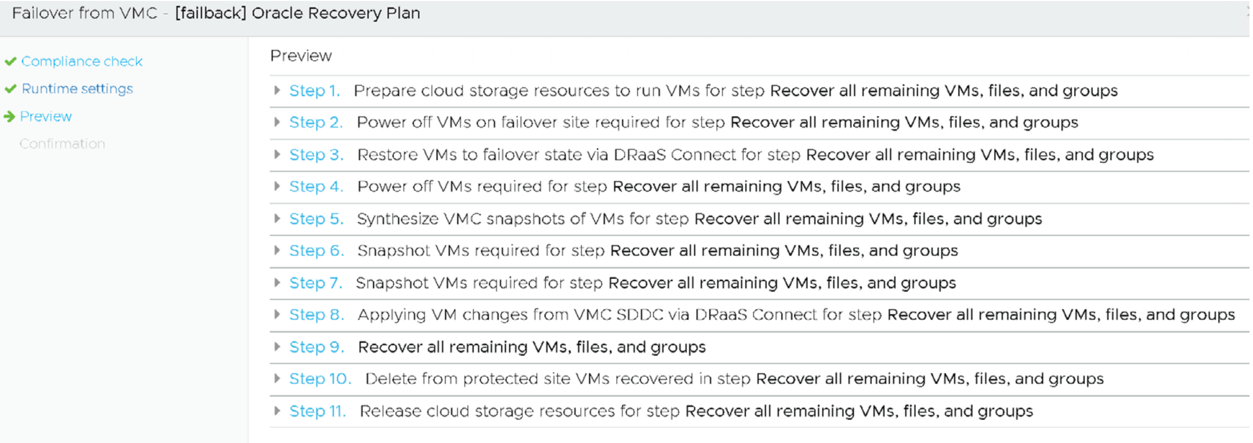
Failover from VMC - **Failback - Oracle Recovery Plan**

Preview

- Step 1. Prepare cloud storage resources to run VMs for step **Recover protection group Oracle Test**
  1. Prepare cloud storage resources to run VMs
- Step 2. Power off VMs on failover site required for step **Recover protection group Oracle Test**
  1. Power off **2** VMs on failover site
- Step 3. Restore VMs to failover state via DRaaS Connect for step **Recover protection group Oracle Test**
  1. Restore **2** VMs on protected site via DRaaS Connect
- Step 4. Power off VMs required for step **Recover protection group Oracle Test**
  1. Power off **2** VMs on protected site
- Step 5. Synthesize VMC snapshots of VMs for step **Recover protection group Oracle Test**
  1. Synthesize VMC snapshots of **2** VMs
- Step 6. Snapshot VMs required for step **Recover all remaining VMs, files, and groups**
  1. Take snapshots of **1** protection groups
- Step 7. Snapshot VMs required for step **Recover all remaining VMs, files, and groups**
  1. Take snapshots of **1** protection groups
- Step 8. Applying VM changes from VMC SDDC via DRaaS Connect for step **Recover protection group Oracle Test**

FIGURE 241. Failback DR Plan Steps Continued

The summary of the failback DR plan steps is shown below:

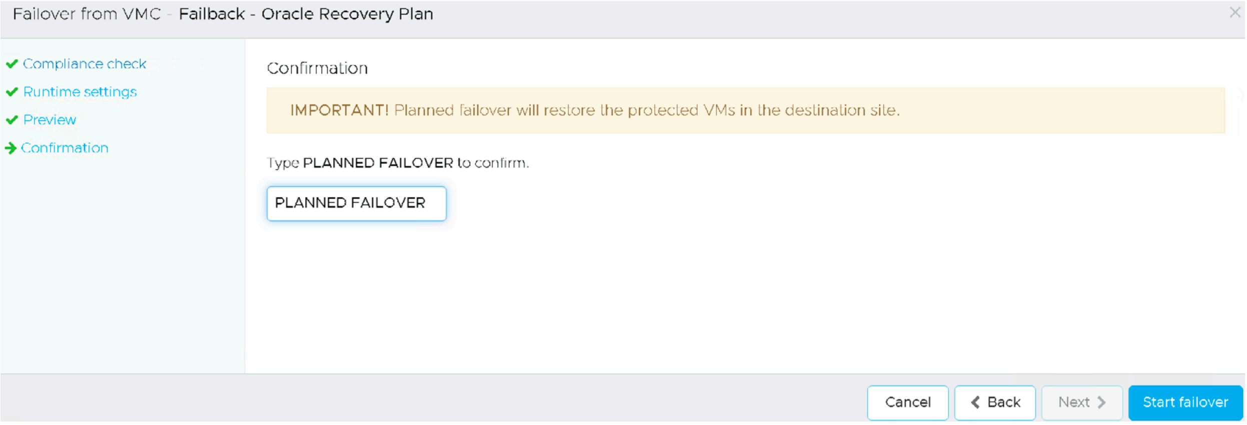


Failover from VMC - **[failback] Oracle Recovery Plan**

Preview

- Step 1. Prepare cloud storage resources to run VMs for step **Recover all remaining VMs, files, and groups**
- Step 2. Power off VMs on failover site required for step **Recover all remaining VMs, files, and groups**
- Step 3. Restore VMs to failover state via DRaaS Connect for step **Recover all remaining VMs, files, and groups**
- Step 4. Power off VMs required for step **Recover all remaining VMs, files, and groups**
- Step 5. Synthesize VMC snapshots of VMs for step **Recover all remaining VMs, files, and groups**
- Step 6. Snapshot VMs required for step **Recover all remaining VMs, files, and groups**
- Step 7. Snapshot VMs required for step **Recover all remaining VMs, files, and groups**
- Step 8. Applying VM changes from VMC SDDC via DRaaS Connect for step **Recover all remaining VMs, files, and groups**
- Step 9. **Recover all remaining VMs, files, and groups**
- Step 10. Delete from protected site VMs recovered in step **Recover all remaining VMs, files, and groups**
- Step 11. Release cloud storage resources for step **Recover all remaining VMs, files, and groups**

FIGURE 242. Failback DR Plan Steps Summary



Confirmation

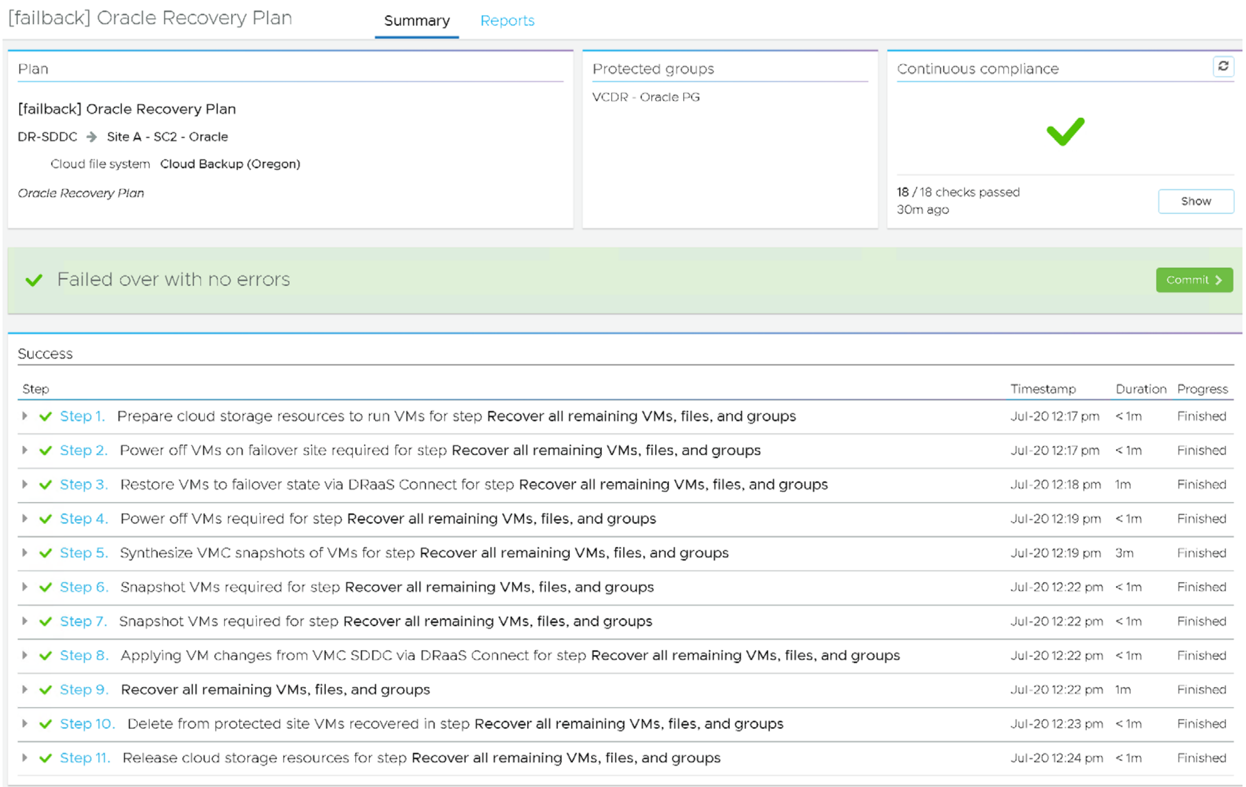
IMPORTANT! Planned failover will restore the protected VMs in the destination site.

Type PLANNED FAILOVER to confirm.

PLANNED FAILOVER

FIGURE 243. Confirmation of Planned Failback

The failback completes successfully.



[failback] Oracle Recovery Plan

DR-SDDC → Site A - SC2 - Oracle

Cloud file system Cloud Backup (Oregon)

Oracle Recovery Plan

VCDR - Oracle PG

18 / 18 checks passed
30m ago

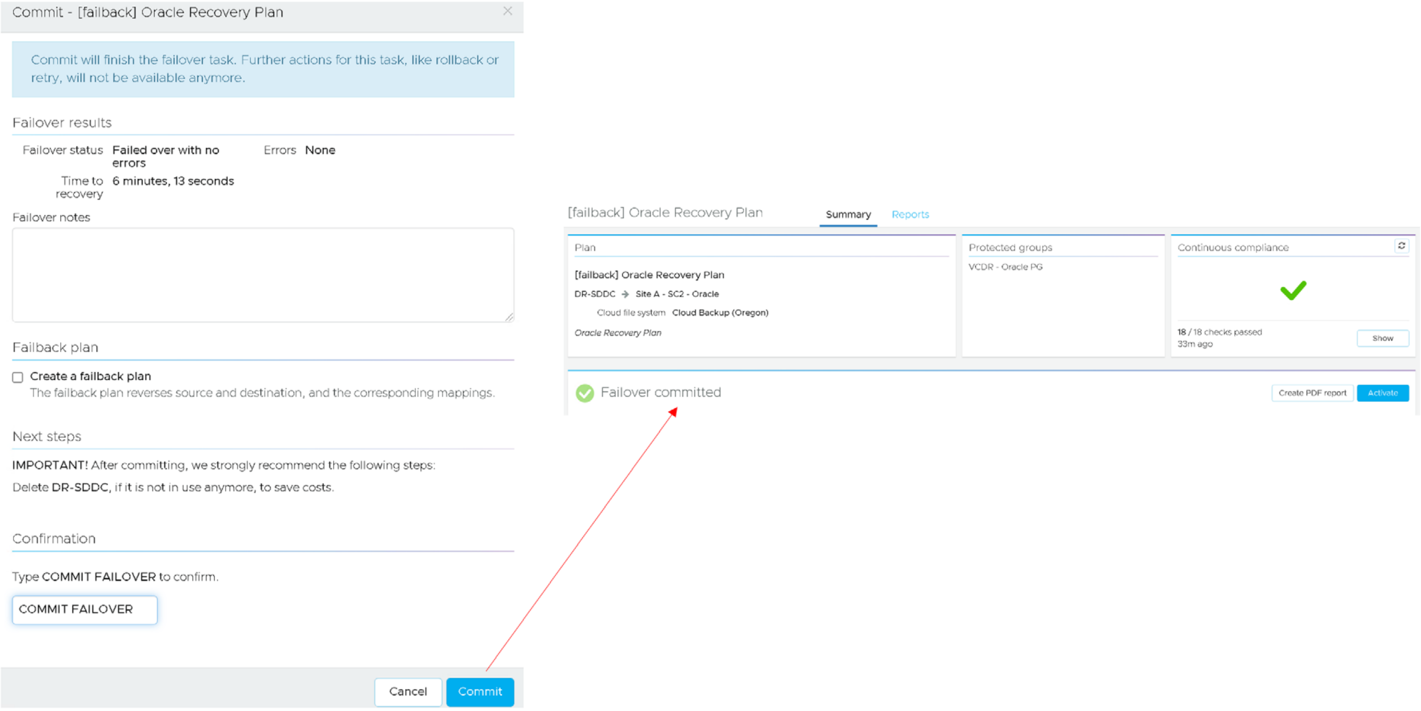
✓ Failed over with no errors

Success

Step	Timestamp	Duration	Progress
✓ Step 1. Prepare cloud storage resources to run VMs for step **Recover all remaining VMs, files, and groups**	Jul-20 12:17 pm	< 1m	Finished
✓ Step 2. Power off VMs on failover site required for step **Recover all remaining VMs, files, and groups**	Jul-20 12:17 pm	< 1m	Finished
✓ Step 3. Restore VMs to failover state via DRaaS Connect for step **Recover all remaining VMs, files, and groups**	Jul-20 12:18 pm	1m	Finished
✓ Step 4. Power off VMs required for step **Recover all remaining VMs, files, and groups**	Jul-20 12:19 pm	< 1m	Finished
✓ Step 5. Synthesize VMC snapshots of VMs for step **Recover all remaining VMs, files, and groups**	Jul-20 12:19 pm	3m	Finished
✓ Step 6. Snapshot VMs required for step **Recover all remaining VMs, files, and groups**	Jul-20 12:22 pm	< 1m	Finished
✓ Step 7. Snapshot VMs required for step **Recover all remaining VMs, files, and groups**	Jul-20 12:22 pm	< 1m	Finished
✓ Step 8. Applying VM changes from VMC SDDC via DRaaS Connect for step **Recover all remaining VMs, files, and groups**	Jul-20 12:22 pm	< 1m	Finished
✓ Step 9. **Recover all remaining VMs, files, and groups**	Jul-20 12:22 pm	1m	Finished
✓ Step 10. Delete from protected site VMs recovered in step **Recover all remaining VMs, files, and groups**	Jul-20 12:23 pm	< 1m	Finished
✓ Step 11. Release cloud storage resources for step **Recover all remaining VMs, files, and groups**	Jul-20 12:24 pm	< 1m	Finished

FIGURE 244. Planned Failback Status

As in the case of a failover, after a failback finishes, commit the plan to make the effects permanent. When you commit a completed failback plan, the plan transitions to the committed state.



Commit - [failback] Oracle Recovery Plan

Commit will finish the failover task. Further actions for this task, like rollback or retry, will not be available anymore.

Failover results

Failover status	Failed over with no errors	Errors	None
Time to recovery	6 minutes, 13 seconds		

Failover notes

Failback plan

□ Create a failback plan
The failback plan reverses source and destination, and the corresponding mappings.

Next steps

IMPORTANT! After committing, we strongly recommend the following steps:
Delete DR-SDDC, if it is not in use anymore, to save costs.

Confirmation

Type COMMIT FAILOVER to confirm.

COMMIT FAILOVER

[failback] Oracle Recovery Plan

Plan

[failback] Oracle Recovery Plan
DR-SDDC → Site A - SC2 - Oracle
Cloud file system Cloud Backup (Oregon)
Oracle Recovery Plan

Protected groups

VCDR - Oracle PG

Continuous compliance

18 / 18 checks passed
33m ago

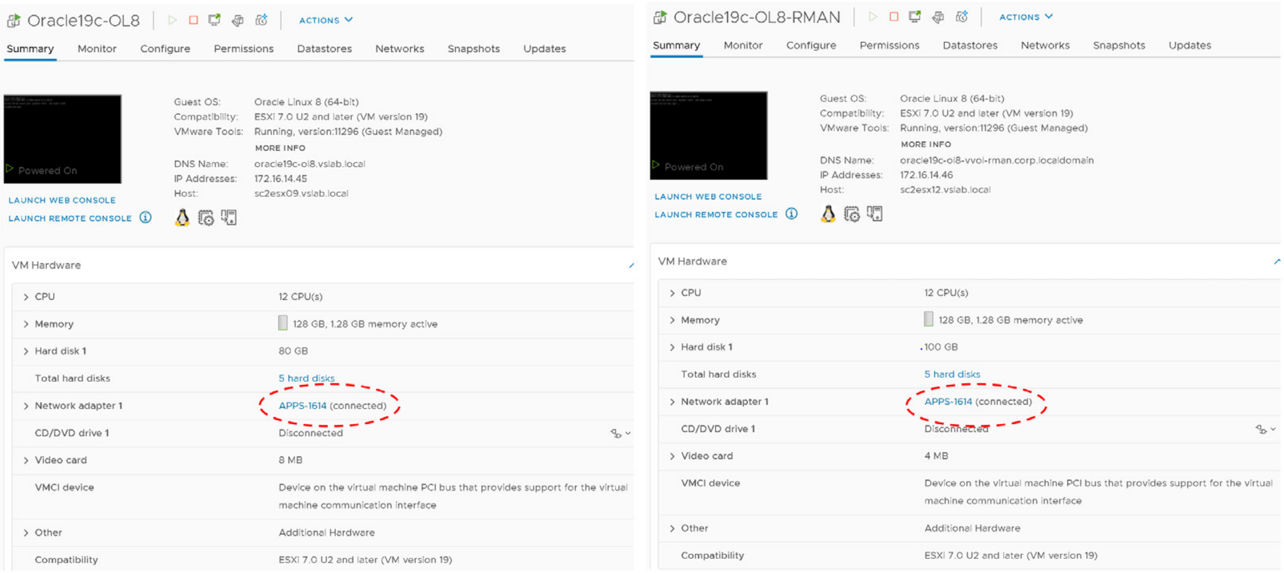
Failover committed

FIGURE 245. Commit to Failover for Planned Failback

The Oracle VM **Oracle19c-OL8** is up with IP address 172.16.14.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.16.14.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

VMware Cloud Disaster Recovery uses regularly scheduled snapshots to replicate to the SCFS. VMware snapshots are point-in-time (PIT) snapshots and are therefore crash-consistent. Write-order fidelity is guaranteed for all VMDKs of the VM.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.16.14.45
Host: sc2esx09.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

Oracle19c-OL8-RMAN

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.16.14.46
Host: sc2esx12.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 246. Oracle VM Oracle19c-OL8 and Oracl19c-OL8-RMAN Status

Following a successful failback, you must clean up the failback source site in preparation for subsequent recovery operations.

Specifically, the stale VMs left behind on the datastores of the failback source site must be deleted to avoid conflicts for future recoveries from the protected site. Similarly, you must demote protection groups on the recovery source.

Learn more about *Running a Failback DR Plan*.

Storage-Level Disaster Recovery

Storage-level disaster recovery can be used to provide storage LUN-level OR vVOLs-level replication from on-premises Site A to Site B.

Using array-based replication with Site Recovery Manager ensures one or more storage arrays at the protected site to replicate data to peer arrays at the recovery site.

With storage replication adapters (SRAs), Site Recovery Manager can be integrated with a wide variety of arrays.

To use array-based replication with Site Recovery Manager, replication must be configured first before one can configure Site Recovery Manager to use it.

As noted in *Supported Backup, Restore and Recovery Operations using Third Party Snapshot Technologies* (Oracle Doc ID 604683.1), third-party storage vendor snapshots must conform to the following requirements:

- Integrated with Oracle's recommended restore and recovery operations above
- Database crash-consistent at the point of the snapshot
- Write-ordering is preserved for each file within a snapshot

On-premises using vSphere VMFS Storage

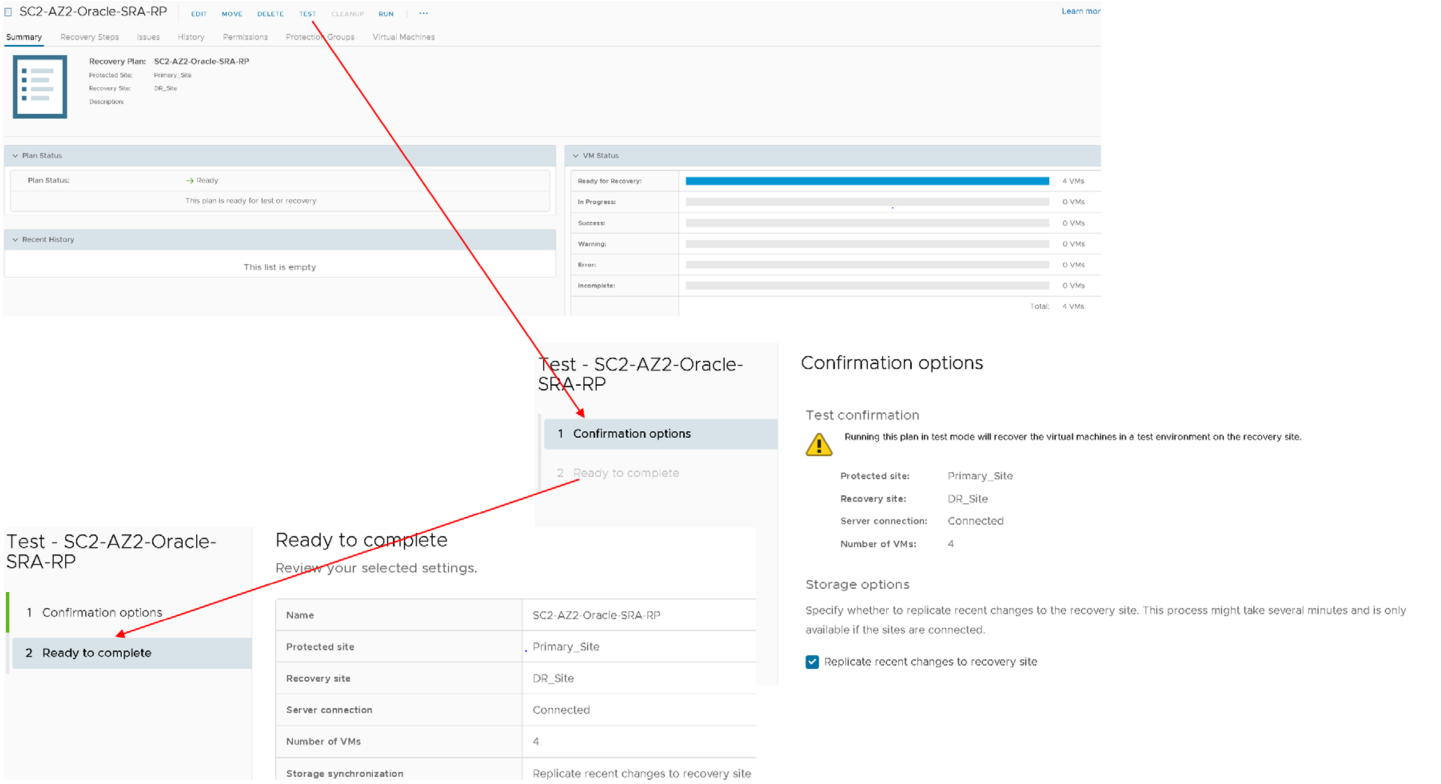
This use case focusses on the utilization of VMware Site Recovery Manager with storage-based replication using Pure Storage to provide disaster recovery on a storage **LUN (VMFS)** level, to both single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** and Oracle RAC **prac19c**, from on-premises Site A to Site B and vice-versa.

Test Recovery Plan

The recovery plan can be tested before being used for planned migration or for disaster recovery.

With array-based replication, as part of testing a recovery plan, the VMs on the protected site are still replicated to the replica VM disk files on the recovery site. During a test recovery, the array creates a snapshot of the volumes hosting the VM disk files on the recovery site. Array replication continues normally while the test is in progress. When you perform cleanup after running a test, the array removes the snapshots that were created earlier as part of the test recovery workflow.

Steps to test the recovery plan **SC2-AZ2-Oracle-SRA-**RP are as shown below:



Recovery Plan: SC2-AZ2-Oracle-SRA-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

This list is empty

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Test - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Test confirmation

Running this plan in test mode will recover the virtual machines in a test environment on the recovery site.

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	4

Storage options

Specify whether to replicate recent changes to the recovery site. This process might take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

Test - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

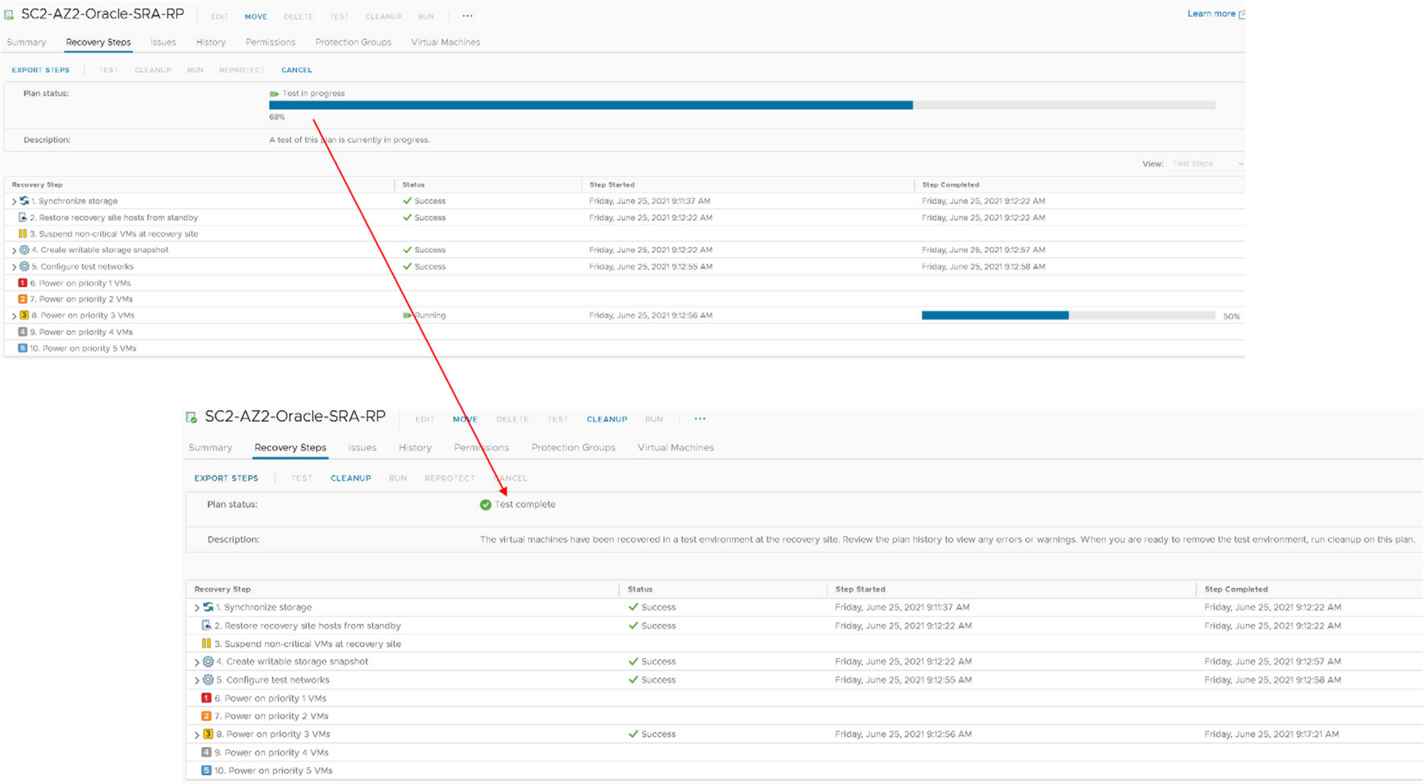
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Storage synchronization	Replicate recent changes to recovery site

FIGURE 247. Test Recovery Plan SC2-AZ2-Oracle-SRA-RP

Testing of the recovery plan **SC2-AZ2-Oracle-SRA-RP** is successful.



Plan status: Test in progress
68%

Description: A test of this plan is currently in progress.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Friday, June 25, 2021 9:11:37 AM	Friday, June 25, 2021 9:12:22 AM
2. Restore recovery site hosts from standby	✓ Success	Friday, June 25, 2021 9:12:22 AM	Friday, June 25, 2021 9:12:22 AM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Friday, June 25, 2021 9:12:22 AM	Friday, June 25, 2021 9:12:57 AM
5. Configure test networks	✓ Success	Friday, June 25, 2021 9:12:55 AM	Friday, June 25, 2021 9:12:58 AM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	Running	Friday, June 25, 2021 9:12:56 AM	50%
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

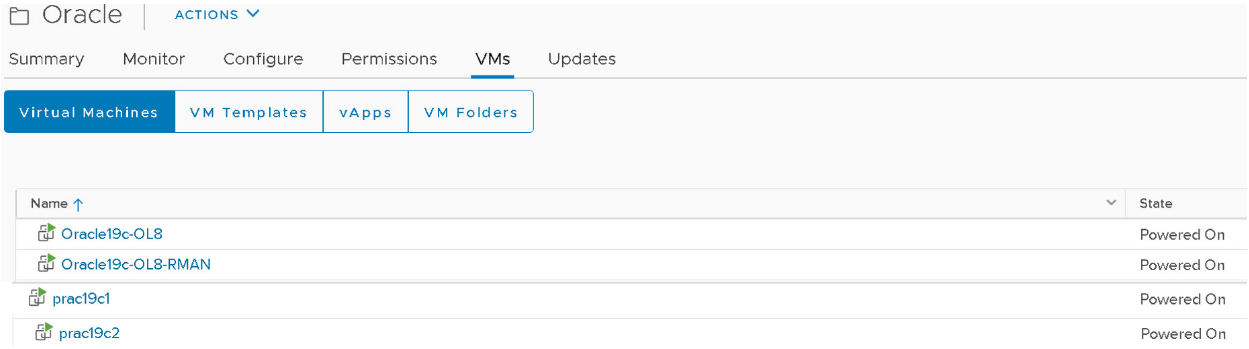
Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Friday, June 25, 2021 9:11:37 AM	Friday, June 25, 2021 9:12:22 AM
2. Restore recovery site hosts from standby	✓ Success	Friday, June 25, 2021 9:12:22 AM	Friday, June 25, 2021 9:12:22 AM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Friday, June 25, 2021 9:12:22 AM	Friday, June 25, 2021 9:12:57 AM
5. Configure test networks	✓ Success	Friday, June 25, 2021 9:12:55 AM	Friday, June 25, 2021 9:12:58 AM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Friday, June 25, 2021 9:12:56 AM	Friday, June 25, 2021 9:17:21 AM
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

FIGURE 248. Test Recovery Plan SC2-AZ2-Oracle-SRA-RP Successful

The protected VMs are still powered on and running on the protected site.

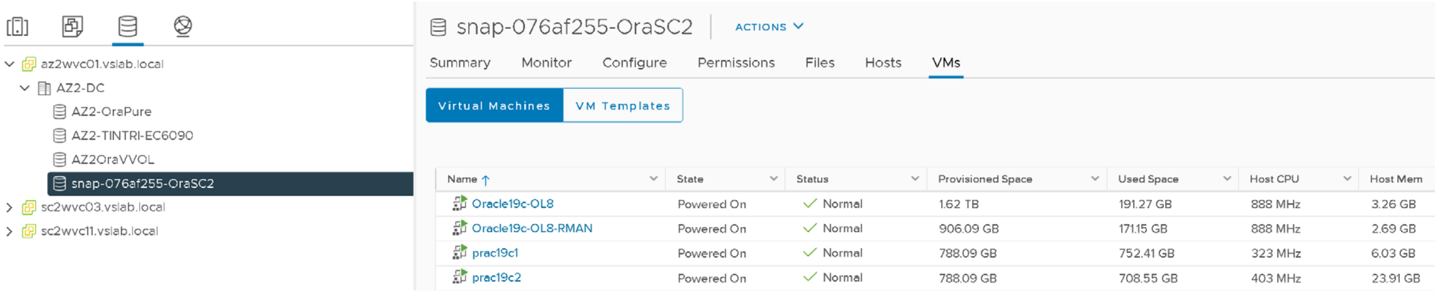


Name ↑	State
Oracle19c-OL8	Powered On
Oracle19c-OL8-RMAN	Powered On
prac19c1	Powered On
prac19c2	Powered On

FIGURE 249. Protected VM Status

During a test recovery, the array creates a snapshot of the volumes hosting the VM's disk files on the recovery site and the datastore on that snapshot is brought up. The VMs on that snapshot's datastores are powered up as below for testing.

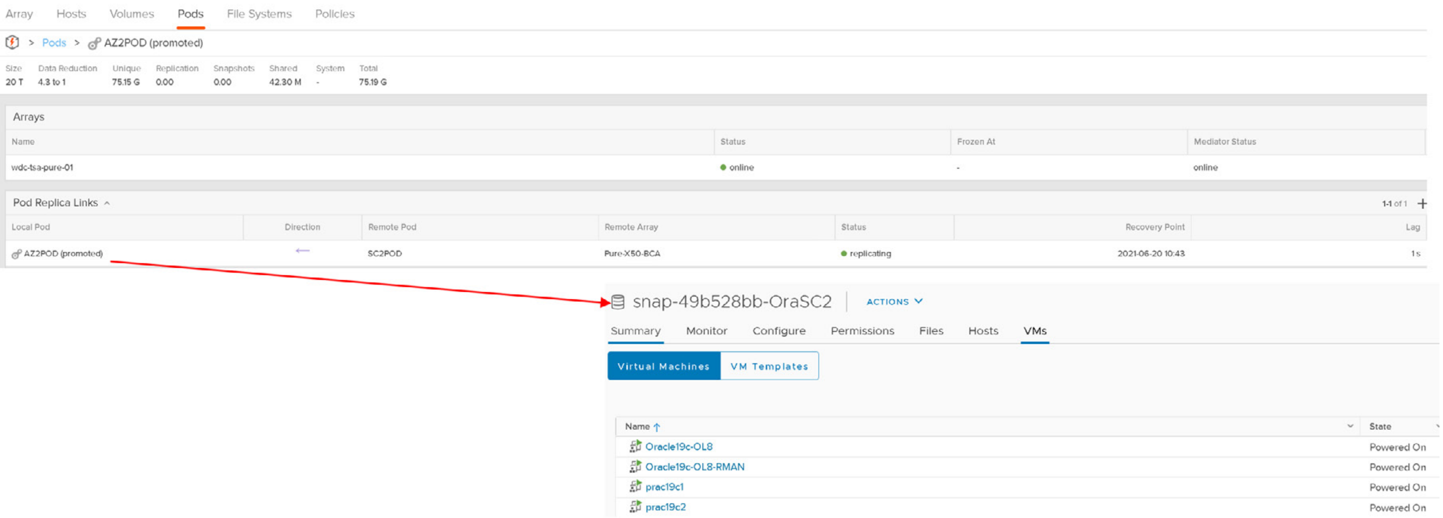
The target pod is promoted with the resignature process for VMFS, which includes a mandatory step adding a name prefix in the form of snap-XXXXXXX (e.g., **snap-076af255-OraSC2**).



Name ↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
Oracle19c-OL8	Powered On	✓ Normal	1.62 TB	191.27 GB	888 MHz	3.26 GB
Oracle19c-OL8-RMAN	Powered On	✓ Normal	906.09 GB	171.15 GB	888 MHz	2.69 GB
prac19c1	Powered On	✓ Normal	788.09 GB	752.41 GB	323 MHz	6.03 GB
prac19c2	Powered On	✓ Normal	788.09 GB	708.55 GB	403 MHz	23.91 GB

FIGURE 250. Test Recovery Plan Storage Snapshot on Site B

The contents of the Site B storage snapshot are as shown below:



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.15 G	0.00	0.00	42.30 M	-	75.19 G

Arrays

Name	Status	Frozen At	Mediator Status
wdc-tsa-pure-01	● online	-	online

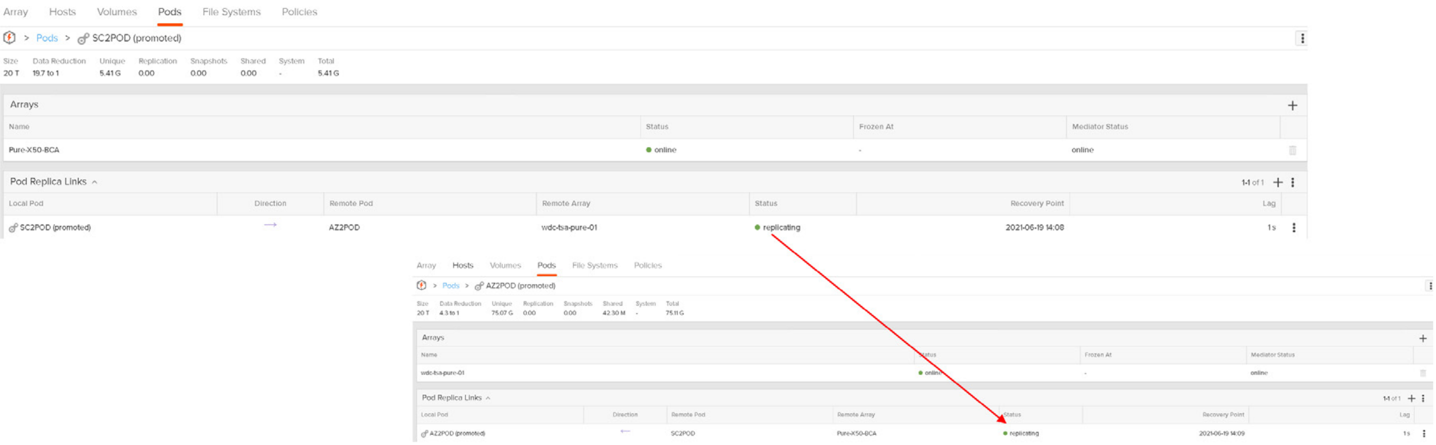
Pod Replica Links ^ 1-1 of 1

Local Pod	Direction	Remote Pod	Remote Array	Status	Recovery Point	Lag
AZ2POD (promoted)	←	SC2POD	Pure-X50-BCA	● replicating	2021-06-20 10:43	1 s

Name ↑	State
Oracle19c-OL8	Powered On
Oracle19c-OL8-RMAN	Powered On
prac19c1	Powered On
prac19c2	Powered On

FIGURE 251. Site B Storage Snapshot Contents

Array replication continues normally while the test is in progress.



Array Hosts Volumes Pods File Systems Policies

Pods > SC2POD (promoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	19.7 to 1	5.41 G	0.00	0.00	0.00	-	5.41 G

Arrays

Name	Status	Frozen At	Mediator Status
Pure-X50-BCA	● online	-	online

Pod Replica Links 1-1 of 1

Local Pod	Direction	Remote Pod	Remote Array	Status	Recovery Point	Lag
SC2POD (promoted)	→	AZ2POD	wdc-tsa-pure-01	● replicating	2021-06-19 14:08	1 s

Array Hosts Volumes Pods File Systems Policies

Pods > AZ2POD (promoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.07 G	0.00	0.00	42.30 M	-	75.11 G

Arrays

Name	Status	Frozen At	Mediator Status
wdc-tsa-pure-01	● online	-	online

Pod Replica Links 1-1 of 1

Local Pod	Direction	Remote Pod	Remote Array	Status	Recovery Point	Lag
AZ2POD (promoted)	←	SC2POD	Pure-X50-BCA	● replicating	2021-06-19 14:09	1 s

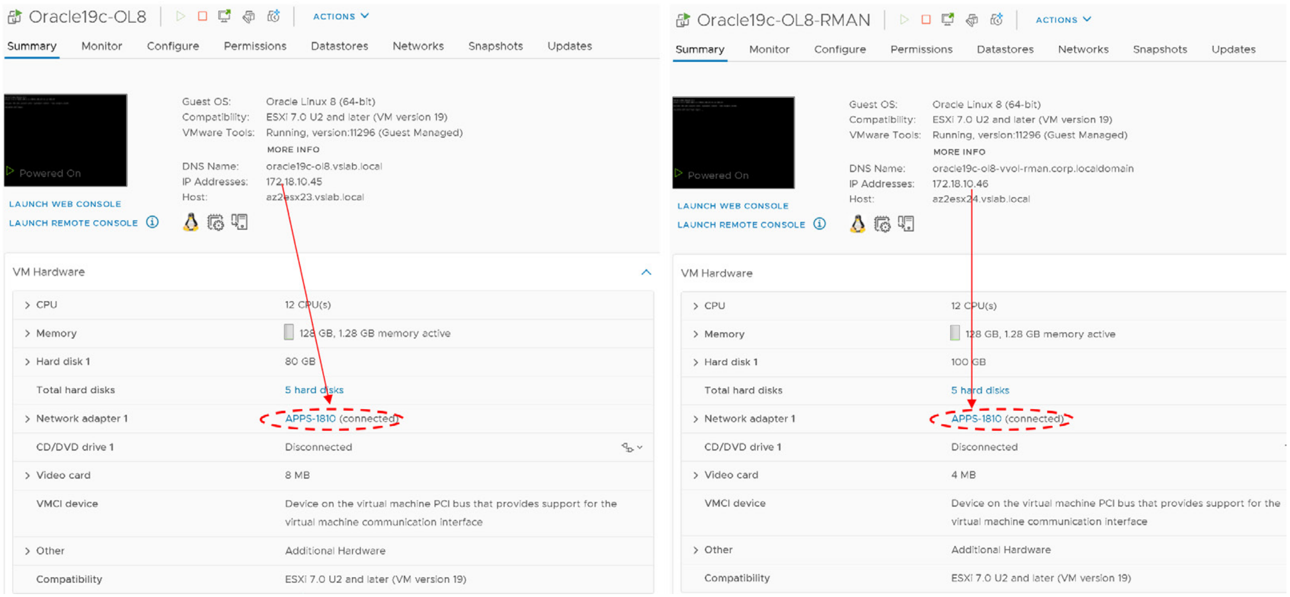
FIGURE 252. Site A and Site B Array Replication in Progress

Both single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered up and connected to the recovery site test network **APPS-1810**. The IP addressing scheme is followed as defined in the network mapping section.

Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database **vvol19c** is up. 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 VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

The storage-based snapshot is crash-consistent and write-ordering is preserved for each file within a snapshot.



Oracle19c-OL8 ACTIONS

Summary Monitor Configure Permissions Datastores Networks Snapshots Updates

Powered On

LAUNCH WEB CONSOLE

LAUNCH REMOTE CONSOLE

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
MORE INFO
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local

VM Hardware

> CPU	12 CPU(s)
> Memory	128 GB, 1.28 GB memory active
> Hard disk 1	80 GB
Total hard disks	5 hard disks
> Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
> Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
> Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

Oracle19c-OL8-RMAN ACTIONS

Summary Monitor Configure Permissions Datastores Networks Snapshots Updates

Powered On

LAUNCH WEB CONSOLE

LAUNCH REMOTE CONSOLE

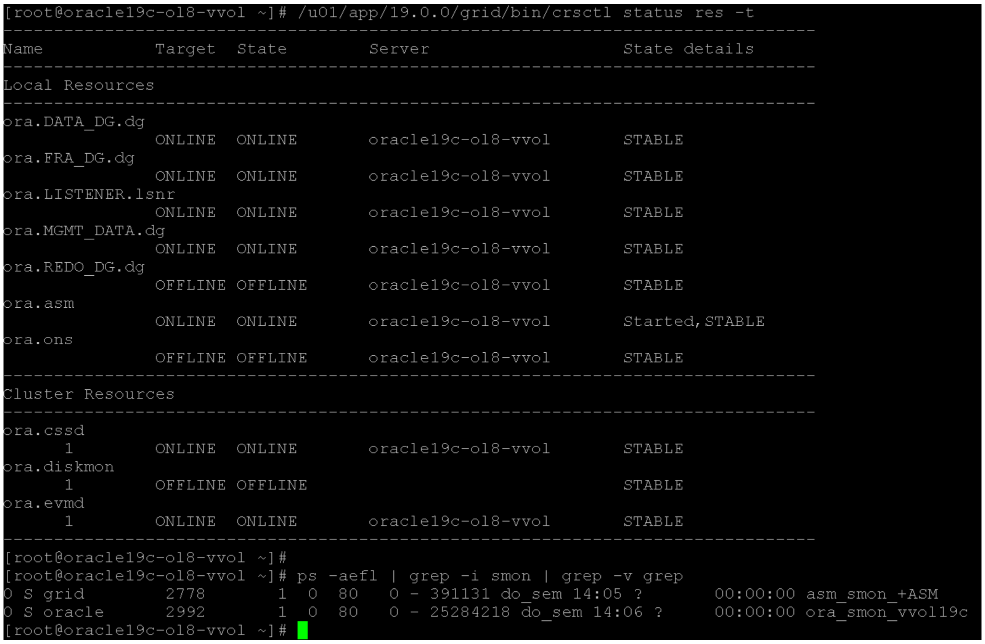
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
MORE INFO
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx24.vslab.local

VM Hardware

> CPU	12 CPU(s)
> Memory	128 GB, 1.28 GB memory active
> Hard disk 1	100 GB
Total hard disks	5 hard disks
> Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
> Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
> Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 253. Oracle VMs Oracle19c-OL8 and Oracle19c-OL8-RMAN Networking Details

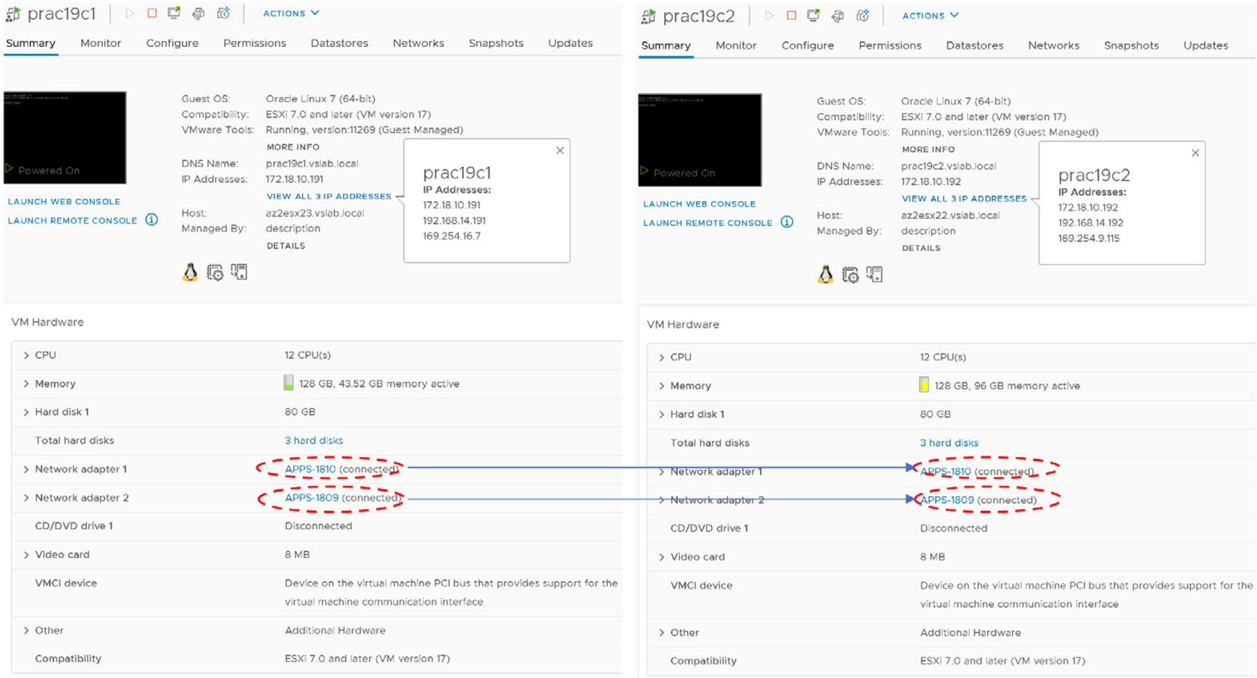
All ASM disk groups are online and the ASM and Oracle instance is up.



```
[root@oracle19c-ol8-vvol ~]# /u01/app/19.0.0/grid/bin/crsctl status res -t
--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.DATA_DG.dg
               ONLINE  ONLINE       oracle19c-ol8-vvol       STABLE
ora.FRA_DG.dg
               ONLINE  ONLINE       oracle19c-ol8-vvol       STABLE
ora.LISTENER.lsnr
               ONLINE  ONLINE       oracle19c-ol8-vvol       STABLE
ora.MGMT_DATA.dg
               ONLINE  ONLINE       oracle19c-ol8-vvol       STABLE
ora.REDO_DG.dg
               OFFLINE OFFLINE      oracle19c-ol8-vvol       STABLE
ora.asm
               ONLINE  ONLINE       oracle19c-ol8-vvol       Started,STABLE
ora.ons
               OFFLINE OFFLINE      oracle19c-ol8-vvol       STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.cssd
      1        ONLINE  ONLINE       oracle19c-ol8-vvol       STABLE
ora.diskmon
      1        OFFLINE OFFLINE                               STABLE
ora.evmd
      1        ONLINE  ONLINE       oracle19c-ol8-vvol       STABLE
--------------------------------------------------------------------------------
[root@oracle19c-ol8-vvol ~]#
[root@oracle19c-ol8-vvol ~]# ps -aefl | grep -i smon | grep -v grep
0 S grid       2778       1  0  80   0 - 391131 do_sem 14:05 ?       00:00:00 asm_smon_+ASM
0 S oracle     2992       1  0  80   0 - 25284218 do_sem 14:06 ?     00:00:00 ora_smon_vvol19c
[root@oracle19c-ol8-vvol ~]#
```

FIGURE 254. Oracle VM Oracle19c-OL8 Services

The Oracle RAC cluster **prac19c** VMs are also powered up. The public interfaces are connected to the recovery site test network **APPS-1810** and private interconnects are connected to the recovery site test network **APPS-1809**. The IP addressing scheme is followed as defined in the network mapping section.



Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.18.10.191
Host: az2esx23.vslab.local
Managed By: description

prac19c1
IP Addresses:
172.18.10.191
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 43.52 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1809 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.18.10.192
Host: az2esx22.vslab.local
Managed By: description

prac19c2
IP Addresses:
172.18.10.192
192.168.14.192
169.254.9.115

VM Hardware

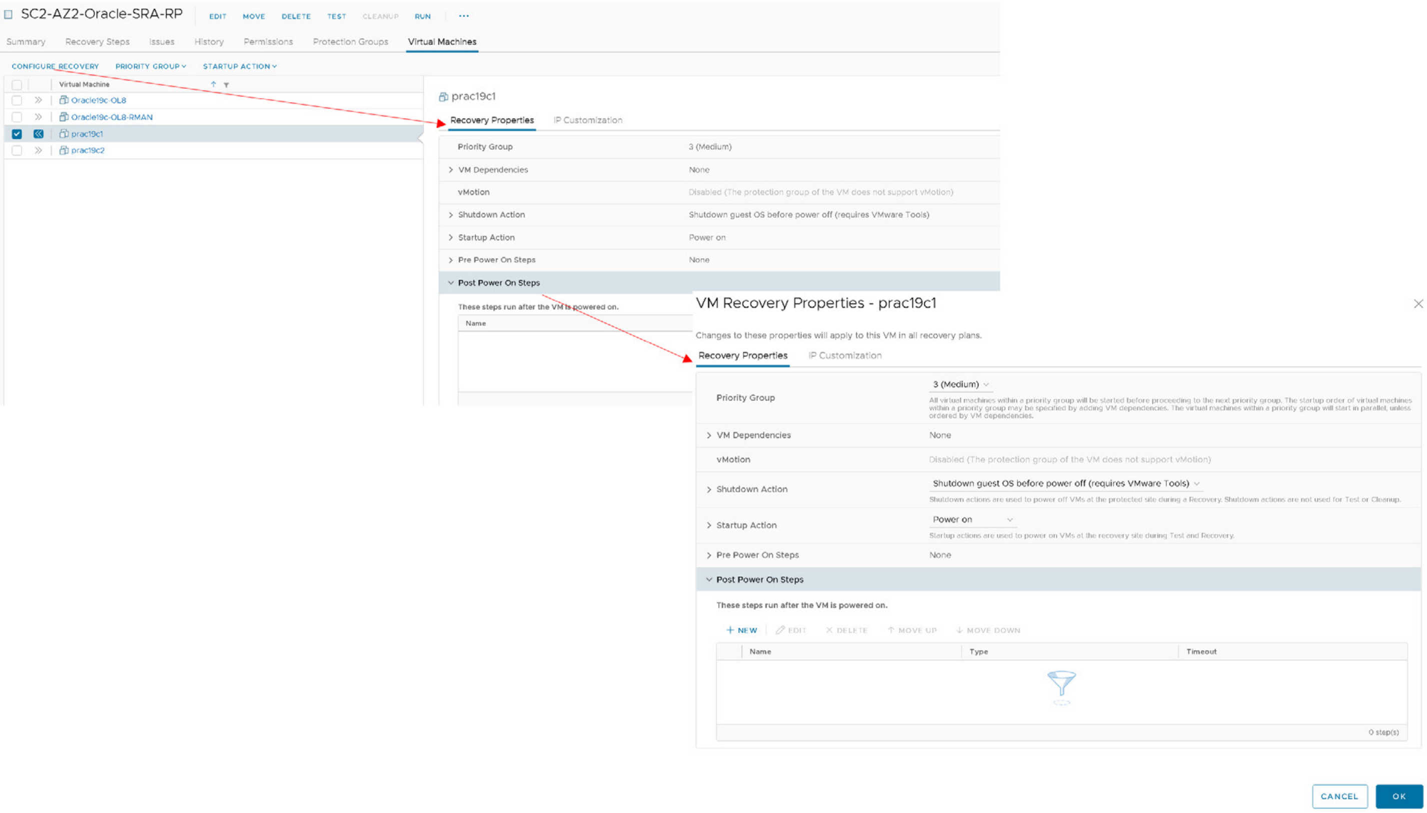
CPU	12 CPU(s)
Memory	128 GB, 96 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1809 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 255. Oracle RAC VM prac19c Networking Details

As part of testing the recovery plan, the network interfaces of the Oracle RAC **prac19c** will be changed to the appropriate test network as defined in the network mappings.

- The VIP and the SCAN IPs have to be changed to the test/recovery network IP scheme in order for the RAC Clusterware to bring up the RAC services.
- The steps to change the RAC VIP IP address can be found in *Oracle 19c Clusterware Administration and Deployment Guide*. The steps to change the Oracle private interconnect IP address can be found in the *Changing Oracle Clusterware Private Network Configuration*.
- The steps to change the RAC SCAN IP addresses can be found in the *My Oracle Support Note How to Update the IP Address of the SCAN VIP Resources (ora.scan{n}.vip) (Doc ID 952903.1)*.
- The steps to change the RAC VIP, scan and private interconnect IP addresses are beyond the scope of this paper.

The recovery plans can be configured and IP customization can be performed for VM networking, if needed.



Priority Group	3 (Medium)
VM Dependencies	None
vMotion	Disabled (The protection group of the VM does not support vMotion)
Shutdown Action	Shutdown guest OS before power off (requires VMware Tools)
Startup Action	Power on
Pre Power On Steps	None
Post Power On Steps	

These steps run after the VM is powered on.

VM Recovery Properties - prac19c1

Changes to these properties will apply to this VM in all recovery plans.

Priority Group	3 (Medium) All virtual machines within a priority group will be started before proceeding to the next priority group. The startup order of virtual machines within a priority group may be specified by adding VM dependencies. The virtual machines within a priority group will start in parallel, unless ordered by VM dependencies.
VM Dependencies	None
vMotion	Disabled (The protection group of the VM does not support vMotion)
Shutdown Action	Shutdown guest OS before power off (requires VMware Tools) Shutdown actions are used to power off VMs at the protected site during a Recovery. Shutdown actions are not used for Test or Cleanup.
Startup Action	Power on Startup actions are used to power on VMs at the recovery site during Test and Recovery.
Pre Power On Steps	None
Post Power On Steps	

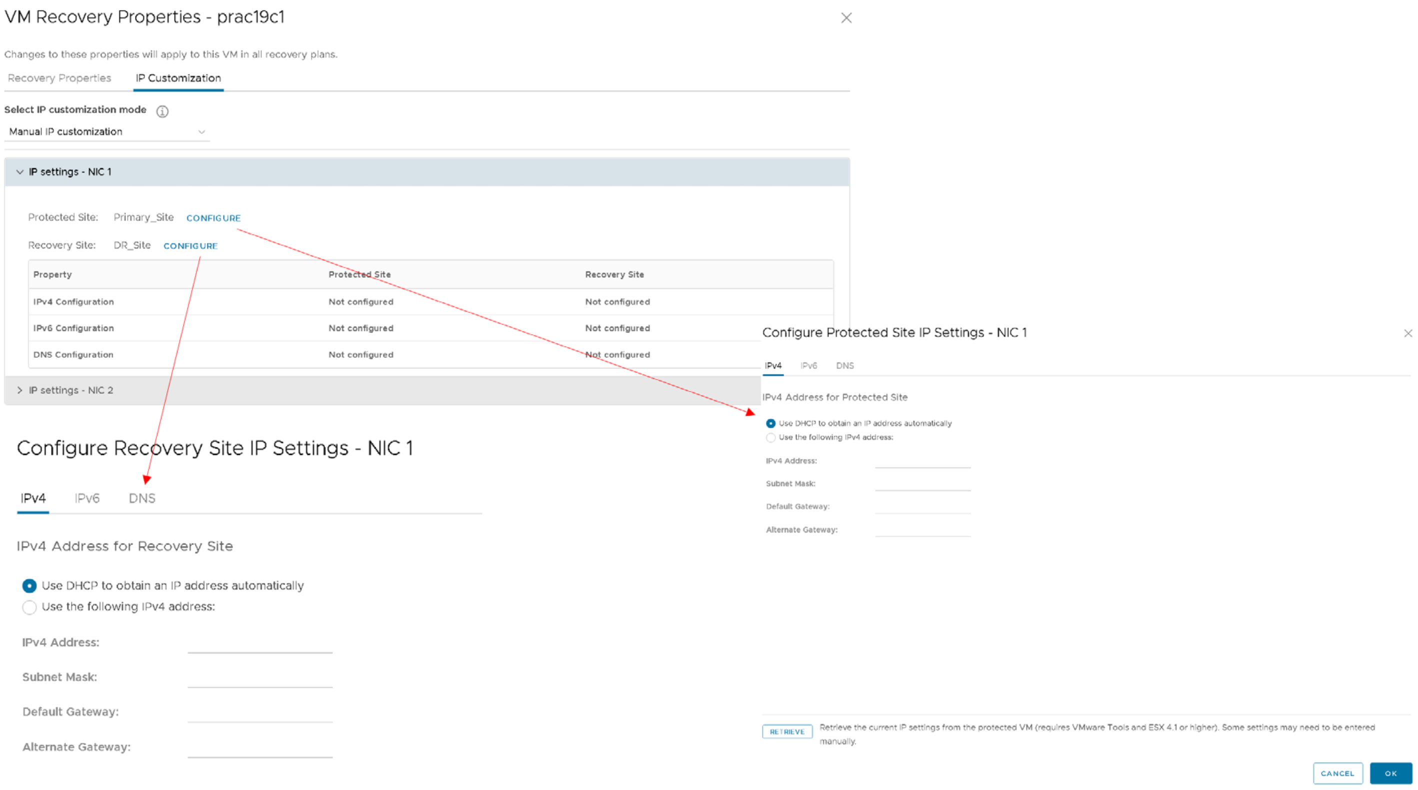
These steps run after the VM is powered on.

Name	Type	Timeout

0 step(s)

FIGURE 256. Recovery Plan IP Customization

IP customization can be performed for VM NIC1 networking, if needed.



VM Recovery Properties - prac19c1

Changes to these properties will apply to this VM in all recovery plans.

Select IP customization mode: Manual IP customization

Protected Site: Primary_Site CONFIGURE

Recovery Site: DR_Site CONFIGURE

Property	Protected Site	Recovery Site
IPv4 Configuration	Not configured	Not configured
IPv6 Configuration	Not configured	Not configured
DNS Configuration	Not configured	Not configured

Configure Recovery Site IP Settings - NIC 1

IPv4 Address for Recovery Site

- ● Use DHCP to obtain an IP address automatically
- ○ Use the following IPv4 address:

IPv4 Address:

Subnet Mask:

Default Gateway:

Alternate Gateway:

Configure Protected Site IP Settings - NIC 1

IPv4 Address for Protected Site

- ● Use DHCP to obtain an IP address automatically
- ○ Use the following IPv4 address:

IPv4 Address:

Subnet Mask:

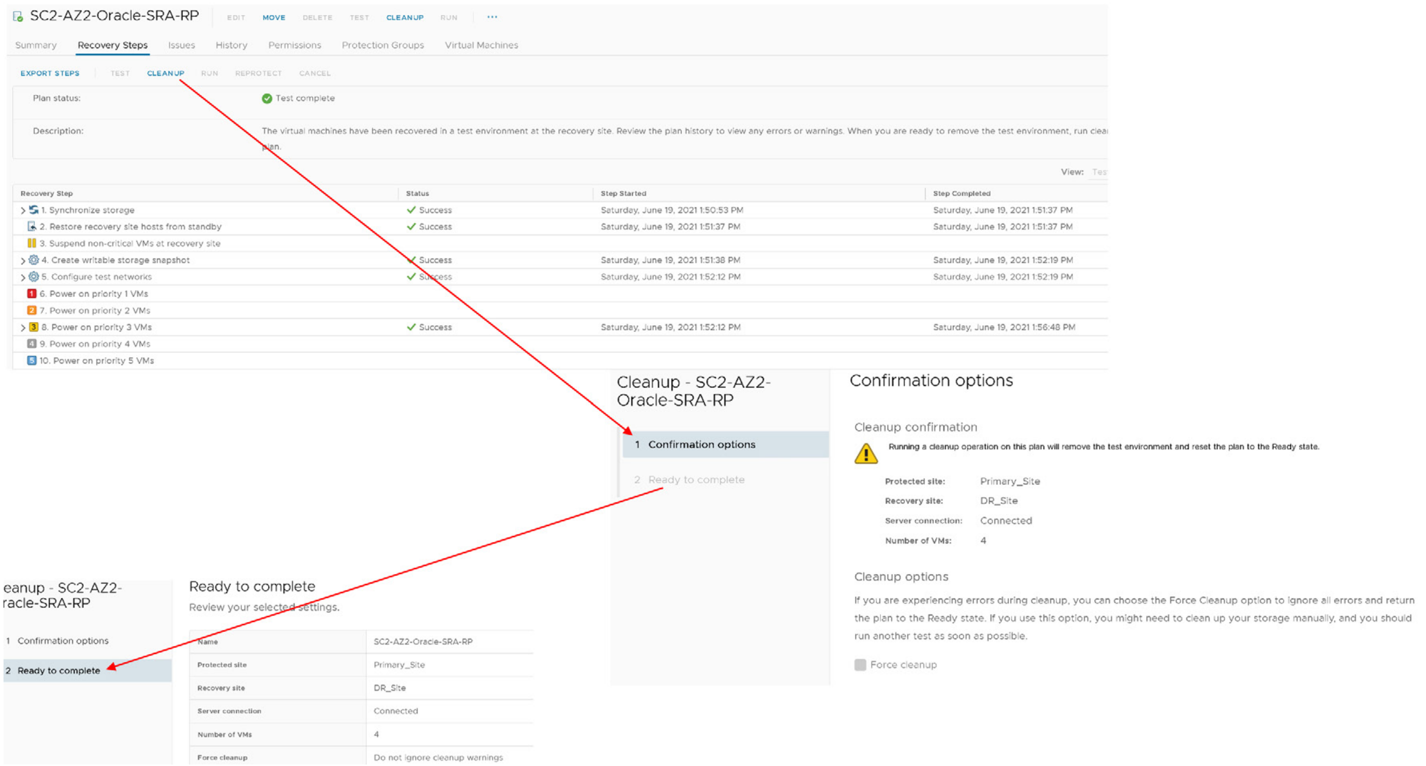
Default Gateway:

Alternate Gateway:

RETRIEVE Retrieve the current IP settings from the protected VM (requires VMware Tools and ESX 4.1 or higher). Some settings may need to be entered manually.

FIGURE 257. Recovery Plan IP Customization Details

When performing cleanup after running a test, the array removes the snapshots that were created earlier as part of the test recovery workflow.



Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run clea plan.

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	✓ Success	Saturday, June 19, 2021 1:50:53 PM	Saturday, June 19, 2021 1:51:37 PM
2. Restore recovery site hosts from standby	✓ Success	Saturday, June 19, 2021 1:51:37 PM	Saturday, June 19, 2021 1:51:37 PM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	✓ Success	Saturday, June 19, 2021 1:51:38 PM	Saturday, June 19, 2021 1:52:19 PM
5. Configure test networks	✓ Success	Saturday, June 19, 2021 1:52:12 PM	Saturday, June 19, 2021 1:52:19 PM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Saturday, June 19, 2021 1:52:12 PM	Saturday, June 19, 2021 1:56:48 PM
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

Cleanup - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Cleanup confirmation

Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	4

Cleanup options

If you are experiencing errors during cleanup, you can choose the Force Cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you might need to clean up your storage manually, and you should run another test as soon as possible.

□ Force cleanup

eanup - SC2-AZ2-racle-SRA-RP

1 Confirmation options

2 Ready to complete

Ready to complete

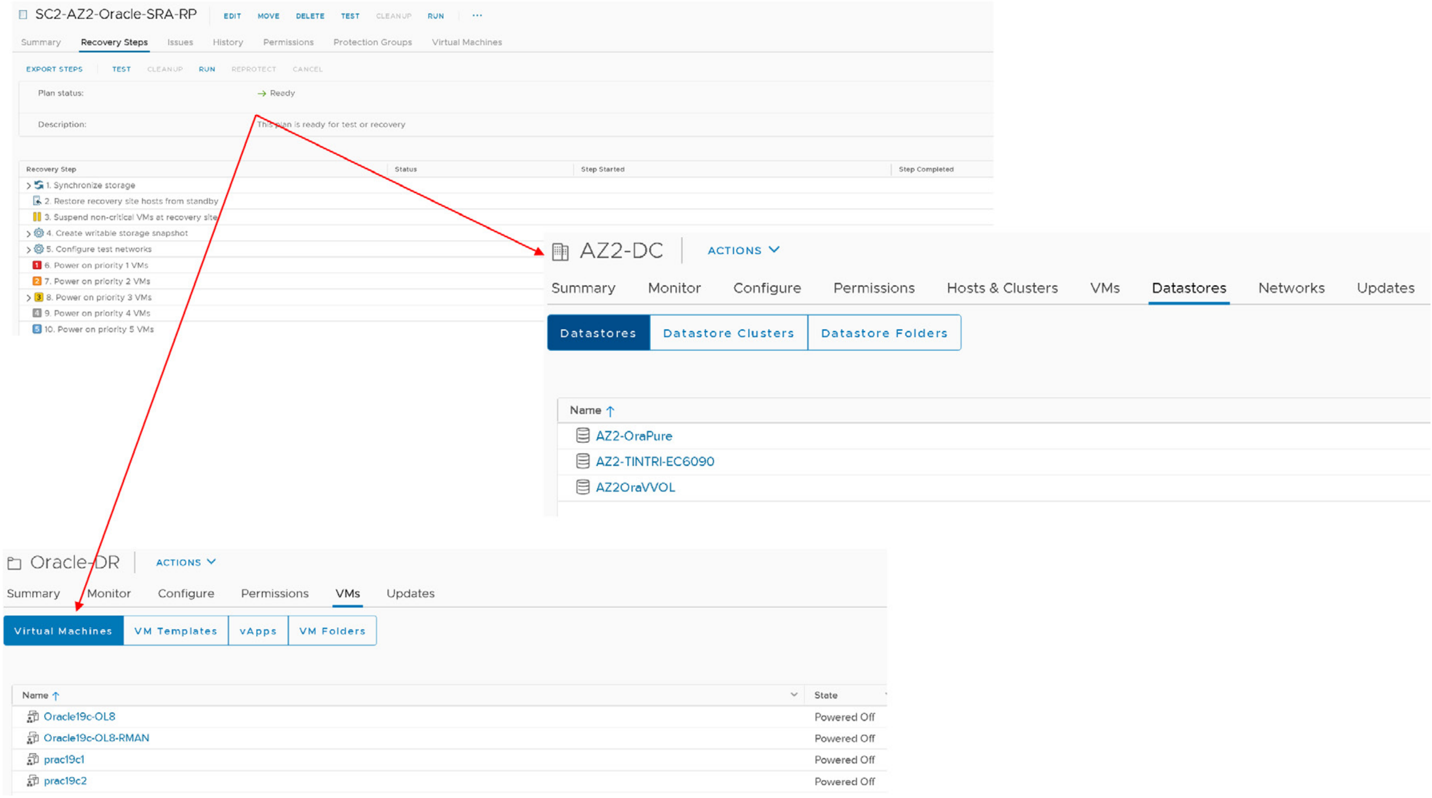
Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 258. Cleanup the Recovery Plan

As part of the cleanup, the VMs on the snapshot datastore are powered off and the placeholder VMs are then placed on the placeholder datastore **AZ2-OraPure**.

The snapshot datastore **snap-49b528bb-OraSC2** is then removed, and the pod will then be demoted, resetting the environment for another test or recovery.



Plan status: → Ready

Description: This plan is ready for test or recovery

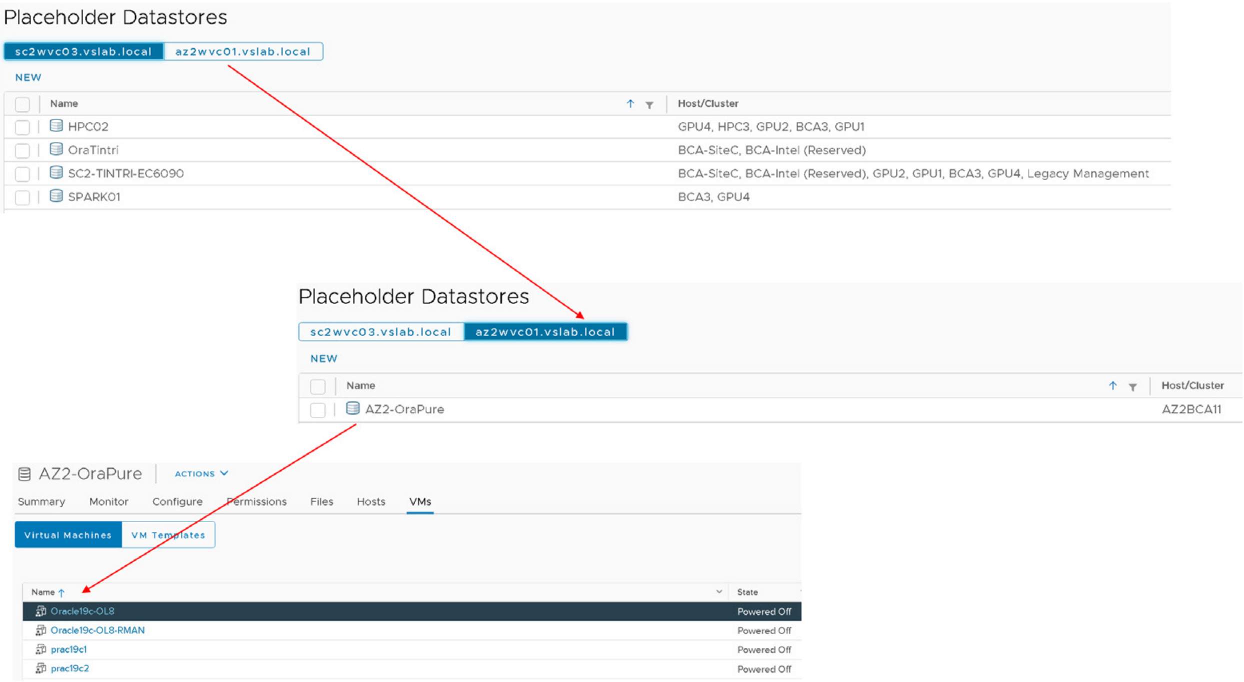
Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage			
2. Restore recovery site hosts from standby			
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot			
5. Configure test networks			
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs			
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

Name ↑
AZ2-OraPure
AZ2-TINTRI-EC6090
AZ2OraVVOL

Name ↑	State
Oracle19c-OL8	Powered Off
Oracle19c-OL8-RMAN	Powered Off
prac19c1	Powered Off
prac19c2	Powered Off

FIGURE 259. Site B Storage and Compute Status

The placeholder datastore with the placeholder VMs are as shown below:



Placeholder Datastores

Name	Host/Cluster
HPC02	GPU4, HPC3, GPU2, BCA3, GPU1
OraTintri	BCA-SiteC, BCA-Intel (Reserved)
SC2-TINTRI-EC6090	BCA-SiteC, BCA-Intel (Reserved), GPU2, GPU1, BCA3, GPU4, Legacy Management
SPARK01	BCA3, GPU4

Placeholder Datastores

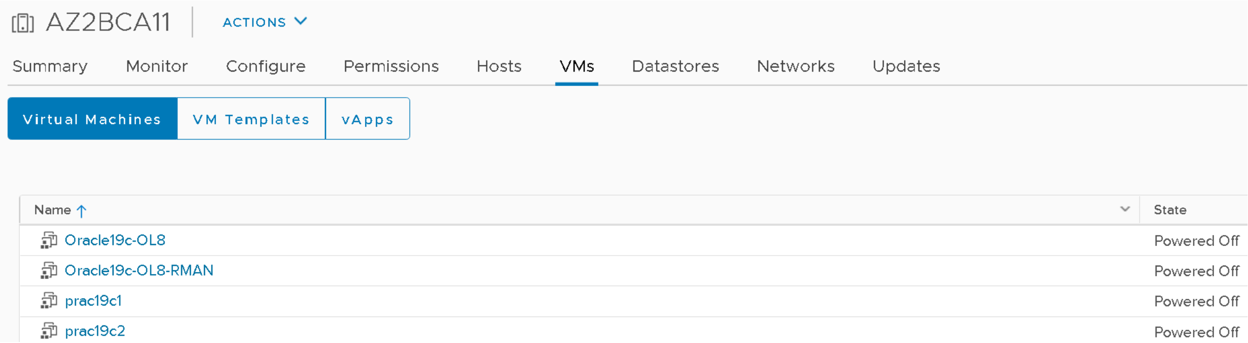
Name	Host/Cluster
AZ2-OraPure	AZ2BCA11

AZ2-OraPure

Name	State
Oracle19c-OL8	Powered Off
Oracle19c-OL8-RMAN	Powered Off
prac19c1	Powered Off
prac19c2	Powered Off

FIGURE 260. Site B Placeholder Datastore and Placeholder VMs

Site B VM status is as shown below:



AZ2BCA11

Name	State
Oracle19c-OL8	Powered Off
Oracle19c-OL8-RMAN	Powered Off
prac19c1	Powered Off
prac19c2	Powered Off

FIGURE 261. Site B VM Status

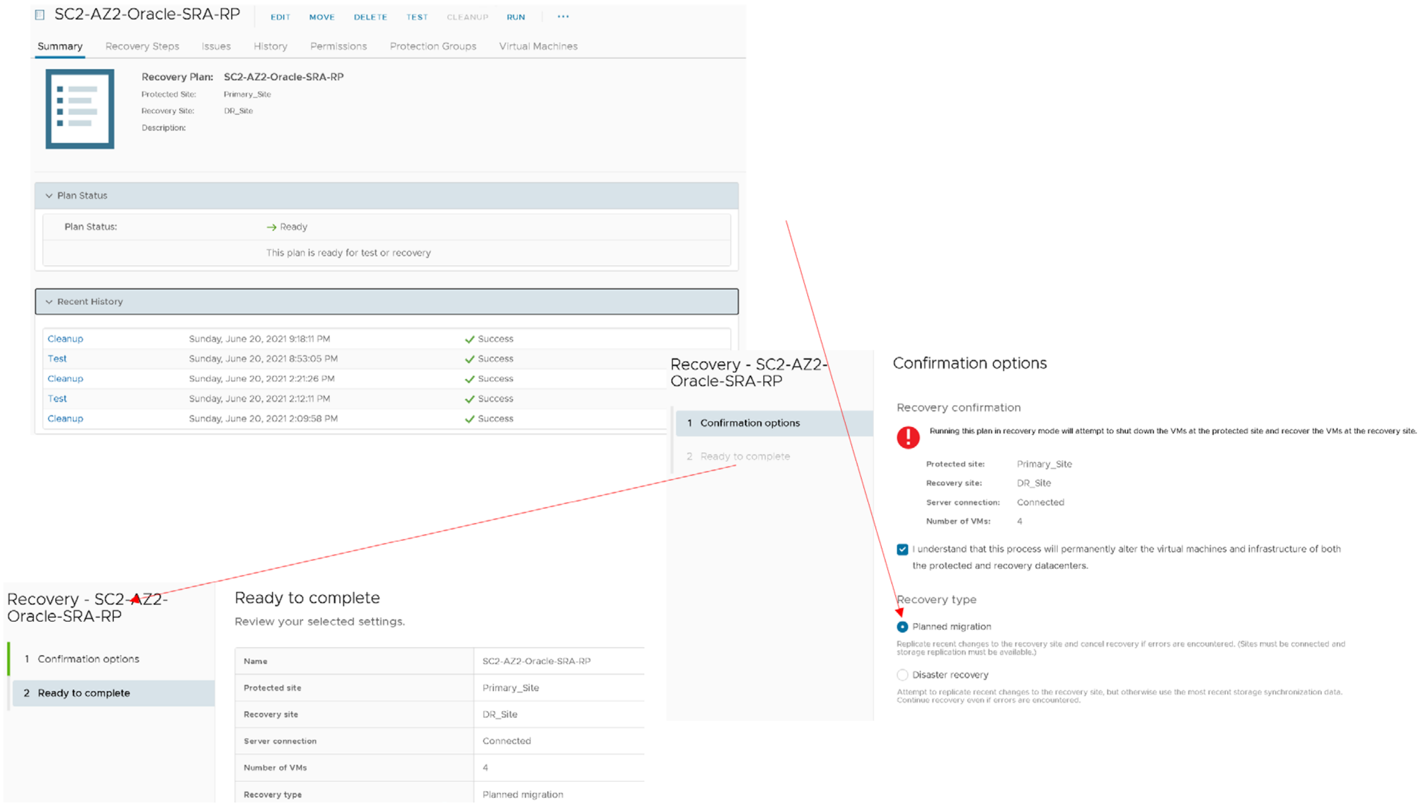
More information on testing a recovery plan with array-based replication can be found in *Testing a Recovery Plan* and *SRM User Guide: FlashArray Continuous Replication (ActiveDR) Workflows*.

Run Recovery Plan for Planned Migration

Performing a planned migration or disaster recovery by running a recovery plan will result in VM migration from the protected site to the recovery site. If the protected site suffers an unforeseen event that might result in data loss, the recovery plan can also be run under unplanned circumstances.

Planned migration – During a planned migration, Site Recovery Manager synchronizes the VM data on the recovery site with the VMs on the protected site. Site Recovery Manager attempts to shut down the protected VMs gracefully and performs a final synchronization to prevent data loss, then powers on the VMs on the recovery site. If errors occur during a planned migration, the plan stops so that the errors can be resolved, and the plan rerun.

Steps to run recovery plan **SC2-AZ2-Oracle-SRA-RP** in planned migration mode are as shown below:



Recovery Plan: SC2-AZ2-Oracle-SRA-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Cleanup	Sunday, June 20, 2021 9:18:11 PM	✓ Success
Test	Sunday, June 20, 2021 8:53:05 PM	✓ Success
Cleanup	Sunday, June 20, 2021 2:21:26 PM	✓ Success
Test	Sunday, June 20, 2021 2:12:11 PM	✓ Success
Cleanup	Sunday, June 20, 2021 2:09:58 PM	✓ Success

Recovery - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options
2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: Primary_Site
Recovery site: DR_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration
Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery
Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options
2 Ready to complete

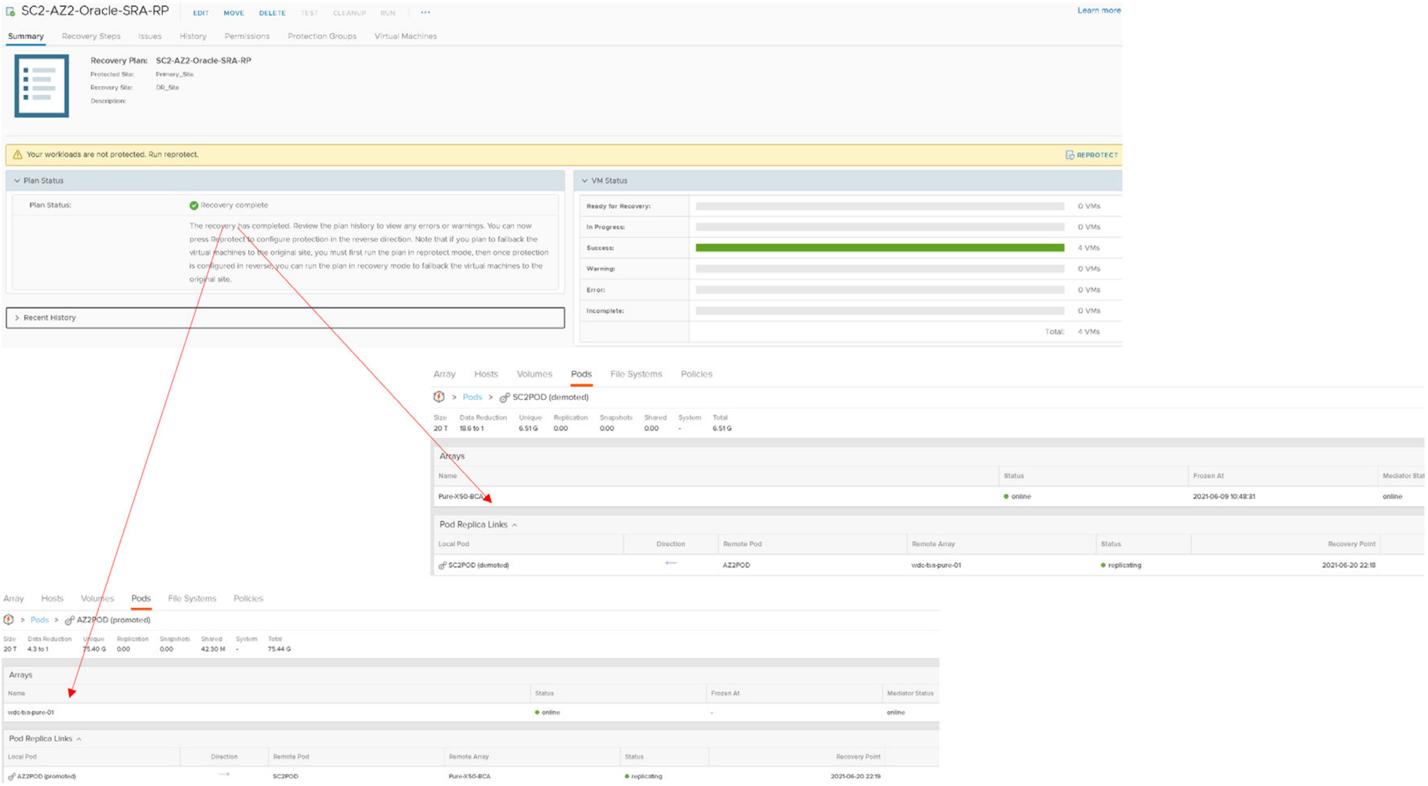
Ready to complete
Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Recovery type	Planned migration

FIGURE 262. Run Recovery Plan SC2-AZ2-Oracle-SRA-RP

A planned migration is very similar to a test recovery in process. Prior to a recovery, a source pod is in the promoted state and the target pod is in the demoted state.

After the planned migration, the datastore **OraSC2** is disconnected, the protected site pod volume **SC2POD::OraSC2** is disconnected from all protected site hosts, and protected site pod **SC2POD::OraSC2 is demoted**. The recovery site pod volume **AZ2POD::OraSC2** is promoted and connected to the recovery site hosts.



Recovery Plan: SC2-AZ2-Oracle-SRA-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Pods > SC2POD (demoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	18.6 to 1	6.51 G	0.00	0.00	0.00	-	6.51 G

Arrays

Name	Status	Frozen At	Mediator Stat
Pure-X50-BCA	● online	2021-06-09 10:48:31	online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status	Recovery Point
SC2POD (demoted)	←	AZ2POD	wdc-tsa-pure-01	● replicating	2021-06-20 22:18

Pods > AZ2POD (promoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.40 G	0.00	0.00	42.30 M	-	75.44 G

Arrays

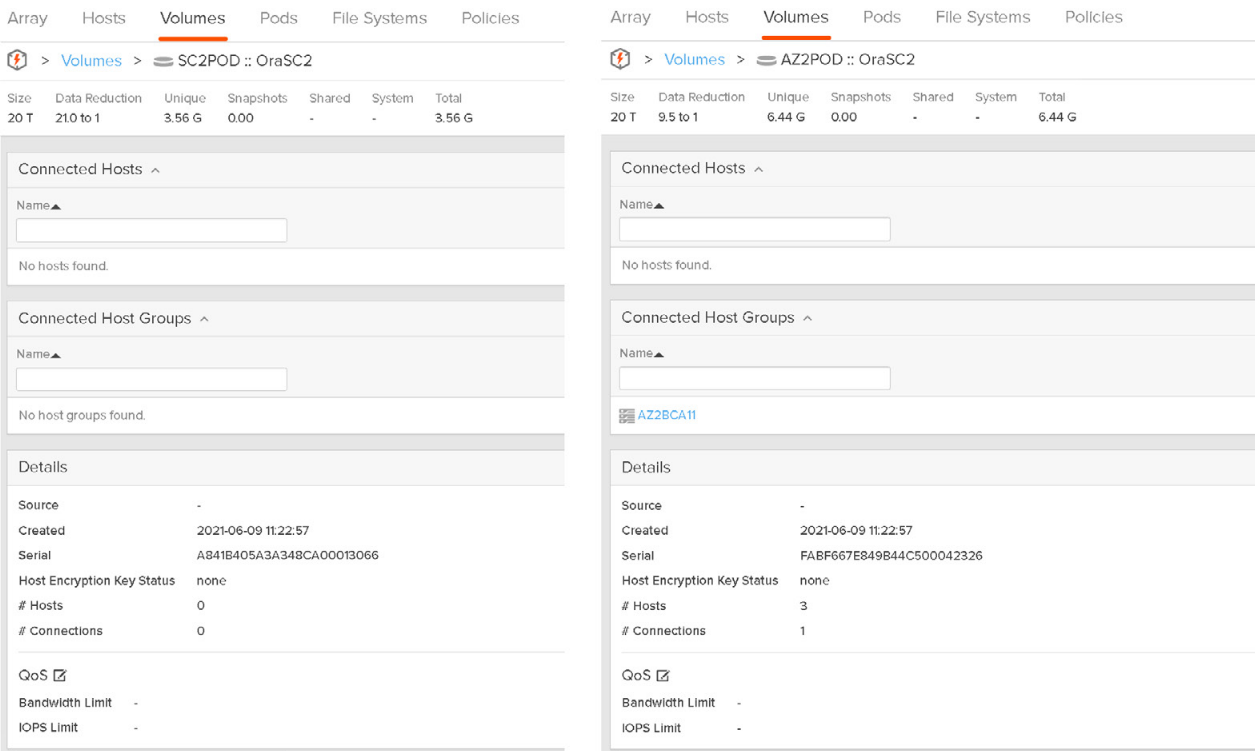
Name	Status	Frozen At	Mediator Status
wdc-tsa-pure-01	● online	-	online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status	Recovery Point
AZ2POD (promoted)	→	SC2POD	Pure-X50-BCA	● replicating	2021-06-20 22:19

FIGURE 263. Recovery Plan SC2-AZ2-Oracle-SRA-RP in Progress

Site A and Site B storage volumes are as shown below:



SC2POD :: OraSC2

Size	Data Reduction	Unique	Snapshots	Shared	System	Total
20 T	21.0 to 1	3.56 G	0.00	-	-	3.56 G

No hosts found.

No host groups found.

Source	-
Created	2021-06-09 11:22:57
Serial	A841B405A3A348CA00013066
Host Encryption Key Status	none
# Hosts	0
# Connections	0
Bandwidth Limit	-
IOPS Limit	-

AZ2POD :: OraSC2

Size	Data Reduction	Unique	Snapshots	Shared	System	Total
20 T	9.5 to 1	6.44 G	0.00	-	-	6.44 G

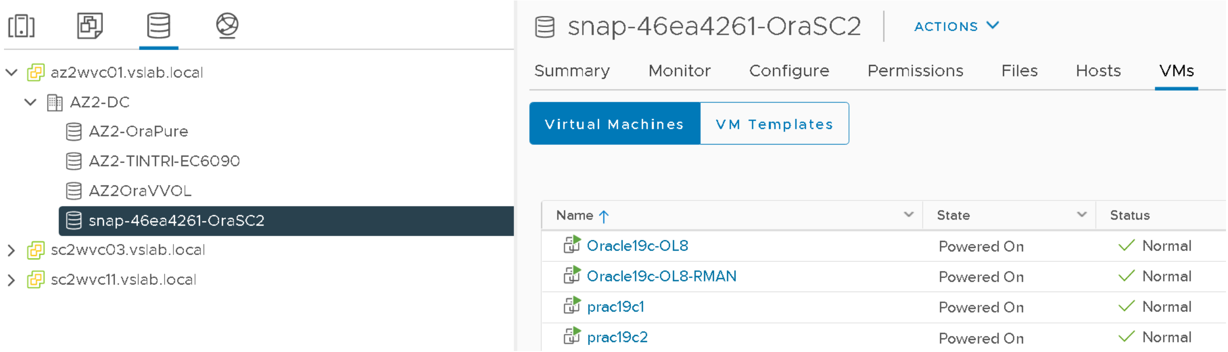
No hosts found.

AZ2BCA11

Source	-
Created	2021-06-09 11:22:57
Serial	FABF667E849B44C500042326
Host Encryption Key Status	none
# Hosts	3
# Connections	1
Bandwidth Limit	-
IOPS Limit	-

FIGURE 264. Site A and Site B Storage Volumes

As part of rescanning the ESXi hosts, the recovery site datastore is resignatured and mounted and the process of resignaturing adds the snap-XXXXXXX prefix to the datastore names. The VMs are then powered on in the resignature process.



Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

FIGURE 265. Resignature of Recovery Site Datastore

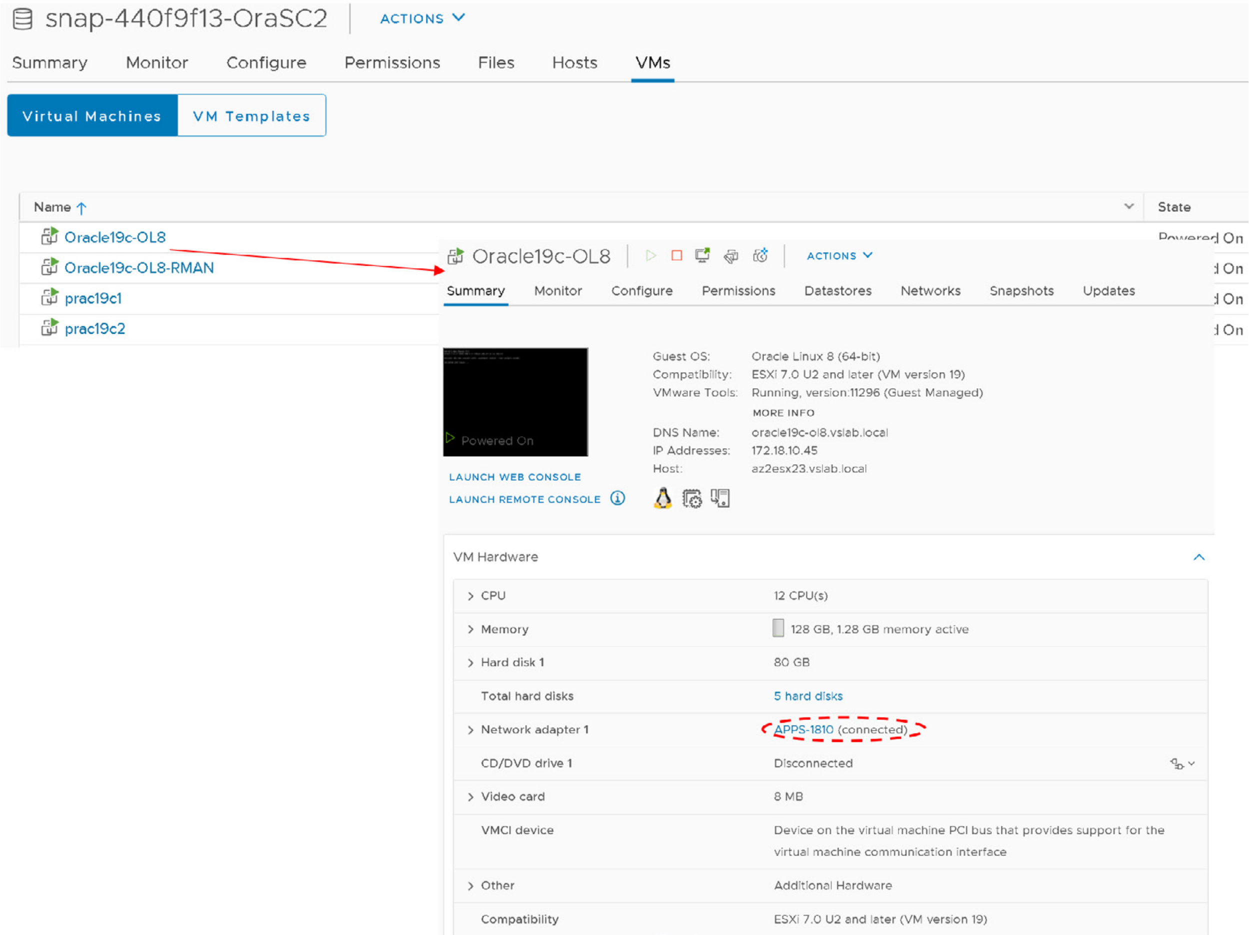
Both single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered up and connected to the recovery site recovery network **APPS-1810**. The IP addressing scheme is followed as defined in the network mapping section.

As in the case of testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

The storage-based snapshot is crash-consistent and write-ordering is preserved for each file within a snapshot.

Oracle VM **Oracle19c-OL8** network details are as shown below:



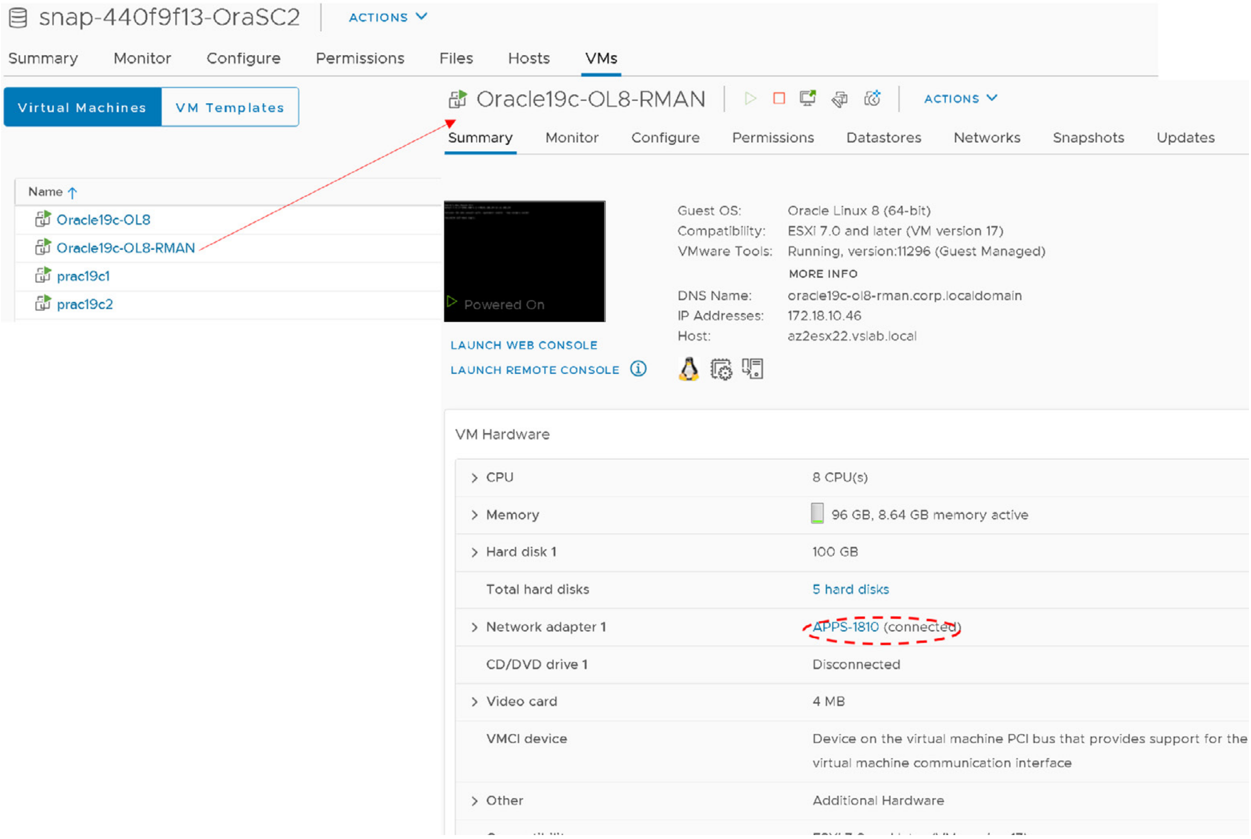
Name	State
Oracle19c-OL8	Powered On
Oracle19c-OL8-RMAN	Powered On
prac19c1	Powered On
prac19c2	Powered On

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 266. Oracle Oracle19c-OL8 Networking Status

Oracle VM **Oracle19c-OL8-RMAN** network details are as shown below:



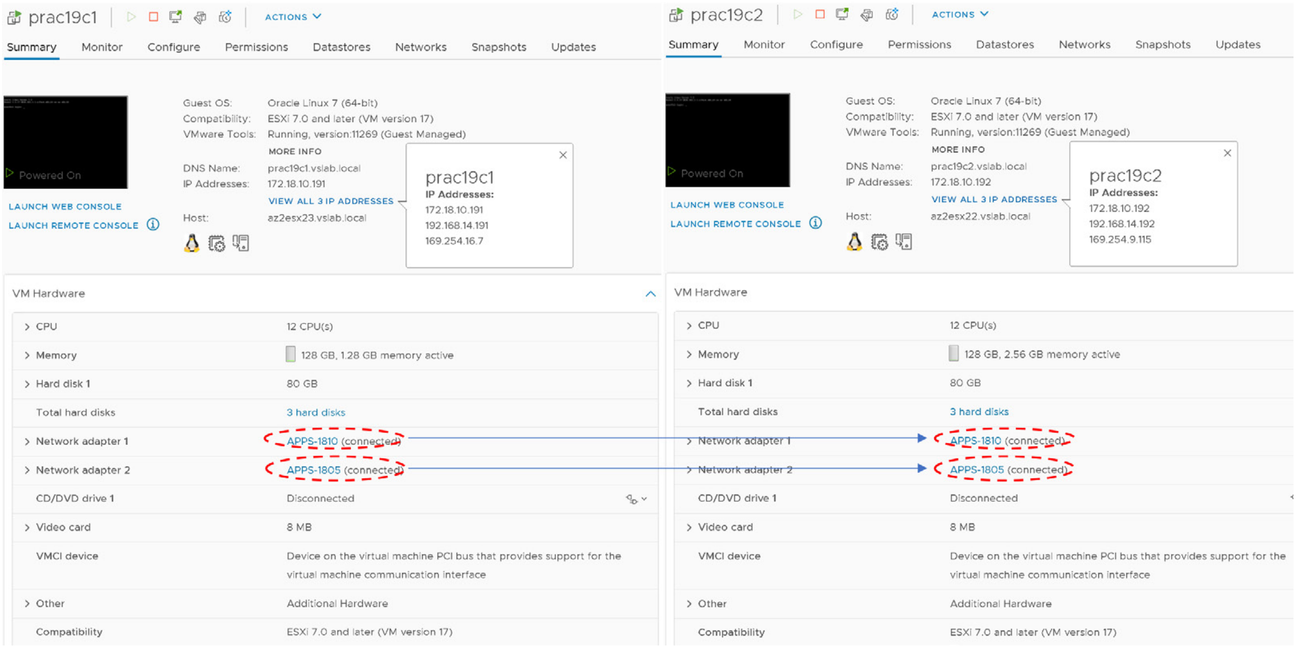
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx22.vslab.local

VM Hardware

CPU	8 CPU(s)
Memory	96 GB, 8.64 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware

FIGURE 267. Oracle Oracle19c-OL8-RMAN Networking Status

Oracle RAC cluster **prac19c** VMs are also powered up. The public interfaces are connected to the recovery site recovery network **APPS-1810** and private interconnects are connected to the recovery site recovery network **APPS-1805**. The IP addressing scheme is followed as defined in the network mapping section.



Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.18.10.191
Host: az2esx23.vslab.local

prac19c1
IP Addresses:
172.18.10.191
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.18.10.192
Host: az2esx22.vslab.local

prac19c2
IP Addresses:
172.18.10.192
192.168.14.192
169.254.9.115

VM Hardware

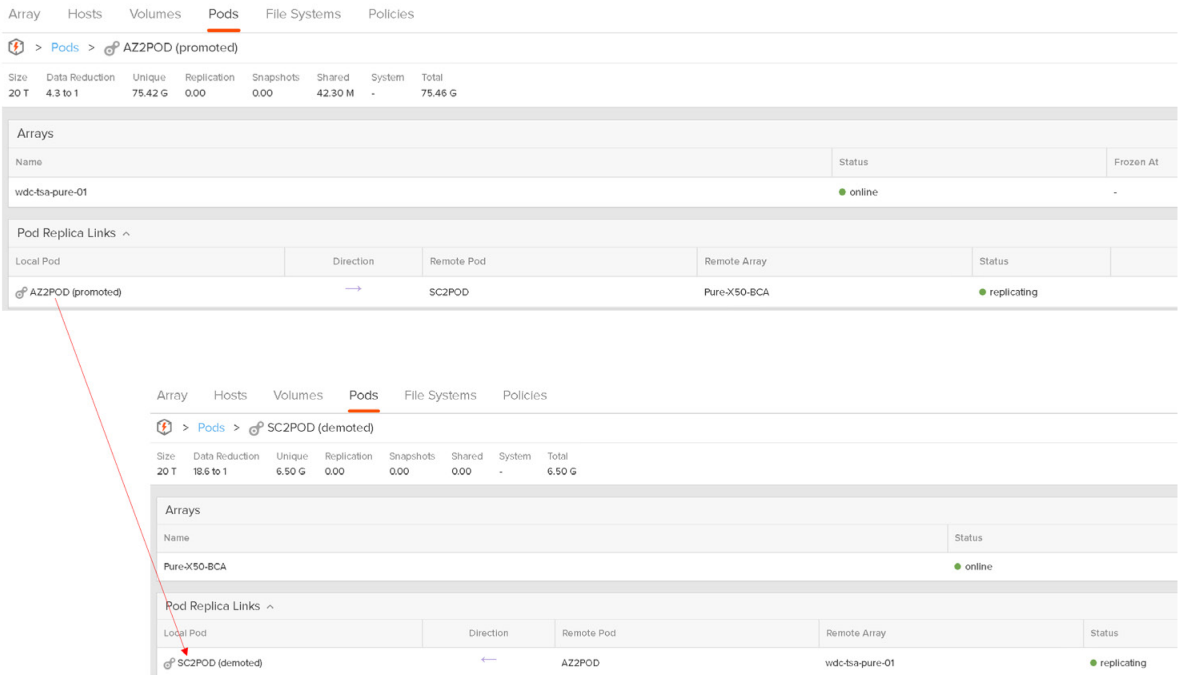
CPU	12 CPU(s)
Memory	128 GB, 2.56 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 268. Oracle RAC prac19c Networking Status

As part of running a planned migration of the recovery plan, the network interfaces of the Oracle RAC **prac19c** will be changed to the appropriate recovery network as defined in the network mappings.

- The VIP and the SCAN IPs have to be changed to the test/recovery network IP scheme in order for the RAC Clusterware to bring up the RAC services.
- The steps to change the RAC VIP IP address can be found in *Oracle 19c Clusterware Administration and Deployment Guide*. The steps to change the Oracle private interconnect IP address can be found in the *Changing Oracle Clusterware Private Network Configuration*.
- The steps to change the RAC SCAN IP addresses can be found in the *My Oracle Support Note How to Update the IP Address of the SCAN VIP Resources (ora.scan{n}.vip) (Doc ID 952903.1)*.
- The steps to change the RAC VIP, scan and private interconnect IP addresses are beyond the scope of this paper.

At the end of the recovery process, the Target Site B is replicating to the Source Site A.



Pods > AZ2POD (promoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.42 G	0.00	0.00	42.30 M	-	75.46 G

Arrays

Name	Status	Frozen At
wdc-tsa-pure-01	● online	-

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
AZ2POD (promoted)	→	SC2POD	Pure-X50-BCA	● replicating

Pods > SC2POD (demoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	18.6 to 1	6.50 G	0.00	0.00	0.00	-	6.50 G

Arrays

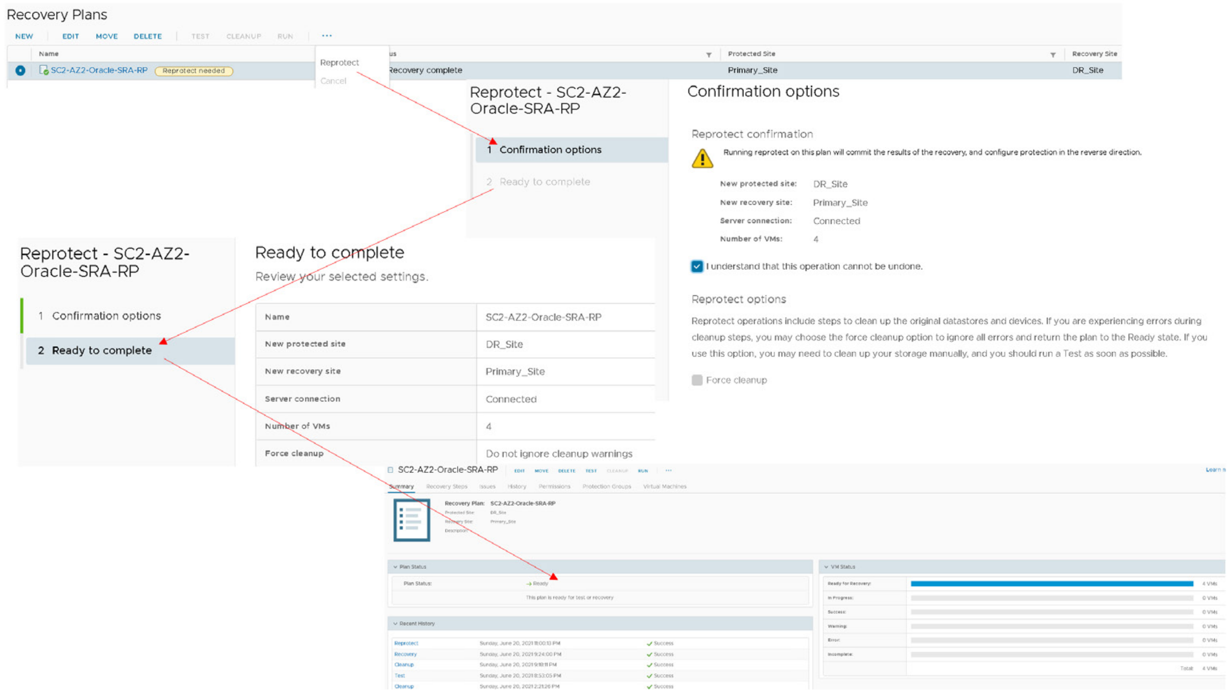
Name	Status
Pure-X50-BCA	● online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
SC2POD (demoted)	←	AZ2POD	wdc-tsa-pure-01	● replicating

FIGURE 269. Storage Replication from Site B to Site A

A **Reprotect** needs to be run on the target Site B back to source Site A to protect the VMs in the reverse direction.



Name	Status	Protected Site	Recovery Site
SC2-AZ2-Oracle-SRA-RP (Reprotect needed)	Recovery complete	Primary_Site	DR_Site

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site:	DR_Site
New recovery site:	Primary_Site
Server connection:	Connected
Number of VMs:	4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
New protected site	DR_Site
New recovery site	Primary_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

SC2-AZ2-Oracle-SRA-RP

Recovery Plan: SC2-AZ2-Oracle-SRA-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Plan Status

Plan Status: → Ready

This plan is ready for test or recovery

Recent History

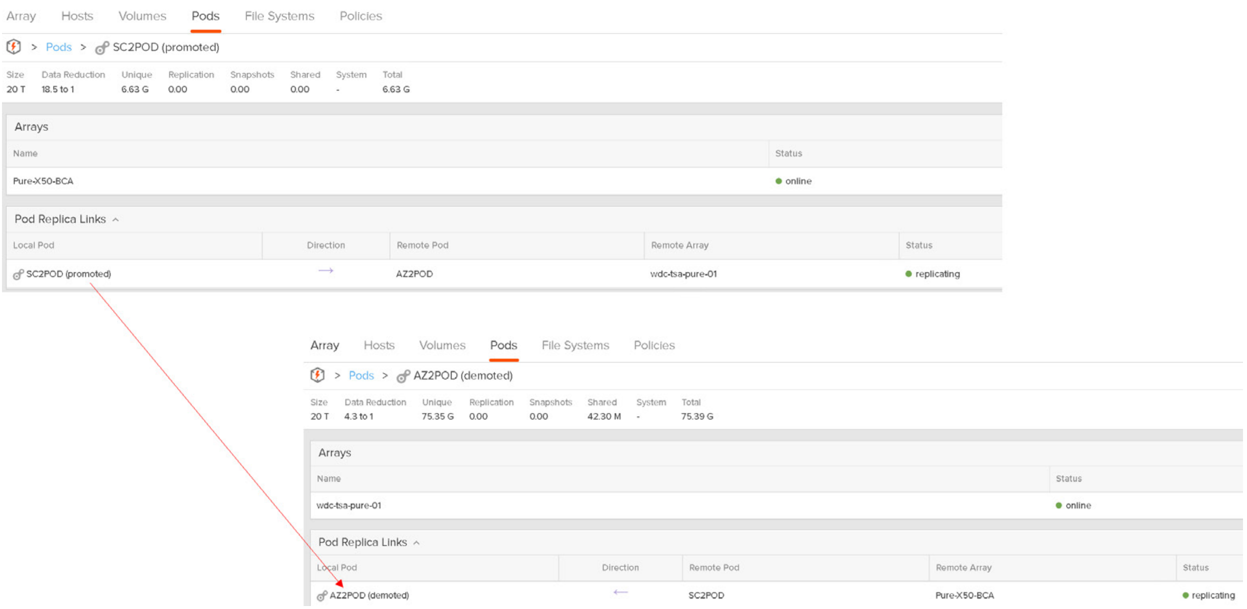
Reprotect	Sunday, June 20, 2021 11:00:13 PM	✓ Success
Recovery	Sunday, June 20, 2021 9:24:00 PM	✓ Success
Cleanup	Sunday, June 20, 2021 9:18:11 PM	✓ Success
Test	Sunday, June 20, 2021 8:53:05 PM	✓ Success
Cleanup	Sunday, June 20, 2021 2:21:26 PM	✓ Success

VM Status

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

FIGURE 270. Run Reprotect on Site B

In order to switch the protected site from Site B to Site A, we can run another planned migration which will switch the protected site from Site B to Site A. Replication will occur from Site A to Site B.



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	18.5 to 1	6.63 G	0.00	0.00	0.00	-	6.63 G

Arrays

Name	Status
Pure-X50-BCA	● online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
SC2POD (promoted)	→	AZ2POD	wdc-tsa-pure-01	● replicating

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.35 G	0.00	0.00	42.30 M	-	75.39 G

Arrays

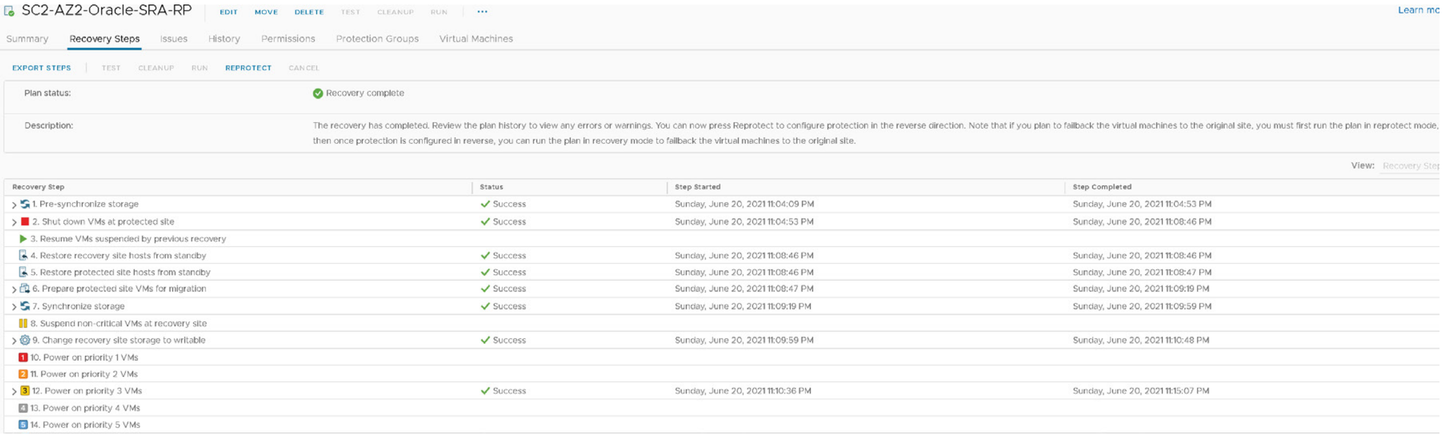
Name	Status
wdc-tsa-pure-01	● online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
AZ2POD (demoted)	←	SC2POD	Pure-X50-BCA	● replicating

FIGURE 271. Storage Replication from Site A to Site B

Planned migration from Site B to Site A is successful.



Plan status: ✓ Recovery complete

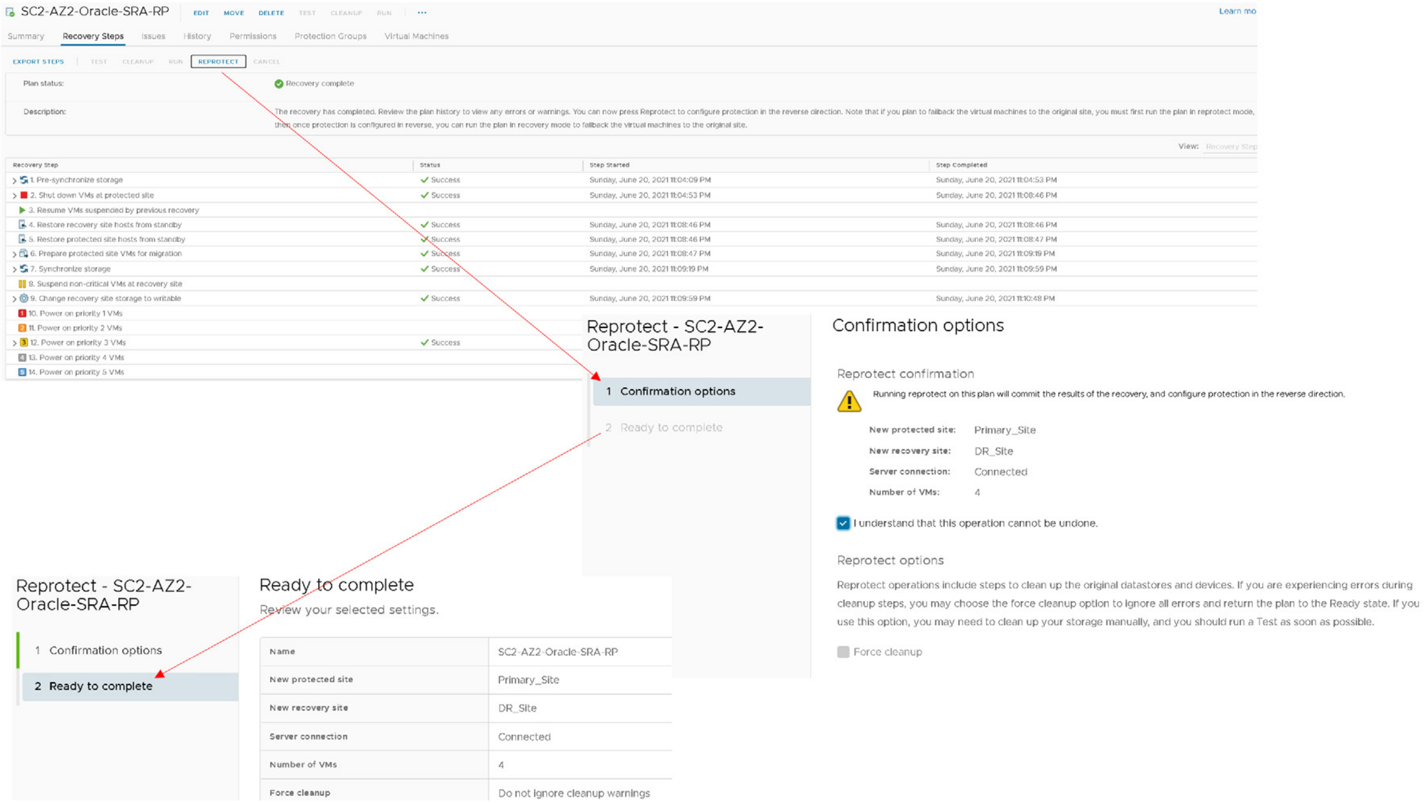
Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

View: Recovery Step

Recovery Step	Status	Step Started	Step Completed
> 1. Pre-synchronize storage	✓ Success	Sunday, June 20, 2021 11:04:09 PM	Sunday, June 20, 2021 11:04:53 PM
> 2. Shut down VMs at protected site	✓ Success	Sunday, June 20, 2021 11:04:53 PM	Sunday, June 20, 2021 11:08:46 PM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Sunday, June 20, 2021 11:08:46 PM	Sunday, June 20, 2021 11:08:46 PM
5. Restore protected site hosts from standby	✓ Success	Sunday, June 20, 2021 11:08:46 PM	Sunday, June 20, 2021 11:08:47 PM
> 6. Prepare protected site VMs for migration	✓ Success	Sunday, June 20, 2021 11:08:47 PM	Sunday, June 20, 2021 11:09:19 PM
> 7. Synchronize storage	✓ Success	Sunday, June 20, 2021 11:09:19 PM	Sunday, June 20, 2021 11:09:59 PM
8. Suspend non-critical VMs at recovery site			
> 9. Change recovery site storage to writable	✓ Success	Sunday, June 20, 2021 11:09:59 PM	Sunday, June 20, 2021 11:10:48 PM
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
> 12. Power on priority 3 VMs	✓ Success	Sunday, June 20, 2021 11:10:36 PM	Sunday, June 20, 2021 11:15:07 PM
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

FIGURE 272. Planned Migration from Site A to Site B Successful

Re-run the reprotect process to protect the VMs on the protected Site A.



SC2-AZ2-Oracle-SRA-RP
EDIT MOVE DELETE TEST CLEANUP RUN ···
Learn mo
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS | TEST CLEANUP RUN REPROTECT CANCEL
View: Recovery Step

Plan status: Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✓ Success	Sunday, June 20, 2021 11:04:09 PM	Sunday, June 20, 2021 11:04:53 PM
2. Shut down VMs at protected site	✓ Success	Sunday, June 20, 2021 11:04:53 PM	Sunday, June 20, 2021 11:08:46 PM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Sunday, June 20, 2021 11:08:46 PM	Sunday, June 20, 2021 11:08:46 PM
5. Restore protected site hosts from standby	✓ Success	Sunday, June 20, 2021 11:08:46 PM	Sunday, June 20, 2021 11:08:47 PM
6. Prepare protected site VMs for migration	✓ Success	Sunday, June 20, 2021 11:08:47 PM	Sunday, June 20, 2021 11:09:19 PM
7. Synchronize storage	✓ Success	Sunday, June 20, 2021 11:09:19 PM	Sunday, June 20, 2021 11:09:59 PM
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✓ Success	Sunday, June 20, 2021 11:09:59 PM	Sunday, June 20, 2021 11:10:48 PM
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
12. Power on priority 3 VMs	✓ Success		
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site:	Primary_Site
New recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

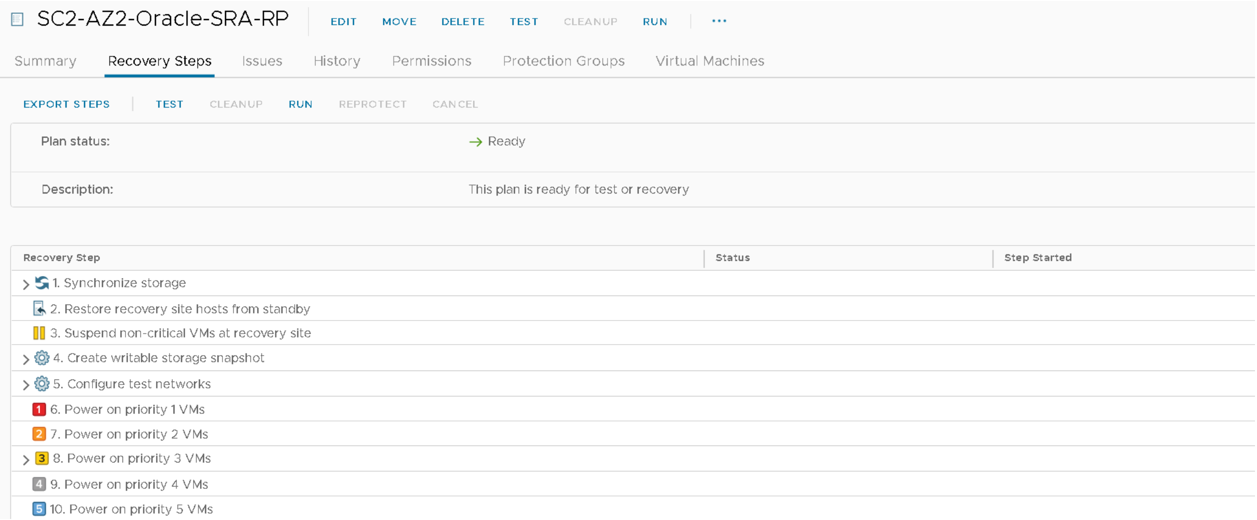
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
New protected site	Primary_Site
New recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 273. Reprotect Site A

The recovery plan **SC2-AZ2-Oracle-SRA-RP** is ready as shown below:



SC2-AZ2-Oracle-SRA-RP
EDIT MOVE DELETE TEST CLEANUP RUN ···
Summary Recovery Steps Issues History Permissions Protection Groups Virtual Machines
EXPORT STEPS | TEST CLEANUP RUN REPROTECT CANCEL

Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby		
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
5. Configure test networks		
6. Power on priority 1 VMs		
7. Power on priority 2 VMs		
8. Power on priority 3 VMs		
9. Power on priority 4 VMs		
10. Power on priority 5 VMs		

FIGURE 274. Recovery Plan Steps

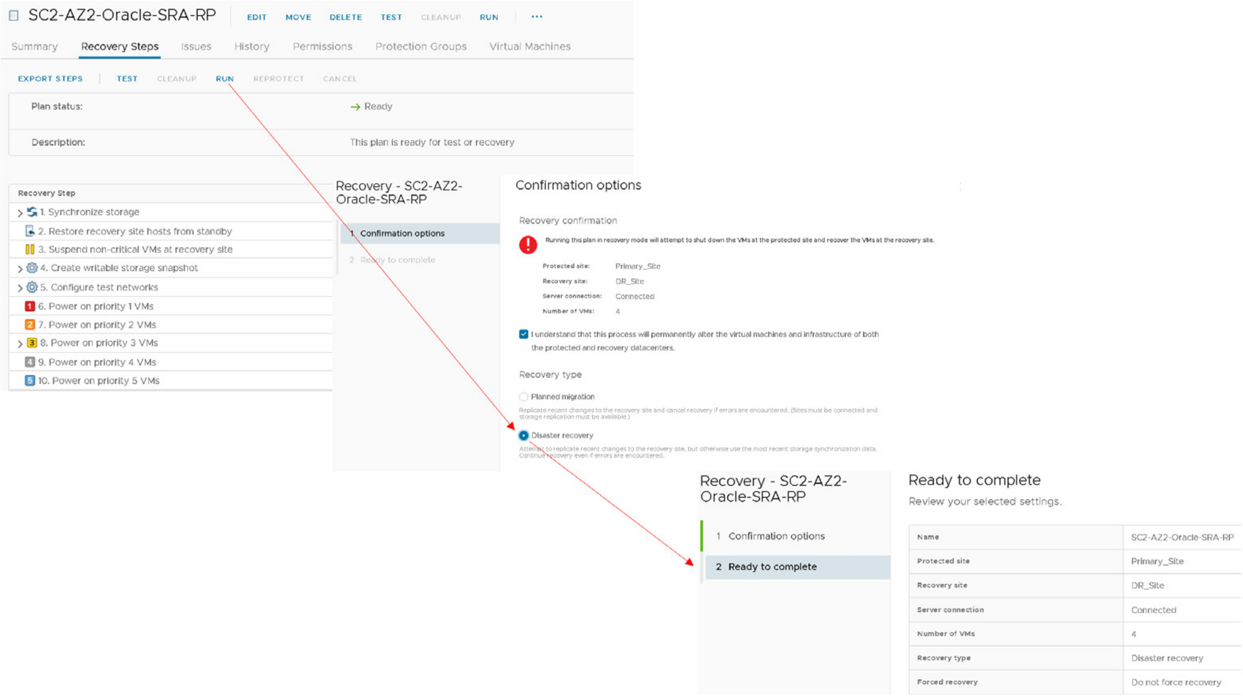
More information on running a planned recovery with array-based replication can be found in the *Run a Recovery Plan* and *SRM User Guide: FlashArray Continuous Replication (ActiveDR) Workflows*.

Run Recovery Plan for Disaster Recovery

Disaster Recovery - During a disaster recovery, Site Recovery Manager first attempts a storage synchronization. If it succeeds, Site Recovery Manager uses the synchronized storage state to recover VMs on the recovery site to their most recent available state, according to the recovery point objective (RPO) that you set when you configure replication

The steps for running the recovery plan for disaster recovery are the same as those employed above with planned migration.

Steps to run the recovery plan **SC2-AZ2-Oracle-SRA-RP** in a disaster recovery mode are as shown below:



Plan status: Ready

Description: This plan is ready for test or recovery

Recovery Step
1. Synchronize storage
2. Restore recovery site hosts from standby
3. Suspend non-critical VMs at recovery site
4. Create writable storage snapshot
5. Configure test networks
6. Power on priority 1 VMs
7. Power on priority 2 VMs
8. Power on priority 3 VMs
9. Power on priority 4 VMs
10. Power on priority 5 VMs

Recovery - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options
2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

○ Planned migration
Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

● Disaster recovery
Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options
2 Ready to complete

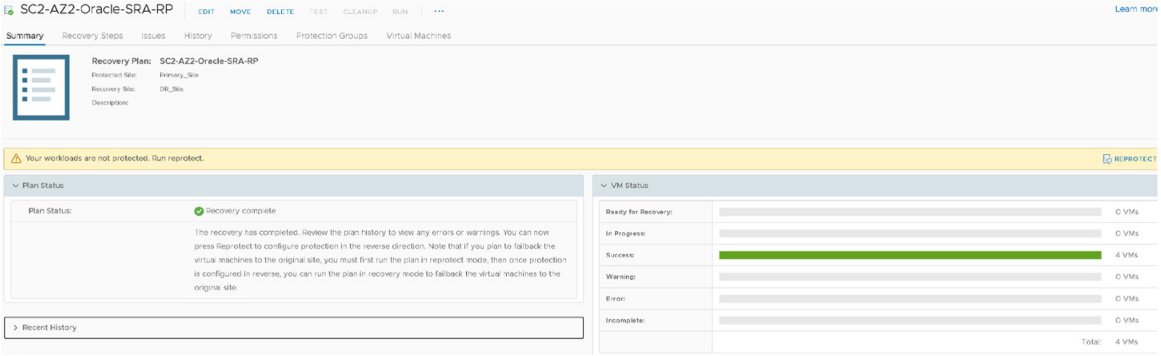
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Recovery type	Disaster recovery
Forced recovery	Do not force recovery

FIGURE 275. Disaster Recovery Use Case for Recovery Plan SC2-AZ2-Oracle-SRA-RP

Recovery plan **SC2-AZ2-Oracle-SRA-RP** in a disaster recovery mode is successful.



Recovery Plan: SC2-AZ2-Oracle-SRA-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Your workloads are not protected. Run reprotect.

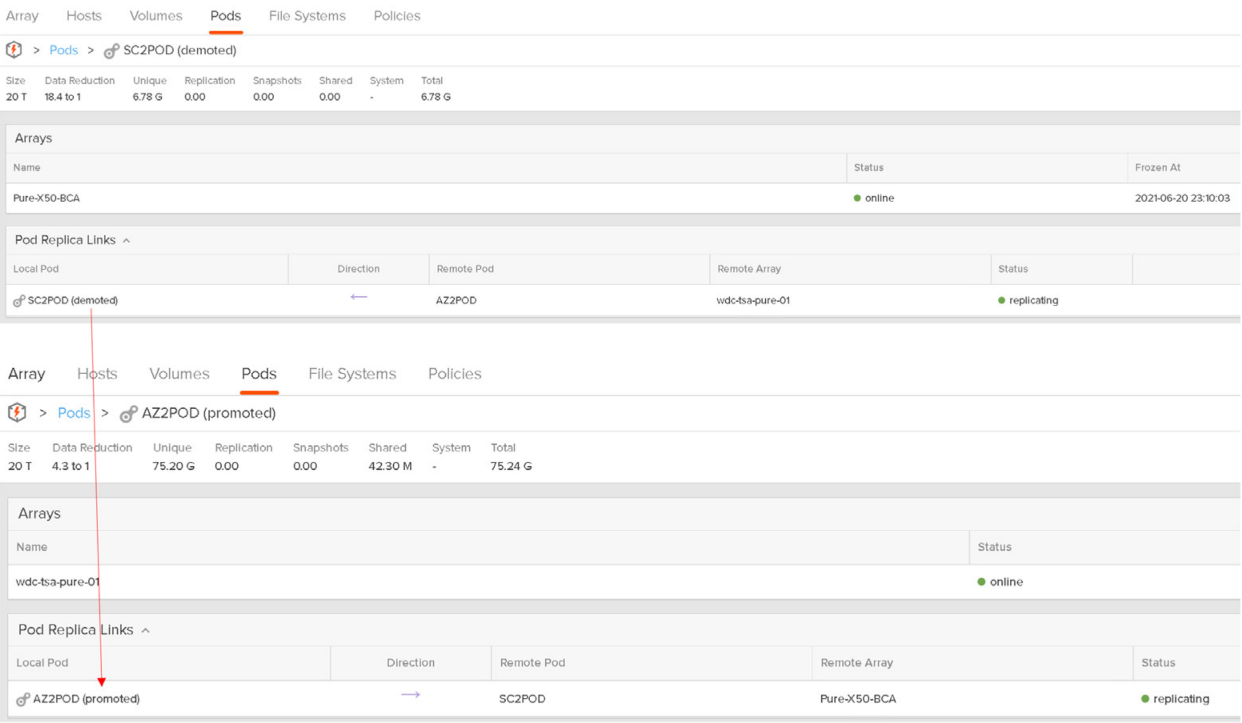
Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

FIGURE 276. Disaster Recovery Use Case for Recovery Plan SC2-AZ2-Oracle-SRA-RP Successful

Site A **SC2POD** is demoted and Site B **AZ2POD** is promoted as shown below:



Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	18.4 to 1	6.78 G	0.00	0.00	0.00	-	6.78 G

Arrays

Name	Status	Frozen At
Pure-X50-BCA	● online	2021-06-20 23:10:03

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
SC2POD (demoted)	←	AZ2POD	wdc-tsa-pure-01	● replicating

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.20 G	0.00	0.00	42.30 M	-	75.24 G

Arrays

Name	Status
wdc-tsa-pure-01	● online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
AZ2POD (promoted)	→	SC2POD	Pure-X50-BCA	● replicating

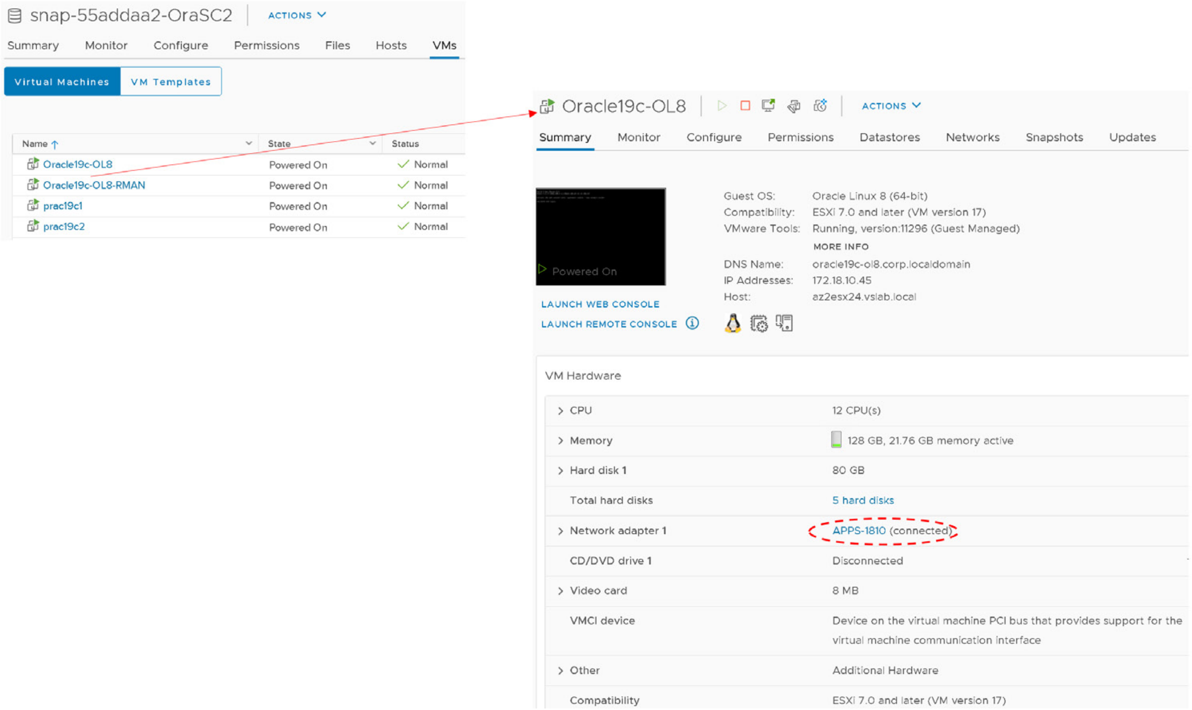
FIGURE 277. Storage Array POD Status on Site A and Site B

Both single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered up and connected to the recovery site recovery network APPS-1810. The IP addressing scheme is followed as defined in the network mapping section.

As in the case of testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

The storage-based snapshot is crash-consistent and write-ordering is preserved for each file within a snapshot.



snap-55addaa2-OraSC2 | ACTIONS

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

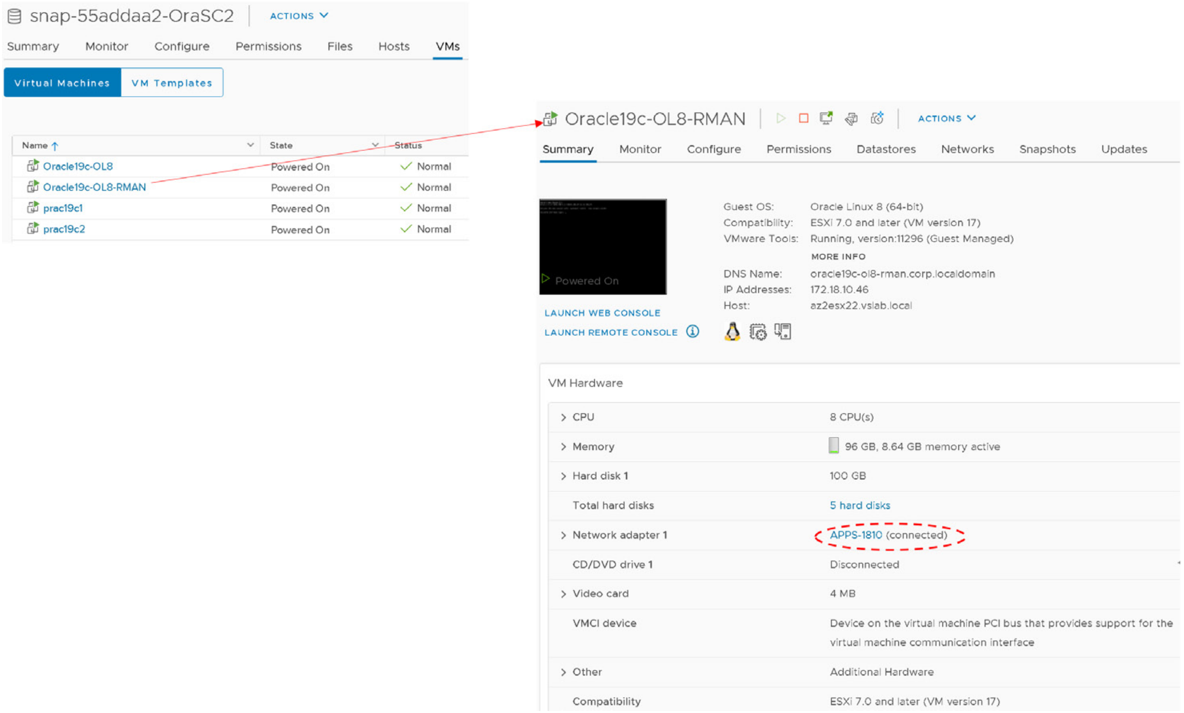
Oracle19c-OL8 | ACTIONS

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
MORE INFO
DNS Name: oracle19c-ol8.corp.localdomain
IP Addresses: 172.18.10.45
Host: az2esx24.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 21.76 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 278. Oracle VM Oracle19c-OL8 Networking Status



snap-55addaa2-OraSC2 | ACTIONS

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

Oracle19c-OL8-RMAN | ACTIONS

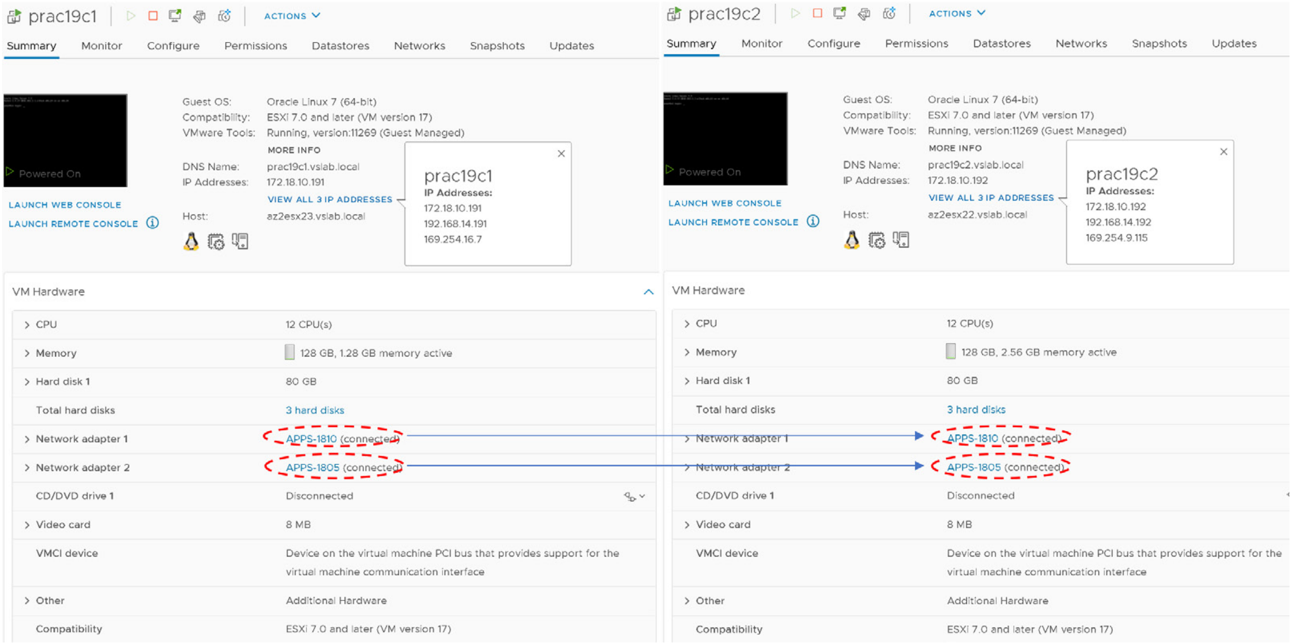
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
MORE INFO
DNS Name: oracle19c-ol8-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx22.vslab.local

VM Hardware

CPU	8 CPU(s)
Memory	96 GB, 8.64 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 279. Oracle VM Oracle19c-OL8-RMAN Networking Status

The Oracle RAC cluster **prac19c** VMs are also powered up. The public interfaces are connected to the recovery site recovery network **APPS-1810** and private interconnects are connected to the recovery site recovery network **APPS-1805**. The IP addressing scheme is followed as defined in the network mapping section.



prac19c1

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.18.10.191
Host: az2esx23.vslab.local

prac19c1
IP Addresses:
172.18.10.191
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

prac19c2

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.18.10.192
Host: az2esx22.vslab.local

prac19c2
IP Addresses:
172.18.10.192
192.168.14.192
169.254.9.115

VM Hardware

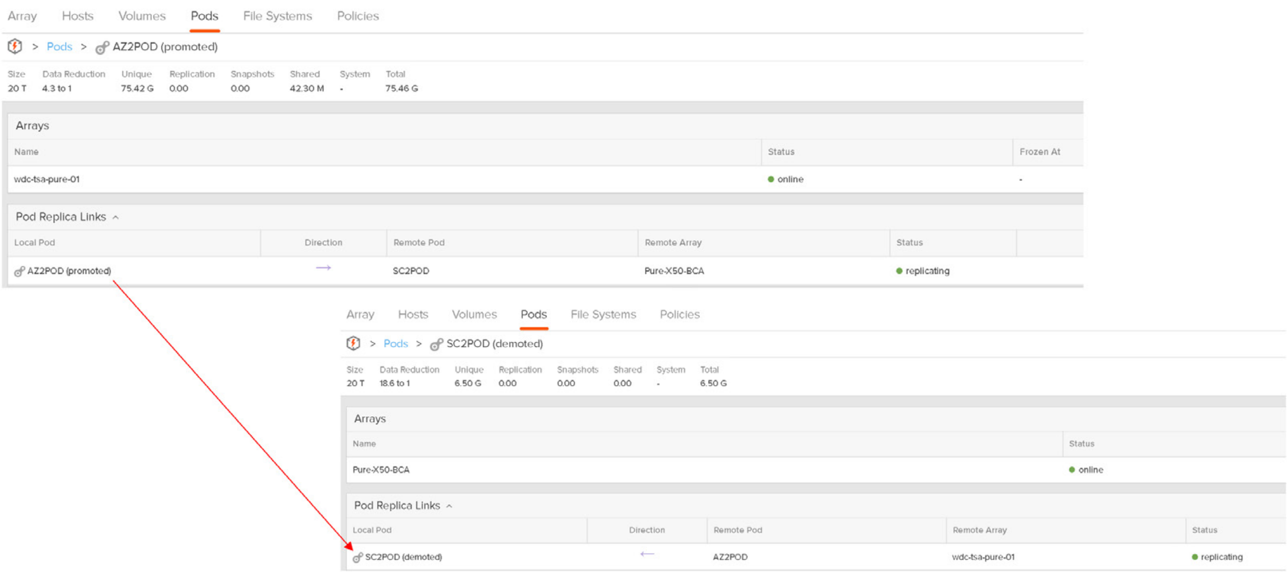
CPU	12 CPU(s)
Memory	128 GB, 2.56 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 280. Oracle RAC prac19c Networking Status

As part of running a disaster recovery exercise of the recovery plan, the network interfaces of the Oracle RAC **prac19c** will be changed to the appropriate recovery network as defined in the network mappings.

- The VIP and the SCAN IPs have to be changed to the test/recovery network IP scheme in order for the RAC Clusterware to bring up the RAC services.
- The steps to change the RAC VIP IP address can be found in *Oracle 19c Clusterware Administration and Deployment Guide*.
  The steps to change the Oracle private interconnect IP address can be found in the *Changing Oracle Clusterware Private Network Configuration*.
- The steps to change the RAC SCAN IP addresses can be found in the *My Oracle Support Note How to Update the IP Address of the SCAN VIP Resources (ora.scan{n}.vip) (Doc ID 952903.1)*.
- The steps to change the RAC VIP, scan and private interconnect IP addresses are beyond the scope of this paper.

At the end of running the recovery plan in disaster recovery mode Target Site B is replicating to the Source Site A.



> Pods > AZ2POD (promoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.42 G	0.00	0.00	42.30 M	-	75.46 G

Arrays

Name	Status	Frozen At
wdc-tsa-pure-01	● online	-

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
AZ2POD (promoted)	→	SC2POD	Pure-X50-BCA	● replicating

> Pods > SC2POD (demoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	18.6 to 1	6.50 G	0.00	0.00	0.00	-	6.50 G

Arrays

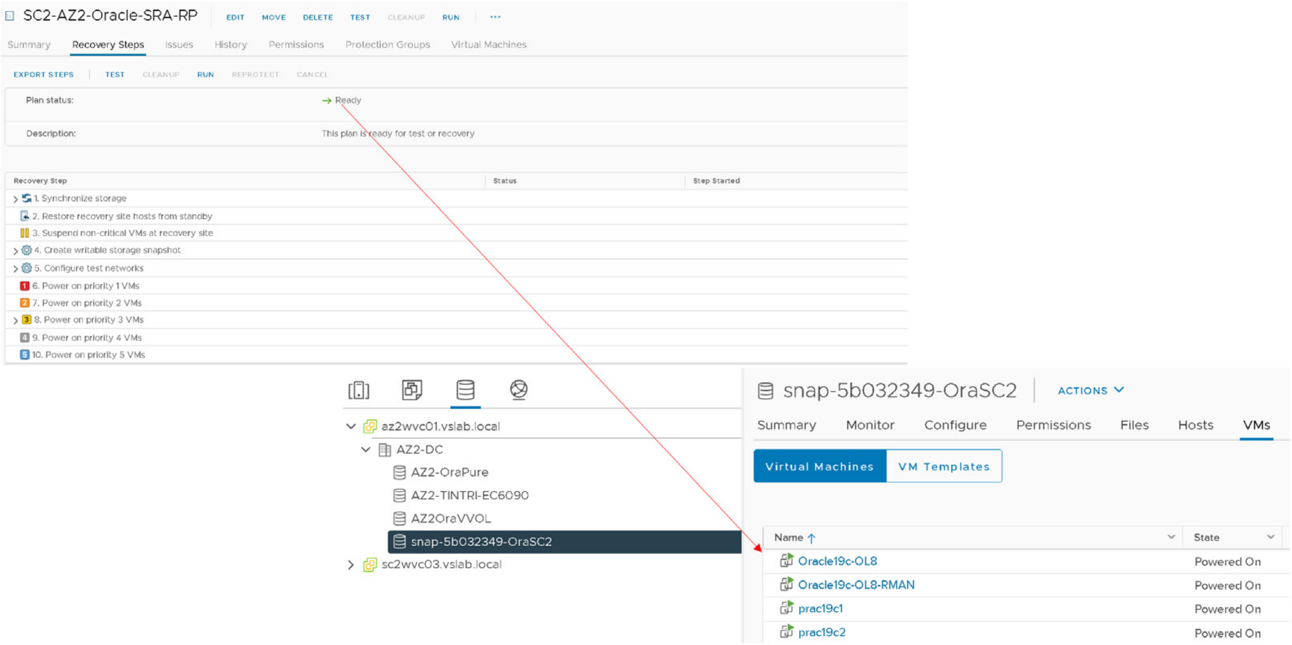
Name	Status
Pure-X50-BCA	● online

Pod Replica Links

Local Pod	Direction	Remote Pod	Remote Array	Status
SC2POD (demoted)	←	AZ2POD	wdc-tsa-pure-01	● replicating

FIGURE 281. Site B Replicating to Site A

The VMs are powered up on the protected Site B.



Plan status: → Ready

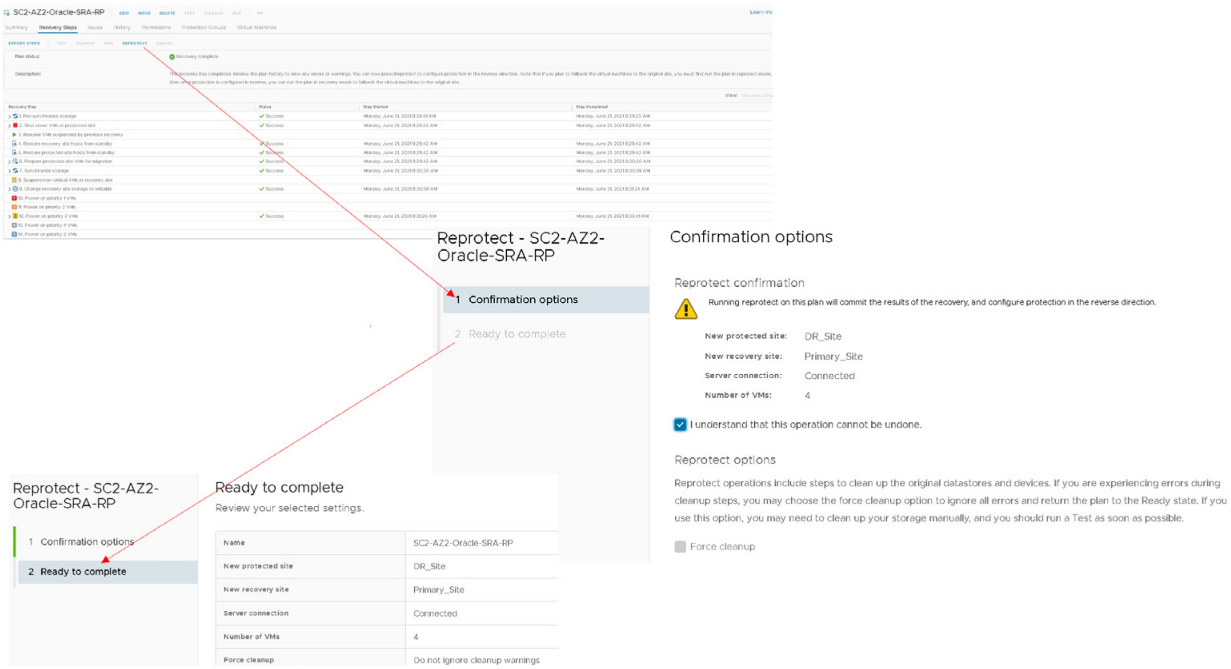
Description: This plan is ready for test or recovery

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby		
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
5. Configure test networks		
6. Power on priority 1 VMs		
7. Power on priority 2 VMs		
8. Power on priority 3 VMs		
9. Power on priority 4 VMs		
10. Power on priority 5 VMs		

Name ↑	State
Oracle19c-OL8	Powered On
Oracle19c-OL8-RMAN	Powered On
prac19c1	Powered On
prac19c2	Powered On

FIGURE 282. Site B VM Status

Reprotect needs to be run on Target Site B back to Source Site A to protect the VMs in the reverse direction.


SC2-AZ2-Oracle-SRA-RP

Plan status: Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✓ Success	Monday, June 21, 2021 8:28:41 AM	Monday, June 21, 2021 8:29:25 AM
2. Shut down VMs at protected site	✓ Success	Monday, June 21, 2021 8:29:25 AM	Monday, June 21, 2021 8:29:42 AM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Monday, June 21, 2021 8:29:42 AM	Monday, June 21, 2021 8:29:42 AM
5. Restore protected site hosts from standby	✓ Success	Monday, June 21, 2021 8:29:42 AM	Monday, June 21, 2021 8:29:42 AM
6. Prepare protected site VMs for migration	✓ Success	Monday, June 21, 2021 8:29:42 AM	Monday, June 21, 2021 8:30:20 AM
7. Synchronize storage	✓ Success	Monday, June 21, 2021 8:30:20 AM	Monday, June 21, 2021 8:30:59 AM
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✓ Success	Monday, June 21, 2021 8:30:59 AM	Monday, June 21, 2021 8:31:24 AM
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
12. Power on priority 3 VMs	✓ Success	Monday, June 21, 2021 8:31:20 AM	Monday, June 21, 2021 8:35:41 AM
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site:	DR_Site
New recovery site:	Primary_Site
Server connection:	Connected
Number of VMs:	4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

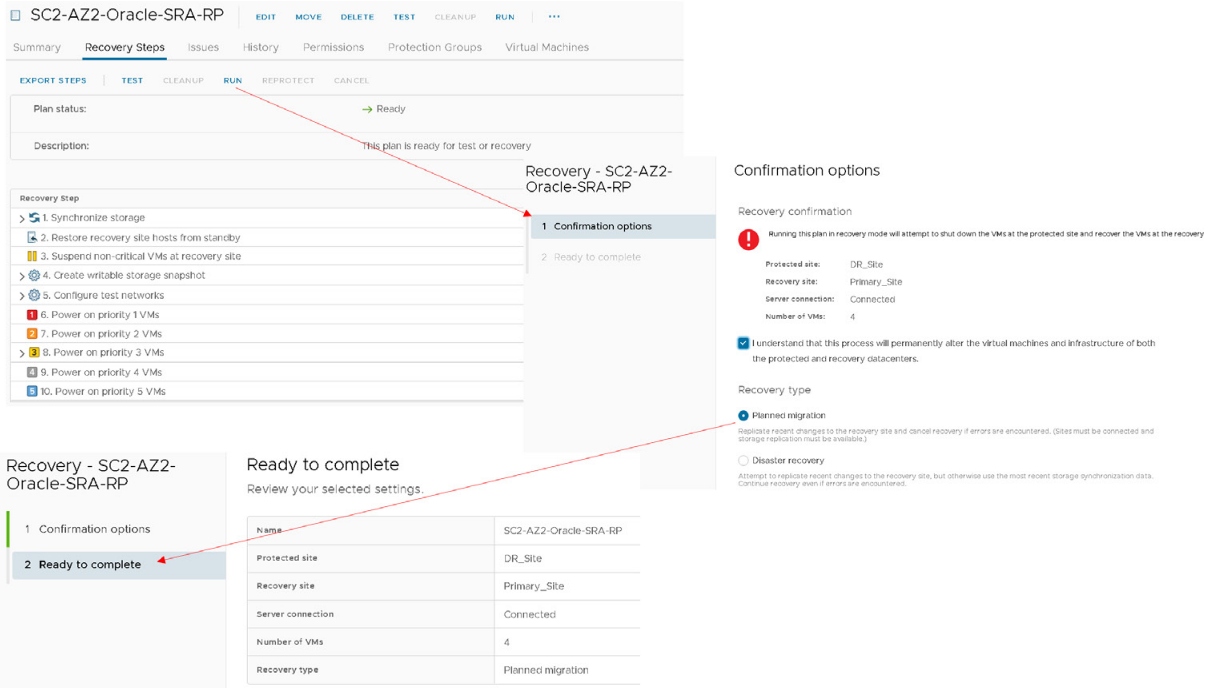
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
New protected site	DR_Site
New recovery site	Primary_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 283. RUN REPROTECT ON SITE B

Once Source Site A is back online, re-run the workflow in planned migration mode, which will reverse the replication direction.


SC2-AZ2-Oracle-SRA-RP

Plan status: → Ready

Description: This plan is ready for test or recovery

Recovery Step
1. Synchronize storage
2. Restore recovery site hosts from standby
3. Suspend non-critical VMs at recovery site
4. Create writable storage snapshot
5. Configure test networks
6. Power on priority 1 VMs
7. Power on priority 2 VMs
8. Power on priority 3 VMs
9. Power on priority 4 VMs
10. Power on priority 5 VMs

Recovery - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery

Protected site:	DR_Site
Recovery site:	Primary_Site
Server connection:	Connected
Number of VMs:	4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

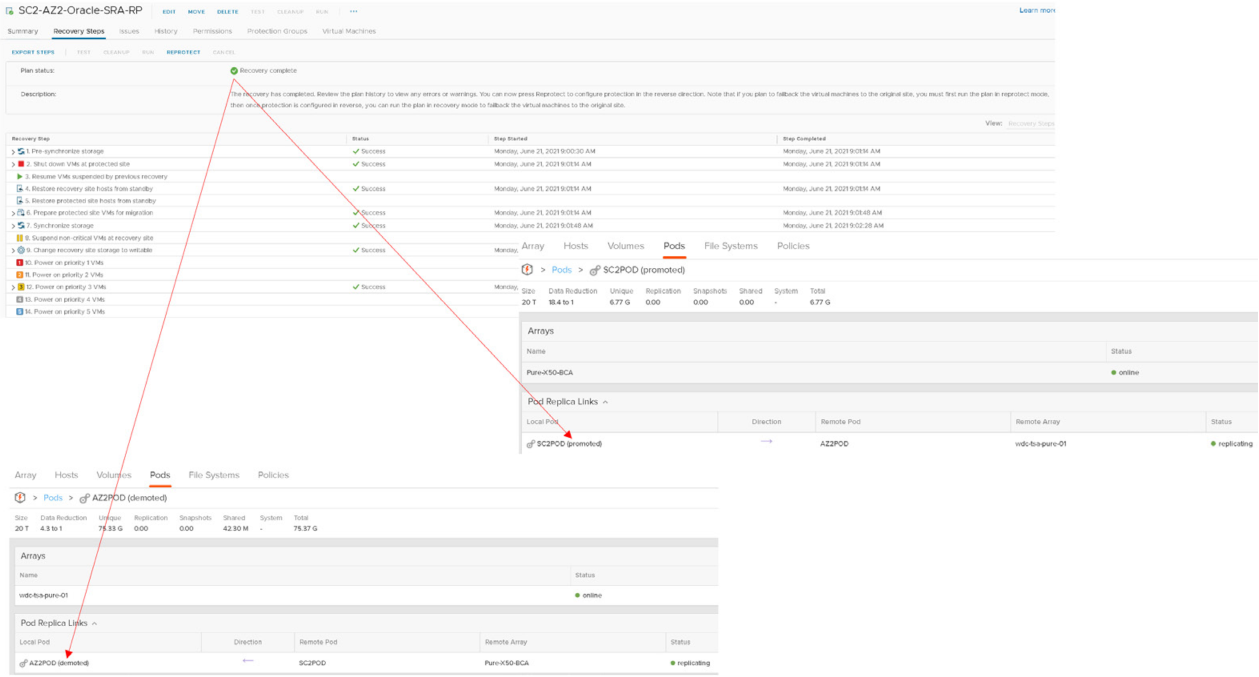
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
Protected site	DR_Site
Recovery site	Primary_Site
Server connection	Connected
Number of VMs	4
Recovery type	Planned migration

FIGURE 284. Run Planned Migration from Site B to Site A

Site A and Site B storage POD status is as shown below:



Plan status: Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to fallback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to fallback the virtual machines to the original site.

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✓ Success	Monday, June 21, 2021 9:00:30 AM	Monday, June 21, 2021 9:01:14 AM
2. Shut down VMs at protected site	✓ Success	Monday, June 21, 2021 9:01:14 AM	Monday, June 21, 2021 9:01:14 AM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Monday, June 21, 2021 9:01:14 AM	Monday, June 21, 2021 9:01:14 AM
5. Restore protected site hosts from standby			
6. Prepare protected site VMs for migration	✓ Success	Monday, June 21, 2021 9:01:14 AM	Monday, June 21, 2021 9:01:48 AM
7. Synchronize storage	✓ Success	Monday, June 21, 2021 9:01:48 AM	Monday, June 21, 2021 9:02:28 AM
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✓ Success	Monday,	
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
12. Power on priority 3 VMs	✓ Success	Monday,	
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

> Pods > SC2POD (promoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	18.4 to 1	6.77 G	0.00	0.00	0.00	-	6.77 G

Arrays

Name	Status
Pure-X50-BCA	● online

Pod Replica Links ^

Local Pod	Direction	Remote Pod	Remote Array	Status
SC2POD (promoted)	→	AZ2POD	wdc-tsa-pure-01	● replicating

> Pods > AZ2POD (demoted)

Size	Data Reduction	Unique	Replication	Snapshots	Shared	System	Total
20 T	4.3 to 1	75.33 G	0.00	0.00	42.30 M	-	75.37 G

Arrays

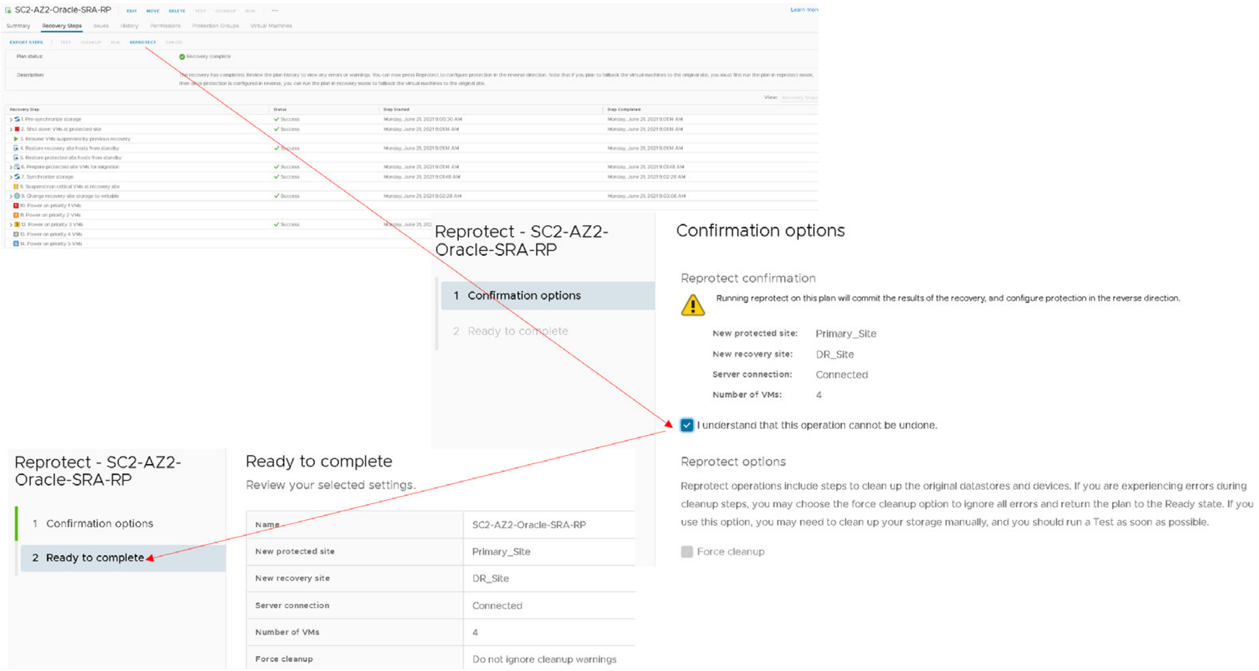
Name	Status
wdc-tsa-pure-01	● online

Pod Replica Links ^

Local Pod	Direction	Remote Pod	Remote Array	Status
AZ2POD (demoted)	←	SC2POD	Pure-X50-BCA	● replicating

FIGURE 285. Site A and Site B Storage POD Status

Reprotect needs to be run on Source Site A back to Target Site B to protect the VMs.



Plan status: Recovery complete

Description: The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to fallback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to fallback the virtual machines to the original site.

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✓ Success	Monday, June 21, 2021 9:00:30 AM	Monday, June 21, 2021 9:01:14 AM
2. Shut down VMs at protected site	✓ Success	Monday, June 21, 2021 9:01:14 AM	Monday, June 21, 2021 9:01:14 AM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Monday, June 21, 2021 9:01:14 AM	Monday, June 21, 2021 9:01:14 AM
5. Restore protected site hosts from standby			
6. Prepare protected site VMs for migration	✓ Success	Monday, June 21, 2021 9:01:14 AM	Monday, June 21, 2021 9:01:48 AM
7. Synchronize storage	✓ Success	Monday, June 21, 2021 9:01:48 AM	Monday, June 21, 2021 9:02:28 AM
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✓ Success	Monday, June 21, 2021 9:02:28 AM	Monday, June 21, 2021 9:03:06 AM
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
12. Power on priority 3 VMs	✓ Success	Monday, June 21, 202	
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: Primary_Site
New recovery site: DR_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

☐ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-RP

1 Confirmation options

2 Ready to complete

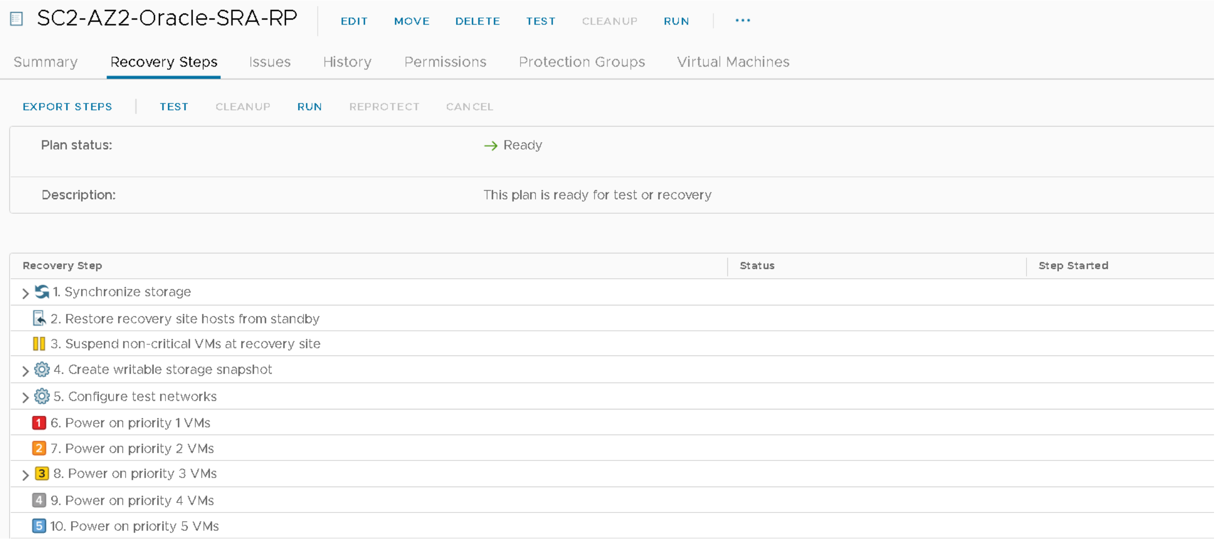
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-RP
New protected site	Primary_Site
New recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 286. Run Reprotect on Site A

The recovery plan steps for Site A are as shown below:

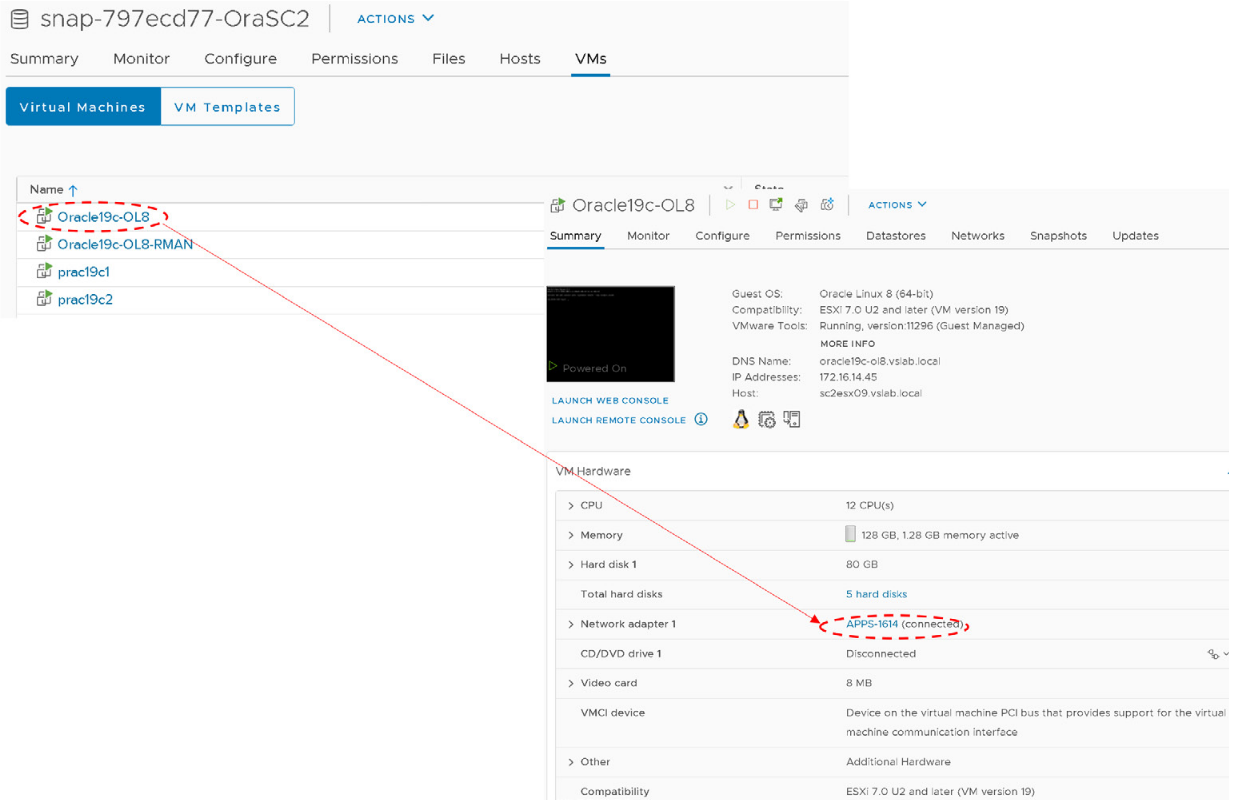


Plan status:	→ Ready
Description:	This plan is ready for test or recovery

Recovery Step	Status	Step Started
1. Synchronize storage		
2. Restore recovery site hosts from standby		
3. Suspend non-critical VMs at recovery site		
4. Create writable storage snapshot		
5. Configure test networks		
6. Power on priority 1 VMs		
7. Power on priority 2 VMs		
8. Power on priority 3 VMs		
9. Power on priority 4 VMs		
10. Power on priority 5 VMs		

FIGURE 287. Recovery Plan Steps on Site A

Single-instance Oracle VM **Oracle19c-OL8** is powered up and connected to protected site network **APPS-1614**.



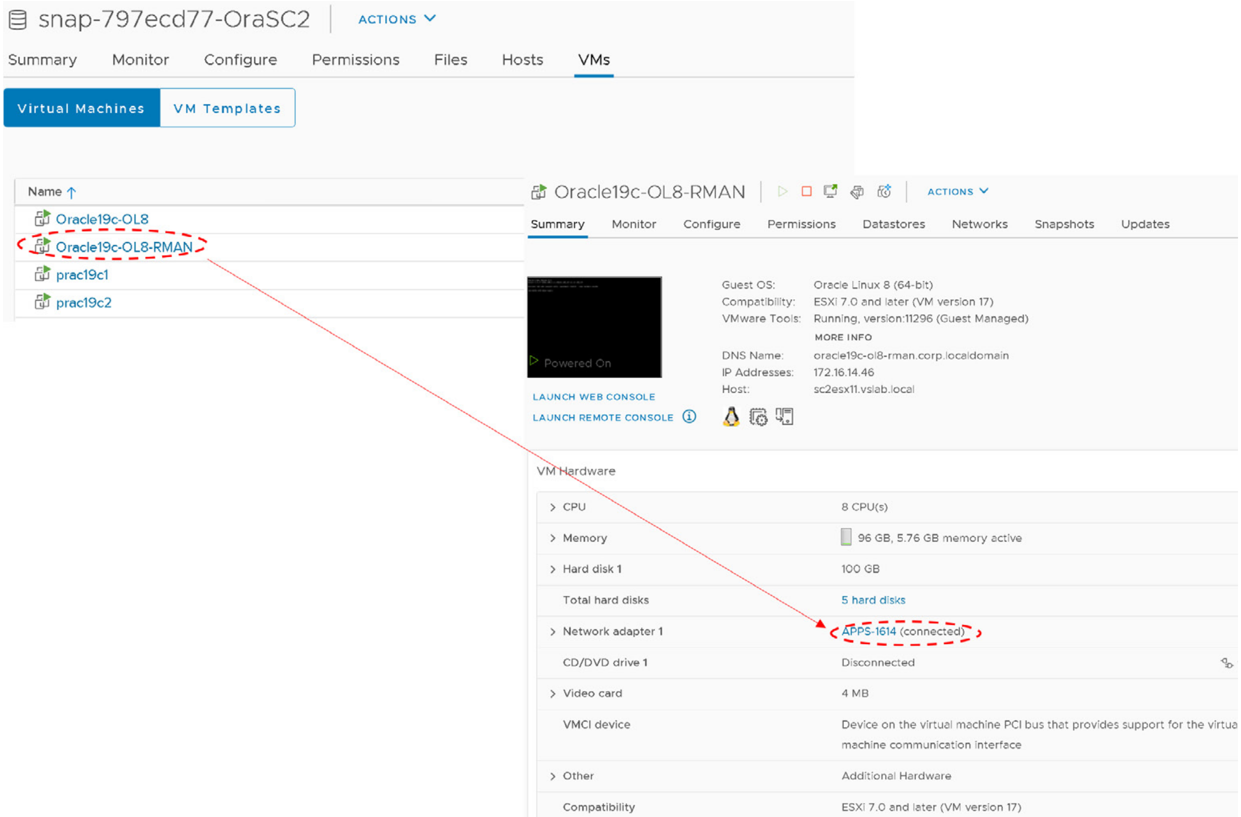
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.16.14.45
Host: sc2esx09.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 288. Oracle VM Oracle19c-OL8 Status

Single-instance Oracle VM **Oracle19c-OL8-RMAN** is powered up and connected to protected site network **APPS-1614**.



Name ↑
Oracle19c-OL8
Oracle19c-OL8-RMAN
prac19c1
prac19c2

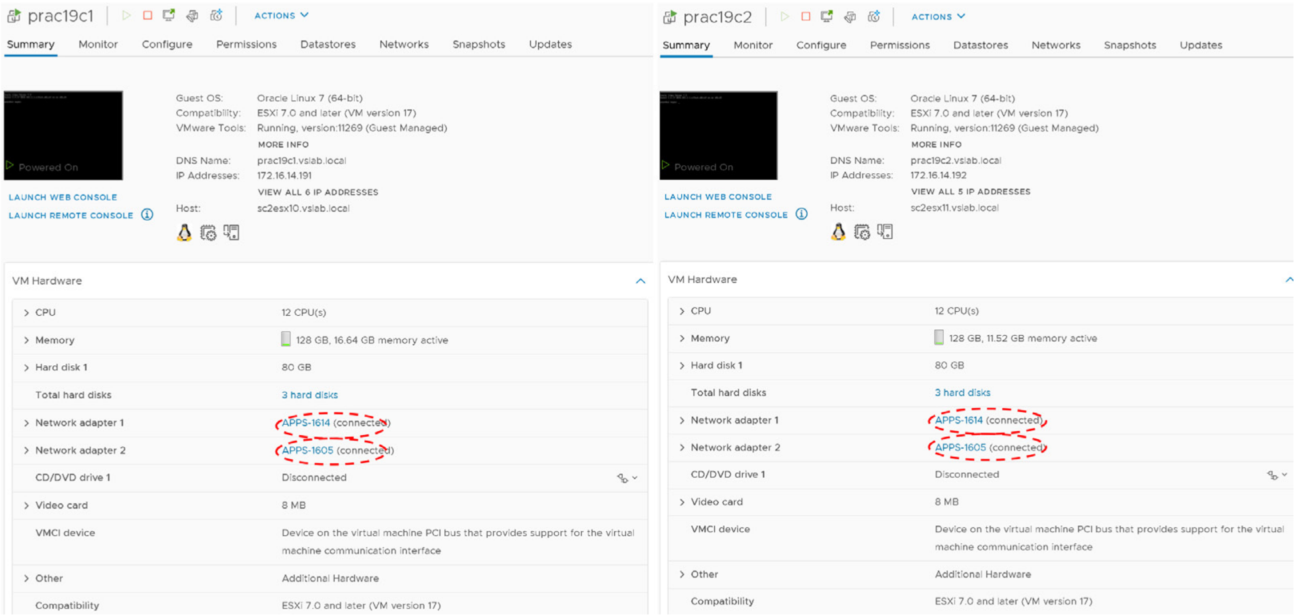
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-rman.corp.localdomain
IP Addresses: 172.16.14.46
Host: sc2esx11.vslab.local

VM Hardware

CPU	8 CPU(s)
Memory	96 GB, 5.76 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtua machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 289. Oracle VM Oracle19c-OL8-RMAN Status

The Oracle RAC cluster **prac19c** VMs are also powered up. The public interfaces are connected to the protected site network **APPS-1614** and private interconnects are connected to the protected site network **APPS-1605**.



Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.16.14.191
Host: sc2esx10.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 16.64 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.16.14.192
Host: sc2esx11.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 290. Oracle RAC VMs prac19c Status

More information on running a disaster recovery with array-based replication can be found in the *Performing a Planned Migration or Disaster Recovery By Running a Recovery Plan* and *SRM User Guide: FlashArray Continuous Replication (ActiveDR) Workflows*.

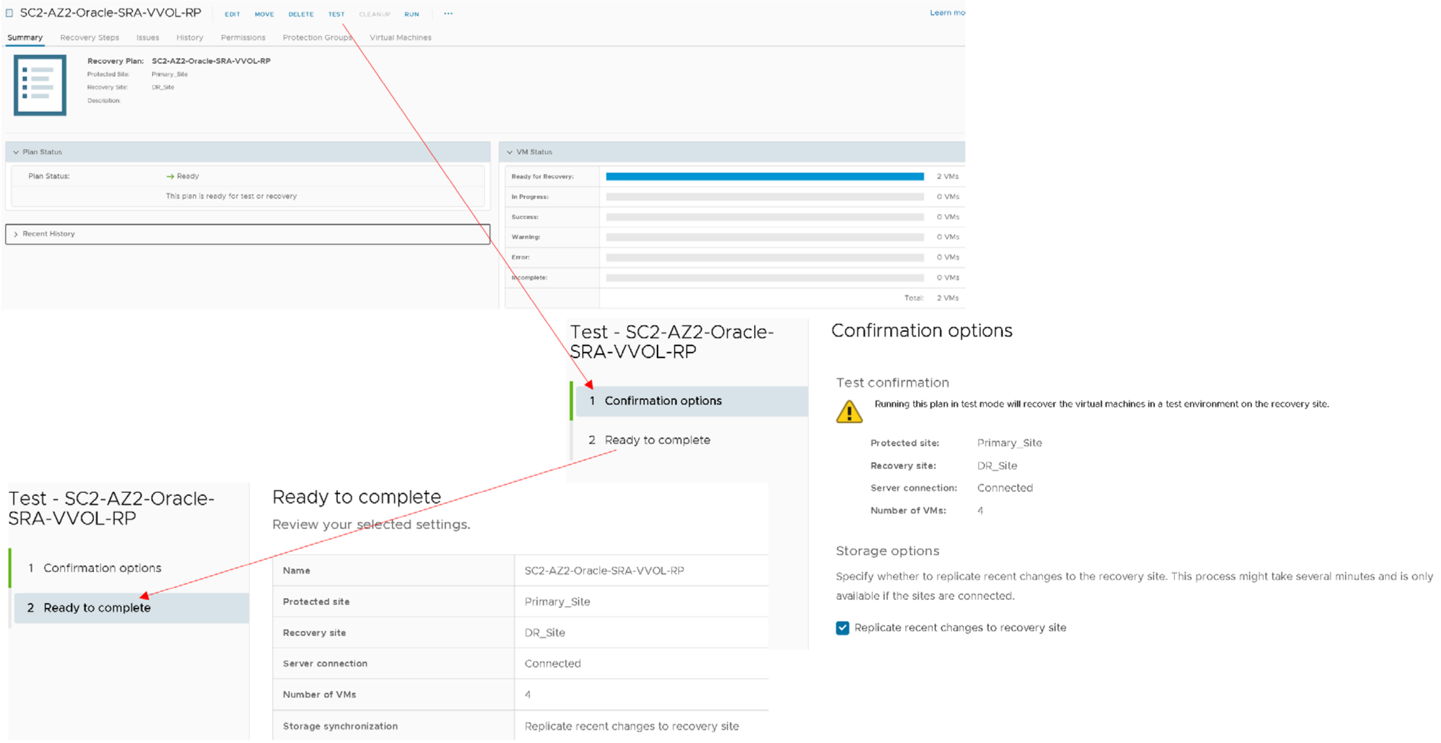
On-premises Using vSphere Virtual Volumes Storage

This use case focusses on the utilization of Site Recovery Manager with storage-based replication using Pure Storage to provide disaster recovery on a **vVOL level**, to both single-instance Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** and Oracle RAC **prac19c**, from on-premises Site A to Site B and vice-versa.

Test Recovery Plan

The steps to test a recovery plan, planned migration of a recovery plan, and actual disaster recovery of a recovery plan for vVOLs, are the same in the case of a storage LUN.

Steps to test the recovery plan **SC2-AZ2-Oracle-SRA-VVOL-RP** are as shown below:



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Ready for Recovery:	2 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	2 VMs

Test - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Test confirmation

Running this plan in test mode will recover the virtual machines in a test environment on the recovery site.

Protected site:	Primary_Site
Recovery site:	DR_Site
Server connection:	Connected
Number of VMs:	4

Storage options

Specify whether to replicate recent changes to the recovery site. This process might take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

Test - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

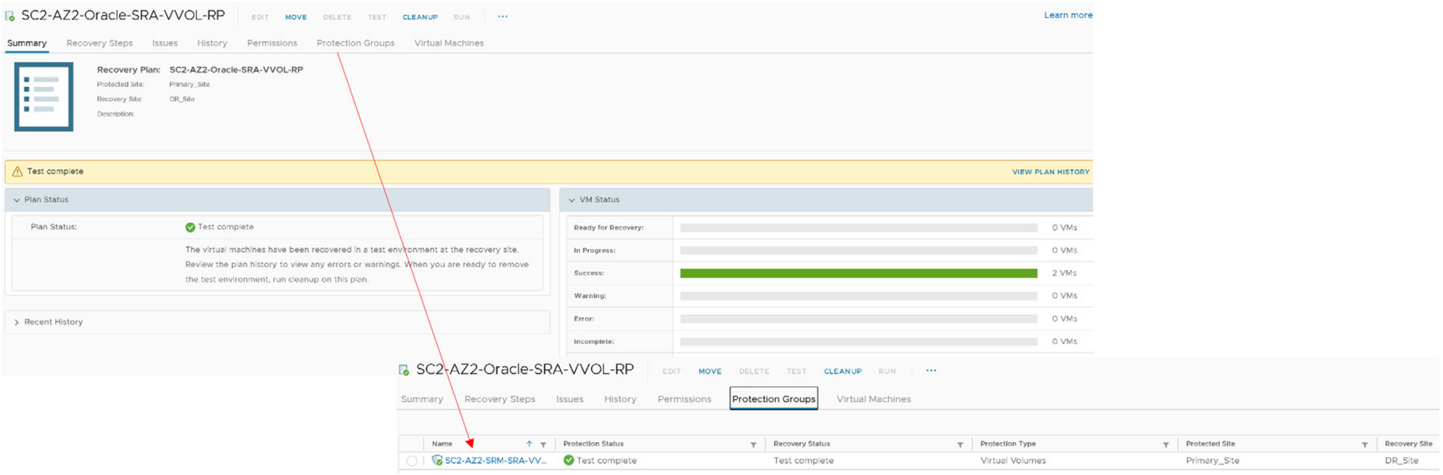
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Storage synchronization	Replicate recent changes to recovery site

FIGURE 291. Test Recovery Plan SC2-AZ2-Oracle-SRA-VVOL-RP for vVOL

The steps to test the recovery plan **SC2-AZ2-Oracle-SRA-VVOL-RP** continue as shown below. The test completes successfully.



SC2-AZ2-Oracle-SRA-VVOL-RP

Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Test complete

Plan Status

Plan Status: Test complete

The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

VM Status

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	2 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs

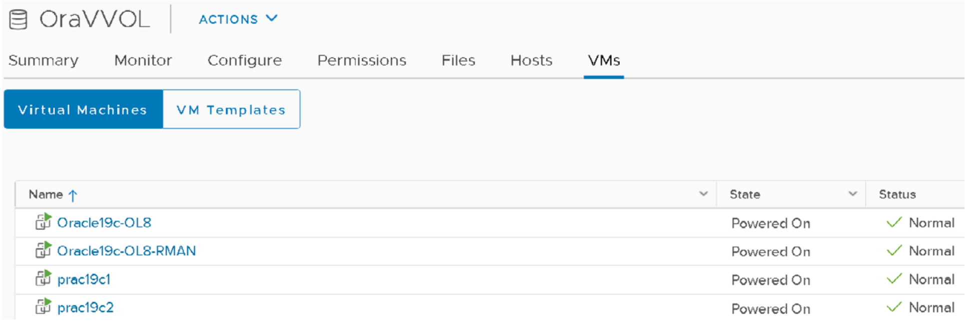
SC2-AZ2-Oracle-SRA-VVOL-RP

Protection Groups

Name	Protection Status	Recovery Status	Protection Type	Protected Site	Recovery Site
SC2-AZ2-SRM-SRA-VV...	Test complete	Test complete	Virtual Volumes	Primary_Site	DR_Site

FIGURE 292. Test Recovery Plan SC2-AZ2-Oracle-SRA-VVOL-RP for vVOL Successful

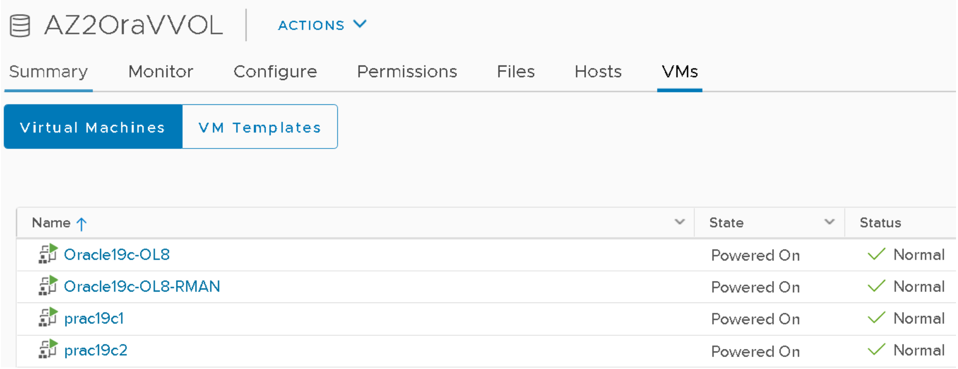
VMs on Protected Site A vVOL datastore **OraVVOL** are still powered on.



Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

FIGURE 293. Protected Site A VMs Status

Both Oracle VM **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** on Recovery Site B vVOL datastore **AZ2OraVVOL** are powered on with the IP addressing scheme set per network mappings to test network **APPS-1810**.



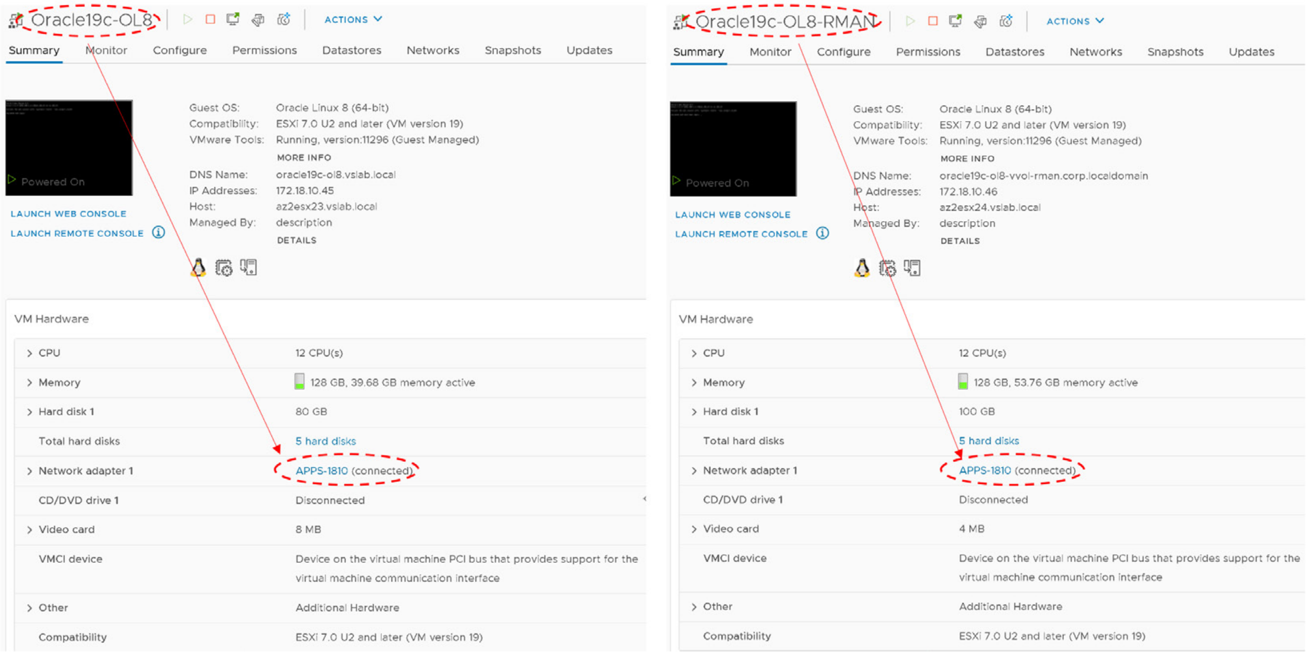
Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

FIGURE 294. Recovery Site B VMs Status

The Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

The storage vVOL-based snapshot is crash-consistent and write-ordering is preserved for each file within a snapshot.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local
Managed By: description

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 39.68 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

Oracle19c-OL8-RMAN

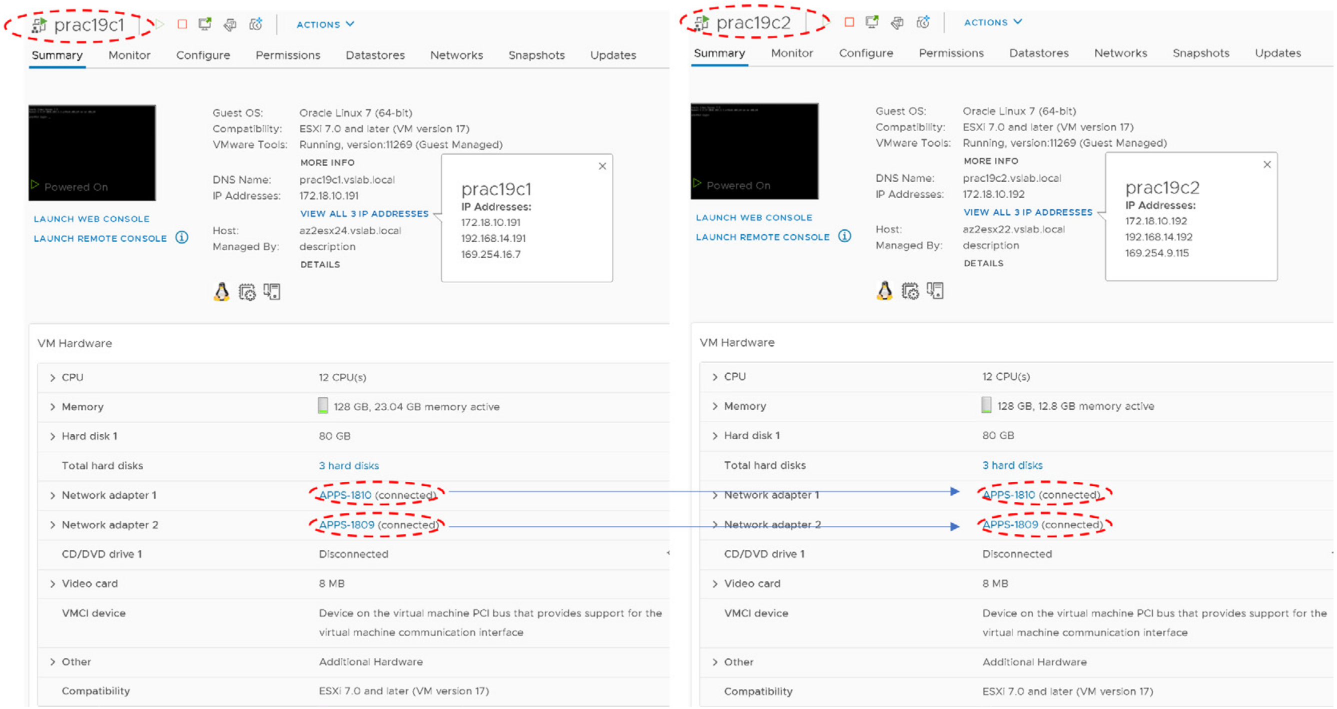
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx24.vslab.local
Managed By: description

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 53.76 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 295. Recovery Site B VMs Networking Details

Oracle RAC **prac19c** VMs on Recovery Site B vVOL datastore **AZ2OraVVOL** are powered on with the public IP addressing scheme set per network mappings to test network **APPS-1810** and the private IP addressing scheme set per network mappings to test network **APPS-1809**.



prac19c1

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.18.10.191
Host: az2esx24.vslab.local
Managed By: description

prac19c1
IP Addresses:
172.18.10.191
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 23.04 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1809 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

prac19c2

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.18.10.192
Host: az2esx22.vslab.local
Managed By: description

prac19c2
IP Addresses:
172.18.10.192
192.168.14.192
169.254.9.115

VM Hardware

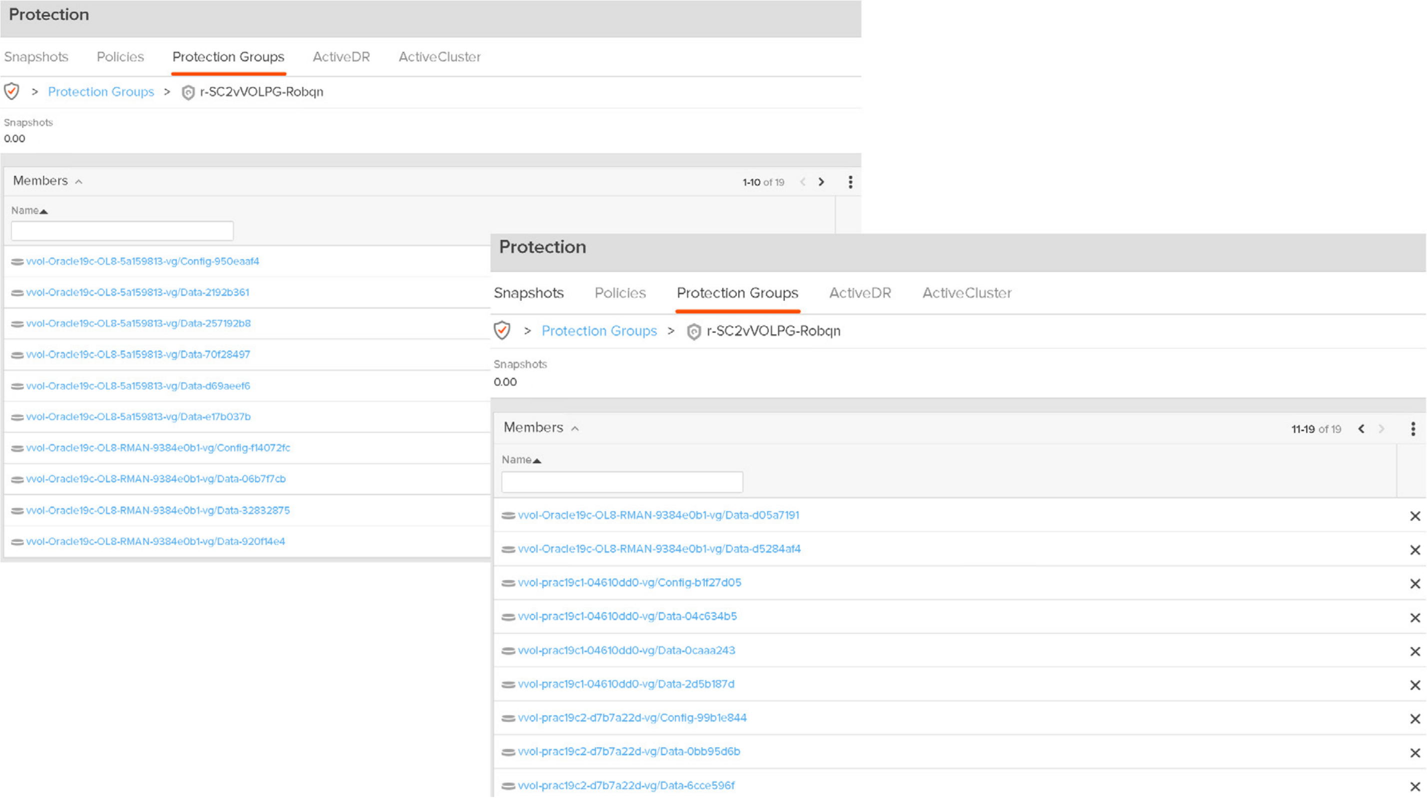
CPU	12 CPU(s)
Memory	128 GB, 12.8 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1809 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 296. Recovery Site B Oracle RAC VMs Networking Details

As part of testing the recovery plan, the network interfaces of the Oracle RAC **prac19c** will be changed to the appropriate test network as defined in the network mappings.

- The VIP and the SCAN IPs have to be changed to the test/recovery network IP scheme in order for the RAC Clusterware to bring up the RAC services.
- The steps to change the RAC VIP IP address can be found in *Oracle 19c Clusterware Administration and Deployment Guide*. The steps to change the Oracle private interconnect IP address can be found in the *Changing Oracle Clusterware Private Network Configuration*.
- The steps to change the RAC SCAN IP addresses can be found in the *My Oracle Support Note How to Update the IP Address of the SCAN VIP Resources (ora.scan{n}.vip) (Doc ID 952903.1)*.
- The steps to change the RAC VIP, scan and private interconnect IP addresses are beyond the scope of this paper.

Site B has Pure Storage protection group **r-SC2vVOLPG-Robqn** created with the replicated VM vVOLs.



Snapshots
0.00

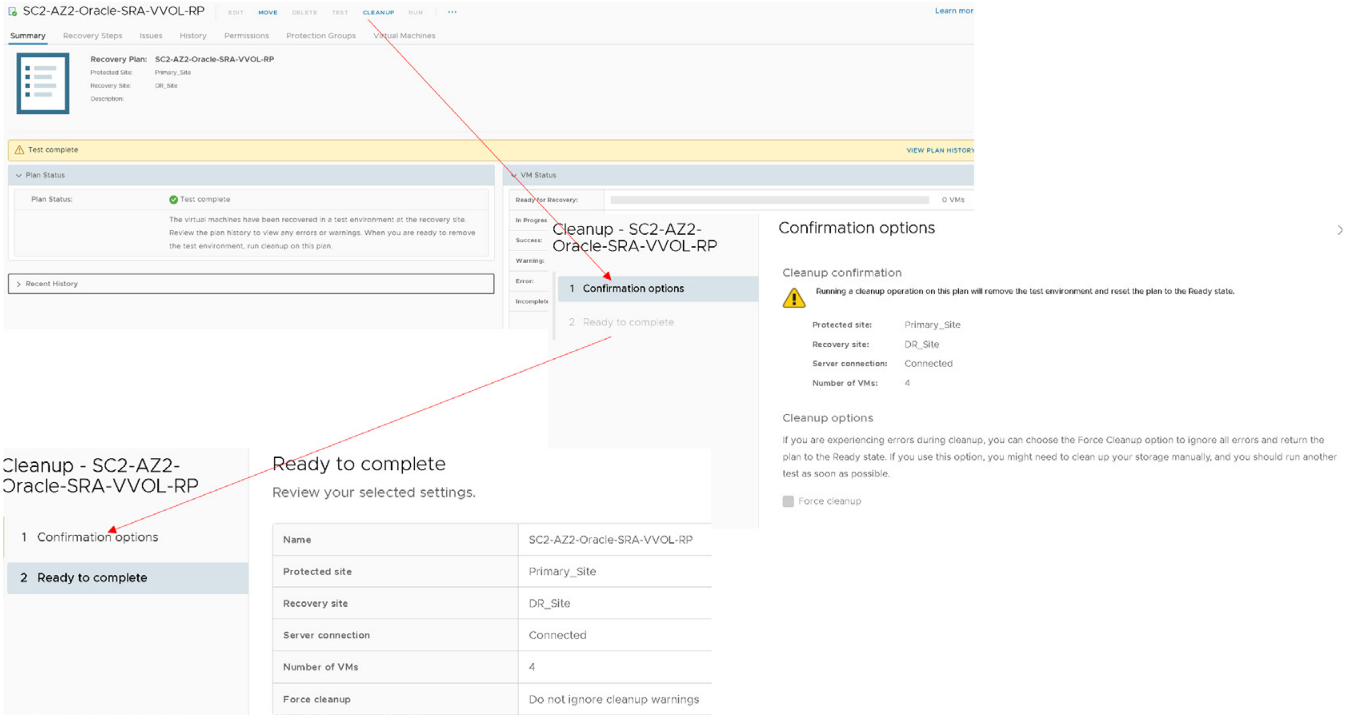
vvol-Oracle19c-OL8-5a159813-vg/Config-950eaaf4
vvol-Oracle19c-OL8-5a159813-vg/Data-2192b361
vvol-Oracle19c-OL8-5a159813-vg/Data-257192b8
vvol-Oracle19c-OL8-5a159813-vg/Data-70f28497
vvol-Oracle19c-OL8-5a159813-vg/Data-d69aeef6
vvol-Oracle19c-OL8-5a159813-vg/Data-e17b037b
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Config-f14072fc
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-06b7f7cb
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-32832875
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-920f14e4

Snapshots
0.00

vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-d05a7191
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-d5284af4
vvol-prac19c1-04610dd0-vg/Config-b1f27d05
vvol-prac19c1-04610dd0-vg/Data-04c634b5
vvol-prac19c1-04610dd0-vg/Data-0caaa243
vvol-prac19c1-04610dd0-vg/Data-2d5b187d
vvol-prac19c2-d7b7a22d-vg/Config-99b1e844
vvol-prac19c2-d7b7a22d-vg/Data-0bb95d6b
vvol-prac19c2-d7b7a22d-vg/Data-6cce596f

FIGURE 297. Recovery Site B Protection Group with Replicated VMs

At the successful completion of the test recovery, perform the cleanup of the test recovery as shown below:



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Test complete

Plan Status: Test complete

The virtual machines have been recovered in a test environment at the recovery site. Review the plan history to view any errors or warnings. When you are ready to remove the test environment, run cleanup on this plan.

Ready for Recovery: 0 VMs

Cleanup - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Cleanup confirmation

Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.

Protected site: Primary_Site
Recovery site: DR_Site
Server connection: Connected
Number of VMs: 4

Cleanup options

If you are experiencing errors during cleanup, you can choose the Force Cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you might need to clean up your storage manually, and you should run another test as soon as possible.

□ Force cleanup

Ready to complete

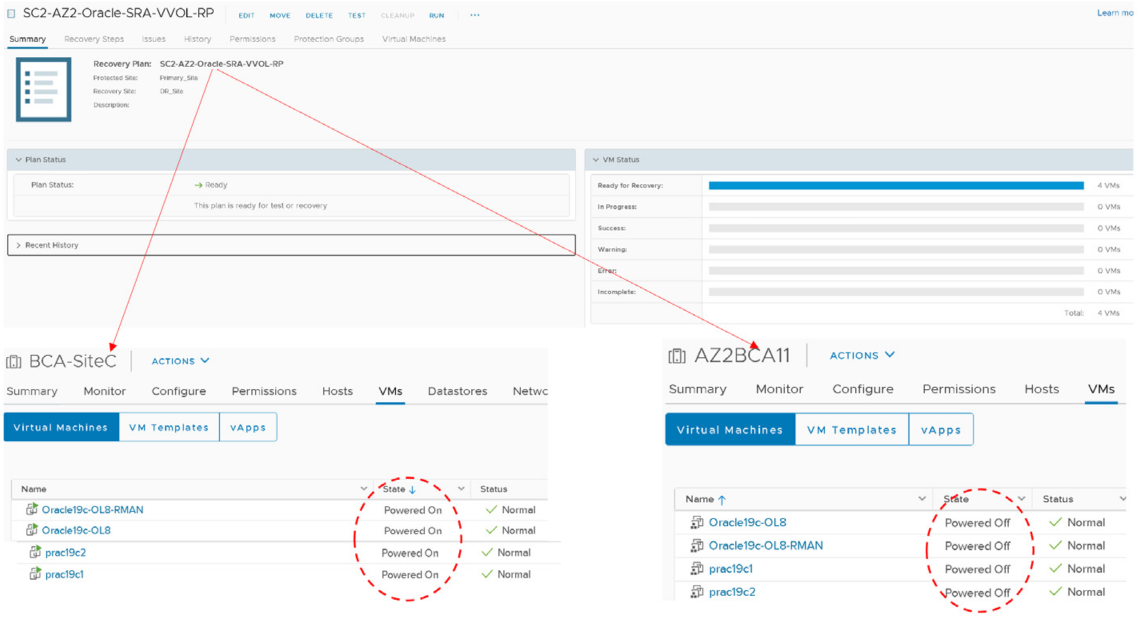
Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 298. Cleanup of Recovery Plan

The cleanup of test recovery is successful.

VMs on Protected Site A vVOL datastore **OraVVOL** are still powered on. We can see placeholder VMs on recovery Site B powered off.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready

This plan is ready for test or recovery

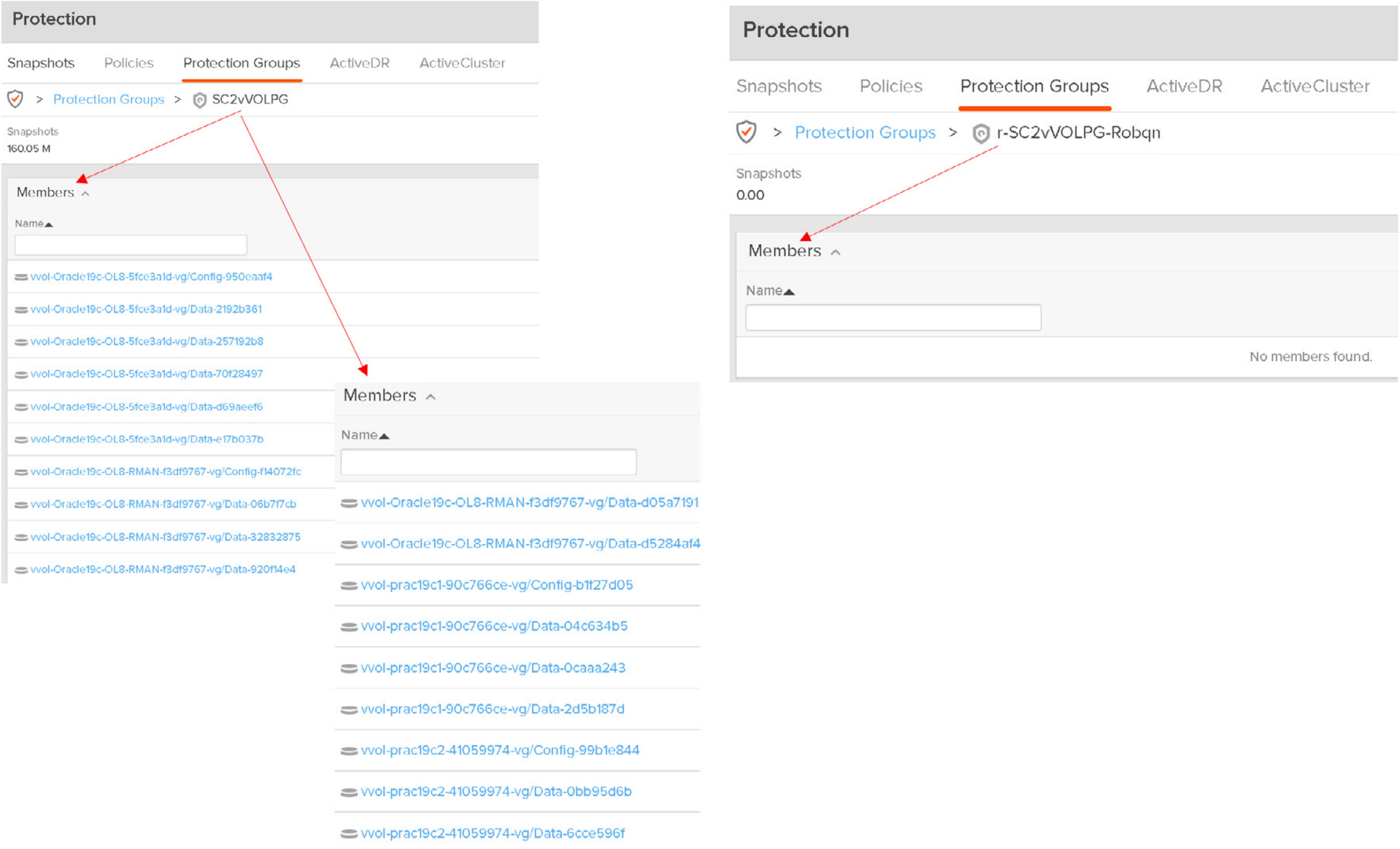
Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Name	State ↓	Status
Oracle19c-OL8-RMAN	Powered On	✓ Normal
Oracle19c-OL8	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal

Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal
prac19c1	Powered Off	✓ Normal
prac19c2	Powered Off	✓ Normal

FIGURE 299. Status of VMs on Protected and Recovery Site

All replicated VM vVOLs have been deleted from the Pure Storage protection group **r-SC2vVOLPG-Robqn**.



Protection

Snapshots | Policies | Protection Groups | ActiveDR | ActiveCluster

> Protection Groups > SC2vVOLPG

Snapshots
160.05 M

Members

Name▲

- vvol-Oracle19c-OL8-5fce3a1d-vg/Config-950eaaf4
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-2192b361
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-257192b8
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-70f28497
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-d69aeef6
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-e17b037b
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Config-f14072fc
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-06b7f7cb
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-32832875
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-920f14e4

Members

Name▲

- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d05a7191
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d5284af4
- vvol-prac19c1-90c766ce-vg/Config-b1f27d05
- vvol-prac19c1-90c766ce-vg/Data-04c634b5
- vvol-prac19c1-90c766ce-vg/Data-0caaa243
- vvol-prac19c1-90c766ce-vg/Data-2d5b187d
- vvol-prac19c2-41059974-vg/Config-99b1e844
- vvol-prac19c2-41059974-vg/Data-0bb95d6b
- vvol-prac19c2-41059974-vg/Data-6cce596f

Protection

Snapshots | Policies | Protection Groups | ActiveDR | ActiveCluster

> Protection Groups > r-SC2vVOLPG-Robqn

Snapshots
0.00

Members

Name▲

No members found.

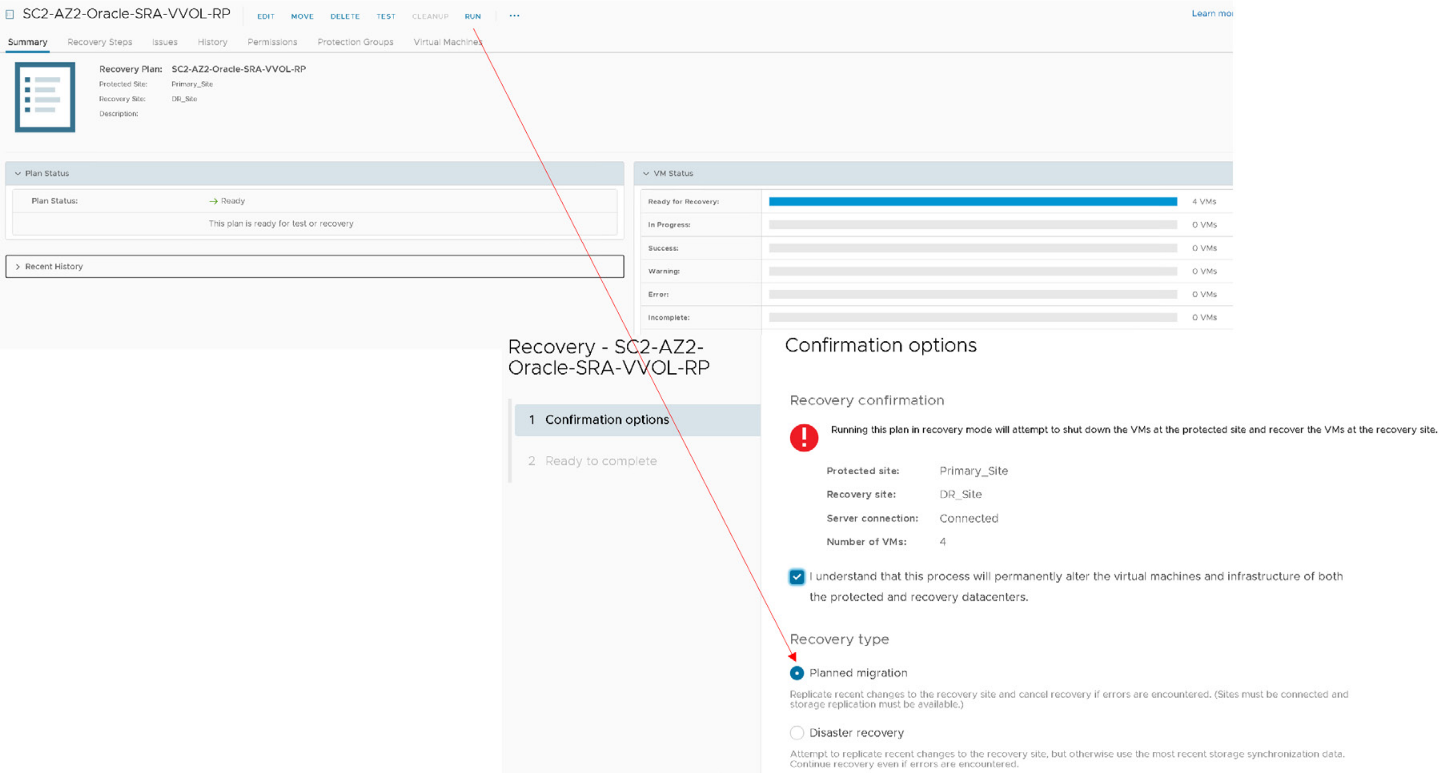
FIGURE 300. Recovery Site vVOLs Status

More information regarding testing a recovery plan with vSphere Virtual Volumes can be found in the *Testing a Recovery Plan* and *SRM User Guide: Configuring Site Recovery Manager vVol-Based Storage Policy Discovery*.

Run Recovery Plan for Planned Migration

The steps to run a planned migration of a recovery plan for vVOLs are the same in the case of a storage LUN.

Steps to run a planned migration of recovery plan **SC2-AZ2-Oracle-SRA-VVOL-RP** are as shown below:



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready
This plan is ready for test or recovery

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs

Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: Primary_Site
Recovery site: DR_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration

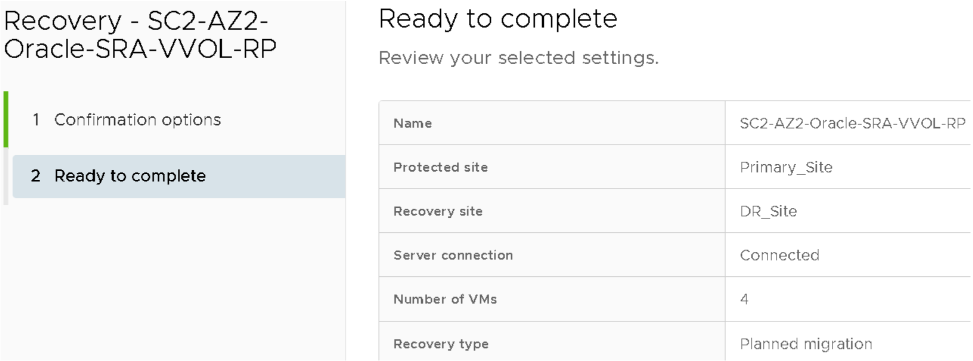
Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

FIGURE 301. Planned Recovery Use Case

The summary of the planned recovery is as shown below:



Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Ready to complete

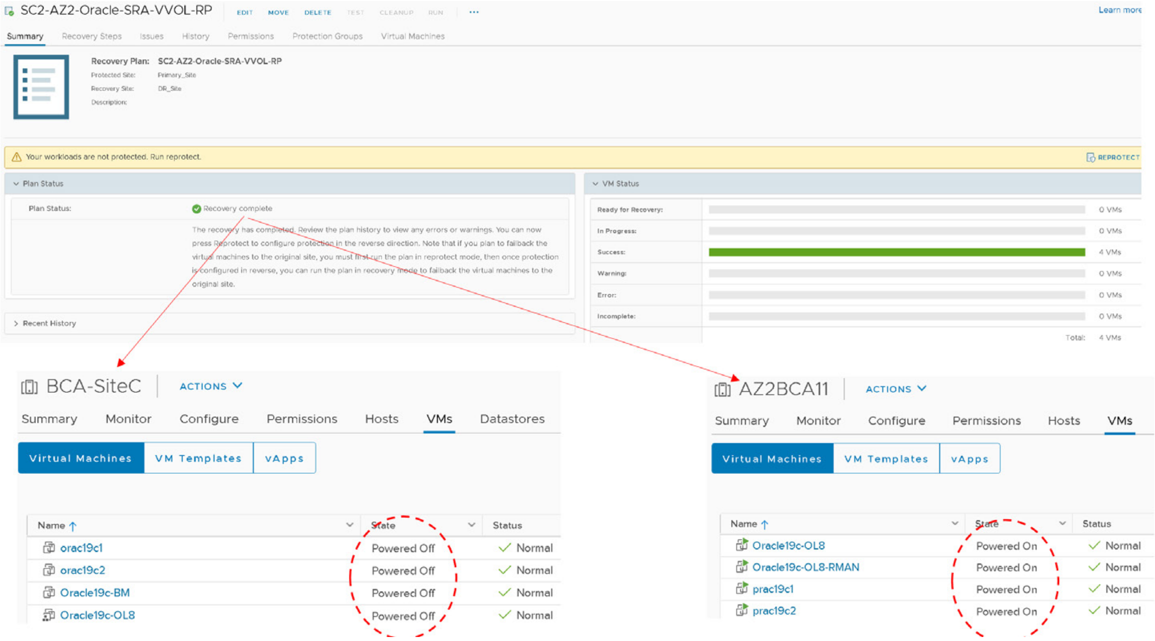
Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Recovery type	Planned migration

FIGURE 302. Planned Recovery Summary

Planned migration of recovery plan **SC2-AZ2-Oracle-SRA-VVOL-RP** is successful.

Protected Site A vVOL VMs are powered off and Recovery Site B vVOL VMs are powered on.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Name ↑	State	Status
orac19c1	Powered Off	✓ Normal
orac19c2	Powered Off	✓ Normal
Oracle19c-BM	Powered Off	✓ Normal
Oracle19c-OL8	Powered Off	✓ Normal

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

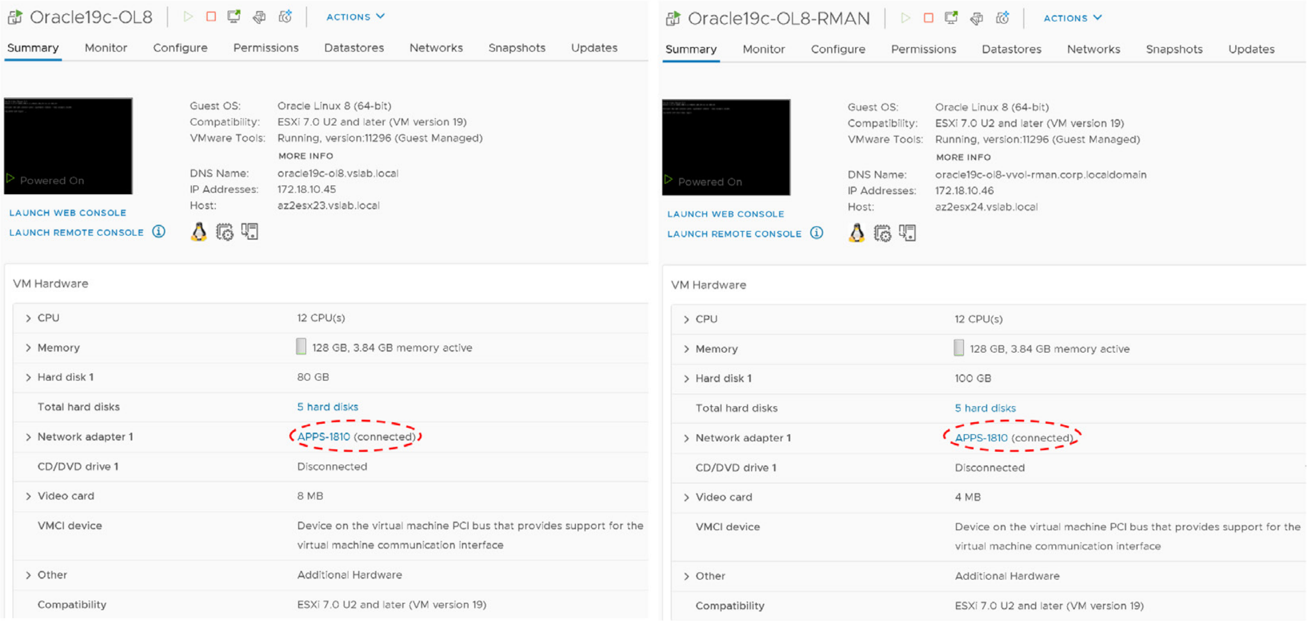
FIGURE 303. Planned Recovery Successful

Recovery Site B vVOL Oracle VM **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined per network mappings to recovery network **APPS-1810**.

As in the case of testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

The storage vVOL-based snapshot is crash-consistent and write-ordering is preserved for each file within a snapshot.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 3.84 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

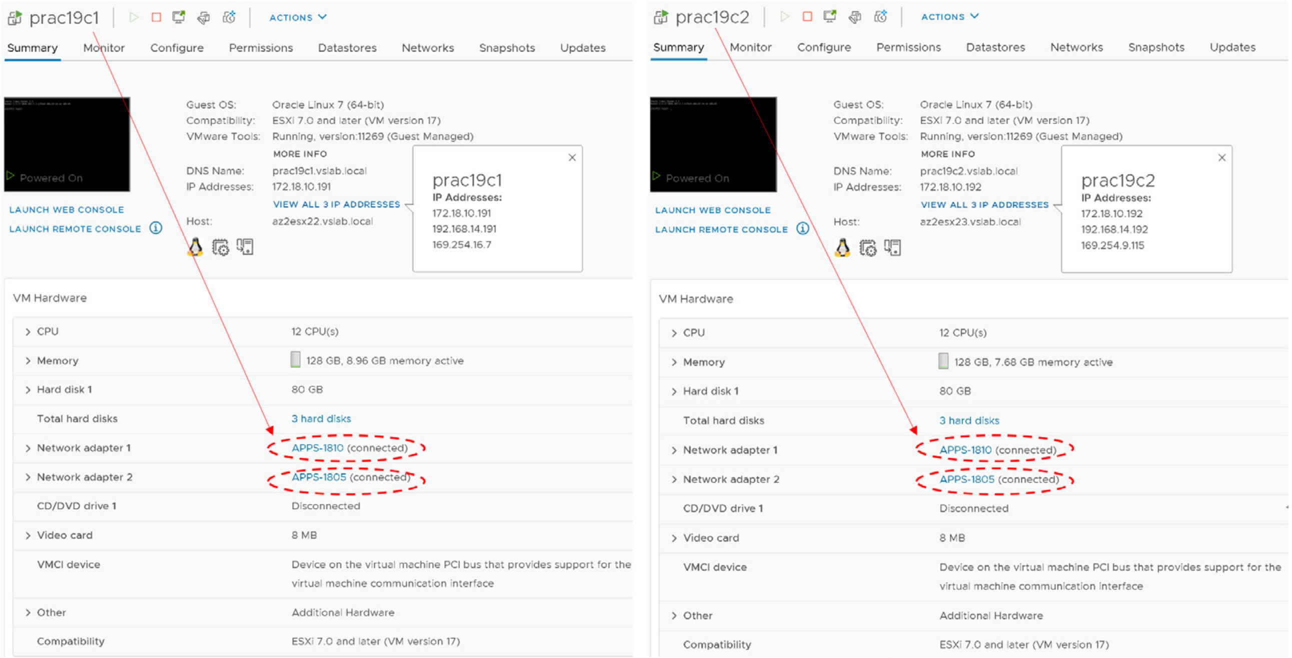
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx24.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 3.84 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 304. Planned Recovery Site VM Status

Recovery Site B vVOL Oracle RAC prac19c is powered on with the public IP addressing scheme set per network mappings to recovery network **APPS-1810**. The private IP addressing scheme is set per network mappings to recovery network **APPS-1805**.



Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.18.10.191
Host: az2esx22.vslab.local

prac19c1
IP Addresses:
172.18.10.191
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 8.96 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.18.10.192
Host: az2esx23.vslab.local

prac19c2
IP Addresses:
172.18.10.192
192.168.14.192
169.254.9.115

VM Hardware

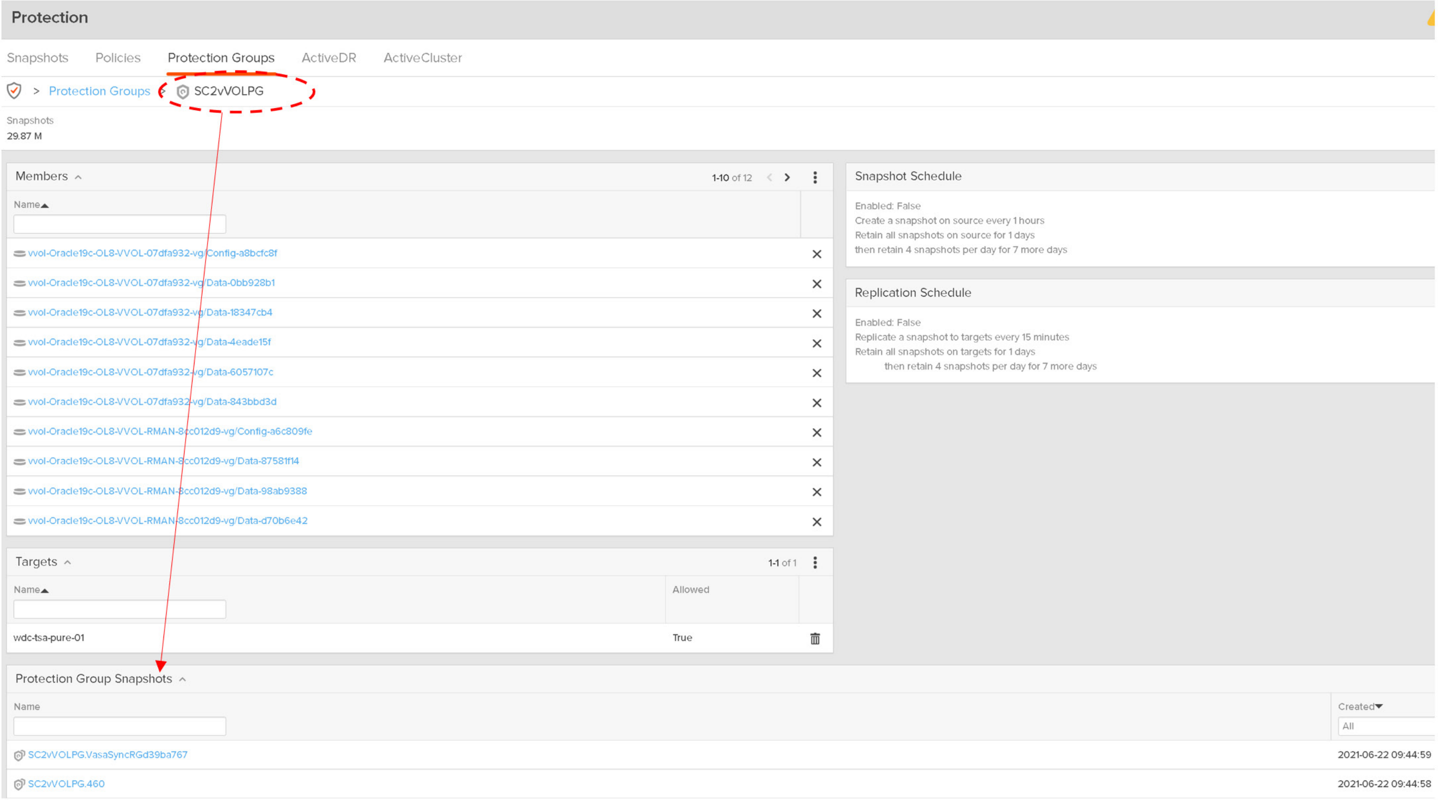
CPU	12 CPU(s)
Memory	128 GB, 7.68 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 305. Planned Recovery Site Oracle RAC VM Status

As part of running a planned migration of the recovery plan, the network interfaces of Oracle RAC prac19c will be changed to the appropriate recovery network as defined in the network mappings.

- The VIP and the SCAN IPs have to be changed to the test/recovery network IP scheme in order for the RAC Clusterware to bring up the RAC services.
- The steps to change the RAC VIP IP address can be found in *Oracle 19c Clusterware Administration and Deployment Guide*. The steps to change the Oracle private interconnect IP address can be found in the *Changing Oracle Clusterware Private Network Configuration*.
- The steps to change the RAC SCAN IP addresses can be found in the *My Oracle Support Note How to Update the IP Address of the SCAN VIP Resources (ora.scan{n}.vip) (Doc ID 952903.1)*.
- The steps to change the RAC VIP, scan and private interconnect IP addresses are beyond the scope of this paper.

Site A has Pure Storage protection group **SC2vVOLPG** with the original VM vVOLs.



Snapshots
29.87 M

Members 1-10 of 12

Name▲	
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Config-a8bcfc8f	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-0bb928b1	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-18347cb4	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-4eade15f	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-6057107c	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-843bbd3d	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Config-a6c809fe	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Data-87581f14	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Data-98ab9388	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Data-d70b6e42	✕

Snapshot Schedule

Enabled: False
Create a snapshot on source every 1 hours
Retain all snapshots on source for 1 days
then retain 4 snapshots per day for 7 more days

Replication Schedule

Enabled: False
Replicate a snapshot to targets every 15 minutes
Retain all snapshots on targets for 1 days
then retain 4 snapshots per day for 7 more days

Targets 1-1 of 1

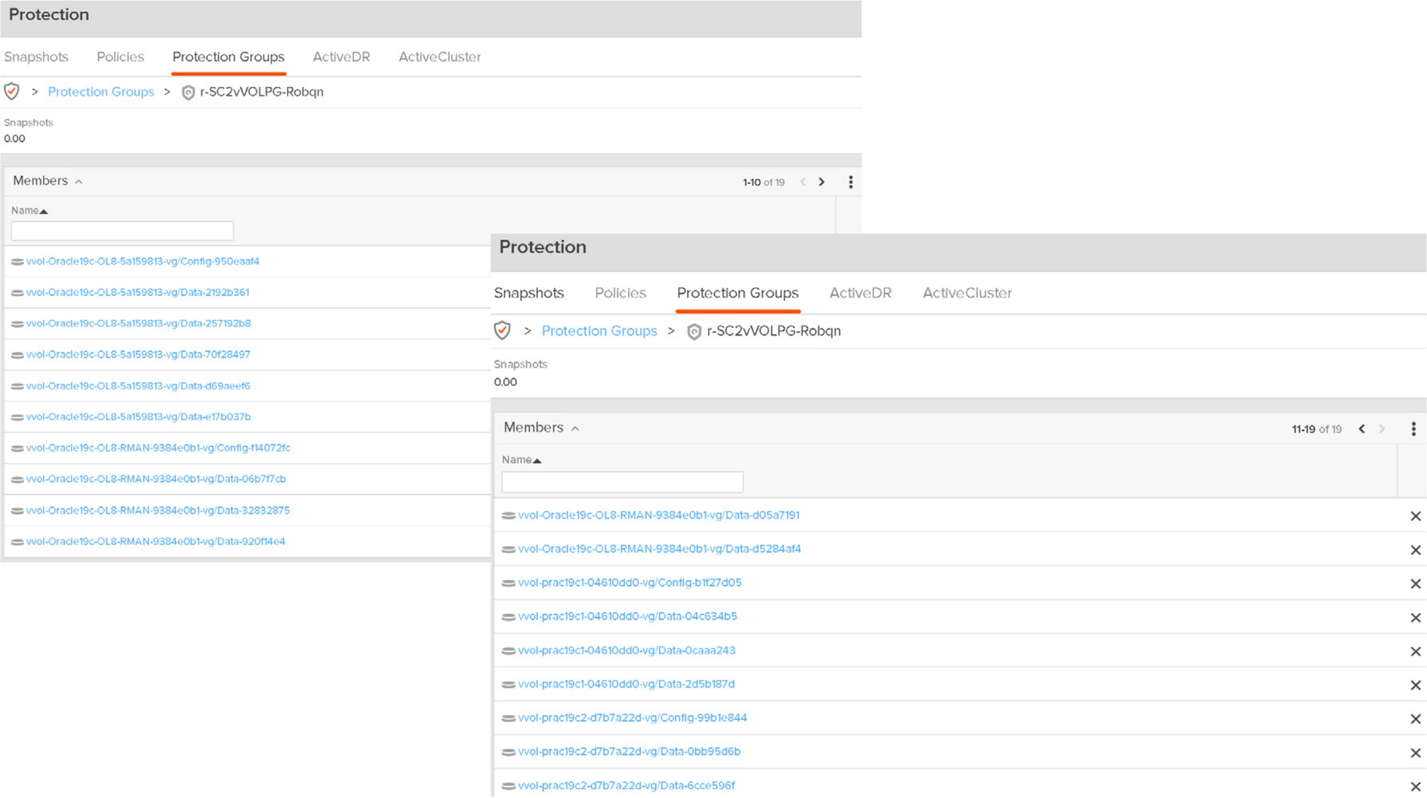
Name▲	Allowed
wdc-tsa-pure-01	True

Protection Group Snapshots

Name	Created▼
SC2vVOLPG.VasaSyncRGd39ba767	2021-06-22 09:44:59
SC2vVOLPG.460	2021-06-22 09:44:58

FIGURE 306. Site A Protection Group

Site B has Pure Storage protection group **r-SC2vVOLPG-Robqn** created with the replicated VM vVols.

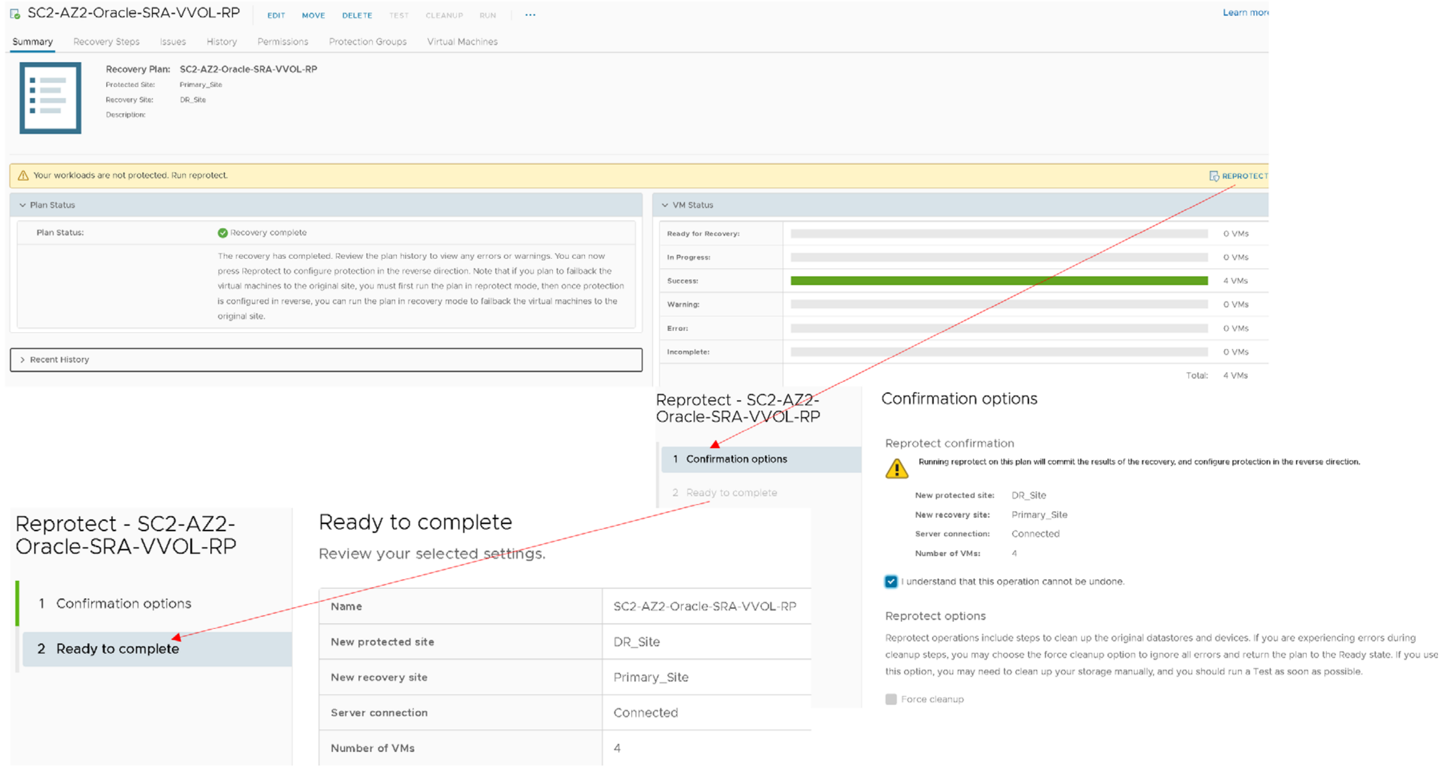


vvol-Oracle19c-OL8-5a159813-vg/Config-950eaaf4
vvol-Oracle19c-OL8-5a159813-vg/Data-2192b361
vvol-Oracle19c-OL8-5a159813-vg/Data-257192b8
vvol-Oracle19c-OL8-5a159813-vg/Data-70f28497
vvol-Oracle19c-OL8-5a159813-vg/Data-d69aeef6
vvol-Oracle19c-OL8-5a159813-vg/Data-e17b037b
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Config-f14072fc
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-06b7f7cb
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-32832875
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-920f14e4

vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-d05a7191
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-d5284af4
vvol-prac19c1-04610dd0-vg/Config-b1f27d05
vvol-prac19c1-04610dd0-vg/Data-04c634b5
vvol-prac19c1-04610dd0-vg/Data-0caaa243
vvol-prac19c1-04610dd0-vg/Data-2d5b187d
vvol-prac19c2-d7b7a22d-vg/Config-99b1e844
vvol-prac19c2-d7b7a22d-vg/Data-0bb95d6b
vvol-prac19c2-d7b7a22d-vg/Data-6cce596f

FIGURE 307. Site B Protection Group with Replicated VMs

At the successful completion of the planned migration, run **Reprotect** to protect Site B, which is now the new protected site.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: DR_Site
New recovery site: Primary_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

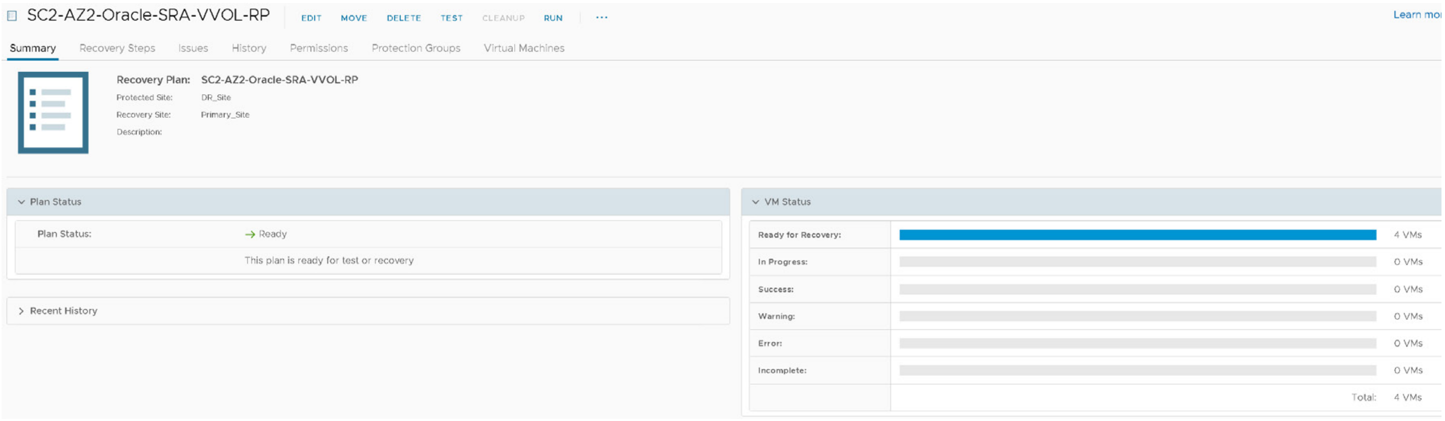
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
New protected site	DR_Site
New recovery site	Primary_Site
Server connection	Connected
Number of VMs	4

FIGURE 308. Reprotect Site B

The reprotect step to protect Site B is successful.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

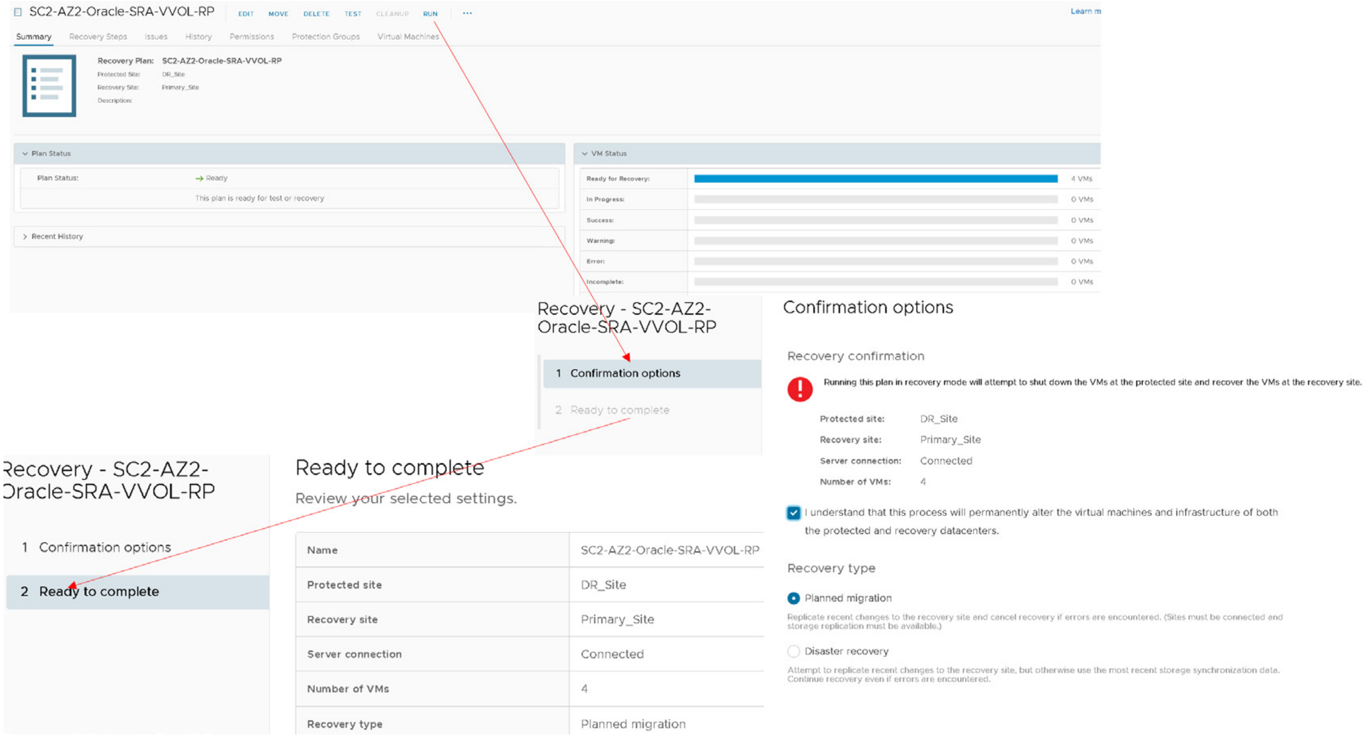
Plan Status: → Ready

This plan is ready for test or recovery

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

FIGURE 309. Reprotect Site B Successful

Run another planned migration to switch the protected site from Site B back to Site A.



SC2-AZ2-Oracle-SRA-VVOL-RP — EDIT MOVE DELETE TEST CLEANUP RUN ··· Learn m

Summary | Recovery Steps | Issues | History | Permissions | Protection Groups | Virtual Machines

Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Plan Status

Plan Status: → Ready
This plan is ready for test or recovery

Recent History

VM Status

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs

Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options
2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: DR_Site
Recovery site: Primary_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration
Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery
Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options
2 Ready to complete

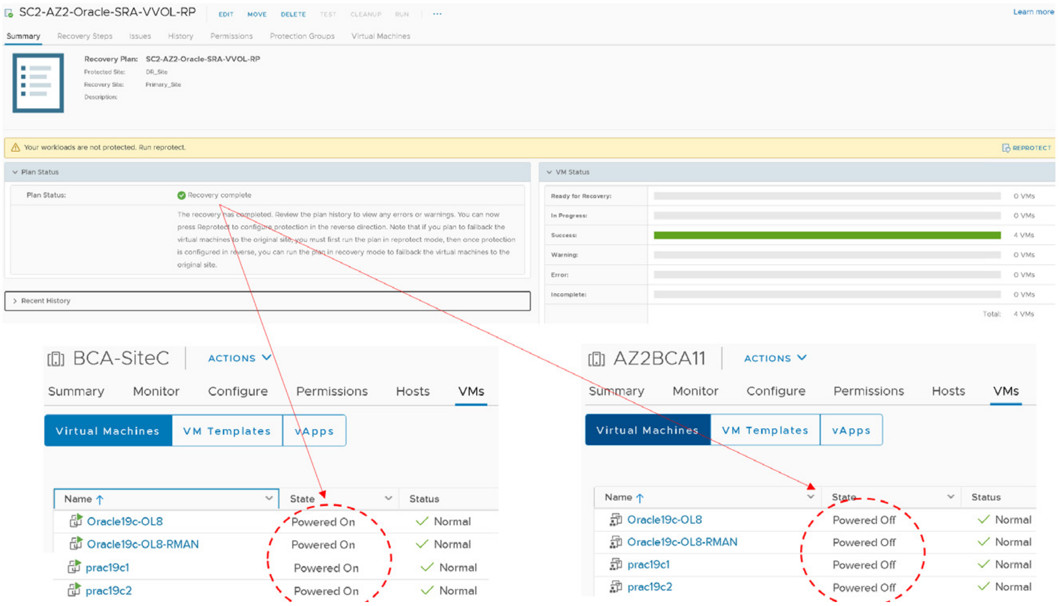
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected site	DR_Site
Recovery site	Primary_Site
Server connection	Connected
Number of VMs	4
Recovery type	Planned migration

FIGURE 310. Run Planned Migration from Site B to Site A

Planned migration from Site B to Site A is successful. VMs on Protected Site A vVOL datastore **OraVVOL** are powered back on and we see the VMs on Recovery Site B are powered off.



SC2-AZ2-Oracle-SRA-VVOL-RP — EDIT MOVE DELETE TEST CLEANUP RUN ··· Learn more

Summary | Recovery Steps | Issues | History | Permissions | Protection Groups | Virtual Machines

Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

⚠ Your workloads are not protected. Run reprotect. REPROTECT

Plan Status

Plan Status: ✓ Recovery complete
The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Recent History

VM Status

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

BCA-SiteC — ACTIONS

Summary | Monitor | Configure | Permissions | Hosts | VMs

Virtual Machines | VM Templates | vApps

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

AZ2BCA11 — ACTIONS

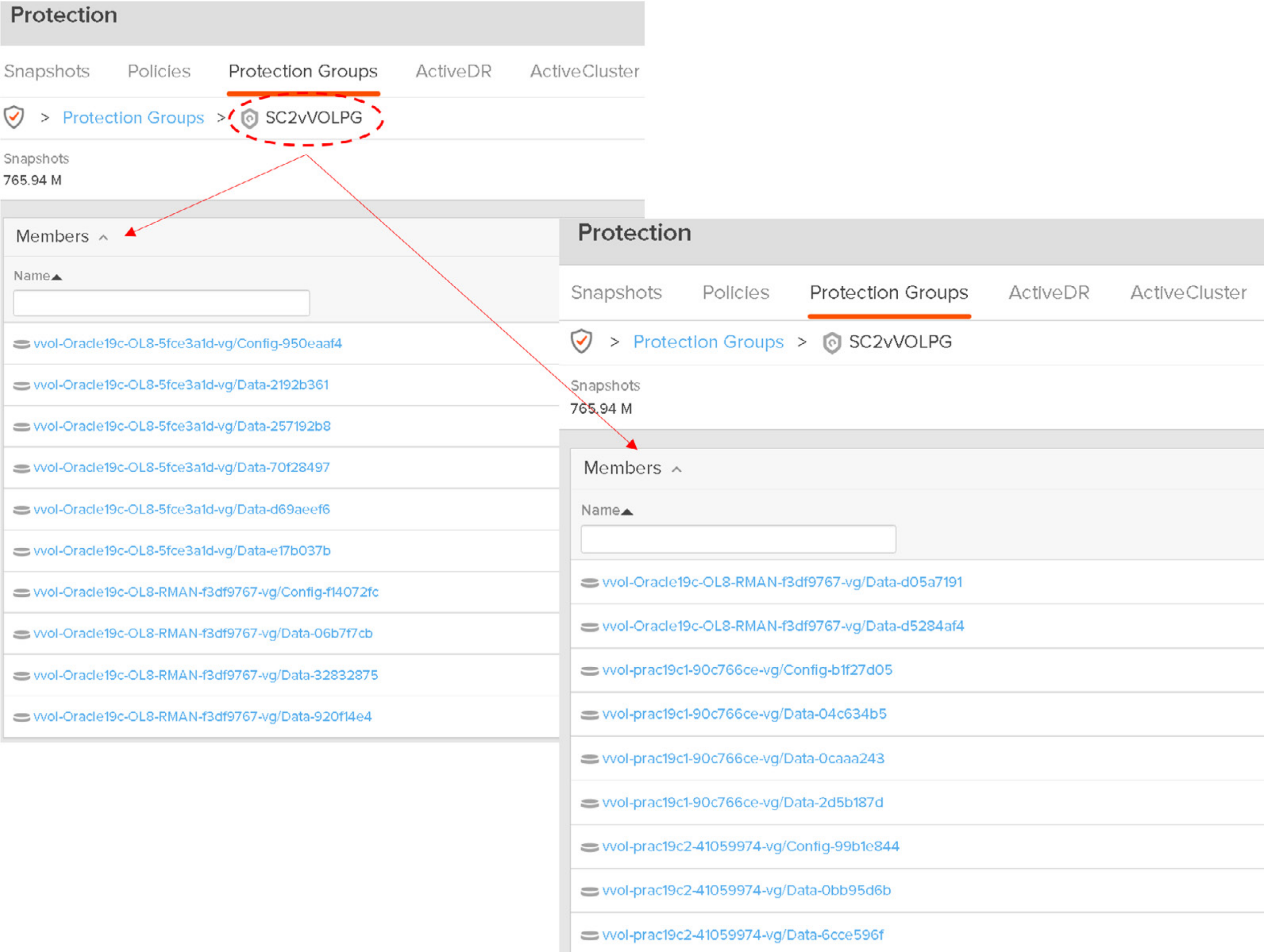
Summary | Monitor | Configure | Permissions | Hosts | VMs

Virtual Machines | VM Templates | vApps

Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal
prac19c1	Powered Off	✓ Normal
prac19c2	Powered Off	✓ Normal

FIGURE 311. Planned Migration from Site B to Site A Successful

Protected Site A protection group **SC2vVOLPG**:



Snapshots
765.94 M

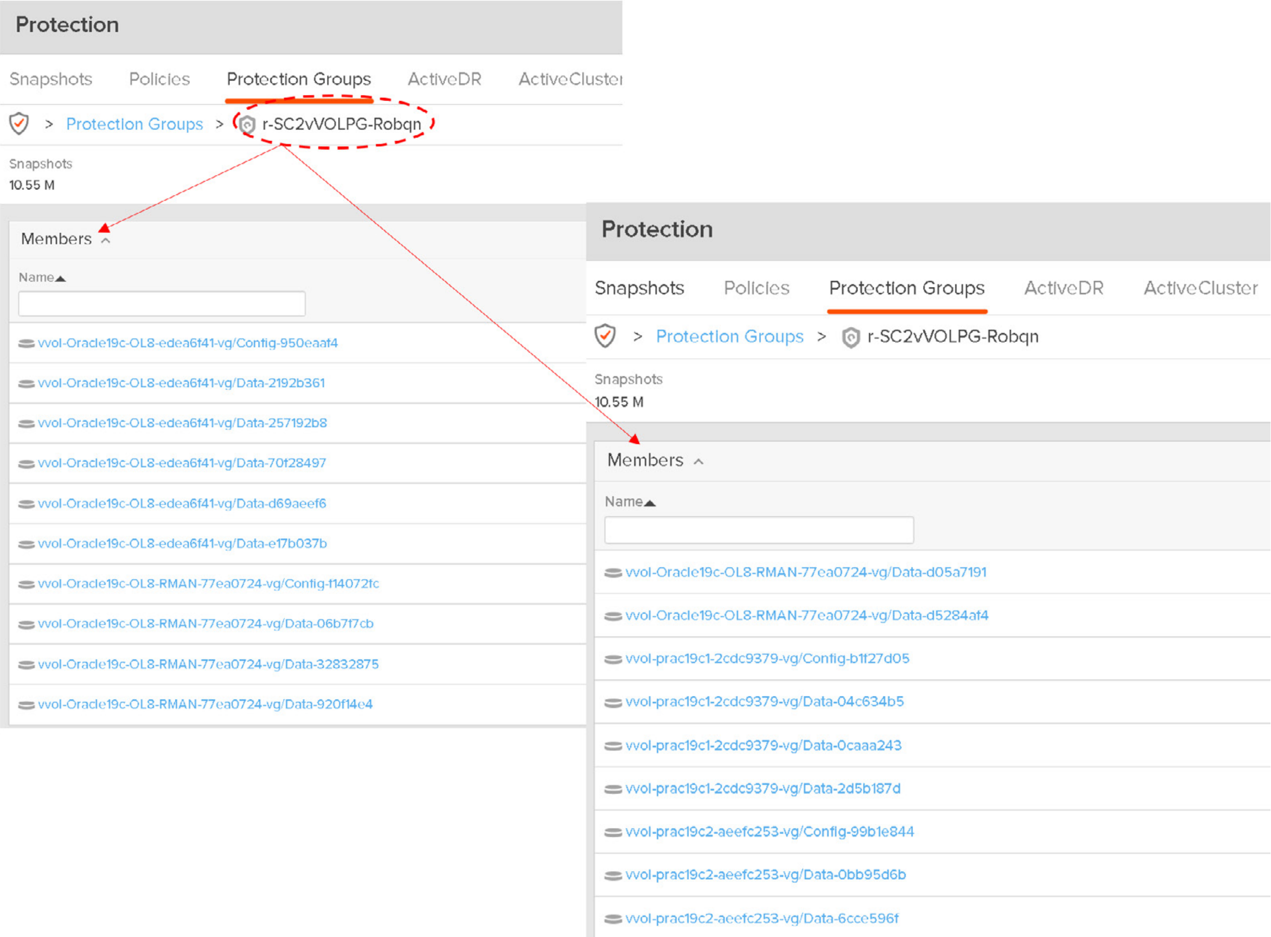
Name▲
vvol-Oracle19c-OL8-5fce3a1d-vg/Config-950eaaf4
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-2192b361
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-257192b8
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-70f28497
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-d69aeef6
vvol-Oracle19c-OL8-5fce3a1d-vg/Data-e17b037b
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Config-f14072fc
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-06b7f7cb
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-32832875
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-920f14e4

Snapshots
765.94 M

Name▲
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d05a7191
vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d5284af4
vvol-prac19c1-90c766ce-vg/Config-b1f27d05
vvol-prac19c1-90c766ce-vg/Data-04c634b5
vvol-prac19c1-90c766ce-vg/Data-0caaa243
vvol-prac19c1-90c766ce-vg/Data-2d5b187d
vvol-prac19c2-41059974-vg/Config-99b1e844
vvol-prac19c2-41059974-vg/Data-0bb95d6b
vvol-prac19c2-41059974-vg/Data-6cce596f

FIGURE 312. Protected Site A Protection Group

Recovery Site B protection group **r-SC2vVOLPG-Robqn**:



Snapshots
10.55 M

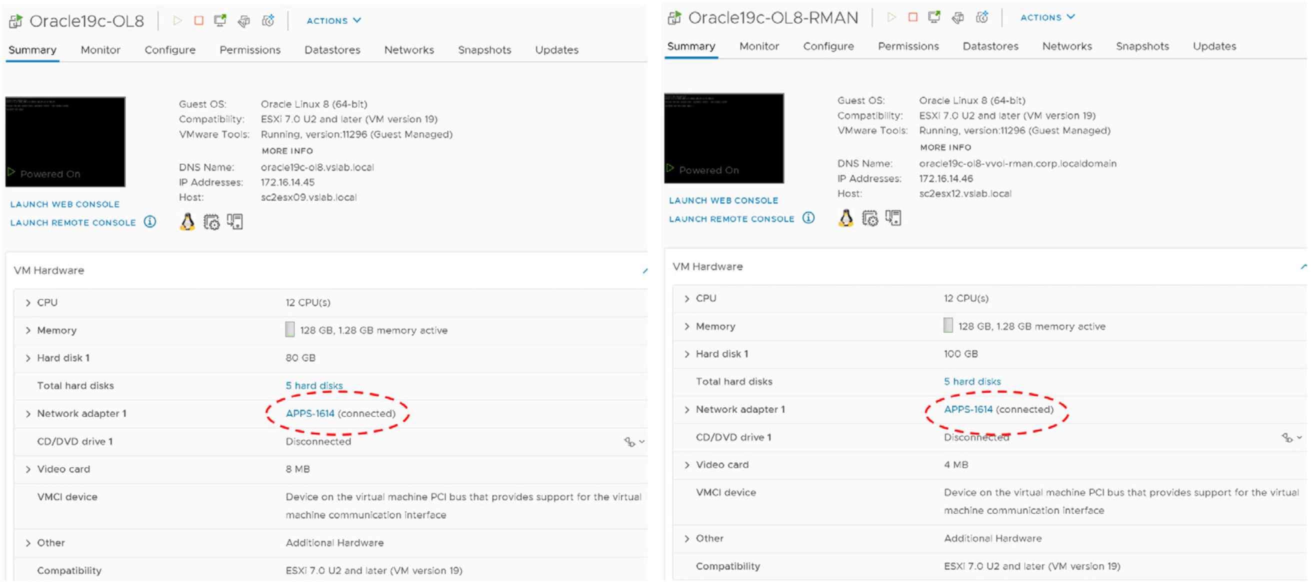
- vvol-Oracle19c-OL8-edea6f41-vg/Config-950eaaf4
- vvol-Oracle19c-OL8-edea6f41-vg/Data-2192b361
- vvol-Oracle19c-OL8-edea6f41-vg/Data-257192b8
- vvol-Oracle19c-OL8-edea6f41-vg/Data-70f28497
- vvol-Oracle19c-OL8-edea6f41-vg/Data-d69aeef6
- vvol-Oracle19c-OL8-edea6f41-vg/Data-e17b037b
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Config-f14072fc
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-06b7f7cb
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-32832875
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-920f14e4

Snapshots
10.55 M

- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-d05a7191
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-d5284af4
- vvol-prac19c1-2cdc9379-vg/Config-b1f27d05
- vvol-prac19c1-2cdc9379-vg/Data-04c634b5
- vvol-prac19c1-2cdc9379-vg/Data-0caaa243
- vvol-prac19c1-2cdc9379-vg/Data-2d5b187d
- vvol-prac19c2-aeefc253-vg/Config-99b1e844
- vvol-prac19c2-aeefc253-vg/Data-0bb95d6b
- vvol-prac19c2-aeefc253-vg/Data-6cce596f

FIGURE 313. Recovery Site B Protection Group

Site A vVOL Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined as per network mappings to the primary network **APPS-1614**.



Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.16.14.45
Host: sc2esx09.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

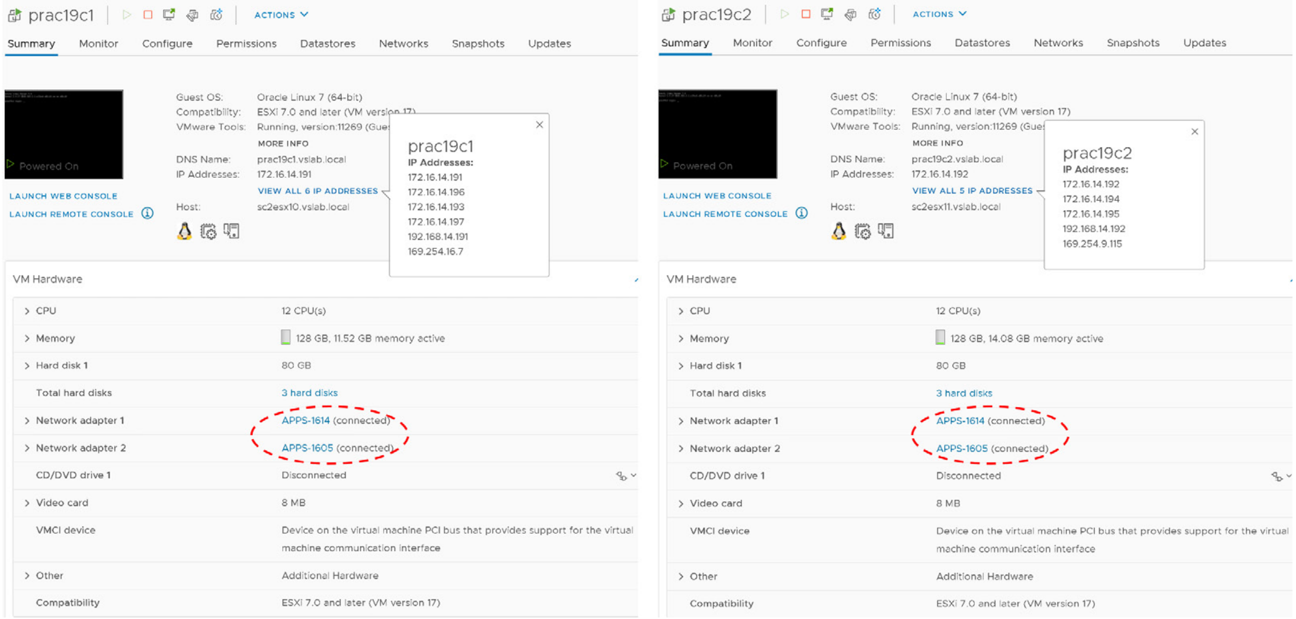
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.16.14.46
Host: sc2esx12.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 314. Site A VMs Status

Site A vVOL Oracle RAC **prac19c** is powered on with the Public IP addressing scheme set as per the network mappings to the primary network **APPS-1614** and private IP addressing scheme set as per the network mappings to the primary network **APPS-1605**.



Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Gue
DNS Name: prac19c1.vslab.local
IP Addresses: 172.16.14.191
Host: sc2esx10.vslab.local

prac19c1
IP Addresses:
172.16.14.191
172.16.14.196
172.16.14.193
172.16.14.197
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Gue
DNS Name: prac19c2.vslab.local
IP Addresses: 172.16.14.192
Host: sc2esx11.vslab.local

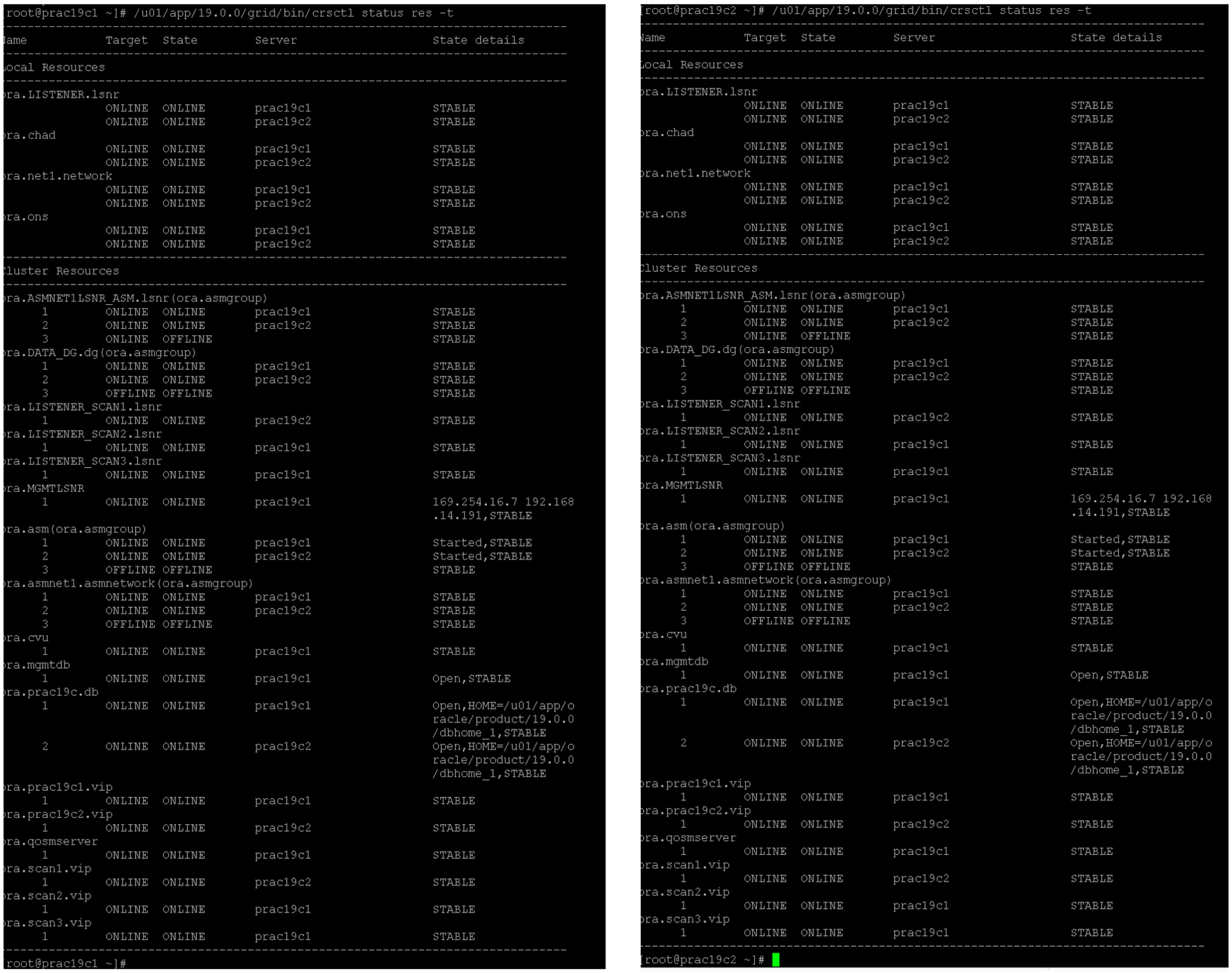
prac19c2
IP Addresses:
172.16.14.192
172.16.14.194
172.16.14.195
192.168.14.192
169.254.9.115

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 14.08 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 315. Site A Oracle RAC VMs Status

All Oracle RAC **prac19c** cluster services are up.

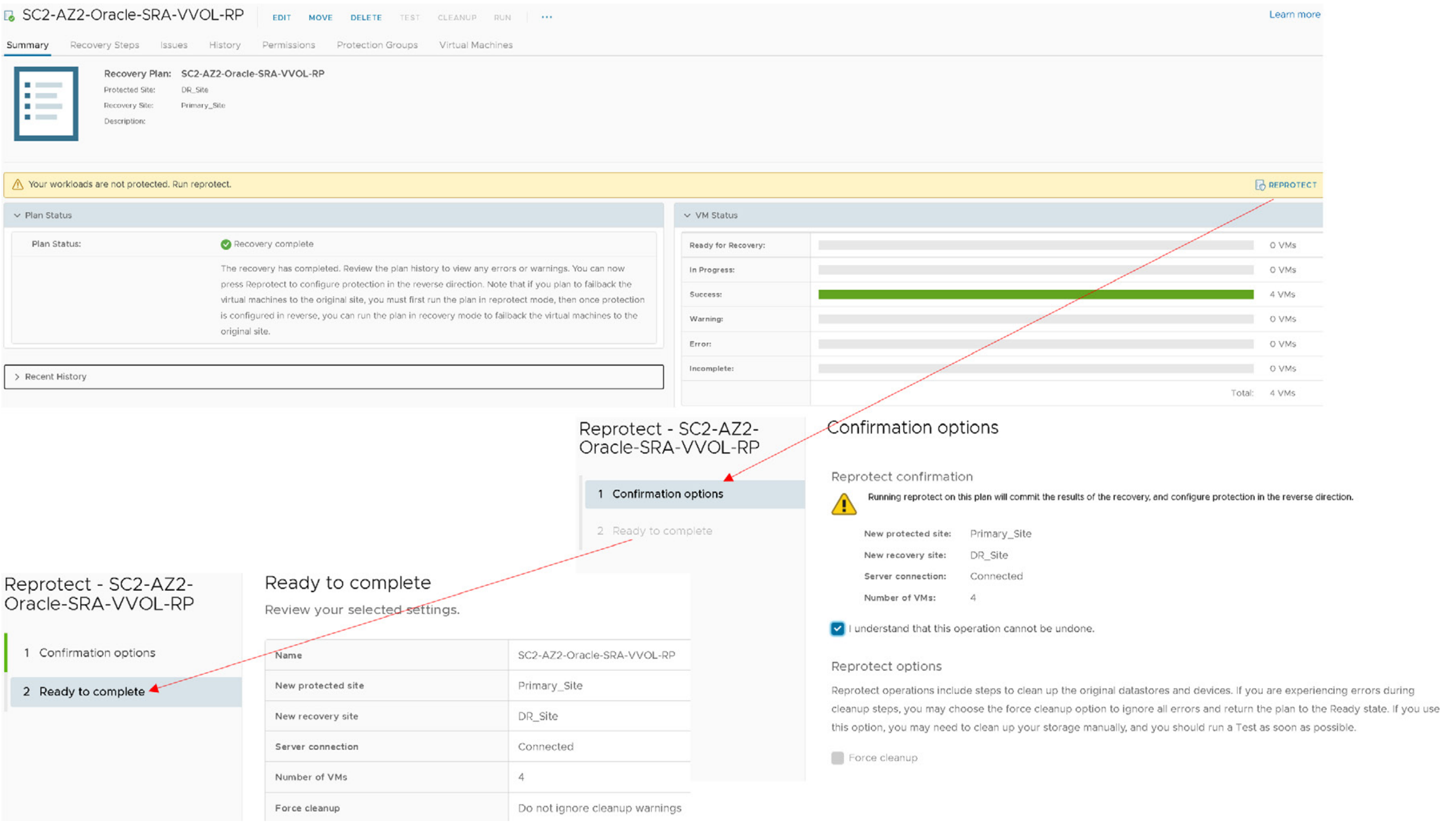


```
[root@prac19c1 ~]# /u01/app/19.0.0/grid/bin/crsctl status res -t
--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.LISTENER.lsnr
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.chad
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.net1.network
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.ons
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.ASMNET1LSNR_ASM.lsnr(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        ONLINE  OFFLINE                               STABLE
ora.DATA_DG.dg(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.LISTENER_SCAN1.lsnr
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.LISTENER_SCAN2.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.LISTENER_SCAN3.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.MGMTLSNR
      1        ONLINE  ONLINE       prac19c1                 169.254.16.7 192.168
                                                             .14.191,STABLE
ora.asm(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 Started,STABLE
      2        ONLINE  ONLINE       prac19c2                 Started,STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.asmnet1.asmnetwork(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.cvu
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.mgmtdb
      1        ONLINE  ONLINE       prac19c1                 Open,STABLE
ora.prac19c.db
      1        ONLINE  ONLINE       prac19c1                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
      2        ONLINE  ONLINE       prac19c2                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
ora.prac19c1.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.prac19c2.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.qosmserver
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan1.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.scan2.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan3.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
--------------------------------------------------------------------------------
[root@prac19c1 ~]#
```

```
[root@prac19c2 ~]# /u01/app/19.0.0/grid/bin/crsctl status res -t
--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.LISTENER.lsnr
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.chad
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.net1.network
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
ora.ons
               ONLINE  ONLINE       prac19c1                 STABLE
               ONLINE  ONLINE       prac19c2                 STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.ASMNET1LSNR_ASM.lsnr(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        ONLINE  OFFLINE                               STABLE
ora.DATA_DG.dg(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.LISTENER_SCAN1.lsnr
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.LISTENER_SCAN2.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.LISTENER_SCAN3.lsnr
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.MGMTLSNR
      1        ONLINE  ONLINE       prac19c1                 169.254.16.7 192.168
                                                             .14.191,STABLE
ora.asm(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 Started,STABLE
      2        ONLINE  ONLINE       prac19c2                 Started,STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.asmnet1.asmnetwork(ora.asmgroup)
      1        ONLINE  ONLINE       prac19c1                 STABLE
      2        ONLINE  ONLINE       prac19c2                 STABLE
      3        OFFLINE OFFLINE                               STABLE
ora.cvu
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.mgmtdb
      1        ONLINE  ONLINE       prac19c1                 Open,STABLE
ora.prac19c.db
      1        ONLINE  ONLINE       prac19c1                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
      2        ONLINE  ONLINE       prac19c2                 Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /dbhome_1,STABLE
ora.prac19c1.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.prac19c2.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.qosmserver
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan1.vip
      1        ONLINE  ONLINE       prac19c2                 STABLE
ora.scan2.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
ora.scan3.vip
      1        ONLINE  ONLINE       prac19c1                 STABLE
--------------------------------------------------------------------------------
[root@prac19c2 ~]#
```

FIGURE 316. Site A Oracle RAC Cluster Services

Run **Reprotect** to reprotect the VMs on Protected Site A.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

⚠ Your workloads are not protected. Run reprotect.

Plan Status: ✓ Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

⚠ Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: Primary_Site
New recovery site: DR_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

☐ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

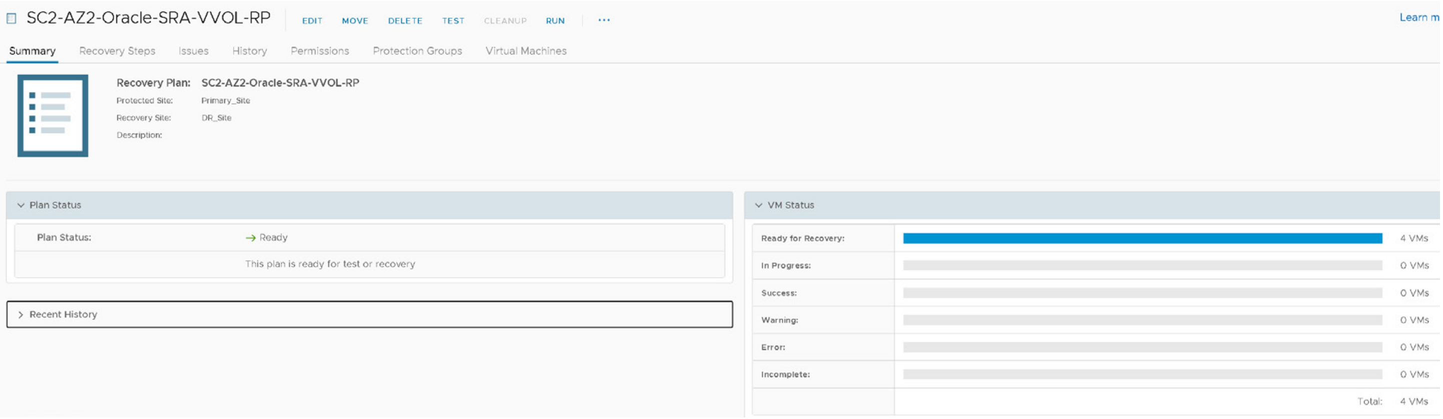
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
New protected site	Primary_Site
New recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 317. Run Reprotect on Site A

Reprotection of Protected Site A vVOL VMs successful.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready

This plan is ready for test or recovery

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

FIGURE 318. Reprotect on Site A Successful

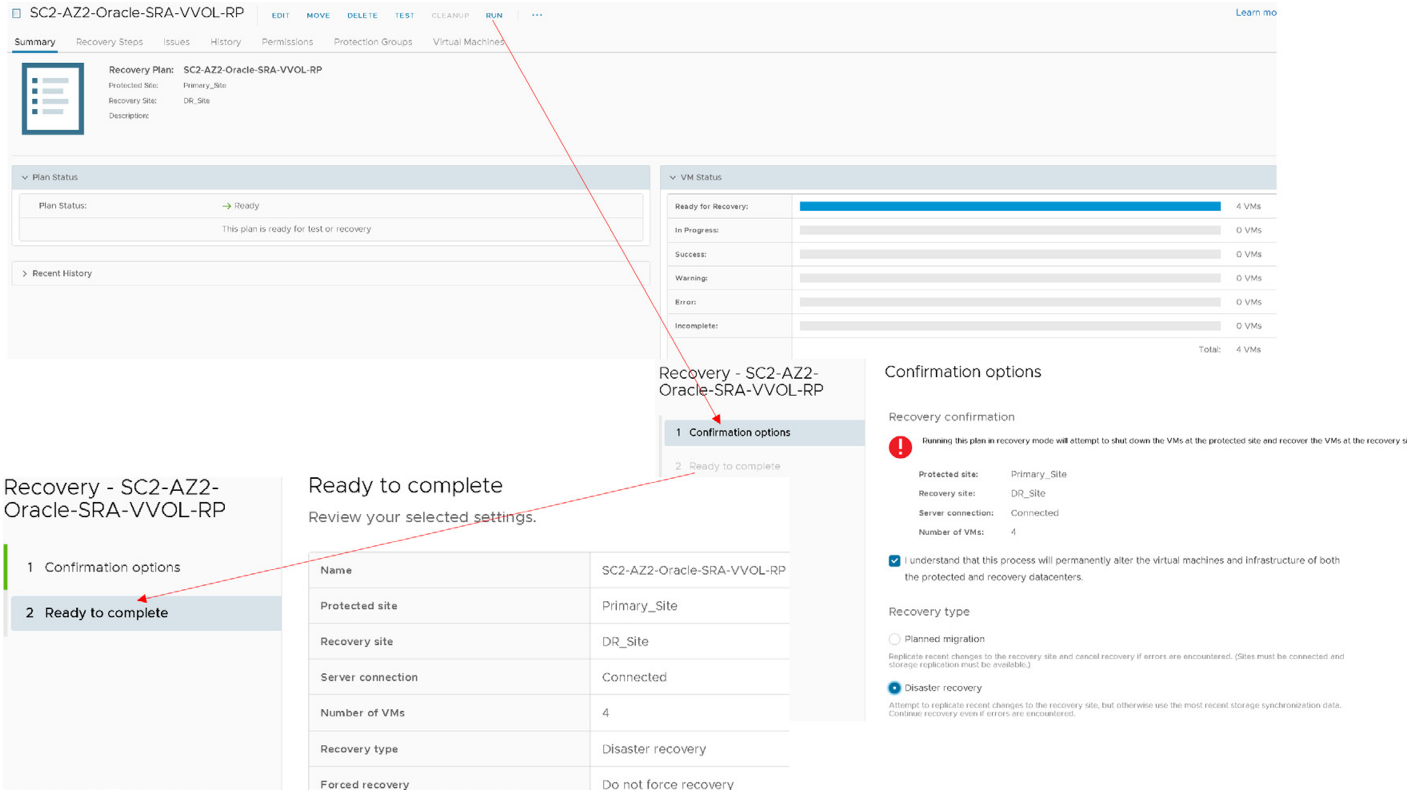
As mentioned above, the steps to run a planned migration of a recovery plan for vVOLs are the same in the case of a storage LUN.

More information on running a planned migration of a recovery plan with vVOL can be found in the *Performing a Planned Migration or Disaster Recovery By Running a Recovery Plan* and SRM User Guide: Configuring Site Recovery Manager vVol-Based Storage Policy Discovery.

Run Recovery Plan for Disaster Recovery

The steps to run a disaster recovery of a recovery plan for vVOL are the same in the case of a storage LUN.

The steps to run a disaster recovery scenario of recovery plan **SC2-AZ2-Oracle-SRA-VVOL-RP** are as shown below:



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status

Plan Status: → Ready

This plan is ready for test or recovery

Recent History

VM Status

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery s

Protected site: Primary_Site
Recovery site: DR_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

○ Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

● Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

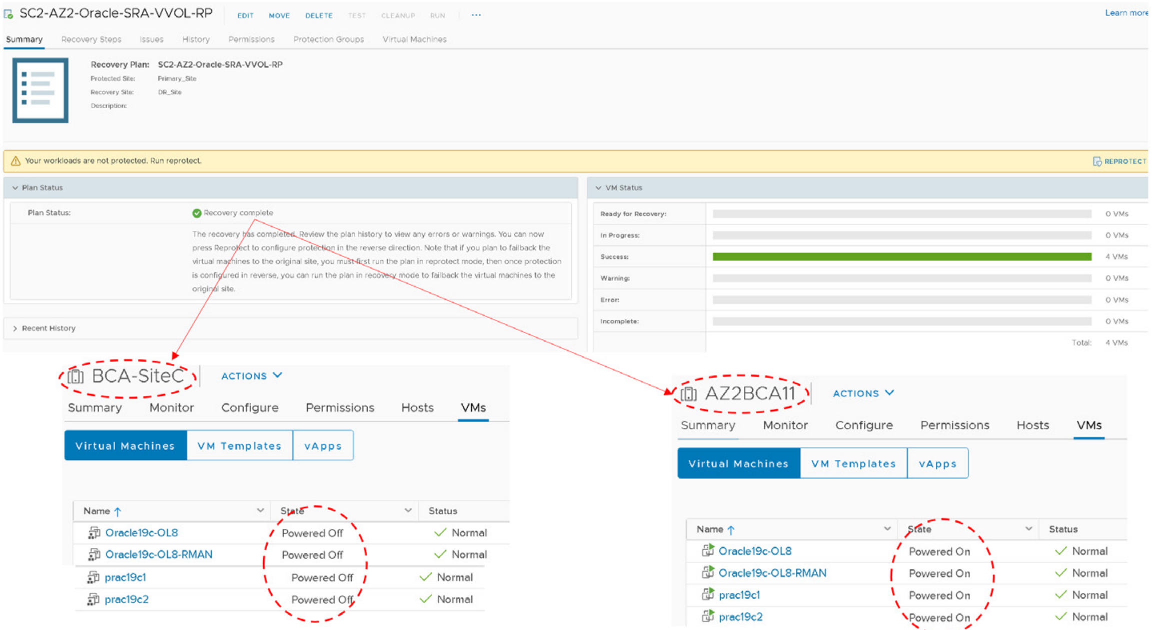
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected site	Primary_Site
Recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Recovery type	Disaster recovery
Forced recovery	Do not force recovery

FIGURE 319. Disaster Recovery of Recovery Plan SC2-AZ2-Oracle-SRA-VVOL-RP

Disaster recovery of recovery **plan SC2-AZ2-Oracle-SRA-VVOL-RP** is successful. Protected Site A vVOL VMs are powered off and Recovery Site B vVOL VMs are powered on.



SC2-AZ2-Oracle-SRA-VVOL-RP

Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

BCA-SiteC

Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal
prac19c1	Powered Off	✓ Normal
prac19c2	Powered Off	✓ Normal

AZ2BCA11

Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

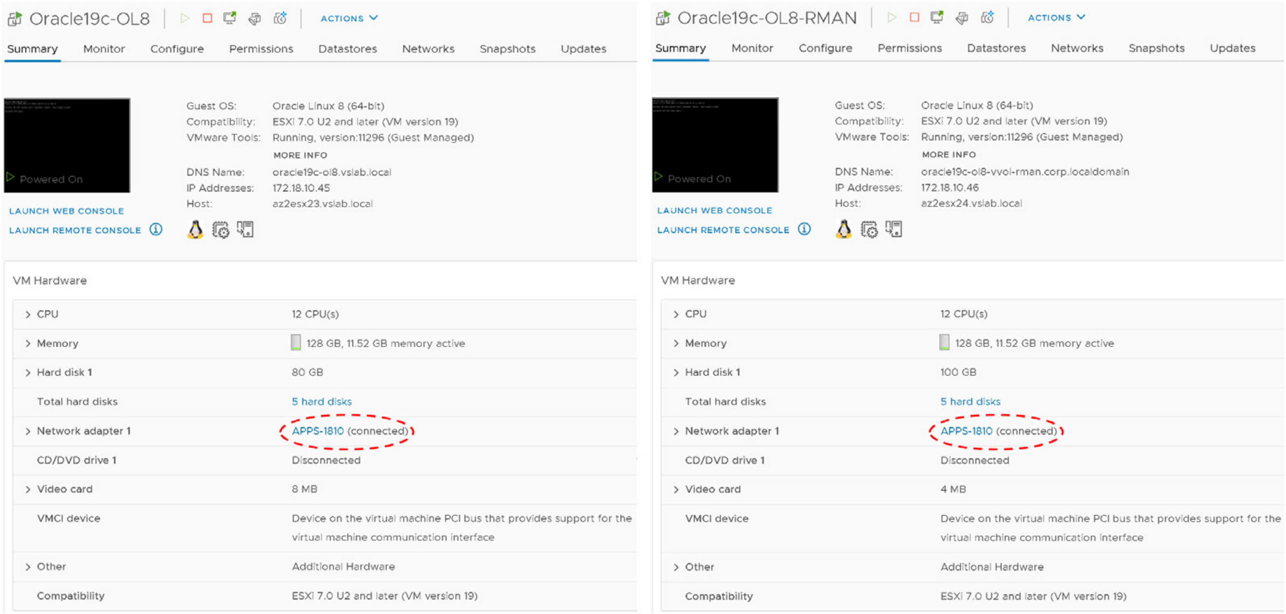
FIGURE 320. Disaster Recovery of Recovery Plan SC2-AZ2-Oracle-SRA-VVOL-RP Successful

Recovery Site B vVOL Oracle VM **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined per network mappings to recovery network **APPS-1810**.

As with testing the recovery plan, the Oracle VM **Oracle19c-OL8** is up with IP address 172.18.10.45 and the database **vvol19c** is up. The alert log for the database shows no errors. Oracle crash recovery is performed when the database starts up, which is normal and expected.

The Oracle VM **Oracle19c-OL8-RMAN** is up with IP address 172.18.10.46 and the database **rmandb** is up. The alert log for the database **rmandb** shows no errors. Oracle crash recovery is performed when the database **rmandb** starts up, which is normal and expected.

The storage vVOL-based snapshot is crash-consistent and write-ordering is preserved for each file within a snapshot.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.18.10.45
Host: az2esx23.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

Oracle19c-OL8-RMAN

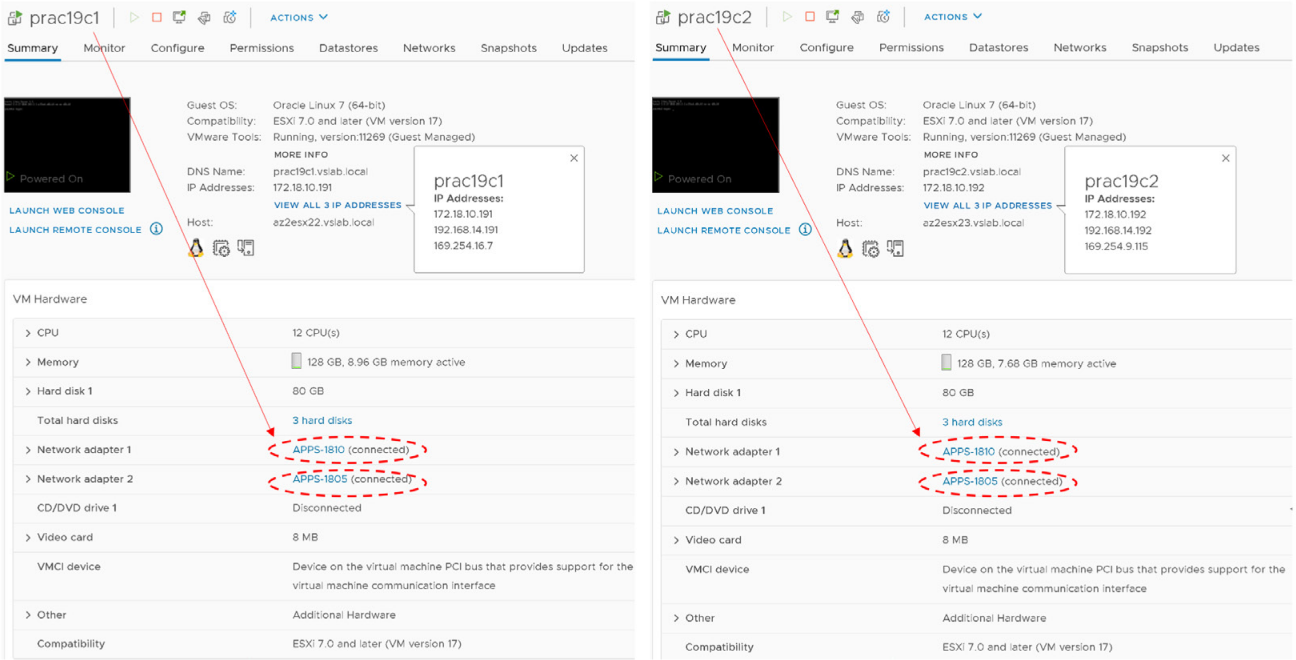
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.18.10.46
Host: az2esx24.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 11.52 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1810 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 321. Recovery Site Oracle VMs Oracle19c-OL8 and Oracle19c-OL8-RMAN Status

Recovery Site B vVOL Oracle RAC **prac19c** is powered on with the public IP addressing scheme set per the network mappings to recovery network **APPS-1810**, and the private IP addressing scheme set per the network mappings to recovery network **APPS-1805**.



prac19c1

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c1.vslab.local
IP Addresses: 172.18.10.191
Host: az2esx22.vslab.local

prac19c1
IP Addresses:
172.18.10.191
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 8.96 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

prac19c2

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: prac19c2.vslab.local
IP Addresses: 172.18.10.192
Host: az2esx23.vslab.local

prac19c2
IP Addresses:
172.18.10.192
192.168.14.192
169.254.9.115

VM Hardware

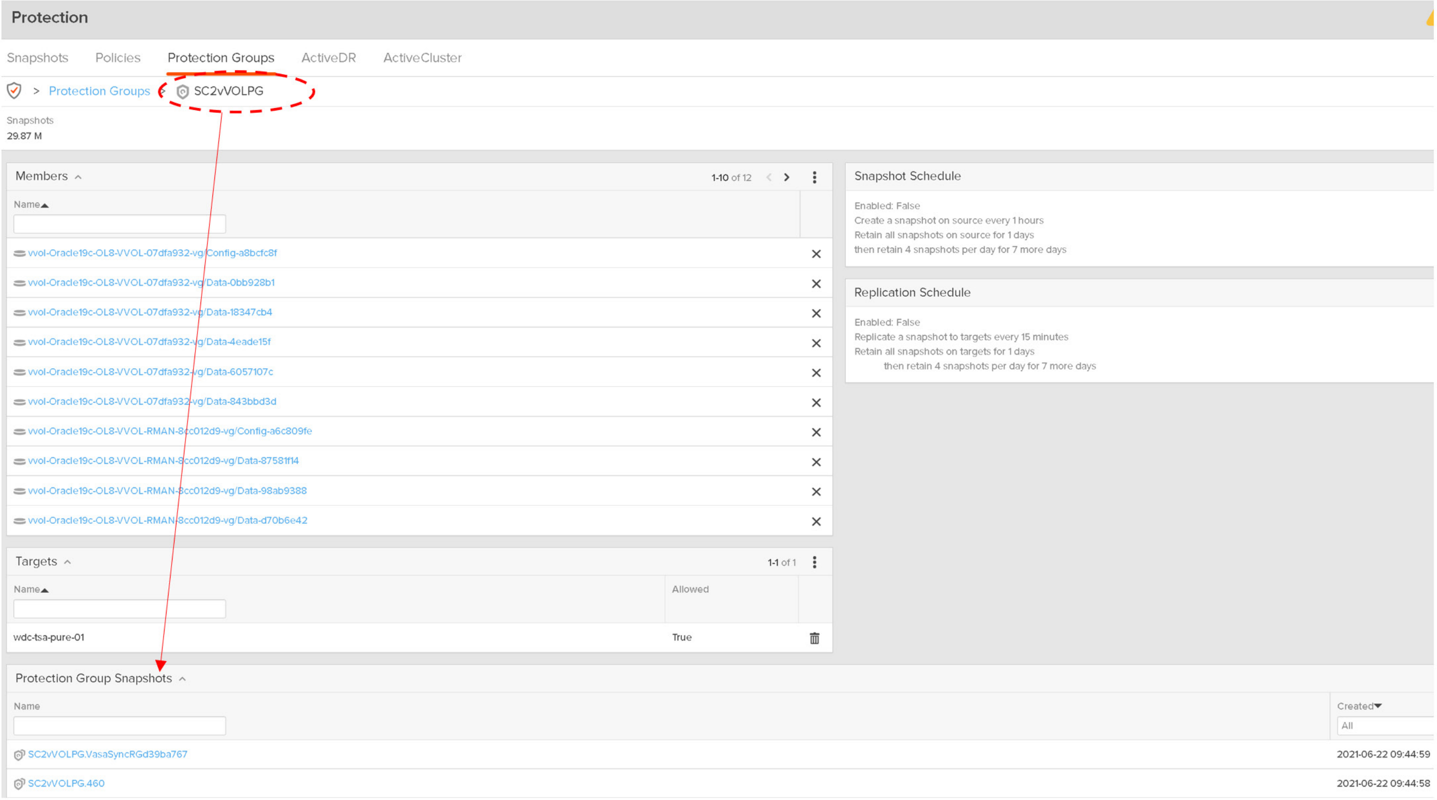
CPU	12 CPU(s)
Memory	128 GB, 7.68 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1810 (connected)
Network adapter 2	APPS-1805 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 322. Recovery Site Oracle RAC prac19c VMs Status

As part of running a disaster recovery of the recovery plan, the network Interfaces of the Oracle RAC **prac19c** will be changed to the appropriate recovery network as defined in the network mappings.

- The VIP and the SCAN IPs have to be changed to the test /recovery network IP scheme in order for the RAC Clusterware to bring up the RAC services.
- The steps to change the RAC VIP IP address can be found in *Oracle 19c Clusterware Administration and Deployment Guide*. The steps to change the Oracle private interconnect IP address can be found in the *Changing Oracle Clusterware Private Network Configuration*.
- The steps to change the RAC SCAN IP addresses can be found in the *My Oracle Support Note How to Update the IP Address of the SCAN VIP Resources (ora.scan{n}.vip) (Doc ID 952903.1)*.
- The steps to change the RAC VIP, scan and private interconnect IP addresses are beyond the scope of this paper.

In event of real disaster, Site A may not be available. As this use case is a DR exercise, Site A is available in this case. Site A has Pure Storage protection group **SC2vVOLPG** with the original VM vVOLs.



Snapshots
29.87 M

Members 1-10 of 12

Name	
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Config-a8bcfc8f	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-0bb928b1	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-18347cb4	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-4eade15f	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-6057107c	✕
vvol-Oracle19c-OL8-VVOL-07dfa932-vg/Data-843bbd3d	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Config-a6c809fe	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Data-87581f14	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Data-98ab9388	✕
vvol-Oracle19c-OL8-VVOL-RMAN-8cc012d9-vg/Data-d70b6e42	✕

Snapshot Schedule

Enabled: False
Create a snapshot on source every 1 hours
Retain all snapshots on source for 1 days
then retain 4 snapshots per day for 7 more days

Replication Schedule

Enabled: False
Replicate a snapshot to targets every 15 minutes
Retain all snapshots on targets for 1 days
then retain 4 snapshots per day for 7 more days

Targets 1-1 of 1

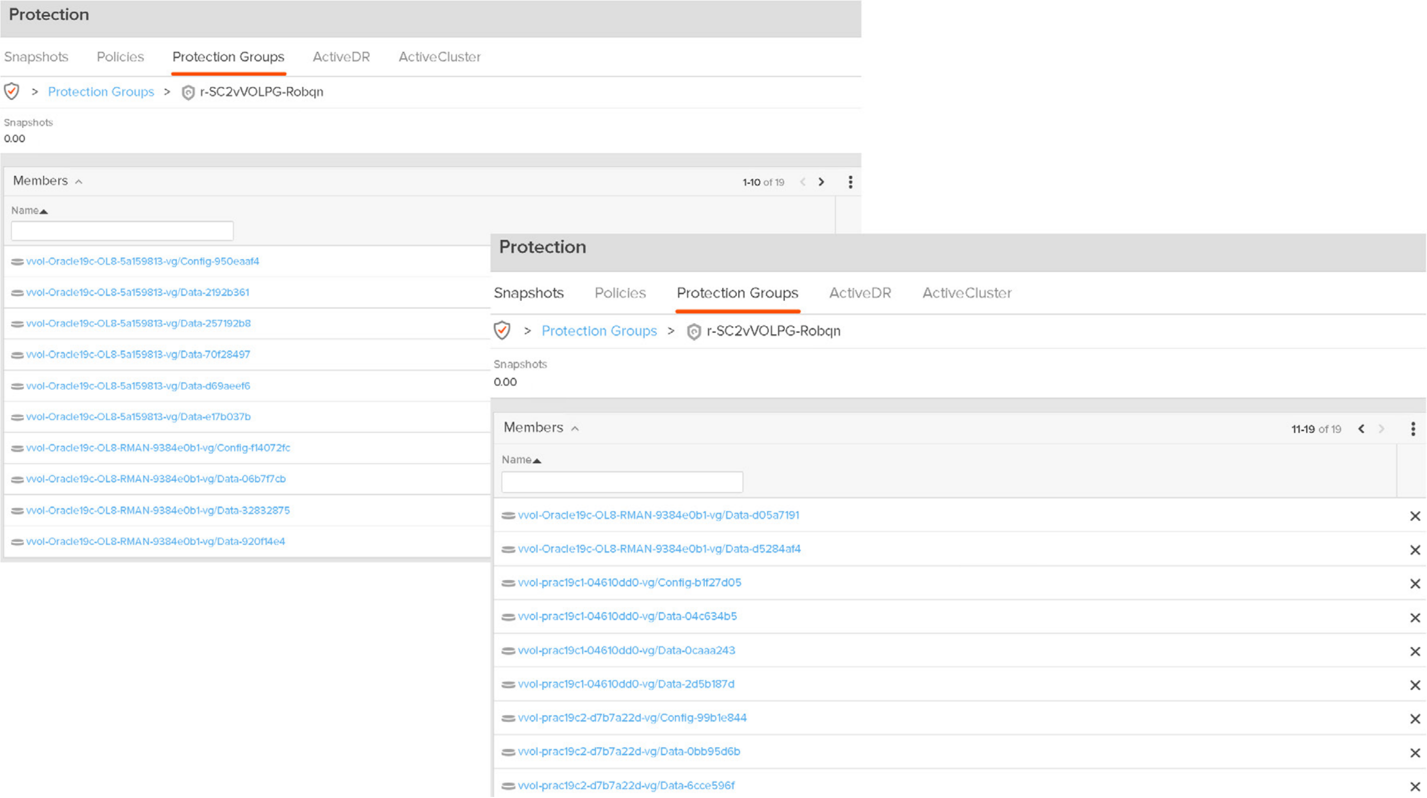
Name	Allowed
wdc-tsa-pure-01	True

Protection Group Snapshots

Name	Created
SC2vVOLPG.VasaSyncRGd39ba767	2021-06-22 09:44:59
SC2vVOLPG.460	2021-06-22 09:44:58

FIGURE 323. Site A Protection Group with VMs

Site B has Pure Storage protection group **r-SC2vVOLPG-Robqn** with the failed-over VM vVOLs.

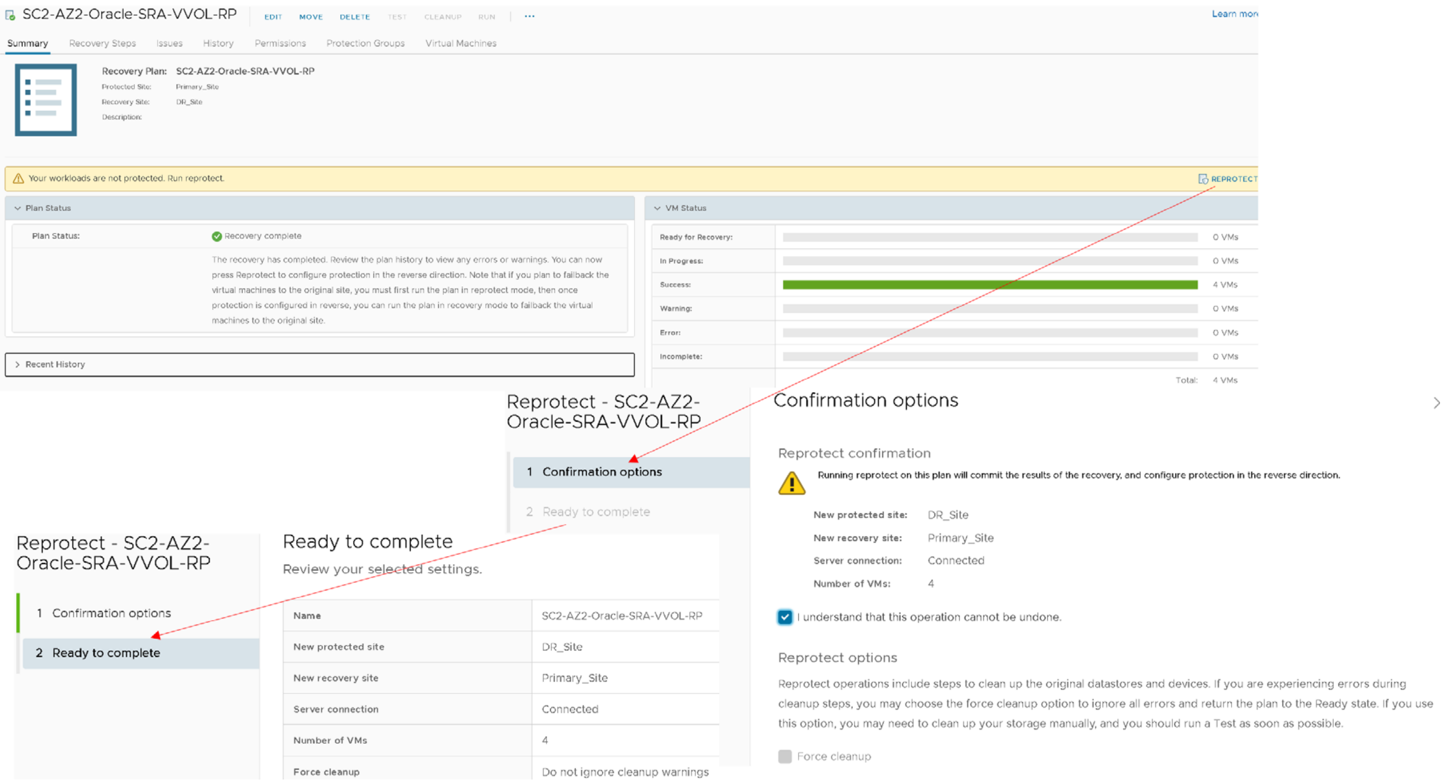


vvol-Oracle19c-OL8-5a159813-vg/Config-950eaaf4
vvol-Oracle19c-OL8-5a159813-vg/Data-2192b361
vvol-Oracle19c-OL8-5a159813-vg/Data-257192b8
vvol-Oracle19c-OL8-5a159813-vg/Data-70f28497
vvol-Oracle19c-OL8-5a159813-vg/Data-d69aeef6
vvol-Oracle19c-OL8-5a159813-vg/Data-e17b037b
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Config-f14072fc
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-06b7f7cb
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-32832875
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-920f14e4

vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-d05a7191
vvol-Oracle19c-OL8-RMAN-9384e0b1-vg/Data-d5284af4
vvol-prac19c1-04610dd0-vg/Config-b1f27d05
vvol-prac19c1-04610dd0-vg/Data-04c634b5
vvol-prac19c1-04610dd0-vg/Data-0caaa243
vvol-prac19c1-04610dd0-vg/Data-2d5b187d
vvol-prac19c2-d7b7a22d-vg/Config-99b1e844
vvol-prac19c2-d7b7a22d-vg/Data-0bb95d6b
vvol-prac19c2-d7b7a22d-vg/Data-6cce596f

FIGURE 324. Site B Protection Group with Failed Over VMs

After the successful completion of the disaster recovery exercise, and ensuring that Site A is back operationally, run **Reprotect** to protect Site B, which is now the new protected site.



Recovery Plan:	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site:	Primary_Site
Recovery Site:	DR_Site
Description:	

Your workloads are not protected. Run reprotect.

Plan Status

Plan Status: ✓ Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

VM Status

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site:	DR_Site
New recovery site:	Primary_Site
Server connection:	Connected
Number of VMs:	4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

☐ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

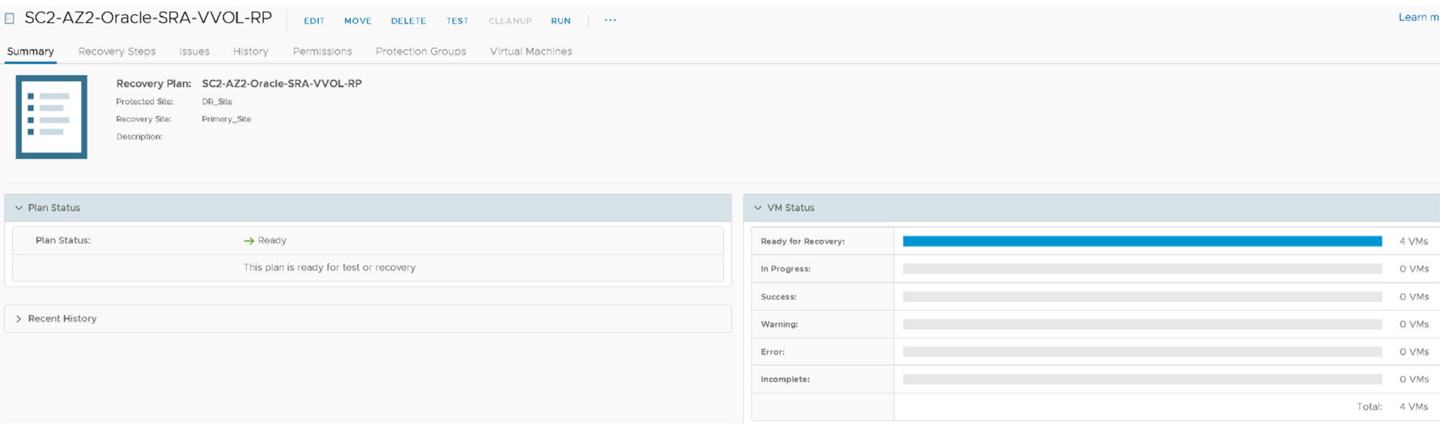
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
New protected site	DR_Site
New recovery site	Primary_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 325. Reprotect Site B VMs

The reprotect step to protect the Site B is successful.



Recovery Plan:	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site:	DR_Site
Recovery Site:	Primary_Site
Description:	

Plan Status

Plan Status: → Ready

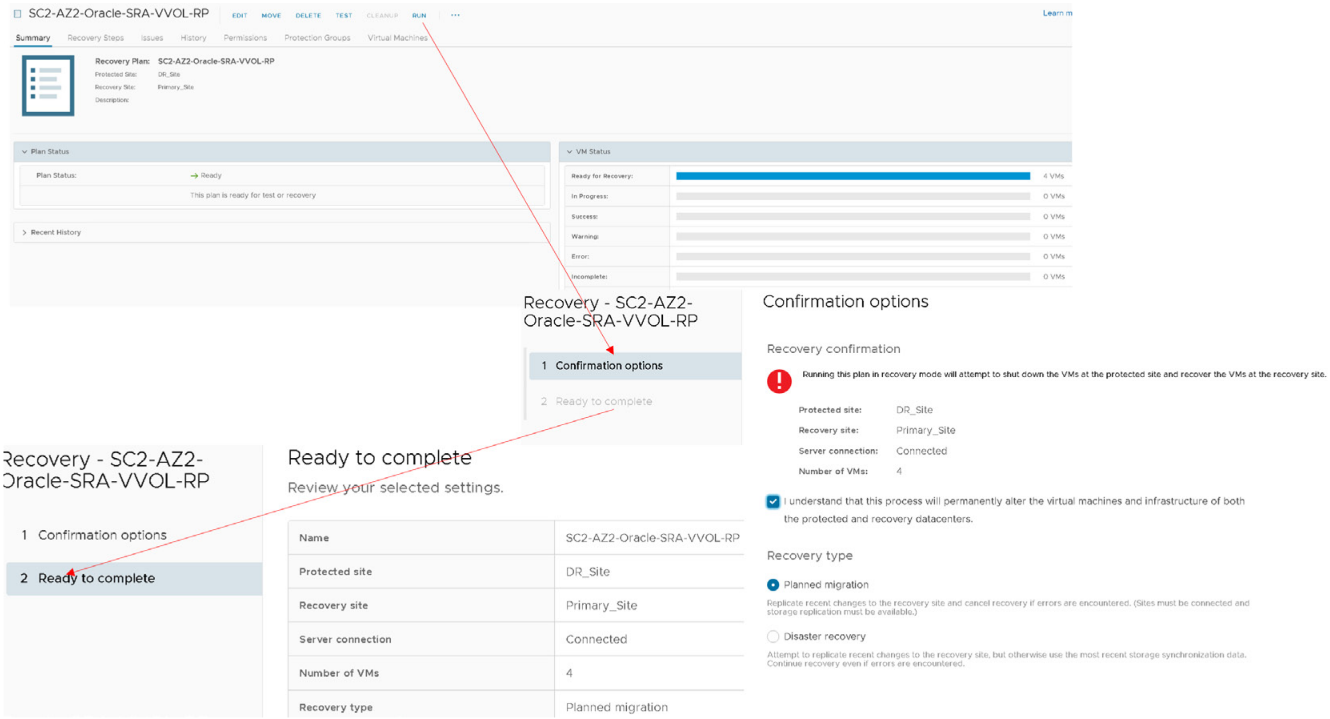
This plan is ready for test or recovery

VM Status

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

FIGURE 326. Reprotect Site B VMs Successful

Run a planned migration to switch the protected site from Site B back to Site A.



SC2-AZ2-Oracle-SRA-VVOL-RP

Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Plan Status

Plan Status: → Ready
This plan is ready for test or recovery

Recent History

VM Status

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs

Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Recovery confirmation

Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

Protected site: DR_Site
Recovery site: Primary_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

Recovery type

● Planned migration

Replicate recent changes to the recovery site and cancel recovery if errors are encountered. (Sites must be connected and storage replication must be available.)

○ Disaster recovery

Attempt to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. Continue recovery even if errors are encountered.

Recovery - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

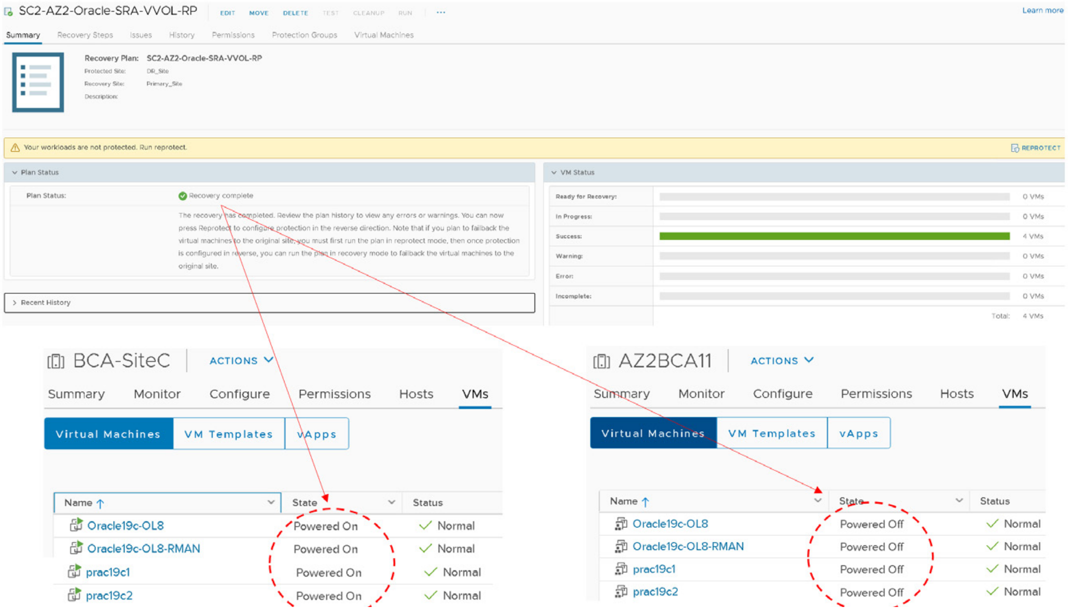
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
Protected site	DR_Site
Recovery site	Primary_Site
Server connection	Connected
Number of VMs	4
Recovery type	Planned migration

FIGURE 327. Planned Migration from Site B to Site A

Planned migration from Site B to Site A is successful. VMs on Protected Site A vVOL datastore **OraVVOL** are powered back on and we see the VMs on Recovery Site B are powered off.



SC2-AZ2-Oracle-SRA-VVOL-RP

Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

⚠ Your workloads are not protected. Run reprotect.

Plan Status

Plan Status: ✓ Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Recent History

VM Status

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

BCA-SiteC

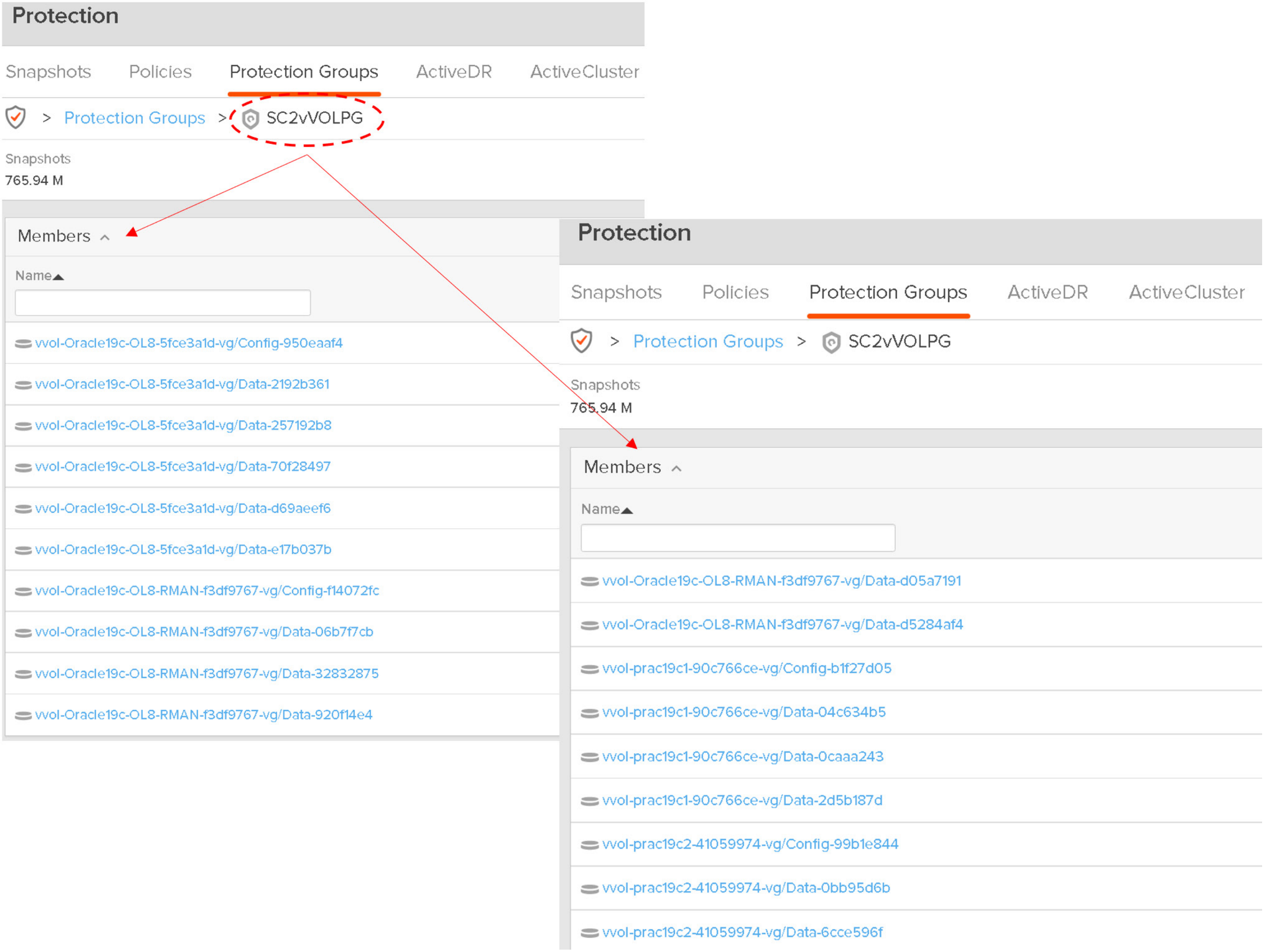
Name ↑	State	Status
Oracle19c-OL8	Powered On	✓ Normal
Oracle19c-OL8-RMAN	Powered On	✓ Normal
prac19c1	Powered On	✓ Normal
prac19c2	Powered On	✓ Normal

AZ2BCA11

Name ↑	State	Status
Oracle19c-OL8	Powered Off	✓ Normal
Oracle19c-OL8-RMAN	Powered Off	✓ Normal
prac19c1	Powered Off	✓ Normal
prac19c2	Powered Off	✓ Normal

FIGURE 328. Site A and Site B VM Status

Protected Site A protection group **SC2vVOLPG**:



Snapshots
765.94 M

Members

- vvol-Oracle19c-OL8-5fce3a1d-vg/Config-950eaaf4
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-2192b361
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-257192b8
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-70f28497
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-d69aeef6
- vvol-Oracle19c-OL8-5fce3a1d-vg/Data-e17b037b
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Config-f14072fc
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-06b7f7cb
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-32832875
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-920f14e4

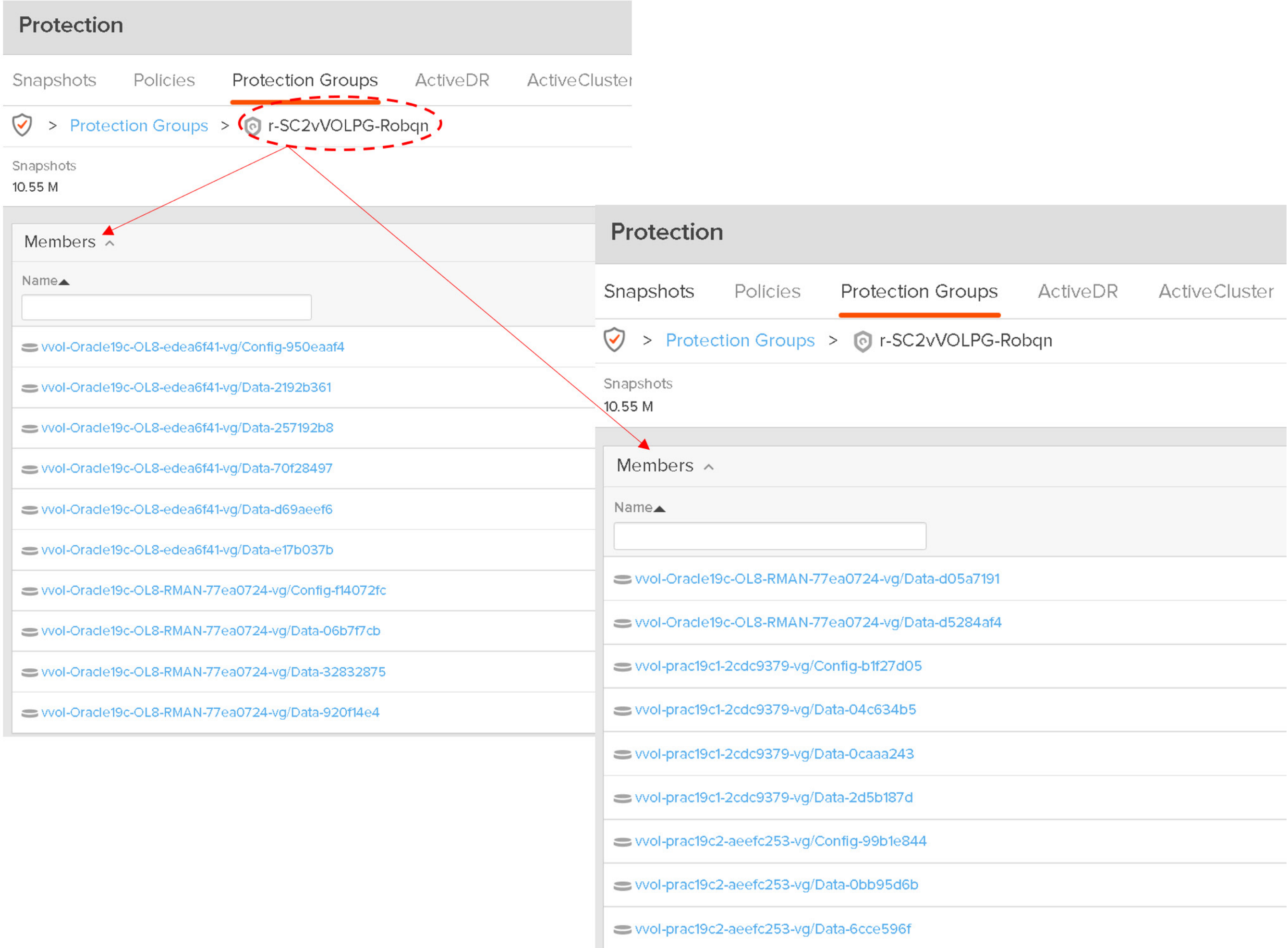
Snapshots
765.94 M

Members

- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d05a7191
- vvol-Oracle19c-OL8-RMAN-f3df9767-vg/Data-d5284af4
- vvol-prac19c1-90c766ce-vg/Config-b1f27d05
- vvol-prac19c1-90c766ce-vg/Data-04c634b5
- vvol-prac19c1-90c766ce-vg/Data-0caaa243
- vvol-prac19c1-90c766ce-vg/Data-2d5b187d
- vvol-prac19c2-41059974-vg/Config-99b1e844
- vvol-prac19c2-41059974-vg/Data-0bb95d6b
- vvol-prac19c2-41059974-vg/Data-6cce596f

FIGURE 329. Site A Protection Group

Recovery Site B protection group **r-SC2vVOLPG-Robqn**:



Snapshots
10.55 M

Members

- vvol-Oracle19c-OL8-edea6f41-vg/Config-950eaaf4
- vvol-Oracle19c-OL8-edea6f41-vg/Data-2192b361
- vvol-Oracle19c-OL8-edea6f41-vg/Data-257192b8
- vvol-Oracle19c-OL8-edea6f41-vg/Data-70f28497
- vvol-Oracle19c-OL8-edea6f41-vg/Data-d69aeef6
- vvol-Oracle19c-OL8-edea6f41-vg/Data-e17b037b
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Config-f14072fc
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-06b7f7cb
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-32832875
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-920f14e4

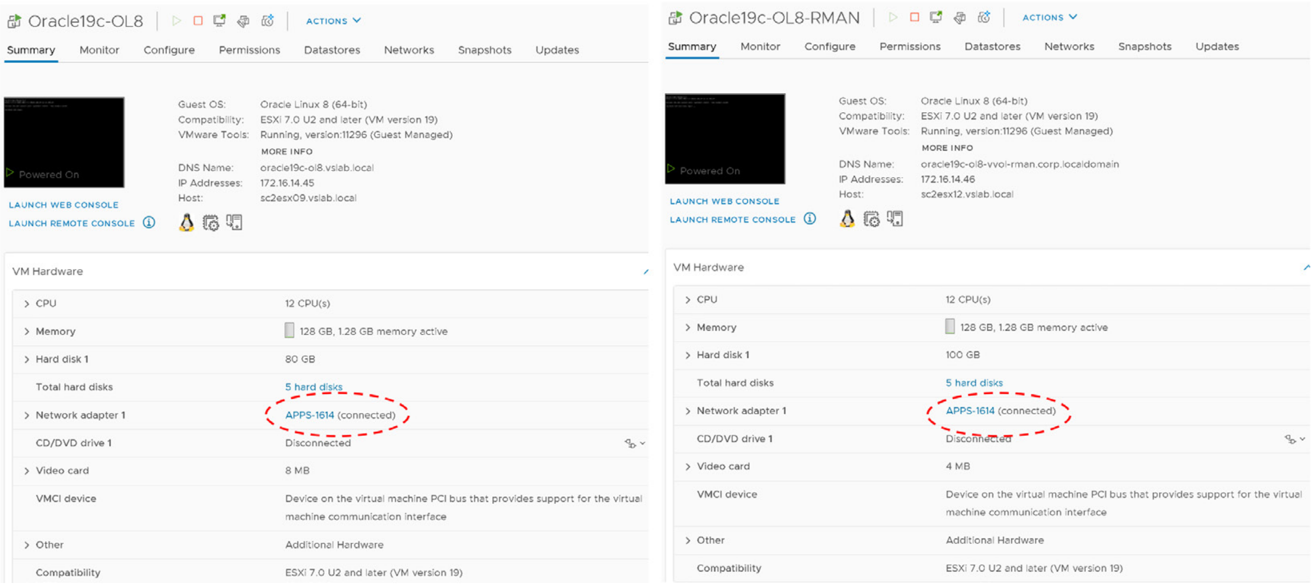
Snapshots
10.55 M

Members

- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-d05a7191
- vvol-Oracle19c-OL8-RMAN-77ea0724-vg/Data-d5284af4
- vvol-prac19c1-2cdc9379-vg/Config-b1f27d05
- vvol-prac19c1-2cdc9379-vg/Data-04c634b5
- vvol-prac19c1-2cdc9379-vg/Data-0caaa243
- vvol-prac19c1-2cdc9379-vg/Data-2d5b187d
- vvol-prac19c2-aeefc253-vg/Config-99b1e844
- vvol-prac19c2-aeefc253-vg/Data-0bb95d6b
- vvol-prac19c2-aeefc253-vg/Data-6cce596f

FIGURE 330. Site B Protection Group

Site A vVOL Oracle VMs **Oracle19c-OL8** and **Oracle19c-OL8-RMAN** are powered on with the IP addressing scheme defined per network mappings to primary network **APPS-1614**.



Oracle19c-OL8

Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8.vslab.local
IP Addresses: 172.16.14.45
Host: sc2esx09.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	80 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

Oracle19c-OL8-RMAN

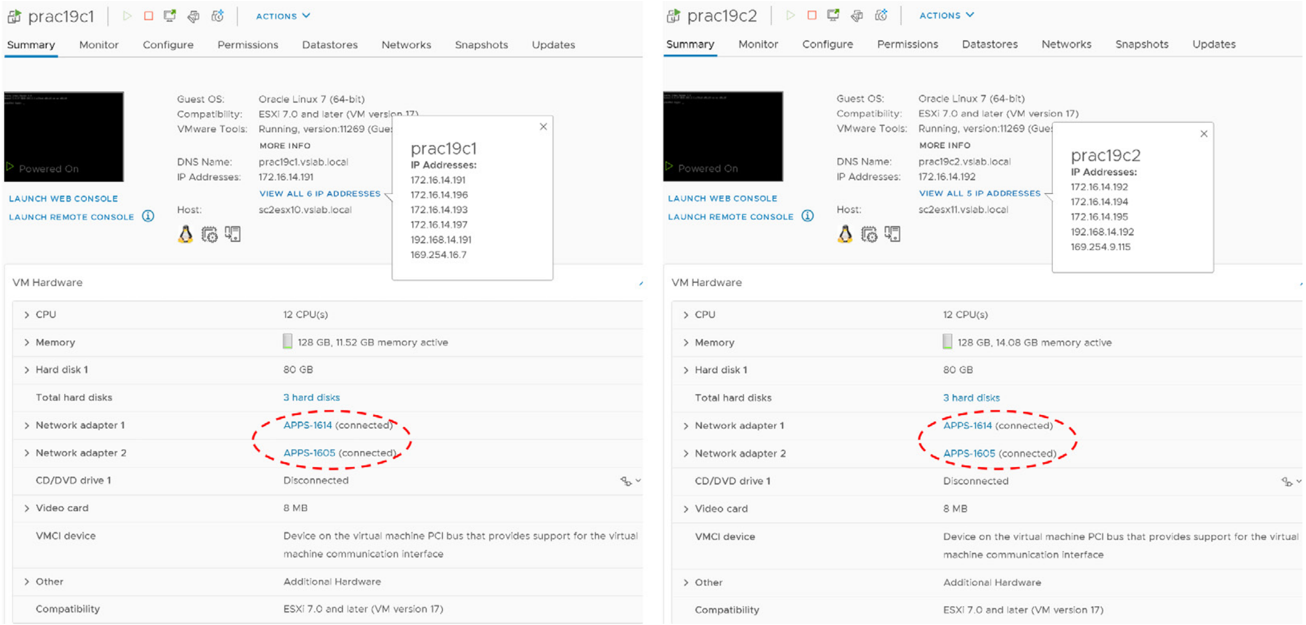
Guest OS: Oracle Linux 8 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:11296 (Guest Managed)
DNS Name: oracle19c-ol8-vvol-rman.corp.localdomain
IP Addresses: 172.16.14.46
Host: sc2esx12.vslab.local

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 1.28 GB memory active
Hard disk 1	100 GB
Total hard disks	5 hard disks
Network adapter 1	APPS-1614 (connected)
CD/DVD drive 1	Disconnected
Video card	4 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

FIGURE 331. Site A Oracle VMs Oracle19c-OL8 and Oracle19c-OL8-RMAN

Site A vVOL Oracle RAC **prac19c** is powered on with the public IP addressing scheme set per network mappings to primary network **APPS-1614** and the private IP addressing scheme set per network mappings to primary network **APPS-1605**.



prac19c1

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Gue
DNS Name: prac19c1.vslab.local
IP Addresses: 172.16.14.191
Host: sc2esx10.vslab.local

prac19c1
IP Addresses:
172.16.14.191
172.16.14.196
172.16.14.193
172.16.14.197
192.168.14.191
169.254.16.7

VM Hardware

CPU	12 CPU(s)
Memory	128 GB, 11.52 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

prac19c2

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 and later (VM version 17)
VMware Tools: Running, version:11269 (Gue
DNS Name: prac19c2.vslab.local
IP Addresses: 172.16.14.192
Host: sc2esx11.vslab.local

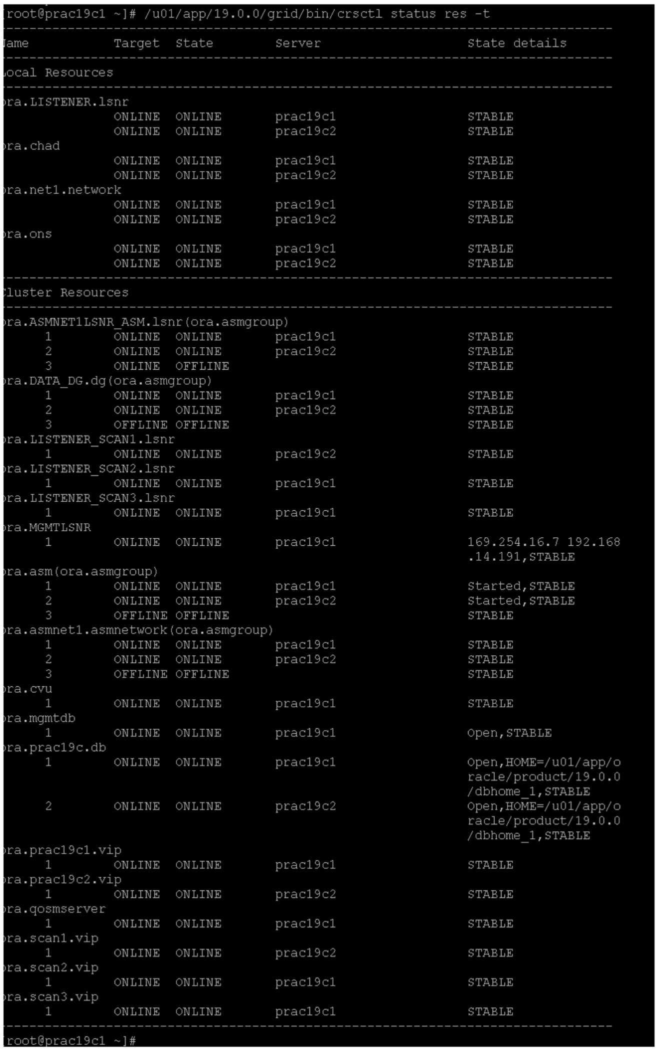
prac19c2
IP Addresses:
172.16.14.192
172.16.14.194
172.16.14.195
192.168.14.192
169.254.9.115

VM Hardware

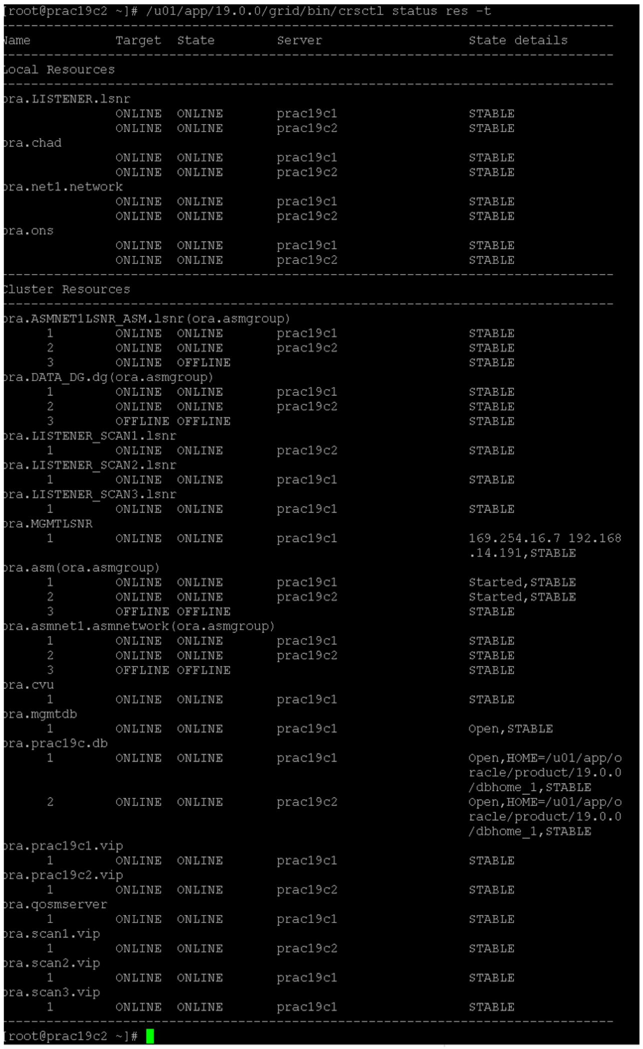
CPU	12 CPU(s)
Memory	128 GB, 14.08 GB memory active
Hard disk 1	80 GB
Total hard disks	3 hard disks
Network adapter 1	APPS-1614 (connected)
Network adapter 2	APPS-1605 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 and later (VM version 17)

FIGURE 332. Site A Oracle RAC prac19c VMs

All Oracle RAC **prac19c** cluster services are up.



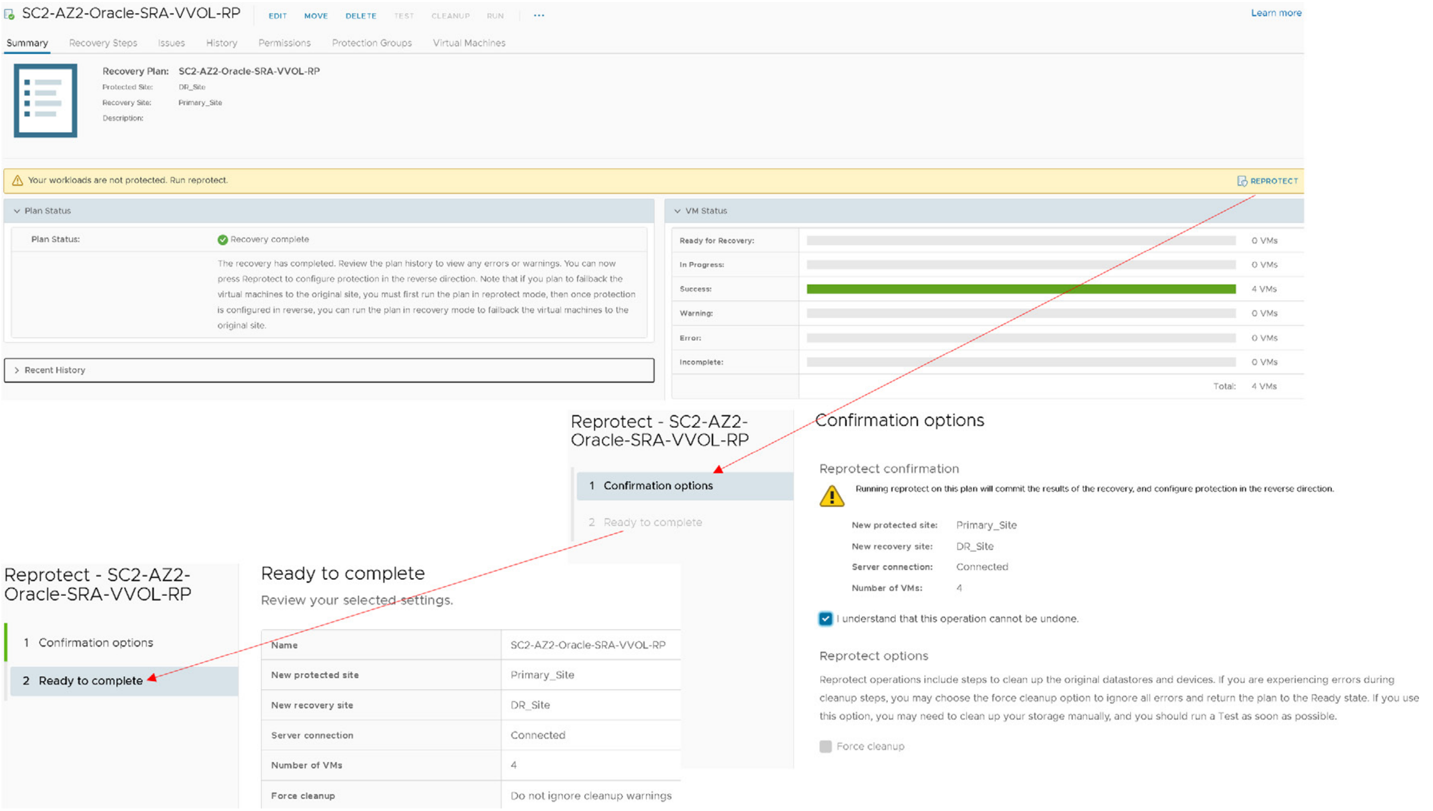
```
[root@prac19c1 ~]# /u01/app/19.0.0/grid/bin/crsctl status res -t
-------------------------------------------------------------------------------
ame           Target  State        Server                   State details
-------------------------------------------------------------------------------
ocal Resources
-------------------------------------------------------------------------------
ra.LISTENER.lsnr
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
ra.chad
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
ra.net1.network
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
ra.ons
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
-------------------------------------------------------------------------------
luster Resources
-------------------------------------------------------------------------------
ra.ASMNET1LSNR_ASM.lsnr(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 STABLE
     2        ONLINE  ONLINE       prac19c2                 STABLE
     3        ONLINE  OFFLINE                               STABLE
ra.DATA_DG.dg(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 STABLE
     2        ONLINE  ONLINE       prac19c2                 STABLE
     3        OFFLINE OFFLINE                               STABLE
ra.LISTENER_SCAN1.lsnr
     1        ONLINE  ONLINE       prac19c2                 STABLE
ra.LISTENER_SCAN2.lsnr
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.LISTENER_SCAN3.lsnr
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.MGMTLSNR
     1        ONLINE  ONLINE       prac19c1                 169.254.16.7 192.168
                                                            .14.191,STABLE
ra.asm(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 Started,STABLE
     2        ONLINE  ONLINE       prac19c2                 Started,STABLE
     3        OFFLINE OFFLINE                               STABLE
ra.asmnet1.asmnetwork(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 STABLE
     2        ONLINE  ONLINE       prac19c2                 STABLE
     3        OFFLINE OFFLINE                               STABLE
ra.cvu
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.mgmtdb
     1        ONLINE  ONLINE       prac19c1                 Open,STABLE
ra.prac19c.db
     1        ONLINE  ONLINE       prac19c1                 Open,HOME=/u01/app/o
                                                            racle/product/19.0.0
                                                            /dbhome_1,STABLE
     2        ONLINE  ONLINE       prac19c2                 Open,HOME=/u01/app/o
                                                            racle/product/19.0.0
                                                            /dbhome_1,STABLE
ra.prac19c1.vip
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.prac19c2.vip
     1        ONLINE  ONLINE       prac19c2                 STABLE
ra.qosmserver
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.scan1.vip
     1        ONLINE  ONLINE       prac19c2                 STABLE
ra.scan2.vip
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.scan3.vip
     1        ONLINE  ONLINE       prac19c1                 STABLE
-------------------------------------------------------------------------------
[root@prac19c1 ~]#
```



```
[root@prac19c2 ~]# /u01/app/19.0.0/grid/bin/crsctl status res -t
-------------------------------------------------------------------------------
ame           Target  State        Server                   State details
-------------------------------------------------------------------------------
ocal Resources
-------------------------------------------------------------------------------
ra.LISTENER.lsnr
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
ra.chad
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
ra.net1.network
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
ra.ons
              ONLINE  ONLINE       prac19c1                 STABLE
              ONLINE  ONLINE       prac19c2                 STABLE
-------------------------------------------------------------------------------
luster Resources
-------------------------------------------------------------------------------
ra.ASMNET1LSNR_ASM.lsnr(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 STABLE
     2        ONLINE  ONLINE       prac19c2                 STABLE
     3        ONLINE  OFFLINE                               STABLE
ra.DATA_DG.dg(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 STABLE
     2        ONLINE  ONLINE       prac19c2                 STABLE
     3        OFFLINE OFFLINE                               STABLE
ra.LISTENER_SCAN1.lsnr
     1        ONLINE  ONLINE       prac19c2                 STABLE
ra.LISTENER_SCAN2.lsnr
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.LISTENER_SCAN3.lsnr
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.MGMTLSNR
     1        ONLINE  ONLINE       prac19c1                 169.254.16.7 192.168
                                                            .14.191,STABLE
ra.asm(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 Started,STABLE
     2        ONLINE  ONLINE       prac19c2                 Started,STABLE
     3        OFFLINE OFFLINE                               STABLE
ra.asmnet1.asmnetwork(ora.asmgroup)
     1        ONLINE  ONLINE       prac19c1                 STABLE
     2        ONLINE  ONLINE       prac19c2                 STABLE
     3        OFFLINE OFFLINE                               STABLE
ra.cvu
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.mgmtdb
     1        ONLINE  ONLINE       prac19c1                 Open,STABLE
ra.prac19c.db
     1        ONLINE  ONLINE       prac19c1                 Open,HOME=/u01/app/o
                                                            racle/product/19.0.0
                                                            /dbhome_1,STABLE
     2        ONLINE  ONLINE       prac19c2                 Open,HOME=/u01/app/o
                                                            racle/product/19.0.0
                                                            /dbhome_1,STABLE
ra.prac19c1.vip
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.prac19c2.vip
     1        ONLINE  ONLINE       prac19c2                 STABLE
ra.qosmserver
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.scan1.vip
     1        ONLINE  ONLINE       prac19c2                 STABLE
ra.scan2.vip
     1        ONLINE  ONLINE       prac19c1                 STABLE
ra.scan3.vip
     1        ONLINE  ONLINE       prac19c1                 STABLE
-------------------------------------------------------------------------------
[root@prac19c2 ~]#
```

FIGURE 333. Site A Oracle RAC prac19c Cluster Services

Run **Reprotect** to reprotect the VMs on Protected Site A.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: DR_Site
Recovery Site: Primary_Site
Description:

Your workloads are not protected. Run reprotect.

Plan Status: Recovery complete

The recovery has completed. Review the plan history to view any errors or warnings. You can now press Reprotect to configure protection in the reverse direction. Note that if you plan to failback the virtual machines to the original site, you must first run the plan in reprotect mode, then once protection is configured in reverse, you can run the plan in recovery mode to failback the virtual machines to the original site.

Ready for Recovery:	0 VMs
In Progress:	0 VMs
Success:	4 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

Confirmation options

Reprotect confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New protected site: Primary_Site
New recovery site: DR_Site
Server connection: Connected
Number of VMs: 4

☑ I understand that this operation cannot be undone.

Reprotect options

Reprotect operations include steps to clean up the original datastores and devices. If you are experiencing errors during cleanup steps, you may choose the force cleanup option to ignore all errors and return the plan to the Ready state. If you use this option, you may need to clean up your storage manually, and you should run a Test as soon as possible.

□ Force cleanup

Reprotect - SC2-AZ2-Oracle-SRA-VVOL-RP

1 Confirmation options

2 Ready to complete

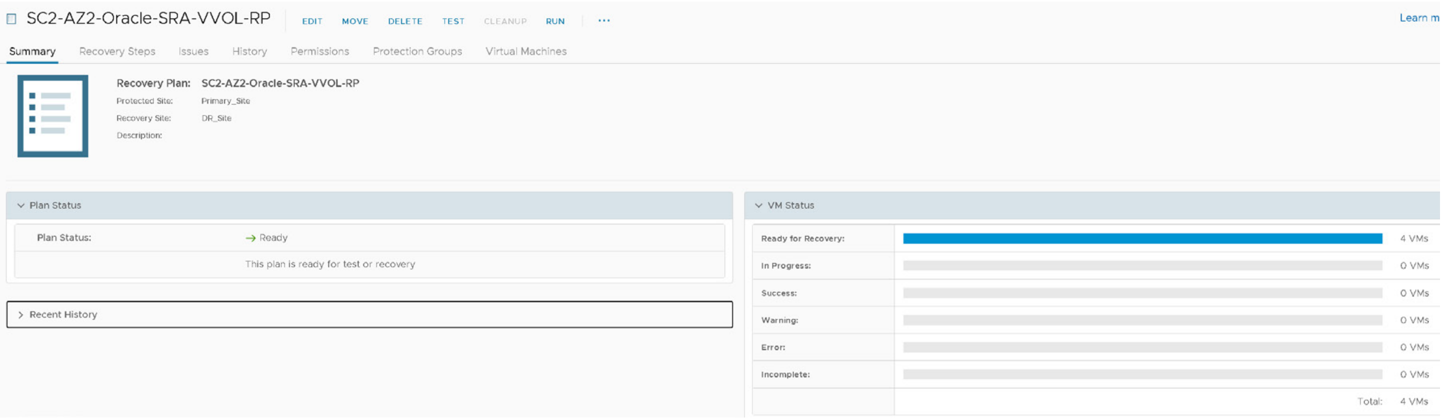
Ready to complete

Review your selected settings.

Name	SC2-AZ2-Oracle-SRA-VVOL-RP
New protected site	Primary_Site
New recovery site	DR_Site
Server connection	Connected
Number of VMs	4
Force cleanup	Do not ignore cleanup warnings

FIGURE 334. Reprotect Site A VMs

Reprotection of Protected Site A vVOL VMs successful.



Recovery Plan: SC2-AZ2-Oracle-SRA-VVOL-RP
Protected Site: Primary_Site
Recovery Site: DR_Site
Description:

Plan Status: → Ready

This plan is ready for test or recovery

Ready for Recovery:	4 VMs
In Progress:	0 VMs
Success:	0 VMs
Warning:	0 VMs
Error:	0 VMs
Incomplete:	0 VMs
Total:	4 VMs

FIGURE 335. Reprotect Site A VMs Successful

More information regarding running a disaster recovery of a recovery plan with vVOL can be found in the Performing a Planned Migration or Disaster Recovery By Running a Recovery Plan and *SRM User Guide: Configuring Site Recovery Manager vVol-Based Storage Policy Discovery*.

Conclusion

Customers have successfully run their business-critical Oracle workloads with high performance demands on VMware vSphere for many years. Virtualization of mission-critical databases adds layers of complexity to the infrastructure, however, making common operations like backup and recovery, cloning, disaster recovery and other day-to-day activities difficult. The most efficient storage operations for mission-critical databases are offloaded to the storage array.

Concerns that often delay virtualization of business-critical database workloads include:

- Rapid database growth and the need to reduce backup windows to meet performance and business SLAs.
- The size of modern databases makes it harder to regularly clone and refresh data from production to QA and other environments.
- Correct choice of business continuity plan to ensure rapid recovery from significant disruption to the operations
- Correct choice of disaster recovery technology to ensure business needs of RTO and RPO are met

A business continuity plan is a detailed strategy and set of systems for ensuring an organization's ability to prevent or rapidly recover from a significant disruption to its operations.

Disaster recovery is an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or even business disruptions related to the COVID-19 pandemic.

The VMware vSphere platform provides many tools for customers to successfully ensure business continuity and disaster recovery for their business-critical databases.

VMware Snapshot and VMware Clone are tools that help achieve point-in-time recovery.

VMware Site Recovery Manager, along with VMware vSphere Replication or array-based replication help protect VMs or entire LUN(s) from partial or complete site failures by replicating the VMs or entire LUN(s) between sites.

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.

VMware Site Recovery brings VMware enterprise-class SDDC disaster recovery-as-a-service to the AWS Cloud.

VMware Cloud Disaster Recovery is an on-demand disaster recovery service that provides an easy-to-use software-as-a-service (SaaS) solution and offers cloud economics to keep your disaster recovery costs under control.

This solution validates the business continuity and disaster recovery functionality of Oracle Single-Instance and Oracle RAC deployments using Pure x50 Storage (VMFS & vVOL) at all three below levels at on-premises and/or VMware clouds:

- Business Continuity
  - Application level
  - vSphere level
  - Storage level
- Disaster Recovery
  - Application level
  - vSphere level
  - Storage level

The choice of the business continuity or disaster recovery solution to adopt depends on application needs, SLAs, RTO, RPO and various other factors.

The above business continuity and disaster recovery methods can be summarized in the illustration below:

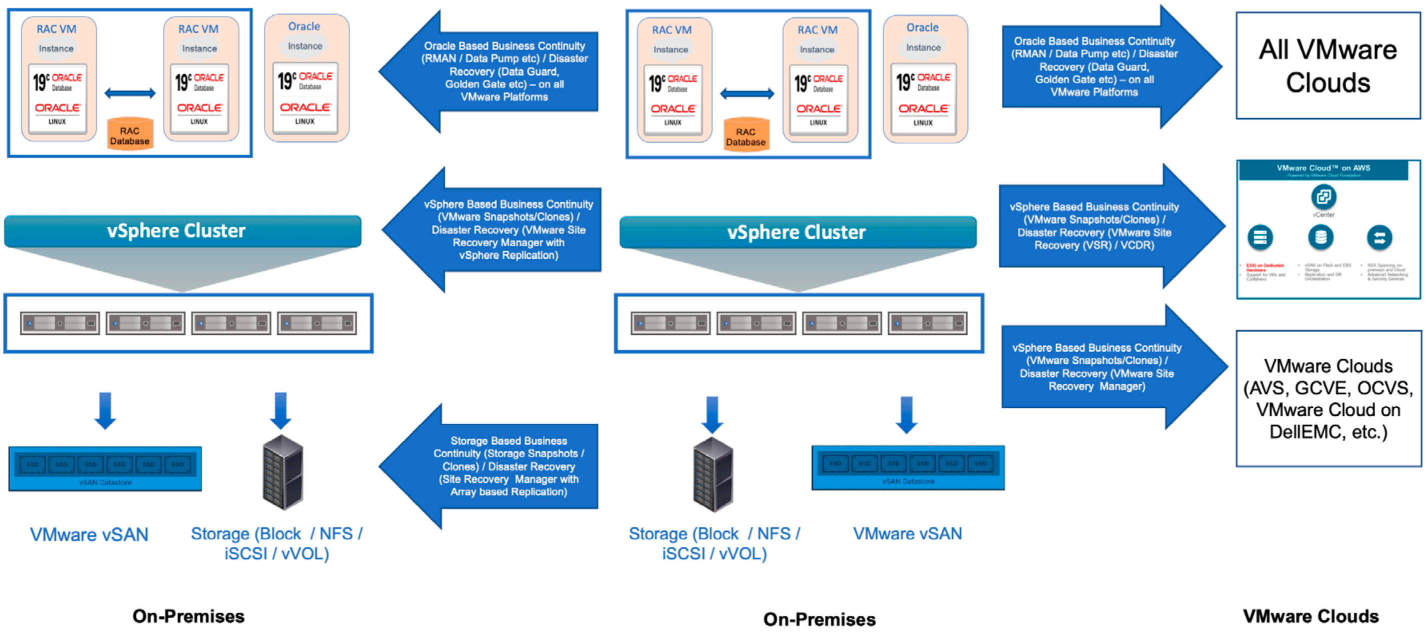

RAC VM
Instance
RAC VM
Instance
Oracle
Instance
19c ORACLE Database
ORACLE LINUX
RAC Database
Oracle Based Business Continuity (RMAN / Data Pump etc) / Disaster Recovery (Data Guard, Golden Gate etc) – on all VMware Platforms
vSphere Cluster
vSphere Based Business Continuity (VMware Snapshots/Clones) / Disaster Recovery (VMware Site Recovery Manager with vSphere Replication)
Storage Based Business Continuity (Storage Snapshots / Clones) / Disaster Recovery (Site Recovery Manager with Array based Replication)
vSAN Datastore
VMware vSAN
Storage (Block / NFS / iSCSI / vVOL)
On-Premises
Oracle Based Business Continuity (RMAN / Data Pump etc) / Disaster Recovery (Data Guard, Golden Gate etc) – on all VMware Platforms
vSphere Based Business Continuity (VMware Snapshots/Clones) / Disaster Recovery (VMware Site Recovery (VSR) / VCDR)
vSphere Based Business Continuity (VMware Snapshots/Clones) / Disaster Recovery (VMware Site Recovery Manager)
All VMware Clouds
VMware Cloud™ on AWS
vCenter
VMware Clouds (AVS, GCVE, OCVS, VMware Cloud on DellEMC, etc.)
VMware Clouds

FIGURE 336. Oracle Business Continuity and Disaster Recovery Summary

Appendix A Oracle Initialization Parameter Configuration

Oracle Initialization Parameters (Oracle19c-OL8)

```
*.audit_file_dest=’/u01/admin/vvol19c/adump’
*.audit_trail=’db’
*.audit_sys_operations=TRUE
*.compatible=12.1.0.0.0
*.control_files=’+DATA_DG/vvol19c/control01.ctl’,’+DATA_DG/vvol19c/control02.ctl’,’+DATA_DG/vvol19c/control03.ctl’
*.db_block_size=8192
*.db_domain=’’
*.db_name=’vvol19c’
*.db_create_file_dest=’+DATA_DG’
*.db_recovery_file_dest=’+FRA_DG’
*.db_recovery_file_dest_size=100G
*.diagnostic_dest=’/u01/admin/vvol19c’
*.enable_pluggable_database=true
*.instance_number=1
*.instance_name=’vvol19c’
*.log_archive_format=’%t_%s_%r.dbf’
*.open_cursors=1000
*.processes=2000
*.parallel_instance_group=’vvol19c’
*.parallel_max_servers=100
*.pga_aggregate_target=256M
*.pga_aggregate_limit=6G
*.remote_login_passwordfile=’exclusive’
*.resource_manager_plan=’’
*.result_cache_max_size=4M
*.sga_max_size=96G
*.sga_target=96G
*.thread=1
*.undo_tablespace=’UNDOTBS01’
*.use_large_pages=’only’
```

Oracle Initialization Parameters (Oracle19c-OL8-RMAN)

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

Oracle RAC Initialization Parameters (prac19c)

```
*.AWR_PDB_AUTOFLUSH_ENABLED=true
*.audit_trail=’db’
*.audit_sys_operations=TRUE
prac19c1.audit_file_dest=’/u01/admin/prac19c1/adump’
prac19c2.audit_file_dest=’/u01/admin/prac19c2/adump’
*.cluster_database=true
*.compatible=12.1.0.0.0
*.control_files=’+DATA_DG/prac19c/control01.ctl’,’+DATA_DG/prac19c/control02.ctl’,’+DATA_DG/prac19c/control03.ctl’
*.db_block_size=8192
*.db_domain=’’
*.db_name=’prac19c’
*.db_recovery_file_dest=’+DATA_DG’
*.db_recovery_file_dest_size=50G
prac19c1.diagnostic_dest=’/u01/admin/prac19c1’
prac19c2.diagnostic_dest=’/u01/admin/prac19c2’
*.enable_pluggable_database=true
prac19c1.instance_number=1
prac19c2.instance_number=2
*.log_archive_format=’%t_%s_%r.dbf’
*.sga_max_size=16G
*.sga_target=16G
*.open_cursors=1000
*.processes=1000
*.parallel_max_servers=100
*.pga_aggregate_target=2G
*.remote_login_passwordfile=’exclusive’
prac19c1.thread=1
prac19c2.thread=2
prac19c1.undo_tablespace=’UNDOTBS01’
prac19c2.undo_tablespace=’UNDOTBS02’
*.use_large_pages=’only’
```

Oracle Initialization Parameters (Oracle19c-OL8-Primary)

```
*.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’
```

Oracle Initialization Parameters (Oracle19c-OL8-Standby)

```
*.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’
```

Custom Quiescing Scripts (Pre-Freeze and Post-Thaw)

Example of main script ‘10-freeze-thaw-databasse-vm-snapshot’ that invokes the freeze and thaw routines:

```
[root@oracle19c-ol8 ~]# cat /etc/vmware-tools/backupScripts.d/10-freeze-thaw-databasse-vm-snapshot
#!/bin/sh

if [[ $1 == “freeze” ]]
then

    echo “This section is executed before the Snapshot is created”
    su - oracle -c /home/oracle/pre-freeze-script

elif [[ $1 == “freezeFail” ]]
then

    echo “This section is executed when a problem occurs during snapshot creation and cleanup is needed since thaw is not executed”
    su - oracle -c “echo “Error in Freeze Operation” > /home/oracle/error.txt”

elif [[ $1 == “thaw” ]]
then

    echo “This section is executed when the Snapshot is removed”
    su - oracle -c /home/oracle/post-thaw-script

else

    echo “Usage: `/bin/basename $0` [ freeze | freezeFail | thaw ]”
    exit 1

fi
[root@oracle19c-ol8 ~]#
```

Database Pre-Freeze scripts:

```
oracle@oracle19c-ol8:vvol19c:/home/oracle> cat pre-freeze-script
#!/bin/bash
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/dbhome_1

sqlplus /nolog <<EOF
conn / as sysdba
alter database begin backup;
exit;
EOF
oracle@oracle19c-ol8:vvol19c:/home/oracle>
```

Database Post-Thaw scripts:

```
oracle@oracle19c-ol8:vvol19c:/home/oracle> cat post-thaw-script
#!/bin/bash
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/dbhome_1

sqlplus /nolog <<EOF
conn / as sysdba
alter database end backup;
exit;
EOF
oracle@oracle19c-ol8:vvol19c:/home/oracle>
```

Reference

White Papers

For additional information, see the following white papers:

- *VMware Hybrid Cloud Best Practices Guide for Oracle Workloads*
- *Oracle VMware Hybrid Cloud High Availability Guide*
- *Virtualizing Oracle Workloads with VMware vSphere Virtual Volumes on VMware Hybrid Cloud*
- *Oracle Database 12c on VMware vSAN – Day 2 Operations and Management*
- *Enabling or disabling simultaneous write protection provided by VMFS using the multi-writer flag (1034165)*

Product Documentation

For additional information, see the following product documentation:

- *VMware vSphere Documentation*
- *Oracle 19c Database Online Documentation*

Other Documentation

For additional information, see the following document:

- *VMware Solutions Lab*

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 technical contributions and help with Lab setup:

- **Cato Grace** – Senior Technical Marketing Architect, CPBU
- **Michael McLaughlin** – Senior Technical Marketing Architect, DRaaS Engineering

Thanks to the following for their reviews:

- **Jason Massae** – Storage Technical Marketing Architect, VMware Core Storage (Storage Product Marketing)

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: VMW-0518-1843_Oracle BC DR VMware Multi-Cloud_1.6_SML 9/21