Dell Technologies PowerStore: VMware Site Recovery Manager Best Practices

May 2024

H18425.5

White Paper

Abstract

This document offers best practices for automated disaster recovery of virtualized workloads using Dell Technologies PowerStore arrays, replication, and VMware Site Recovery Manager.

Copyright

Contents

Executive summary

Introduction

Data-center consolidation by way of x86 virtualization is a trend that has gained tremendous momentum and offers many benefits. Although the physical nature of a server is transformed once it is virtualized, the necessity for data protection remains. Virtualization opens the door to new and flexible opportunities in data protection, data recovery, replication, and business continuity. This document offers best practices for automated disaster recovery of virtualized workloads using Dell Technologies PowerStore, replication, and VMware Site Recovery Manager (SRM).

Audience

This document is intended for IT administrators, storage architects, partners, and Dell Technologies employees. This audience also includes individuals who may evaluate, acquire, manage, operate, or design a Dell Technologies networked storage environment using PowerStore systems.

Revisions

Date	Part number/ revision	Description
July 2020		Initial release
October 2020		SPA remote system requirement update
December 2020	H18425	Addition of vmware-dr.xml file location for Photon OS based appliance
October 2021	H18425.1	Template update
June 2022	H18425.2	Addition of vVOL replication
August 2023	H18425.3	Addition of metro volume support
October 2023	H18425.4	Updated for PowerStoreOS 3.6
May 2024	H18425.5	Update for PowerStoreOS 4.0

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Authors: Jason Boche, Jason Gates

Contributor: Robert Weilhammer

Note: For links to other documentation for this topic, see the PowerStore Info Hub.

Introduction

Document overview

This paper provides configuration examples, tips, recommended settings, and other storage guidelines to follow while integrating VMware Site Recovery Manager (SRM) with Dell Technologies PowerStore. In addition to basic configuration, this document also answers frequently asked questions about VMware interactions with Site Recovery Manager.

We recommend reading the Site Recovery Manager documentation provided on vmware.com before beginning an SRM implementation.

PowerStore overview

PowerStore achieves new levels of operational simplicity and agility. It uses a container-based microservices architecture, advanced storage technologies, and integrated machine learning to unlock the power of your data. PowerStore is a versatile platform with a performance-centric design that delivers multidimensional scale, always-on data reduction, and support for next-generation media.

PowerStore brings the simplicity of public cloud to on-premises infrastructure, streamlining operations with an integrated machine-learning engine and seamless automation. It also offers predictive analytics to easily monitor, analyze, and troubleshoot the environment. PowerStore is highly adaptable, providing the flexibility to host specialized workloads directly on the appliance and modernize infrastructure without disruption. It also offers investment protection through flexible payment solutions and data-in-place upgrades.

Terminology

The following table provides definitions for some of the terms that are used in this document.

Table 1. Terminology

Term	Definition
Appliance	Solution containing a base enclosure and attached expansion enclosures. The size of an appliance could be only the base enclosure or the base enclosure plus expansion enclosures.
Asynchronous replication	Replication method which allows replicating data over long distances and maintaining a replica at a destination site. Updates to the destination image can be issued manually, or automatically based on a customizable RPO.
Bandwidth	Amount of data, represented in MB/s, which can be transferred in a given period.
Common base	Pair of snapshots that are taken on a replication source and destination storage resource which have the same point-in-time image.
Destination storage resource	Storage resource that is used for disaster recovery in a replication session. This term is also known as a target image.
Fibre Channel FC) protocol	Protocol used to perform IP and SCSI commands over a Fibre Channel network.
File system	Storage resource that can be accessed through file-sharing protocols such as SMB or NFS.

Term	Definition
Internal snapshot (replication snapshot)	Unified snapshots created by the system that are part of an asynchronous replication session. These snapshots are only visible in the PowerStore CLI or PowerStore REST API, and manual modification is not possible. Each asynchronous replication session uses up to two internal snapshots that are taken on the source and destination storage resources. Each session also takes up one read/write snapshot on the destination storage system. The last successful internal read-only (RO) snapshots for source and destination storage resources and are used as a common base.
iSCSI	Provides a mechanism for accessing block-level data storage over network connections.
Network-attached storage (NAS) server	File-level storage server used to host file systems. A NAS server is required to create file systems that use SMB or NFS shares.
Network File System (NFS)	An access protocol that allows data access from Linux or UNIX hosts on a network.
PowerStore base enclosure	Enclosure containing both nodes (node A and node B) and 25 NVMe drive slots
PowerStore cluster	Multiple appliances in a single grouping. Clusters can consist of one appliance or more. Up to four PowerStore T appliances can be clustered by adding appliances as required.
PowerStore Command Line Interface (PSTCLI)	Tool which can be installed on an operating system to manage a PowerStore system. It allows a user to perform tasks on the storage system by typing commands instead of using the user interface.
PowerStore expansion enclosure	Enclosure that can be attached to a base enclosure to provide additional storage.
PowerStore Manager	An HTML5 management interface for creating storage resources and configuring and scheduling protection of stored data on PowerStore. PowerStore Manager can be used for all management of PowerStore native replication.
PowerStore node	Storage controller that provides the processing resources for performing storage operations and servicing I/O between storage and hosts. Each PowerStore appliance contains two nodes.
PowerStore Q model	Container-based storage system that is running on purpose-built hardware. This storage system supports unified (block and file) workloads, or block-optimized workloads. The PowerStore Q model supports Quad-Level Cell (QLC) NVMe SSDs for data storage.
PowerStore Representational State Transfer (REST) API	Set of resources (objects), operations, and attributes that provide interactive, scripted, and programmatic management control of the PowerStore cluster.
PowerStore T model	Container-based storage system that is running on purpose-built hardware. This storage system supports unified (block and file) workloads, or block-optimized workloads. The PowerStore T model supports Triple-Level Cell (TLC) NVMe SSDs for data storage.

Term	Definition
RecoverPoint for Virtual Machines	Protects virtual machines (VMs) in a VMware environment with VM-level granularity and provides local or remote replication for any point-in-time recovery. This feature is integrated with VMware vCenter and has integrated orchestration and automation capabilities.
Recovery point objective (RPO)	Acceptable amount of data, which is measured in units of time, that may be lost due to a failure. For example, if a storage resource has a one-hour RPO, data that is written to the storage resource within the last hour may be lost when the replication session is failed over to the destination storage resource.
Recovery time objective (RTO)	Duration of time in which a business process must be restored after a disaster recovery plan is run. For example, an RTO of one hour requires restoring data access within one hour after a disaster is declared and the disaster recovery plan performed.
Remote systems	Relationship that is configured between two PowerStore systems.
Replication session	Relationship that is configured between two storage resources of the same type on different systems, and automatically synchronizes data from one resource to another.
Server Message Block (SMB)	Network file-sharing protocol, also known as CIFS, used by Microsoft Windows environments. SMB is used to provide access to files and folders to Windows hosts on a network.
Snapshot	Also called a unified snapshot, a snapshot is a point-in-time view of a storage resource or data stored on a storage resource. A user can recover files from a snapshot, restore a storage resource from a snapshot, or provide snapshot data access to a host. When a snapshot is taken, it creates an exact copy of the source storage resource and shares all blocks of data with it. As data changes on the source, new blocks are allocated and written to. Unified snapshot technology can be used to take a snapshot of a block or file storage resource.
Storage resource	Top-level object that a user can provision which is associated with a specific quantity of storage. All host access and data-protection activities are performed at this level. In this document, storage resources refer to resources that support replication such as volumes, volume groups, and thin clones.
Thin clone	Read/write copy of a thin block storage resource (volume, volume group, or VMware vSphere VMFS datastore) that shares blocks with the parent resource.
Unisphere Manager for RecoverPoint	Web-based interface for managing RecoverPoint replication. It serves as a single pane of glass for replicating storage resources of multiple storage systems that are configured to use RecoverPoint. Consistency groups are created, replicated, and recovered through this interface.
User snapshot	Snapshot that is created manually by the user or by a protection policy with an associated snapshot rule. This snapshot type is different than an internal snapshot, which the system takes automatically using asynchronous replication.

Term	Definition
Virtual Volumes (vVols)	VMware storage framework which allows VM data to be stored on individual Virtual Volumes. This ability allows data services to be applied at a VM-granularity level while using Storage Policy Based Management (SPBM).
Volume	A block-level storage device that can be shared out using a protocol such as iSCSI or Fibre Channel. It represents a SCSI logical unit.
Volume group	Storage instance which contains one or more volumes within a storage system. Volume groups can be configured with write-order consistency and help organize the storage that is allocated for particular hosts.
vStorage API for Array Integration (VAAI)	VMware API that allows storage-related tasks to be offloaded to the storage system.
vSphere API for Storage Awareness (VASA)	VMware API that provides additional insight about the storage capabilities in vSphere.

Setup prerequisites

Introduction

Verify the solution requirements listed in this section before deploying or upgrading your environment.

Storage Replication Adapter

The PowerStore Storage Replication Adapter (SRA) must be installed on each SRM server. PowerStore offers SRAs for both the Photon operating-system based SRM appliance and the Windows-based SRM installation. You can download the SRAs from the VMware website. We recommend using the most current version of the SRA to ensure optimal compatibility and available features. See the SRA release notes and product documentation to determine SRA compatibility with SRM versions.

Note: See the SRA release notes for specific requirements or features noted for the SRA. For example, at the time of this publication the SRA cannot work if more than one remote system is configured on PowerStore. This means that a 1:1 appliance replication relationship must be maintained between the protected site and the recovery site.

PowerStore

SRM- and array-based replication of block volumes requires two PowerStore appliances replicating between each other in one or both directions. You can replicate virtual machines that are based on PowerStore NFS and vVols using vSphere replication, or consider using RecoverPoint for Virtual Machines as an alternative.

VMware vSphere and SRM

Compatible versions of VMware SRM, VMware vCenter Server, and vSphere hosts are required. To see a list of software versions required for SRM to function, check the VMware Product Interoperability Matrix. SRM is supported with vCenter Server for Essentials, vCenter Server Foundation, and vCenter Server Standard.

Site Recovery Manager architecture

Introduction

This section describes array-based replication architecture for single- and dual-protected sites.

Array-based replication: single protected site

This configuration (shown in Figure 1) is generally used when the secondary site does not have any virtual machines that SRM must protect. The secondary site exists solely for disaster-recovery purposes. The infrastructure at the recovery site must be available and online to run the SRM recovery plan.

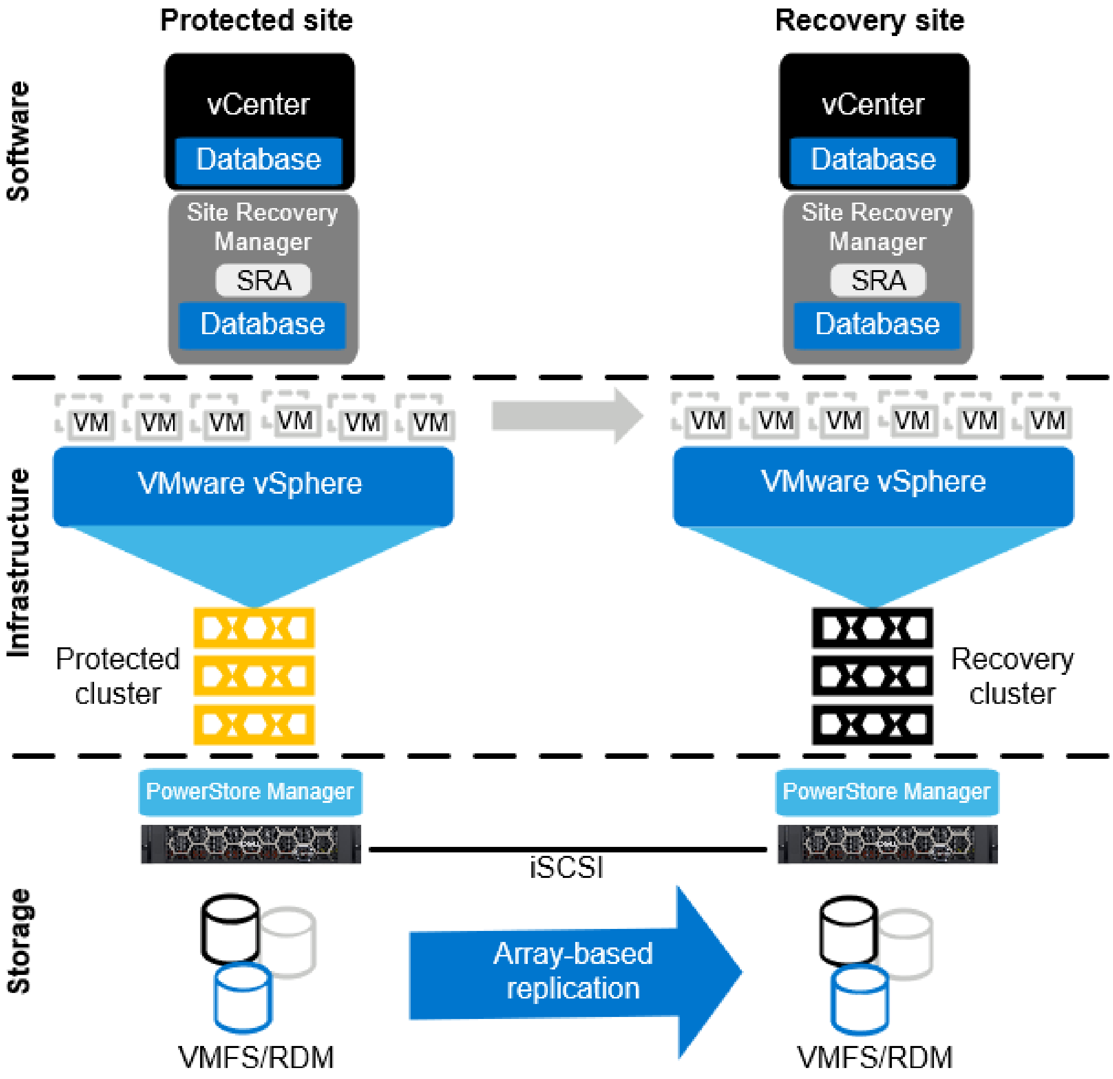


Figure 1. **Architecture for a single protected site with array-based replication**

Array-based replication: dual protected site

This configuration (shown in Figure 2) is generally used when both sites have virtual machines that need to be protected by SRM. Each site replicates its virtual machines to the opposing site where they can be recovered.

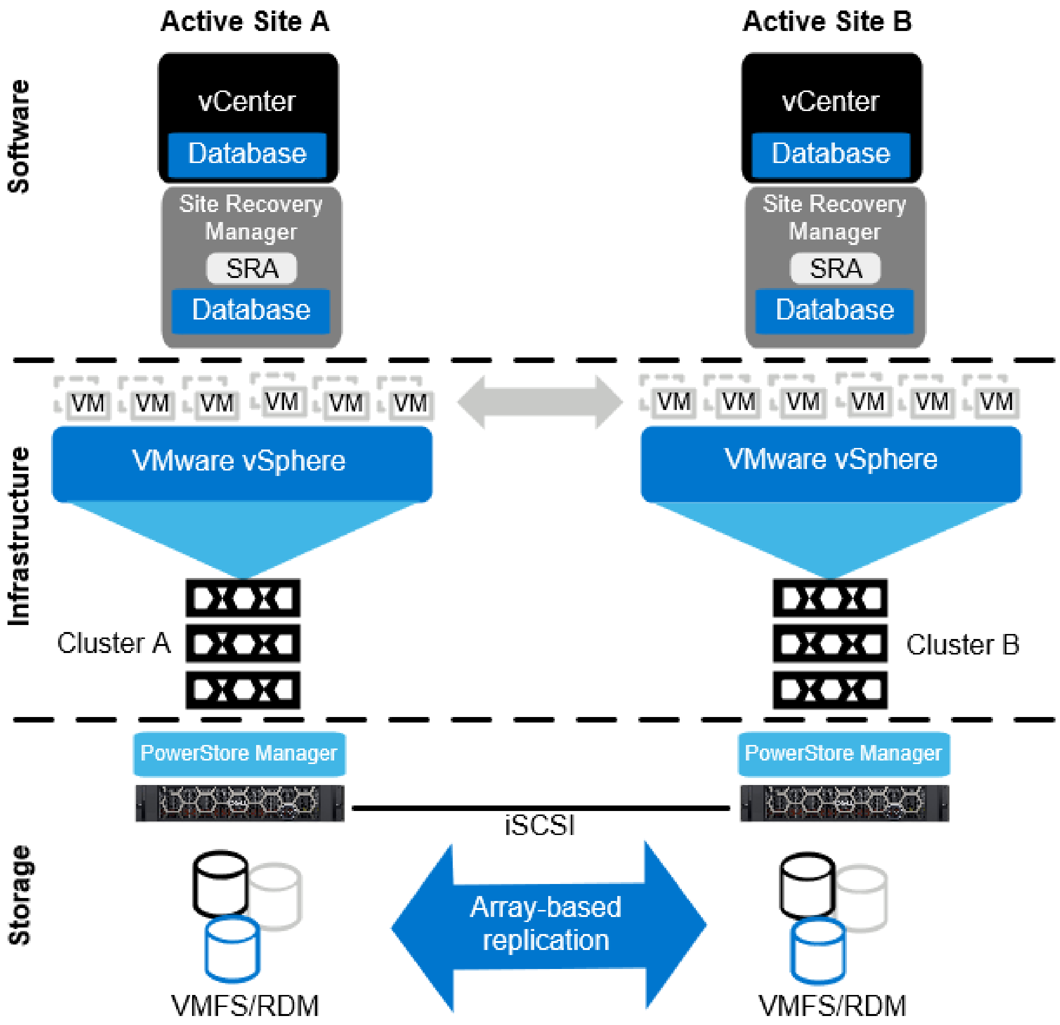


Figure 2. Architecture for a dual protected site with array-based replication

vSphere replication: single protected site

vSphere replication can be used in addition to or in place of array-based replication (see Figure 3). Here are two of the main advantages of vSphere replication over array-based replication:

- It enables a granular selection of individual powered-on VMs to be replicated instead of entire datastores of VMs.
- vSphere datastore objects abstract the underlying storage vendor, model, protocol, and type. This behavior means that replication can be carried out between different array models and protocols, including local storage.

vSphere replication, along with other feature support for vSphere replication added in SRM 8, makes SRM appealing and adaptable as a DR solution for organizations with storage or budget constraints.

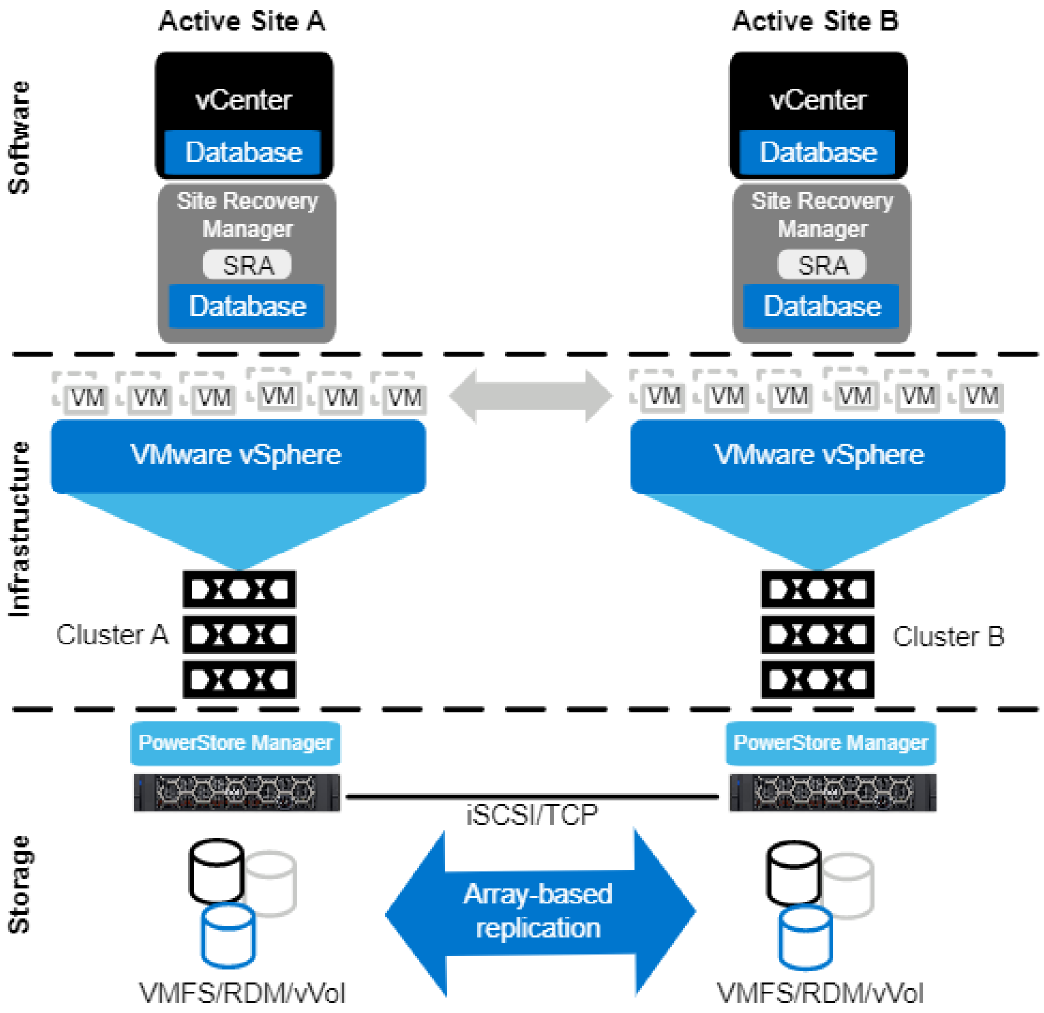


Figure 3. Configuration for a dual protected site with vVol replication

vSphere replication: dual protected site

vSphere replication also supports the active/active site model (see Figure 4). In each vSphere replication architecture diagram, replication is handled by the vSphere hosts that use the vSphere network stack. An array-based SRA is not present in vSphere replication architecture. These figures do not represent all the components of vSphere replication. A deployment of vSphere replication consists of multiple virtual appliances at each site and on each vSphere host that handles the movement of data between sites. Go to VMware Documentation for a detailed look at vSphere replication.

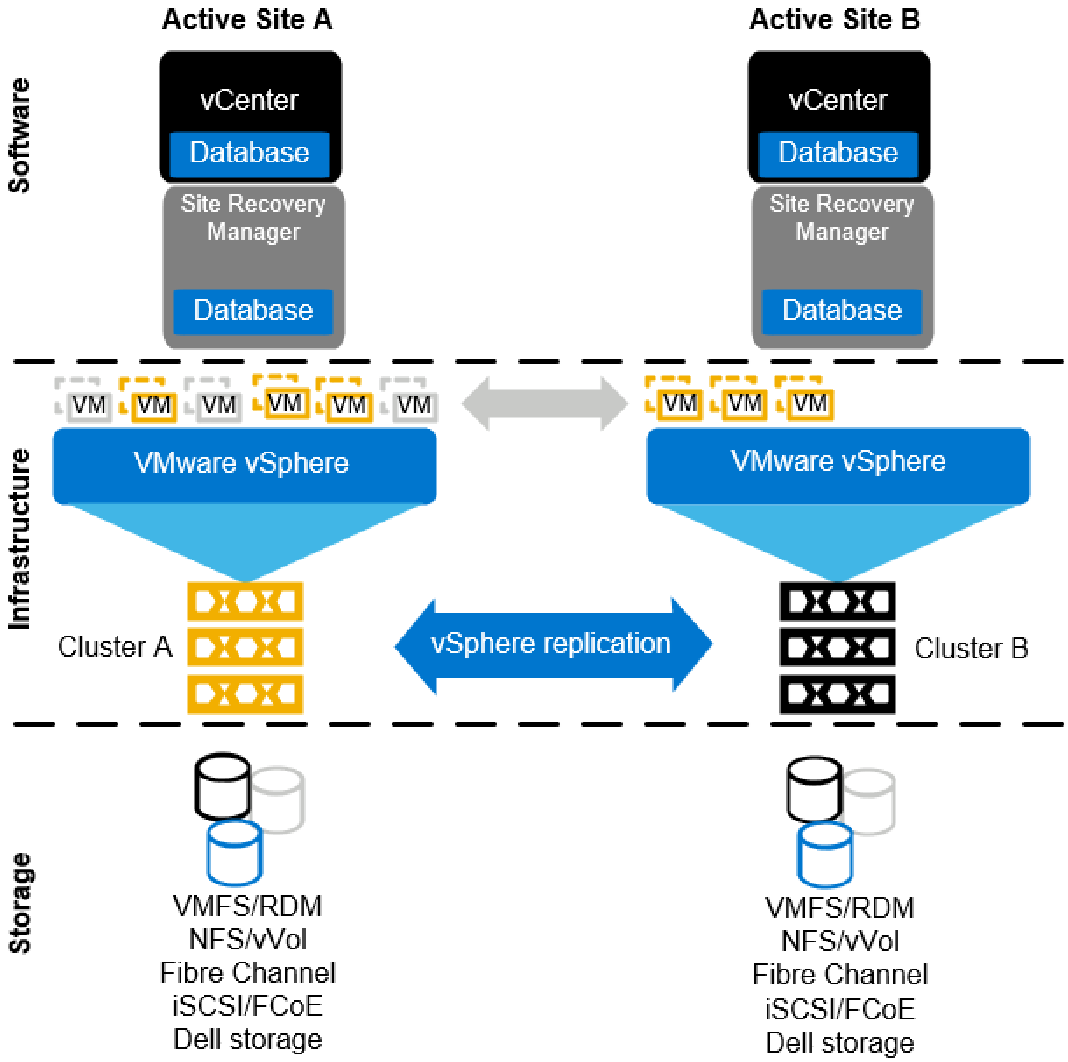


Figure 4. Configuration for a dual-protected site with vSphere replication

Note: You can use vSphere replication to replicate virtual machines that are based on PowerStore NFS and vVols. Alternately, consider using RecoverPoint for Virtual Machines.

PowerStore Manager configuration

Introduction

This section provides best practices for configuring PowerStore Manager.

PowerStore Manager availability

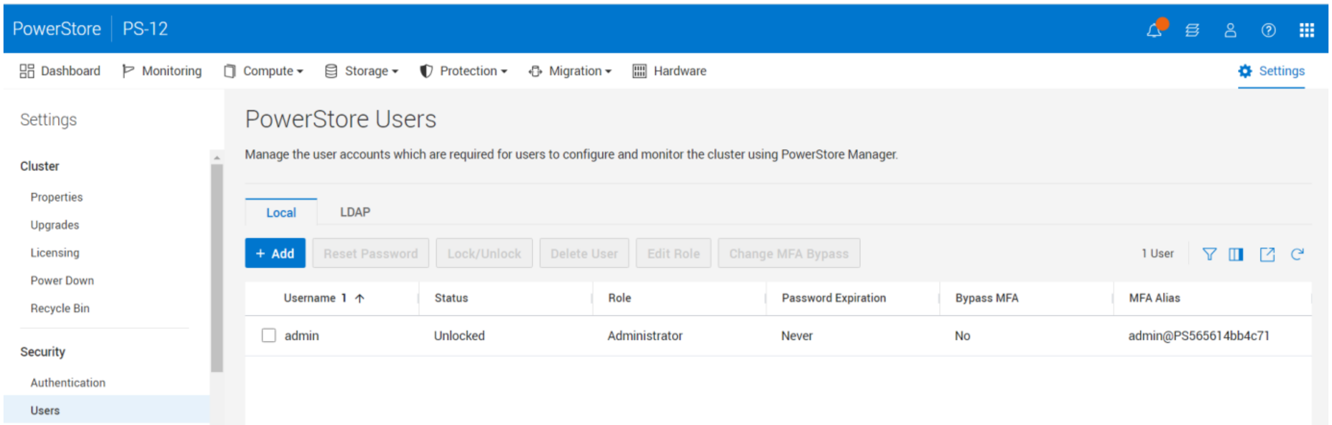
As described in Site Recovery Manager architecture, PowerStore Manager is a critical piece in the SRM infrastructure because it processes all calls from the SRA and performs the storage-related workflow tasks at the recovery site.

PowerStore Manager is natively integrated and deployed with each PowerStore appliance, so there are no architectural decisions required regarding where to deploy PowerStore Manager. If the recovery-site PowerStore appliance is healthy and available, the requirement for PowerStore Manager availability is met. Ensure that monitoring and alerting processes are in place for each PowerStore appliance.

PowerStore Manager logins

For SRM to function, the SRA must use login credentials that have rights to the respective PowerStore appliances that are replicating the virtual-machine volumes.

Keep in mind that each PowerStore appliance, whether it is at the protected or remote site, maintains its own user-access database. Credentials are required for PowerStore appliances at both sites. For example, if PS-22 is replicating virtual-machine volumes to PS-17, the credentials that the SRAs use must have administrator privileges to both appliances PS-22 and PS-17. Figure 5 shows the default admin credential that is used to manage the PowerStore appliance.



PowerStore Users

Manage the user accounts which are required for users to configure and monitor the cluster using PowerStore Manager.

Username 1 ↑	Status	Role	Password Expiration	Bypass MFA	MFA Alias
□ admin	Unlocked	Administrator	Never	No	admin@PS565614bb4c71

Figure 5. PowerStore Users menu in PowerStore Manager

Creating dedicated SRA access accounts

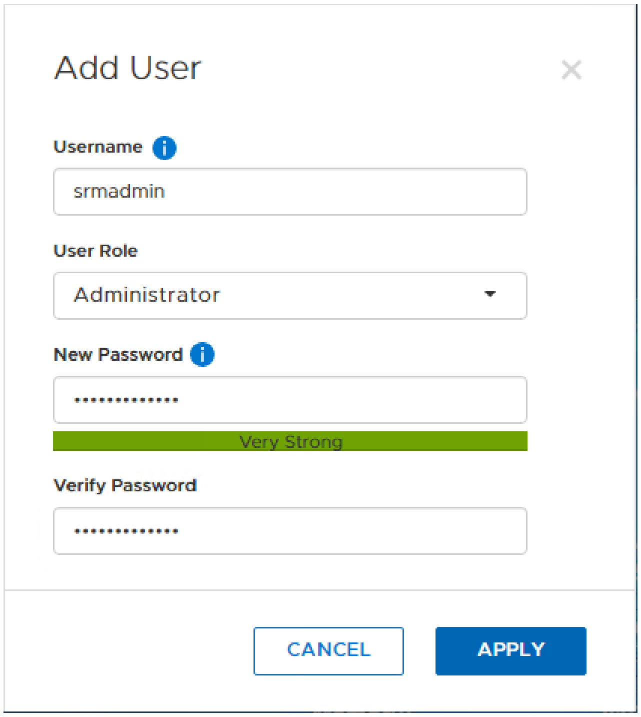
For the SRA to have uninterrupted access to both arrays, we recommend creating dedicated accounts for SRM. Using dedicated accounts on each array helps ensure that service is not unintentionally disrupted due to a password rotation, account lockout, account disablement, or account deletion.

Use these example steps to create dedicated accounts:

1. Create an account named srmadmin on both the protected-site array and the recovery-site array.

   This account requires administrator privileges, and the password assigned must meet PowerStore password complexity requirements. For added security, create unique account names on each system with unique passwords. The account names and passwords are arbitrary.

2. Create an account in PowerStore Manager named **srmadmin**.



Add User

Username: srmadmin

User Role: Administrator

New Password: •••••••••••••

Very Strong

Verify Password: •••••••••••••

The **srmadmin** account can now be used within the SRM Array Manager configuration.

Note: Each PowerStore appliance, whether it is at the protected or remote site, maintains its own user access database. Credentials are required for PowerStore appliances at both sites.

Modifying SRM settings for larger environments

VMware Site Recovery Manager ships with a default configuration that is tuned for a large cross-section of environments. However, each environment is unique in terms of architecture, infrastructure, size, and recovery time objective (RTO). Larger or more-complex SRM environments may require tuning adjustments in SRM (listed in the following bullet points) for SRM workflows to carry out their assigned tasks properly. For more information about making adjustments to accommodate such environments, see the SRM documentation section Modify Settings to Run Large Site Recovery manager Environments.

- storage.commandTimeout – Min: 0 Default: 300

  This option specifies the timeout allowed (in seconds) for running SRA commands in array-based-replication-related workflows. Increasing this value is typically required for larger environments. Recovery plans with many datastores to manage may fail if the storage-related commands take longer than five minutes to complete. For larger environments, increase this value (for example, to 3600 or higher) in the advanced SRM settings.

- storage.maxConcurrentCommandCnt – Min: 0 Default: 5

  This option specifies the maximum number of concurrent SRA operations allowed.

- storageProvider.hostRescanRepeatCnt – Min: 0 Default: 1

  This option specifies the number of additional host rescans during test, planned-migration, and recovery workflows. This feature was not available in SRM 5.0 and was reintroduced in SRM 5.0.1. Increase this value (for example, to 2 or higher) in the advanced SRM settings.

- storageProvider.hostRescanTimeoutSec – Min: 0 Default: 300

  This option specifies the timeout allowed (in seconds) for host rescans during test, planned migration, and recovery workflows. Recovery plans with many datastores or hosts will fail if the host rescans take longer than five minutes to complete. Increase this value (for example, to 600 or higher) in the advanced SRM settings.

- defaultMaxBootAndShutdownOpsPerCluster – Default: off

  This option specifies the maximum number of concurrent power-on operations performed by SRM at the cluster object level. To enable the option globally, specify a numerical value (such as 32) by modifying the vmware-dr.xml file. You can add this option anywhere in the <config> section, and restart the Site Recovery Manager Server service after making a change.

  ```
  <config>
    <defaultMaxBootAndShutdownOpsPerCluster>32
  </defaultMaxBootAndShutdownOpsPerCluster>
  </config>
  ```

  You can configure this value per cluster by editing the **srmMaxBootShutdownOps** in vSphere DRS Advanced Options. This value overrides a value specified in the vmare-dr.xml file.

- defaultMaxBootAndShutdownOpsPerHost – Default: off

  This option specifies the maximum number of concurrent power-on operations performed by SRM at the host object level. To enable this option, specify a numerical value (such as 4) by modifying the vmware-dr.xml file. You can add this option anywhere in the <config> section, and restart the Site Recovery Manager Server service after making a change.

  ```
  <config>
    <defaultMaxBootAndShutdownOpsPerHost>4
  </defaultMaxBootAndShutdownOpsPerHost>
  </config>
  ```

The **vmware-dr.xml** file is located in the **config** directory that resides in the SRM installation folder. The specific location varies depending on the operating system and SRM version. For example:

- Windows:

  C:\Program Files\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml

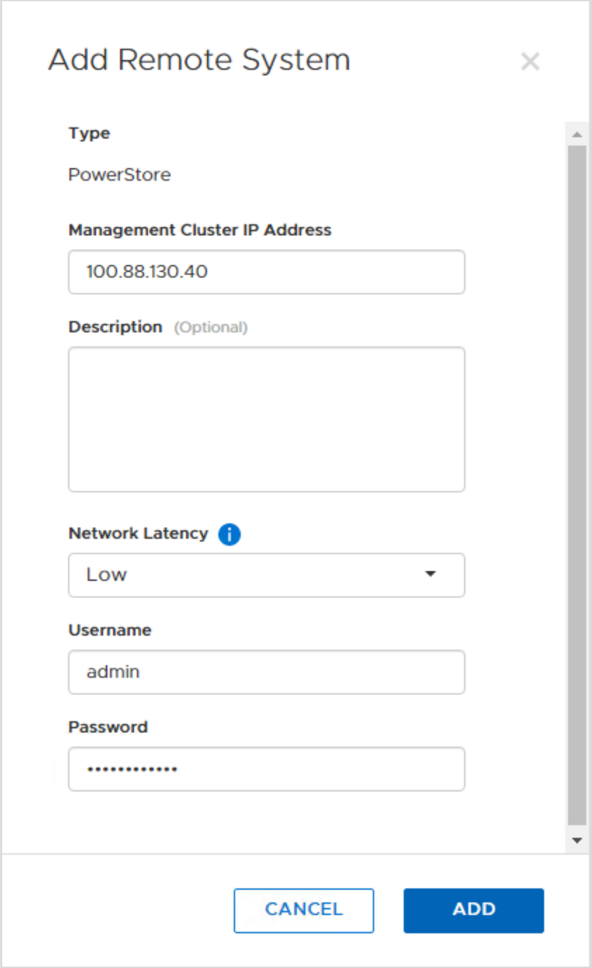
- Virtual Appliance:

  /opt/vmware/srm/conf/vmware-dr.xml

Replication configuration

Introduction

PowerStore replication, in coordination with Site Recovery Manager (SRM), can provide a robust and scalable disaster-recovery solution. Since each snapshot and replication strategy affects recovery differently, choosing the correct protection policy to meet business requirements is important. PowerStore asynchronous replication features can be configured using PowerStore Manager, PowerStore CLI, or REST API. RecoverPoint for Virtual Machines supports VM replication for PowerStore and is configured using the Unisphere Manager for RecoverPoint user interface. PowerStore replication uses iSCSI through Ethernet (LAN) connections. When the replication interfaces are created and cabled to the network on both systems, the remote system connection between the arrays can be made. Once a remote system is configured on one of the systems participating in replication, it is automatically created on the peer system.


Add Remote System

Type
PowerStore

Management Cluster IP Address
100.88.130.40

Description (Optional)

Network Latency
Low

Username
admin

Password
••••••••••••

Figure 6. Adding a remote system for replication

Asynchronous replication

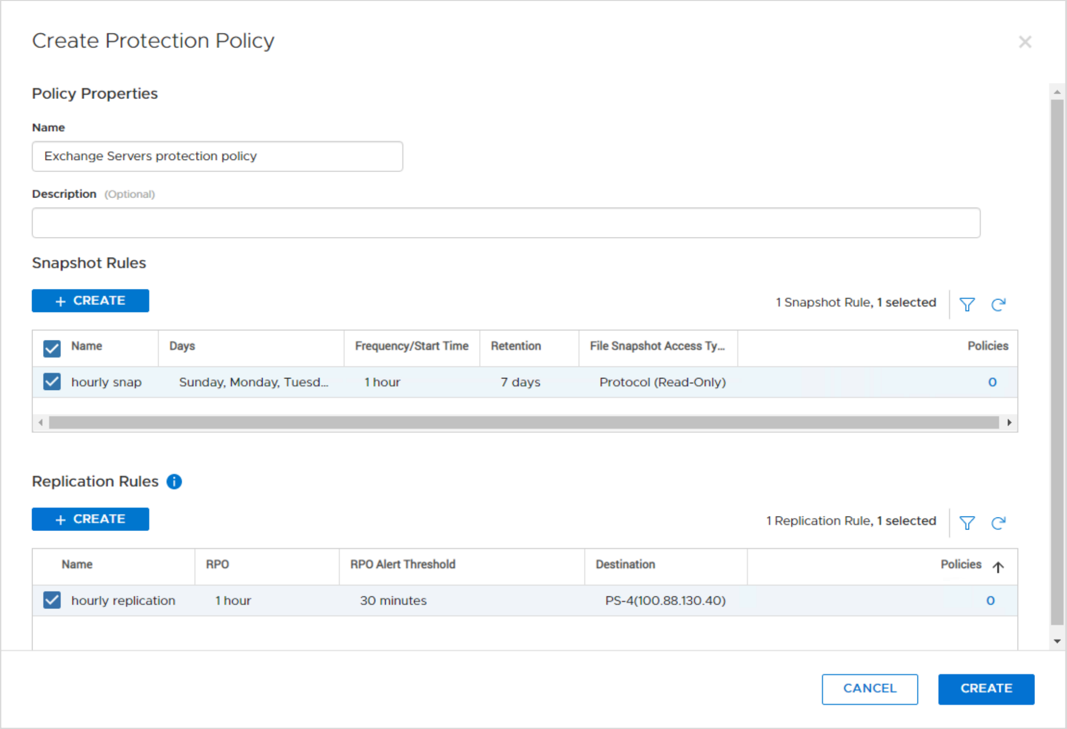
With asynchronous replication, the I/O must be committed to and acknowledged by the source system so the data can be transferred to the destination in an independent timeframe. Supported storage resources for native asynchronous block replication are volumes, volume groups, and thin clones.

Note: Volume groups are treated as single entities when they are replicated. For virtual machines or tiered applications spanning multiple volumes, consider using volume groups to tie snapshot and replication schedules to the entire application group of volumes. This practice ensures point-in-time consistency across the volumes replicated to the recovery site.

Remote replication between PowerStore systems uses policy-based protection. Asynchronous replication configuration is defined in replication rules (see Figure 7). Protection policies allow the user to configure remote and local protection using replication, snapshot rules, or both. The policies combine one or more rules to fulfill the protection requirements for a storage resource on PowerStore at the protected site. For a valid configuration, a protection policy must contain at least one protection rule whether it is a local or remote protection rule. Each protection policy can contain up to one replication rule, one backup rule and up to four snapshot rules.

The replication rule defines the parameter for the asynchronous replication on PowerStore and is set up on PowerStore at the protected site. The required information for creating a rule includes the PowerStore system at the recovery site, the RPO, and the alert threshold for the planned replication session. When a protection policy with a replication rule is assigned to a storage resource, the configured RPO in the rule is used to set up the internal event scheduler for recurring replication of the storage resource.

For minimal RPO compliance issues, replication cycles are scheduled at 50% of the RPO value and are based on the hour. For example, a one-hour RPO leads to a replication event every 30 minutes to ensure enough overlapping to meet the target of a one-hour RPO. The scheduled RPO events for this example are at *x*:00 and *x*:30 every hour. The events for the RPO are based on the configured time and not on the amount of data which is written on the source storage resource. Asynchronous replications usually have more flexible bandwidth requirements. This ability makes it the most common replication method for organizations that allow an RPO that is greater than zero (some amount of data will be lost when recovering from an asynchronous replication). Another benefit of PowerStore asynchronous replication is that the snapshots are transferred to the destination volume. By default, SRM recovers data from the most recent replicated snapshot. However, all snapshots replicated to the recovery site are available for recovery using PowerStore manager or APIs.



Create Protection Policy

Policy Properties

Name

Exchange Servers protection policy

Description (Optional)

Snapshot Rules

1 Snapshot Rule, 1 selected

☑ Name	Days	Frequency/Start Time	Retention	File Snapshot Access Ty...	Policies
☑ hourly snap	Sunday, Monday, Tuesd...	1 hour	7 days	Protocol (Read-Only)	0

Replication Rules

1 Replication Rule, 1 selected

Name	RPO	RPO Alert Threshold	Destination	Policies
☑ hourly replication	1 hour	30 minutes	PS-4(100.88.130.40)	0

Figure 7. Creating a protection policy for an SRM protection group of volumes with one hour RPO

Note: Protection policies applied to a replicated volume carry over from the source to the destination after failover and reprotection workflows are run. Using the previous example, if the Exchange Server recovery plan is run and the volumes are failed over and reprotected, they maintain an hourly snapshot and hourly asynchronous replication to the peer storage array.

Remote system network latency

Replication traffic can be tuned for higher efficiency depending on the expected network latency. If the network to the remote system has an expected latency below five milliseconds, keep the default value of **Low**. Otherwise, select **High**. Depending on the selection, different iSCSI portals with optimized buffer settings are used for the replication data traffic.

Snapshots and application consistency

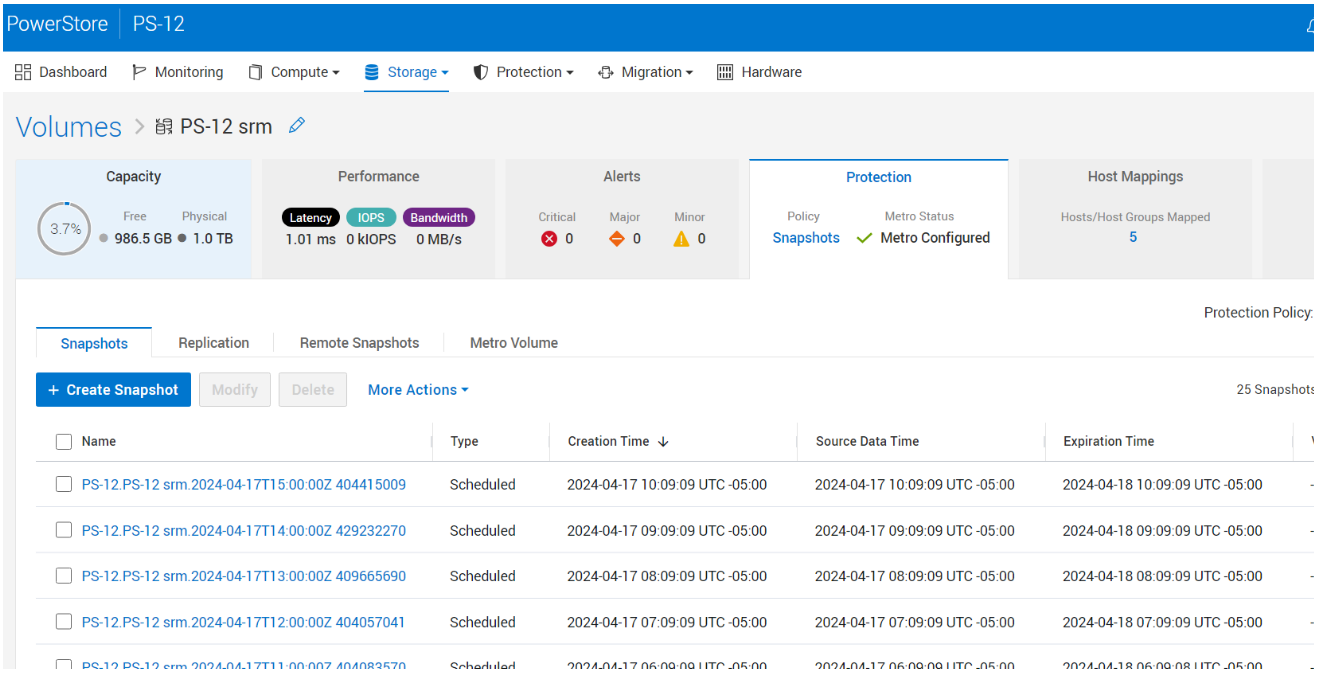
Asynchronous replication uses snapshots to provide point-in-time images as the source of RPO-based updates to the destination. These snapshots are used to maintain the common base images between the source and replicated resource across systems. Snapshots that replication creates and maintains are not visible in PowerStore Manager. When replication is configured, any snapshots created on the source resource are automatically replicated in chronological order to the destination system during the next RPO-based update (see Figure 8). There are several methods available for creating snapshots: PowerStore Manager, protection policies, PowerStore REST API, and PSTCLI. When replicated, SRM may use a thin clone of the snapshot to present recovered data to the vSphere cluster. Snapshots created in PowerStore Manager, or a protection policy are considered crash consistent. You can use other methods that result in application consistency within the snapshot. For example, where supported, you can use Dell Technologies AppSync to create application-consistent snapshots. This practice ensures that all incoming I/O for a given application is quiesced and flushed before a snapshot is created. Another method is to use vSphere snapshots with quiescence captured inside a replicated PowerStore snapshot. Either of these examples results in application-consistent snapshots being replicated to the recovery site.

When using vSphere snapshots, there are two important facts to recognize:

- The VM is replicated to the destination site in a vSphere snapshot state. It should be addressed to prevent the VM from running continuously over a long time in a vSphere snapshot state.
- The application and data consistency are contained within the frozen-parent virtual disk, and crash-consistent data is contained in the delta virtual disk.

When the SRM recovery plan workflow is carried out, SRM registers the VM into inventory at the destination site. Then, it powers on the VM with no special attention given to the current snapshot state of the VM. This means that SRM powers on the VM using the delta, resulting in recovery from a crash-consistent state. To recover the VM from the frozen-parent disk with application and data consistency, revert the VM to the previous snapshot using the vSphere Snapshot Manager before powering on the VM. Once this process is done, you can delete (close) the snapshot and power on the VM. This process ensures the VM is powered on from its frozen-parent disk and the delta disk, and the crash-consistent data in it is destroyed.

If manually carrying out the previous process on a large scale, this can erode efforts made toward meeting the recovery plan RTO and is not the best use of SRM. In such instances, it is more efficient and consistent to script the snapshot management process using Microsoft PowerShell. You can carry out this process as a pre-power-on step (or potentially post-power-on step) for the VM using a custom recovery task.

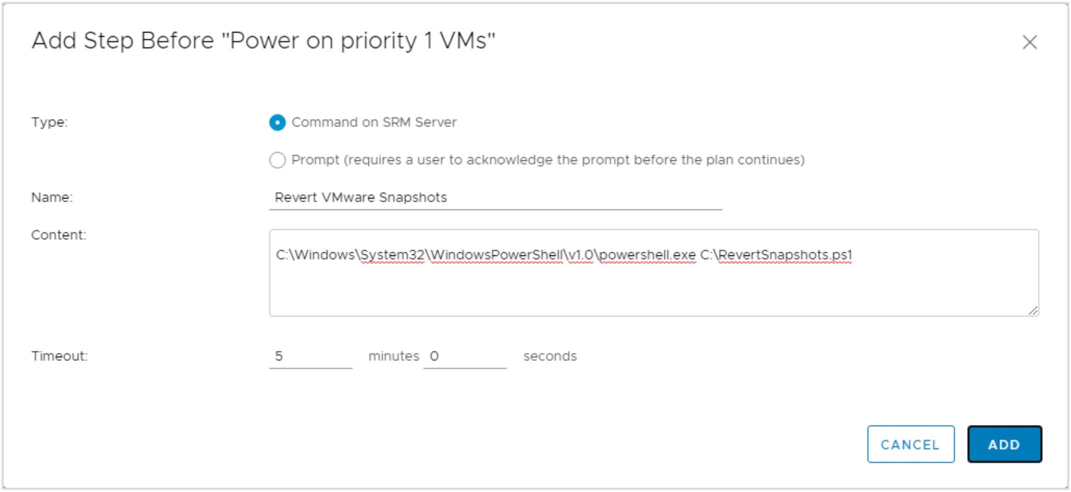


Name	Type	Creation Time ↓	Source Data Time	Expiration Time
PS-12.PS-12 srm.2024-04-17T15:00:00Z 404415009	Scheduled	2024-04-17 10:09:09 UTC -05:00	2024-04-17 10:09:09 UTC -05:00	2024-04-18 10:09:09 UTC -05:00
PS-12.PS-12 srm.2024-04-17T14:00:00Z 429232270	Scheduled	2024-04-17 09:09:09 UTC -05:00	2024-04-17 09:09:09 UTC -05:00	2024-04-18 09:09:09 UTC -05:00
PS-12.PS-12 srm.2024-04-17T13:00:00Z 409665690	Scheduled	2024-04-17 08:09:09 UTC -05:00	2024-04-17 08:09:09 UTC -05:00	2024-04-18 08:09:09 UTC -05:00
PS-12.PS-12 srm.2024-04-17T12:00:00Z 404057041	Scheduled	2024-04-17 07:09:09 UTC -05:00	2024-04-17 07:09:09 UTC -05:00	2024-04-18 07:09:09 UTC -05:00
PS-12.PS-12 srm.2024-04-17T11:00:00Z 404083570	Scheduled	2024-04-17 06:09:09 UTC -05:00	2024-04-17 06:09:09 UTC -05:00	2024-04-18 06:09:08 UTC -05:00

Figure 8. PowerStore Manager showing snapshots replicated to the recovery site

Custom recovery tasks

If the environment requires a custom recovery strategy, both Dell Technologies storage and VMware have robust API sets to customize the recovery steps where needed. APIs include PowerShell cmdlets, PowerStore REST API, and PSTCLI. The APIs can be used for tasks such as managing snapshots, creating thin clones, mapping volumes, and managing replications. Within the same script, the VMware cmdlets can rescan HBAs, manipulate vDisks, add virtual machines to inventory, and perform most other tasks required for recovery, as shown in Figure 9.



Add Step Before "Power on priority 1 VMs"

Type: ● Command on SRM Server

○ Prompt (requires a user to acknowledge the prompt before the plan continues)

Name: Revert VMware Snapshots

Content:

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe C:\RevertSnapshots.ps1
```

Timeout: 5 minutes 0 seconds

Figure 9. Custom recovery task in a Site Recovery Manager recovery plan

Note: For more information about REST API, use SwaggerUI (https://<PowerStore>/swaggerui) or see the *Dell Technologies PowerStore REST API Developers Guide* on the PowerStore Info Hub.

Site Recovery Manager configuration

Introduction

This section provides guidance and best practices for configuring Site Recovery Manager.

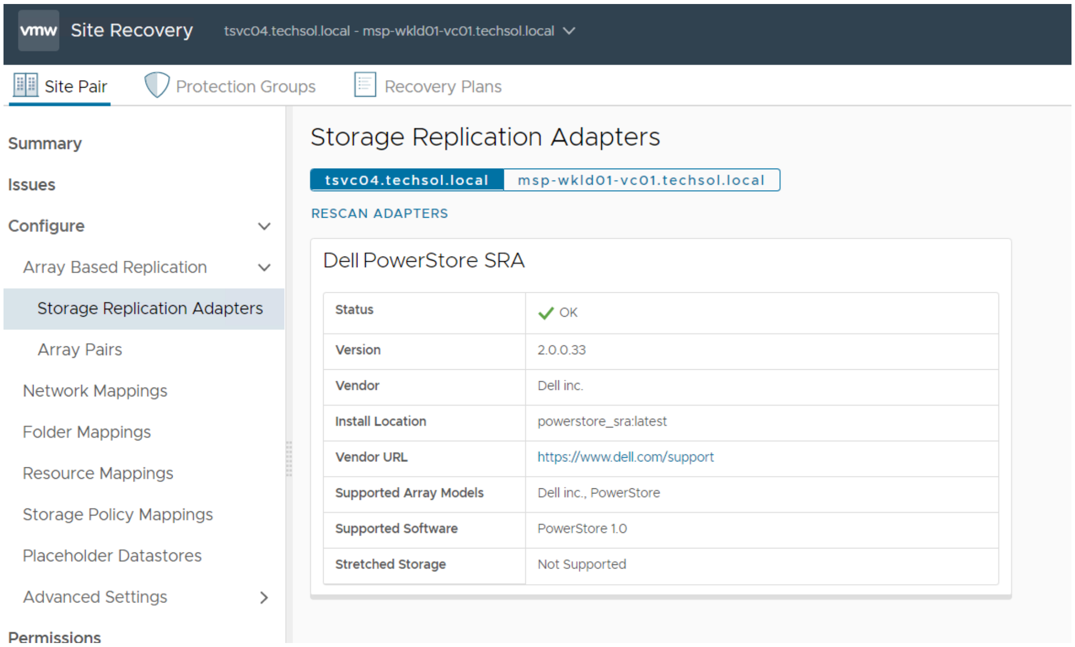
SRA installation

The PowerStore Storage Replication Adapter (SRA) must be installed on each SRM server. PowerStore offers SRAs for both the Photon operating-system-based SRM appliance and the Windows-based SRM installation. You can download the SRAs from the VMware website. We recommend using the most current version of the SRA to ensure optimal compatibility and available features. See the release notes and product documentation to determine SRA compatibility with SRM versions. The video Dell Technologies PowerStore - Storage Replication Adapter Installation demonstrates the installation process of the SRA on both operating systems.

Note: SRM supports installing multiple Storage Replication Adapters. This ability is beneficial when storage arrays of different types exist in the data center.

Configuring the array managers

To allow SRM to manage PowerStore storage, the SRA must be able to communicate with PowerStore. You can configure the array manager from the Array Managers module. You must add an array manager for each site in the unified interface, as shown in the following figures.



Dell PowerStore SRA

Status	✓ OK
Version	2.0.0.33
Vendor	Dell inc.
Install Location	powerstore_sra:latest
Vendor URL	https://www.dell.com/support
Supported Array Models	Dell inc., PowerStore
Supported Software	PowerStore 1.0
Stretched Storage	Not Supported

Figure 10. Examine the installed SRAs

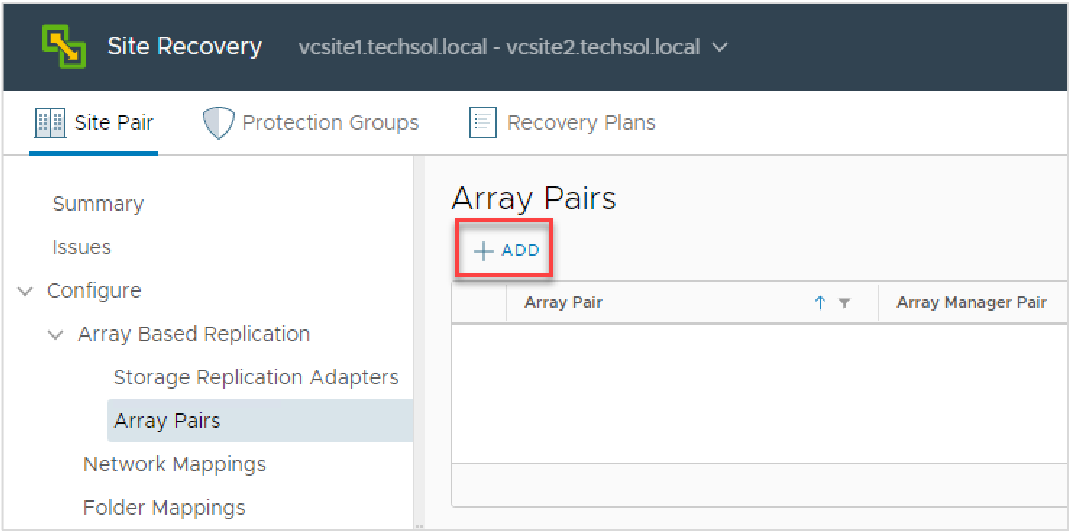
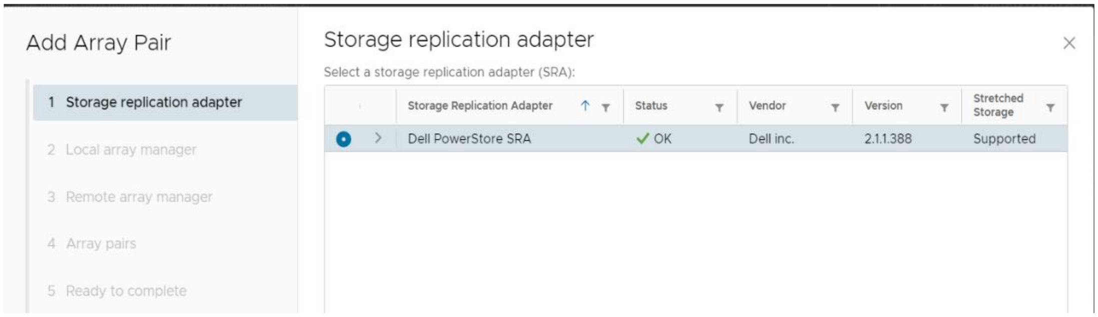


Figure 11. Adding an array manager

To perform the required process to configure the protected site array managers and the recovery site array managers for pairing, complete the following steps:

1. Choose the installed SRA.

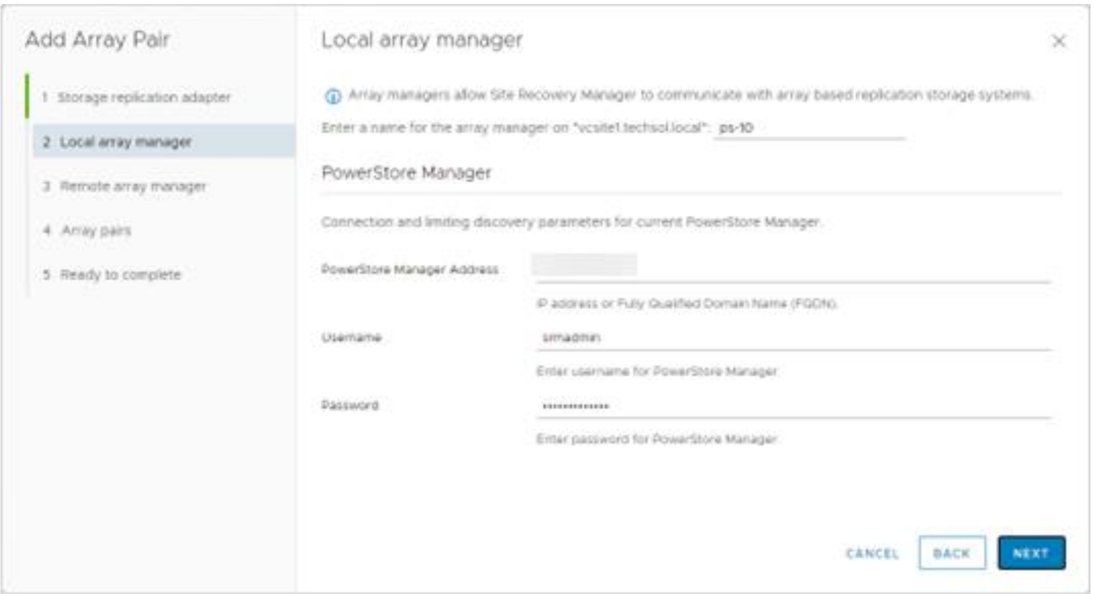


Storage replication adapter

Select a storage replication adapter (SRA):

		Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
●	>	Dell PowerStore SRA	✓ OK	Dell inc.	2.1.1.388	Supported

2. Provide the **local** PowerStore connection parameters for the local array manager.



Local array manager

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vcsite1.techsol.local": ps-10

PowerStore Manager

Connection and limiting discovery parameters for current PowerStore Manager.

PowerStore Manager Address:

IP address or Fully Qualified Domain Name (FQDN)

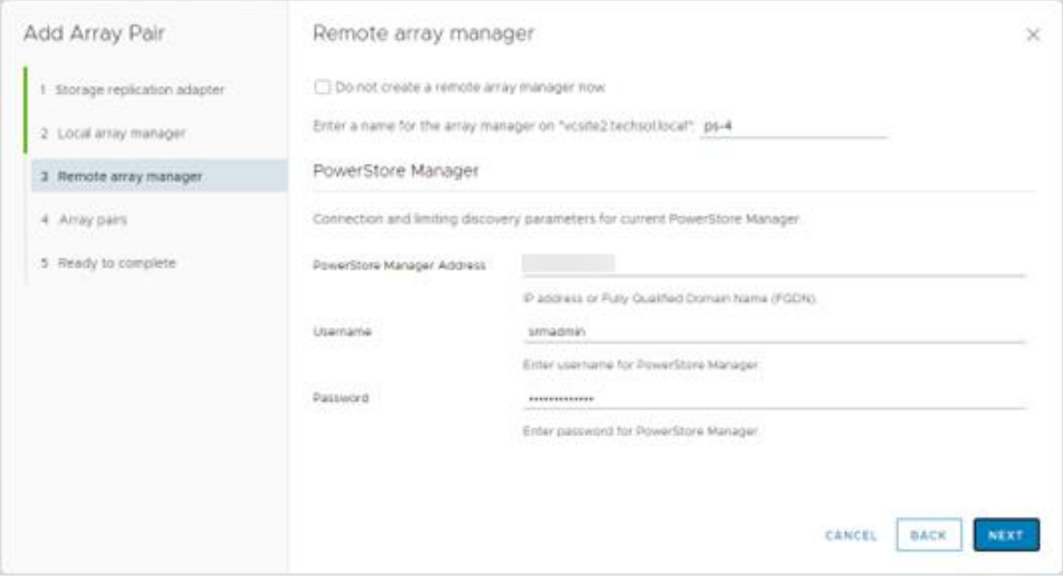
Username: srmadmin

Enter username for PowerStore Manager

Password: ••••••••••••••

Enter password for PowerStore Manager

3. Provide the **remote** PowerStore connection parameters for the remote array manager.



Add Array Pair

1 Storage replication adapter
2 Local array manager
3 Remote array manager
4 Array pairs
5 Ready to complete

Remote array manager

□ Do not create a remote array manager now

Enter a name for the array manager on "vcsite2.techsol.local": ps-4

PowerStore Manager

Connection and limiting discovery parameters for current PowerStore Manager

PowerStore Manager Address:
IP address or Fully Qualified Domain Name (FQDN)

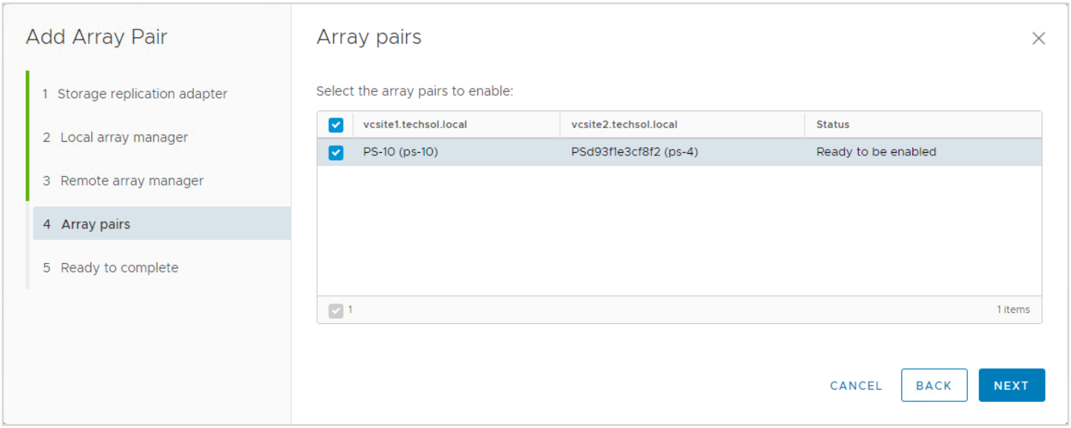
Username: srmadmin
Enter username for PowerStore Manager

Password: ••••••••••••••
Enter password for PowerStore Manager

CANCEL BACK NEXT

Creating array pairs

When an array manager is added to each of the two sites in SRM, the arrays must be paired so that replicated volumes can be discovered by SRM as eligible devices (see Figure 12). In older versions of SRM, pairing was performed after the initial installation of SRM. However, as of SRM 8.7, you can perform pairing as part of the process of adding array managers to sites.



Add Array Pair

1 Storage replication adapter
2 Local array manager
3 Remote array manager
4 Array pairs
5 Ready to complete

Array pairs

Select the array pairs to enable:

☑	vcsite1.techsol.local	vcsite2.techsol.local	Status
☑	PS-10 (ps-10)	PSd93f1e3cf8f2 (ps-4)	Ready to be enabled

☑ 1 1 items

CANCEL BACK NEXT

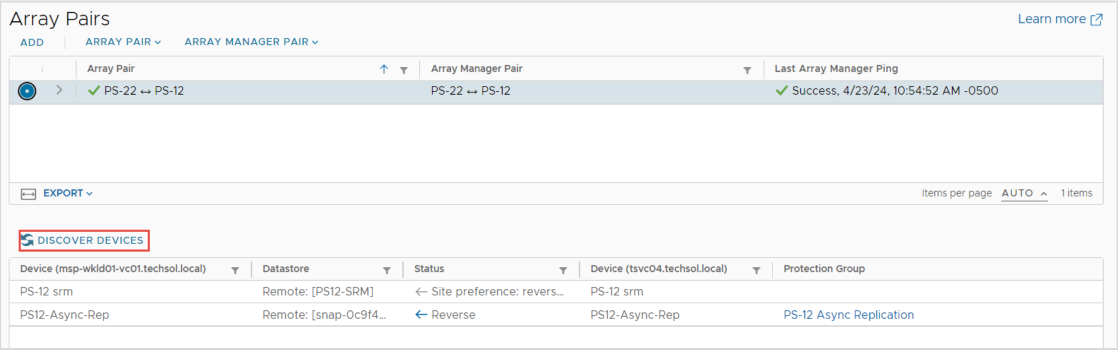
Figure 12. Creating array pairs

Arrays cannot be unpaired when there are downstream SRM dependencies such as protection groups.

Array manager device discovery

Whenever a new replicated datastore or RDM is added to the environment, the arrays should be rescanned within SRM for new devices. The array pair device discovery tool is located in the **Array Based Replication** > **Array Pairs** menu. Run the device discovery on both arrays to ensure a consistent list of devices. Non-replicated volumes are not discovered and displayed as eligible devices in SRM. Keep this in mind as a troubleshooting tip if datastores or RDMs are not listed as eligible devices in SRM. Conversely, SRM discovers all replicated volumes as devices.

Select **Discover Devices**, as shown in Figure 13, to invoke an SRA query of PowerStore to obtain the newest array-based replicated device information.



Array Pairs

Array Pair	Array Manager Pair	Last Array Manager Ping
✓ PS-22 ↔ PS-12	PS-22 ↔ PS-12	✓ Success, 4/23/24, 10:54:52 AM -0500

Device (msp-wkld01-vc01.techsol.local)	Datastore	Status	Device (tsvc04.techsol.local)	Protection Group
PS-12 srm	Remote: [PS12-SRM]	← Site preference: revers...	PS-12 srm	
PS12-Async-Rep	Remote: [snap-0c9f4...	← Reverse	PS12-Async-Rep	PS-12 Async Replication

Figure 13. Discover the devices of array pairs

Creating placeholder datastores

If not completed, create a small VMFS datastore at the disaster recovery site as a placeholder for VM configuration files. For each protected virtual machine, SRM creates a shadow VM at the recovery site. This VM serves as a placeholder for CPU, memory, and network resources required to perform a test, disaster recovery, or planned-migration plan.

Although this datastore must only be large enough to hold the configuration files for all the recoverable virtual machines, creating a standard-sized 500 GB datastore will suffice. PowerStore thinly provisions the volume, making this a space-efficient standard.

Note: The minimum PowerStore volume size is 1 MB. The minimum VMFS volume size is 2 GB. However, for practical reasons, the placeholder datastore should be at least 5 GB or larger. A smaller datastore will likely trigger ongoing vSphere datastore capacity alarms in the vSphere Client UI.

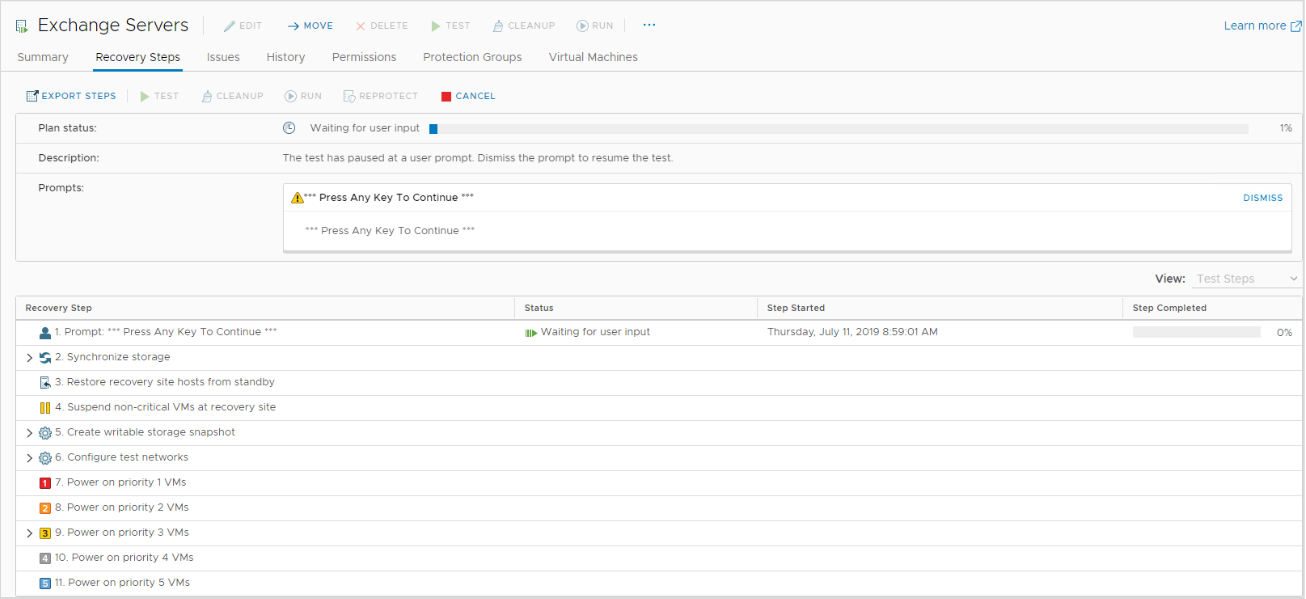
Typically, only one placeholder datastore per site is required. This is because the disaster recovery and migration processes unregister and reregister the recovered virtual machine with the .vmx file on the recovered volume. The placeholder volume does not need to be replicated or protected because VMware SRM places only transient data on this volume that can be easily regenerated within the UI.

Protection group considerations

With the placeholder datastore ready, you can create protection groups. Replicated datastore volumes are the foundation that protection groups are built upon. A protection group is effective immediately after being created. Once a VM is protected, it is essentially pinned to the datastore (or datastores) where the .vmx and .vmdk files reside. SRM does not support manually moving files that belong to a virtual machine off a datastore; the VM is not protected or replicated from its original datastore or datastores. Automated Storage DRS (SDRS) and VMware Storage vMotion can be sparingly used with SRM-protected VMs if certain guidelines are followed. See the VMware *Site Recovery Manager Administration Guide*.

Recovery plan considerations

When creating recovery plans, a best practice to further automate DR failover or planned migration may be to add prompts or SRM server-side commands to the recovery plan. The SRM server-side commands could be application-specific or related to storage management and integrate a PowerStore REST API or PSTCLI script into the recovery plan. When the recovery plan runs, it pauses on prompts while SRM server commands are performed without a pause, as shown in Figure 14.



Plan status: Waiting for user input 1%

Description: The test has paused at a user prompt. Dismiss the prompt to resume the test.

Prompts: *** Press Any Key To Continue *** DISMISS

*** Press Any Key To Continue ***

View: Test Steps

Recovery Step	Status	Step Started	Step Completed
1. Prompt: *** Press Any Key To Continue ***	Waiting for user input	Thursday, July 11, 2019 8:59:01 AM	0%
2. Synchronize storage			
3. Restore recovery site hosts from standby			
4. Suspend non-critical VMs at recovery site			
5. Create writable storage snapshot			
6. Configure test networks			
7. Power on priority 1 VMs			
8. Power on priority 2 VMs			
9. Power on priority 3 VMs			
10. Power on priority 4 VMs			
11. Power on priority 5 VMs			

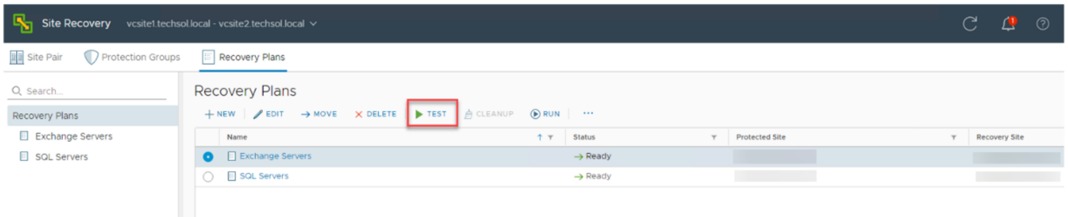
Figure 14. Recovery plan added step prompting to continue

Note: For more information about REST API, use SwaggerUI (https://<PowerStore>/swaggerui) or see the *REST API Developers Guide* and the *REST API Reference Guide* on the PowerStore Info Hub.

Recovery plan testing and running

Testing the recovery plan is not disruptive to the storage replications, production volumes, and VMs because the test plan uses thin clone volumes from replicated snapshots at the recovery site. When testing a recovery plan, any tests, changes, or updates can be performed on the recovered VMs because they are discarded when the test recovery plan cleanup occurs. While the test plan is running, production VMs and replication continue to run without interruption.

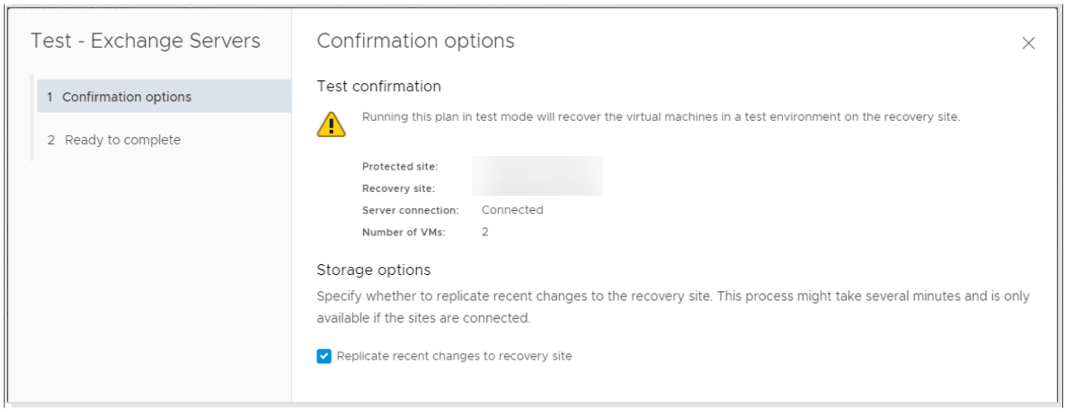
To test a disaster recovery plan, right-click the recovery plan, and click **Test**, as shown in Figure 15.



	Name	Status	Protected Site	Recovery Site
●	Exchange Servers	Ready	[redacted]	[redacted]
○	SQL Servers	Ready	[redacted]	[redacted]

Figure 15. Testing **a recovery plan**

When testing or running recovery plans, SRM does not have integrated mechanisms to determine whether the replicated volumes are fully synchronized before the storage is prepared for recovery. In other words, data may be actively replicating to the secondary site which could influence the outcome of the recovery. As a best practice, check **Replicate recent changes to recovery site** when running a test plan, as shown in Figure 16. This action ensures that all data is successfully replicated to the secondary site.



Test - Exchange Servers

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: [redacted]
Recovery 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.

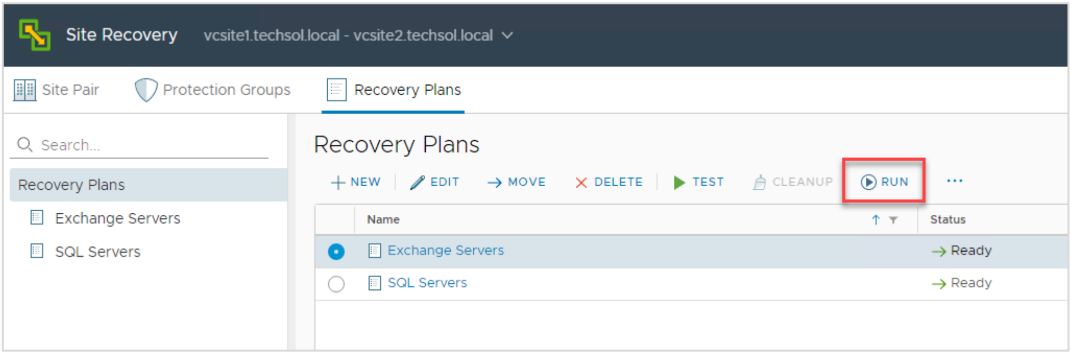
☑ Replicate recent changes to recovery site

Figure 16. Replicate recent changes to recovery site during test plans

Note: The Replicate recent changes feature results in a longer running plan. The extra time is used to synchronize the volumes between sites. During a disaster-recovery cutover, the Replicate recent changes to recovery site option may or may not be available. For planned migrations using SRM, this step is required to proceed.

When choosing to run a planned migration or disaster recovery plan (as opposed to running a test), keep in mind this procedure is disruptive. It results in VMs being powered off at the primary site, replication mirrors being broken, and VMs being recovered at the secondary site.

1. In the event of a disaster or planned migration, right-click the recovery plan, and click **Run**.



Recovery Plans
- Exchange Servers
- SQL Servers

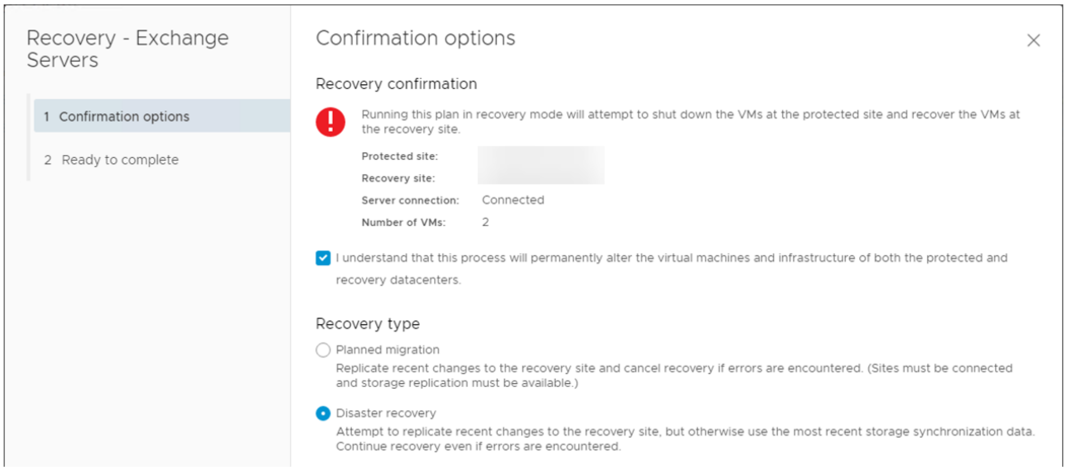
Recovery Plans

	Name	Status
●	Exchange Servers	Ready
○	SQL Servers	Ready

Note: Before running a planned migration plan, run a test recovery of the plan.

2. Acknowledge the safety precaution message to run a live plan.

Confirmation of recovery process. When the process is started, virtual machines will start to failover.



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:	[redacted]
Recovery site:	
Server connection:	Connected
Number of VMs:	2

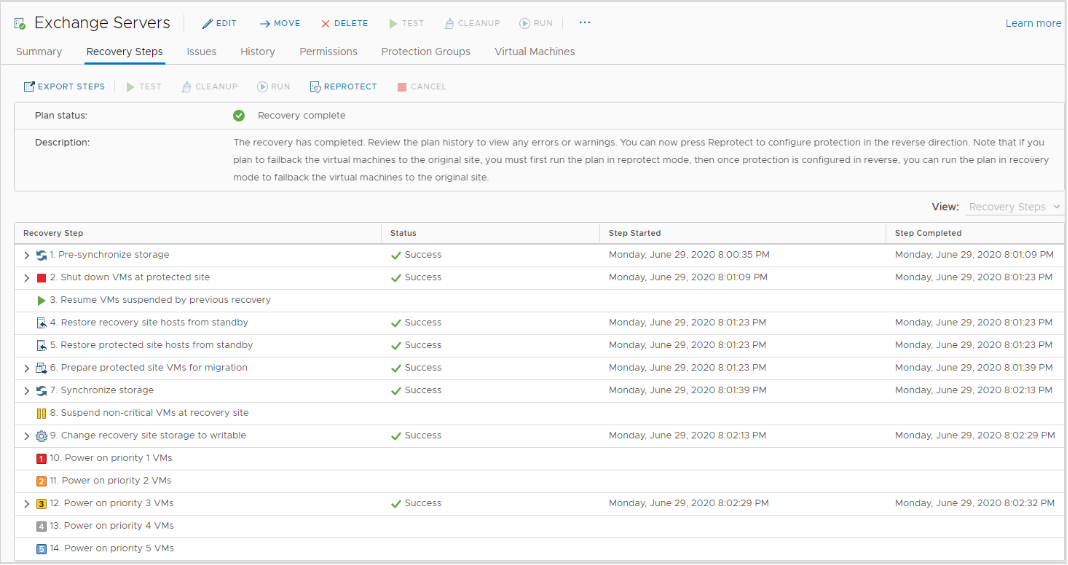
☑ I understand that this process will permanently alter the virtual machines and infrastructure of both the protected and recovery datacenters.

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.

3. Review the success of the recovery plan after it completes.



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 Steps

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize storage	✓ Success	Monday, June 29, 2020 8:00:35 PM	Monday, June 29, 2020 8:01:09 PM
2. Shut down VMs at protected site	✓ Success	Monday, June 29, 2020 8:01:09 PM	Monday, June 29, 2020 8:01:23 PM
3. Resume VMs suspended by previous recovery			
4. Restore recovery site hosts from standby	✓ Success	Monday, June 29, 2020 8:01:23 PM	Monday, June 29, 2020 8:01:23 PM
5. Restore protected site hosts from standby	✓ Success	Monday, June 29, 2020 8:01:23 PM	Monday, June 29, 2020 8:01:23 PM
6. Prepare protected site VMs for migration	✓ Success	Monday, June 29, 2020 8:01:23 PM	Monday, June 29, 2020 8:01:39 PM
7. Synchronize storage	✓ Success	Monday, June 29, 2020 8:01:39 PM	Monday, June 29, 2020 8:02:13 PM
8. Suspend non-critical VMs at recovery site			
9. Change recovery site storage to writable	✓ Success	Monday, June 29, 2020 8:02:13 PM	Monday, June 29, 2020 8:02:29 PM
10. Power on priority 1 VMs			
11. Power on priority 2 VMs			
12. Power on priority 3 VMs	✓ Success	Monday, June 29, 2020 8:02:29 PM	Monday, June 29, 2020 8:02:32 PM
13. Power on priority 4 VMs			
14. Power on priority 5 VMs			

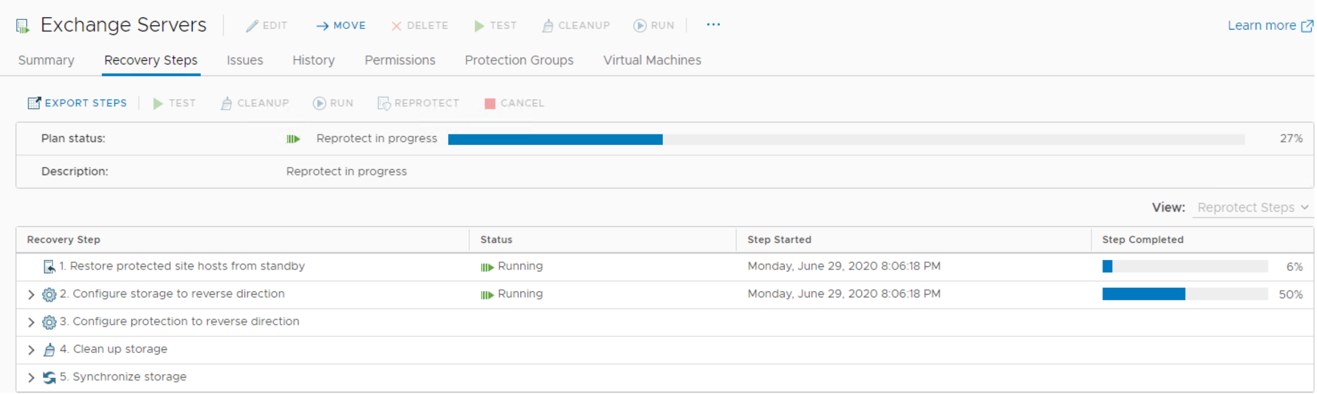
Reprotect and failback

Introduction

After VMs are migrated to another site using the disaster-recovery or planned-migration features in SRM, they are in an active running state on the network at the alternate site. However, they are vulnerable to a site failure with no SRM protection. Previous versions of SRM required a manual reprotection of the VMs at the recovery site. Today, SRM automates the reprotection process and prepares the virtual machines for failback.

Reprotection

After protected VMs are migrated or failed over to the secondary site as part of disaster recovery, the VMs are unprotected and are no longer replicated to a recovery site. Following the migration of protected virtual machines, SRM enables automating the reprotection of the VMs. The reprotection is carried out in a series of automated steps, as shown in Figure 17.



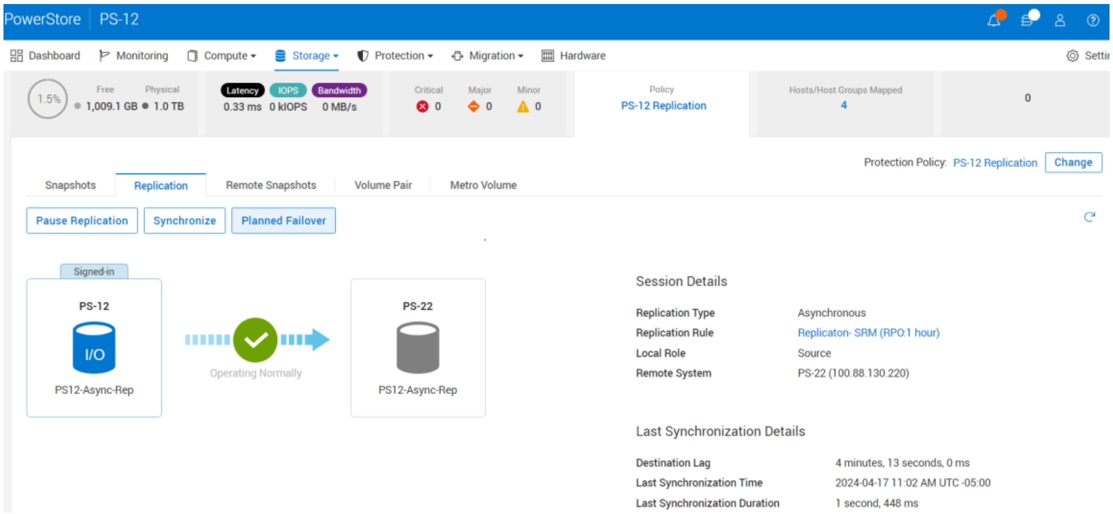
Plan status: Reprotect in progress 27%

Description: Reprotect in progress

Recovery Step	Status	Step Started	Step Completed
1. Restore protected site hosts from standby	Running	Monday, June 29, 2020 8:06:18 PM	6%
2. Configure storage to reverse direction	Running	Monday, June 29, 2020 8:06:18 PM	50%
3. Configure protection to reverse direction			
4. Clean up storage			
5. Synchronize storage			

Figure 17. **Reprotect workflow of the Exchange Servers protection group being performed**

During a reprotect, SRM commands the SRA to start storage replication for each of the datastores or volumes in the protection group. This action occurs in the opposite direction compared to the replication topology before the failover. The protection group that was originally set up at the primary site is migrated to the secondary site. Placeholder VMs that were originally set up at the secondary site are now created at the opposite site (the new recovery site) on its respective placeholder datastore (Figure 18).



Session Details

Replication Type	Asynchronous
Replication Rule	Replicaton- SRM (RPO:1 hour)
Local Role	Source
Remote System	PS-22 (100.88.130.220)

Last Synchronization Details

Destination Lag	4 minutes, 13 seconds, 0 ms
Last Synchronization Time	2024-04-17 11:02 AM UTC -05:00
Last Synchronization Duration	1 second, 448 ms

Figure 18. **Replication direction and session status can be monitored in PowerStore Manager**

Failback

Failback is an SRM term that describes the ability to perform a subsequent disaster recovery or planned migration after a successful recovery and reprotect. The benefit that failback introduced in SRM 5.x is the automated ability to move back and forth between sites with minimal effort. This capability facilitates several use cases including the ability to run production applications at the disaster recovery site, resource balancing, and improved disaster recovery infrastructure ROI.

Note: Before running the Failback recovery plan, run a test recovery of the plan.

Asynchronous replication for vVol based VMs

Introduction

PowerStore supports VASA 4.0 native storage based asynchronous replication for vVol based VMs. This feature uses VMware Storage Policies and requires VMware Site Recovery Manager instances in both sites. The following section gives a brief overview how vVol replication is implemented in PowerStoreOS. See also the PowerStore VMware integration White Paper for vVol based VMs or VMware Site Recovery Manager product documentation.

Licensing

Asynchronous replication of vVol based VMs is included at no extra cost for supported PowerStore clusters.

Theory of operation

The configuration of asynchronous replication for vVol based VMs requires a remote system pair as describe in an earlier section configured for two PowerStore Model T clusters running PowerStoreOS 4.0 or later. Each of the PowerStore Clusters for vVol replication needs registration in vCenter as a storage provider. VASA 4.0 API is used to exchange information between PowerStore Cluster and the associated vCenter. The VMware Storage Policy which could be assigned to VMs in vCenter leverage the same replication rules in PowerStore Manager as used for other PowerStore asynchronous replications. Asynchronous replication for vVol based VMs also use the same snapshot based async replication technology as native block replication which is described in section native asynchronous block replication. Once a VMware Storage Policy with PowerStore replication is assigned to a vVol based VM, a replication session is created on PowerStore for VM vVol resources in the same resource group. VMware resource groups can be selected when a VMware Storage Policy is configured for a VM. VMware SRM uses these VMware resource groups to manage the protected VMs in Replication Groups. An SRM Recovery Plan controls the PowerStore replication session for vVols in a replication group during test failover, failover, and reprotection. After a VM has a VMware Storage Policy assigned, and the Resource Group is in a Replication Group with Protection Plan in SRM, a placeholder VM on destination vCenter and PowerStore is created. The storage container for placeholder VM is part of the site pair configuration in SRM.

Supported replication flows

For replication of Resource Groups on PowerStore different combinations of source and destination vVol Storage Container are possible.

- One or more Resource Groups from a single Storage Container to a single Storage Container on a different PowerStore cluster
- One or more different Resource Groups on a single Storage Container to different Storage Container on different PowerStore clusters
- Resource Groups from Storage Containers on different PowerStore clusters to a single Storage Container
- Multiple replications in different directions
- Combinations of all of the above.

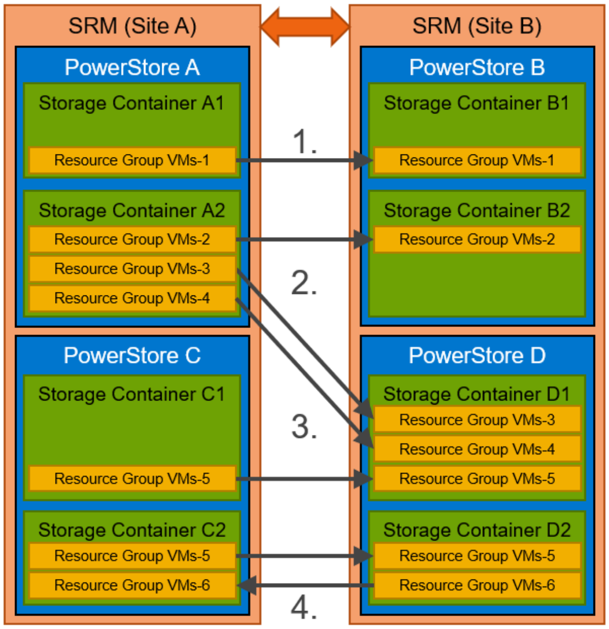


Figure 19. Supported replication flows

Replication Operations

The main operations for a protected VM are available in VMware SRM only. This section provides an overview of available Operations in PowerStore Manager and VMware Site Recovery Manager.

vVol replication operations in PowerStore Manager

Operations for a replication session in PowerStore Manager always affect all vVols in the same resource group. A resource group is configured during the protection of a VM when assigning the VMware Protection Policy in vCenter.

Synchronize

With Synchronize operations, a manual replication is executed for all vVols in the replication group covered by the replication session.

Pause

This operationpauses the replication session for all vVols in the replication group at the current state. After pausing a vVol replication session, the scheduled RPO replications are disabled.

Resume

The resume operation resumes a paused replication. It also enables the schedules for RPO based replications.

vVol replication operations in VMware SRM

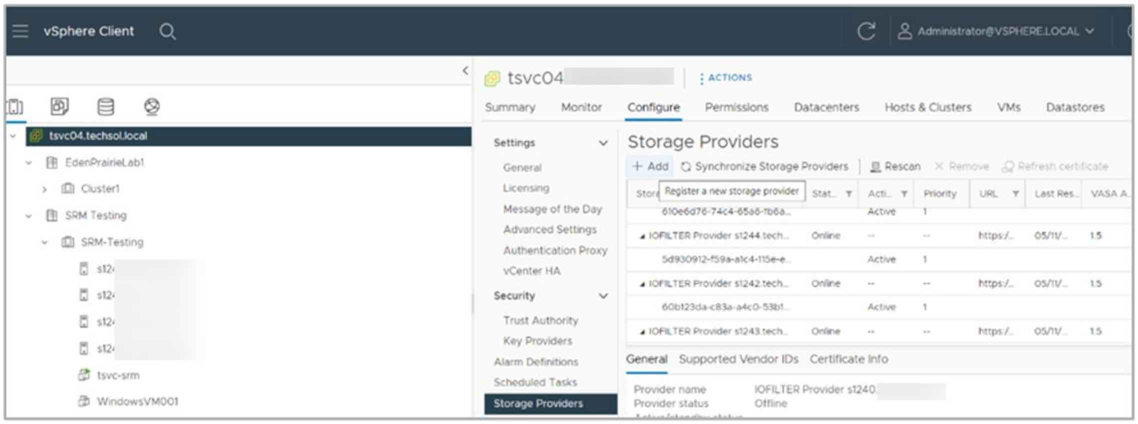
All vVol replication operations in SRM are based on an underlying Replication Group. Each Replication Group can contain multiple resources groups.

vVol Replication configuration

VASA Provider

vSphere API for Storage Awareness (VASA) is a VMware-defined and vendor-neutral API that enables vSphere to determine the capabilities of a storage system. The API requests basic storage information from PowerStore, which is used for monitoring and reporting storage details to the user in vSphere. PowerStore includes a native VASA 4.0 provider, which enables the vVols storage framework. The VASA provider must be registered in vSphere to use vVols. This registration can be done as part of the vCenter server connection process in PowerStore Manager.

- To register the VASA provider directly from PowerStore Manager, browse to **Compute** > **vCenter Server Connection.**
- To register the VASA provider in vSphere, browse to **vCenter** > **Storage Providers** > **Configure**. Click **Add** and provide the information as shown in Figure 20.



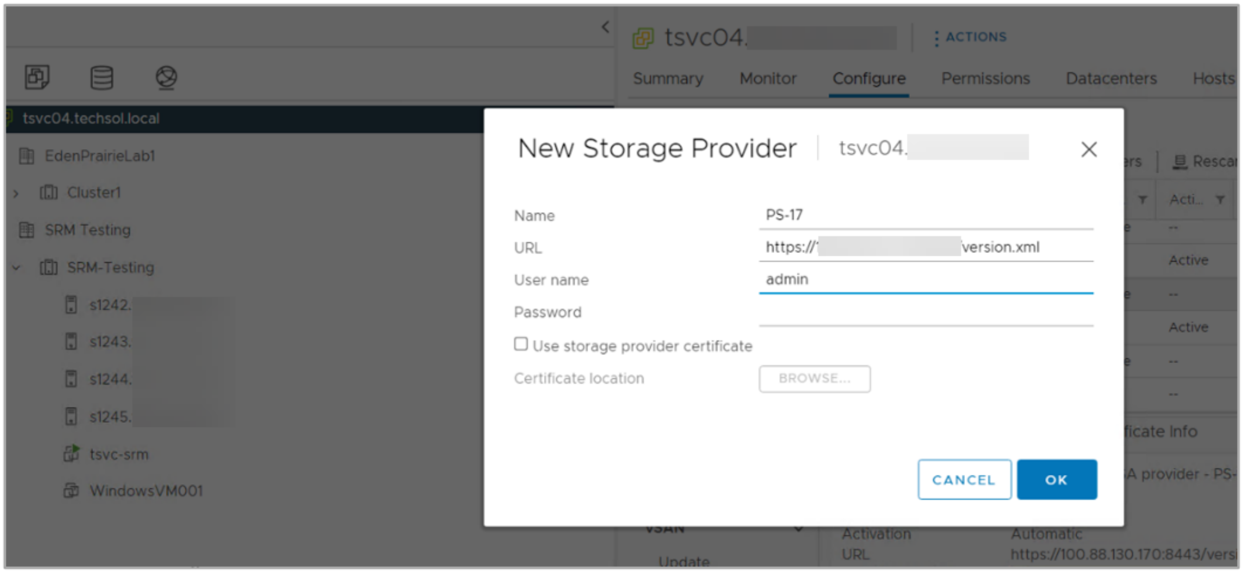
Storage Providers

Stor	Stat...	Acti...	Priority	URL	Last Res...	VASA A...
610e6d76-74c4-65a6-1b6a...		Active	1			
IOFILTER Provider s1244.tech...	Online	--	--	https:/...	05/11/...	1.5
5d930912-f59a-a1c4-115e-e...		Active	1			
IOFILTER Provider s1242.tech...	Online	--	--	https:/...	05/11/...	1.5
60b123da-c83a-a4c0-53b1...		Active	1			
IOFILTER Provider s1243.tech...	Online	--	--	https:/...	05/11/...	1.5

Provider name IOFILTER Provider s1240.[redacted]
Provider status Offline

Figure 20. Add Storage Provider to vCenter

Note: vCenter Server registers the storage provider and establishes a secure SSL connection with it.



New Storage Provider | tsvc04.[redacted]

Name: PS-17

URL: https://[redacted]version.xml

User name: admin

Password:

☐ Use storage provider certificate

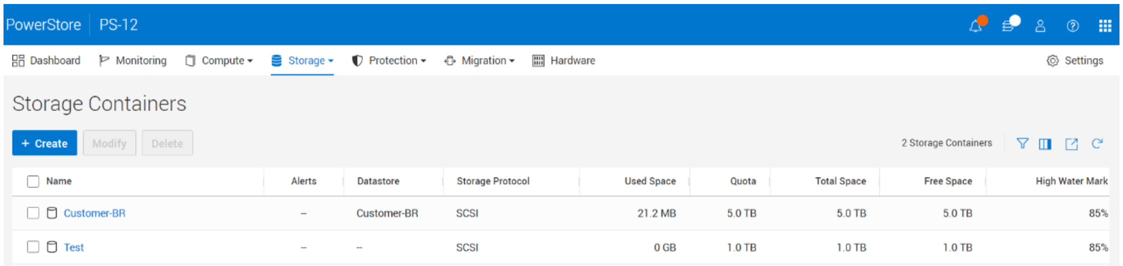
Certificate location: BROWSE...

CANCEL   OK

Figure 21. Storage Provider configuration

Storage containers

A storage container is used to present vVol storage from PowerStore to vSphere. vSphere mounts the storage container as a vVol datastore and makes it available for VM storage.



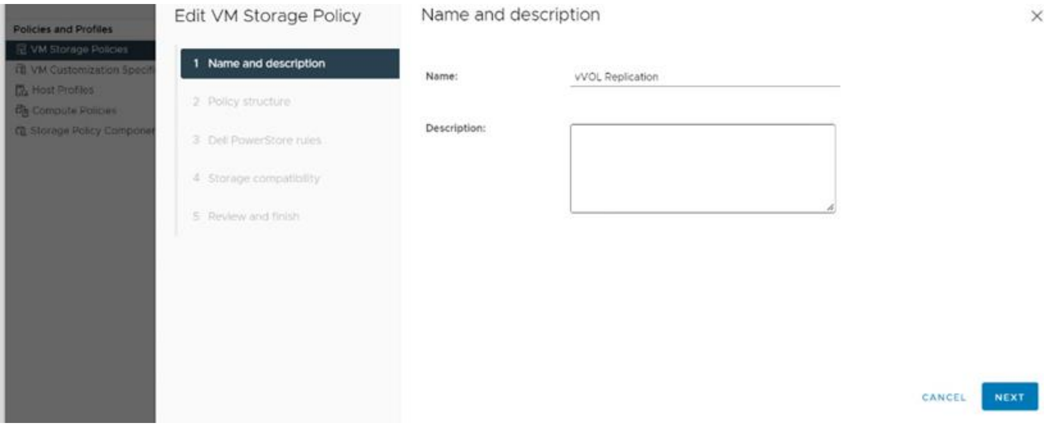
Storage Containers

Name	Alerts	Datastore	Storage Protocol	Used Space	Quota	Total Space	Free Space	High Water Mark
Customer-BR	–	Customer-BR	SCSI	21.2 MB	5.0 TB	5.0 TB	5.0 TB	85%
Test	–	–	SCSI	0 GB	1.0 TB	1.0 TB	1.0 TB	85%

Figure 22. PowerStore Manager showing Storage Containers

Policy Based Management

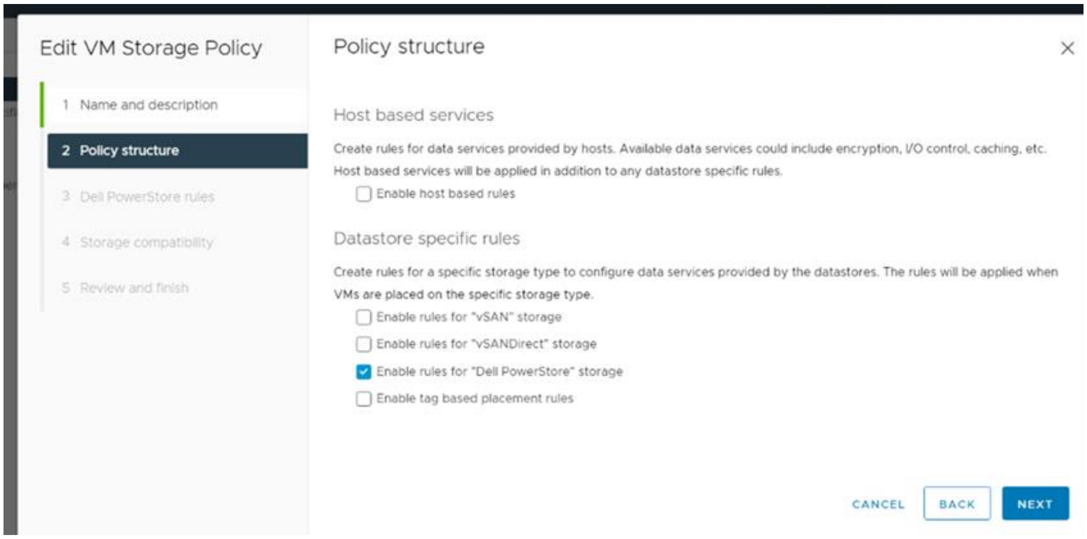
vVols leverage Storage Policy Based Management (SPBM) to ensure VMs have the appropriate storage and replication capabilities. After you configure your virtual volumes storage for replication, information about replication capabilities and replication groups is delivered from the array by the storage provider. To create a storage policy, go to the **Policies and Profiles** > **VM Storage Polices** page in vSphere. Click **Create VM Storage Policy.**



Name: vVOL Replication

Description:

Figure 23. Create a vVOL replication policy



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

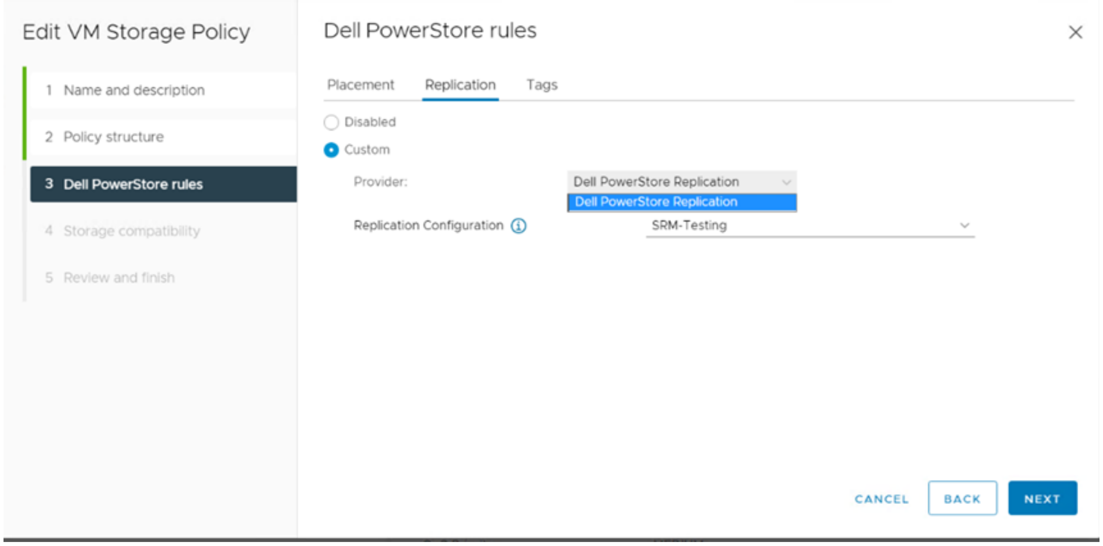
☐ Enable rules for "vSANDirect" storage

☑ Enable rules for "Dell PowerStore" storage

☐ Enable tag based placement rules

Figure 24. Enable rules for DELL.POWERSTORE.VVOL storage

This shows selecting the replication provider which is Dell PowerStore replication.



○ Disabled

● Custom

Provider: Dell PowerStore Replication

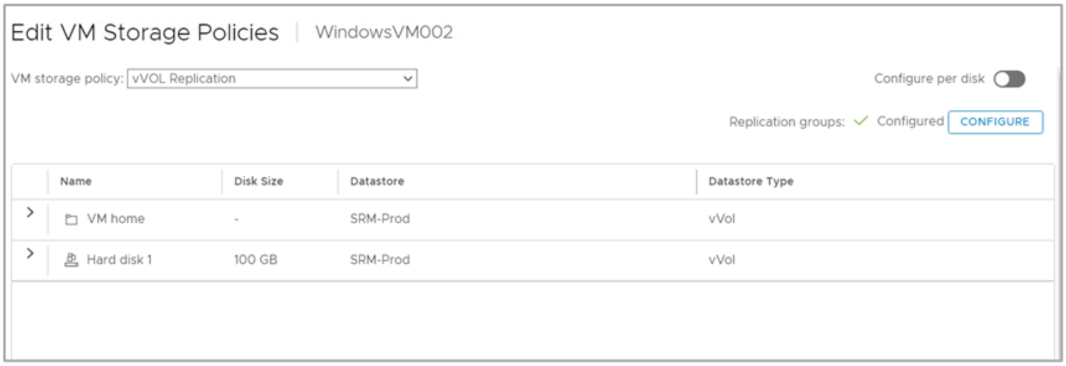
Dell PowerStore Replication

Replication Configuration ⓘ SRM-Testing

Figure 25. Select Replication, enable Dell PowerStore Provide

Automatic VM Protection

After configuring the replication policy and the PowerStore replication partner, you are ready to protect virtual machines. When applying the replication policy to a virtual machine, that virtual machine will be replicated to the target array. Virtual machines deployed on vVol with replication storage policies will automatically be protected by SRM.



Edit VM Storage Policies | WindowsVM002

VM storage policy: vVOL Replication

Configure per disk

Replication groups: ✓ Configured

Name	Disk Size	Datastore	Datastore Type
VM home	-	SRM-Prod	vVol
Hard disk 1	100 GB	SRM-Prod	vVol

Figure 26. Confirm VM storage policy is set

Note: The Replication session will also be displayed in PowerStore Manager.

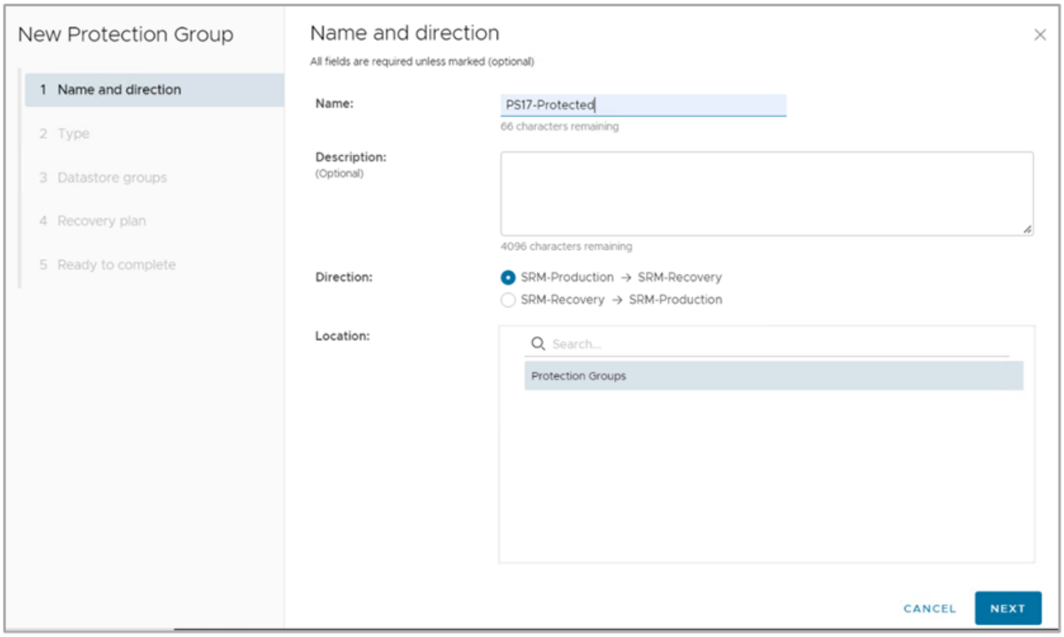
vVOL with SRM

Introduction

With Dell Technologies and VMWare's tight integration of vVols with SRM, there is no need for a Storage Replication Adaptor (SRA). The VASA provider handles all operations with the PowerStore array. Replication configuration and management can be done directly from vCenter and it integrates fully with policy-based management and virtual machine template deployments.

Protection

vVol protection with SRM contains the same processes as using array-based replication, which is covered in this document. With fault domains in place and associated storage policies, protection is simplified with assigning a storage policy to the virtual machine and placing it onto storage that complies with that policy. The following screenshots show the workflow steps within SRM to create protection groups and recovery plans.



New Protection Group

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

Name and direction

All fields are required unless marked (optional)

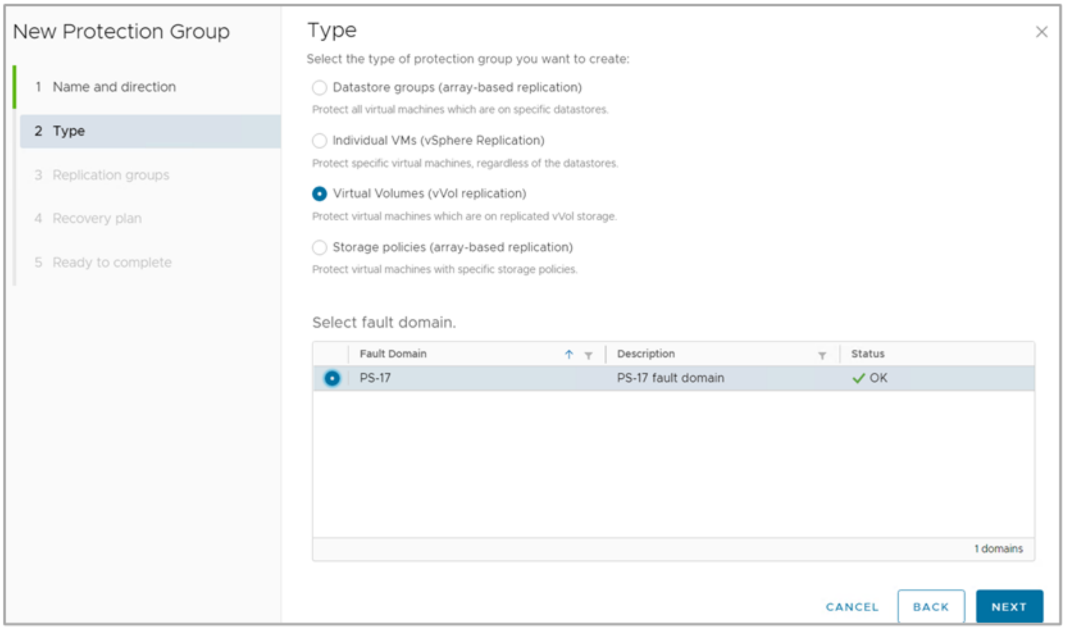
Name: PS17-Protected
66 characters remaining

Description:
(Optional)
4096 characters remaining

Direction:
● SRM-Production → SRM-Recovery
○ SRM-Recovery → SRM-Production

Location:
Search...
Protection Groups

Figure 27. **Create Protection Group**



New Protection Group

1 Name and direction
2 Type
3 Replication 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.

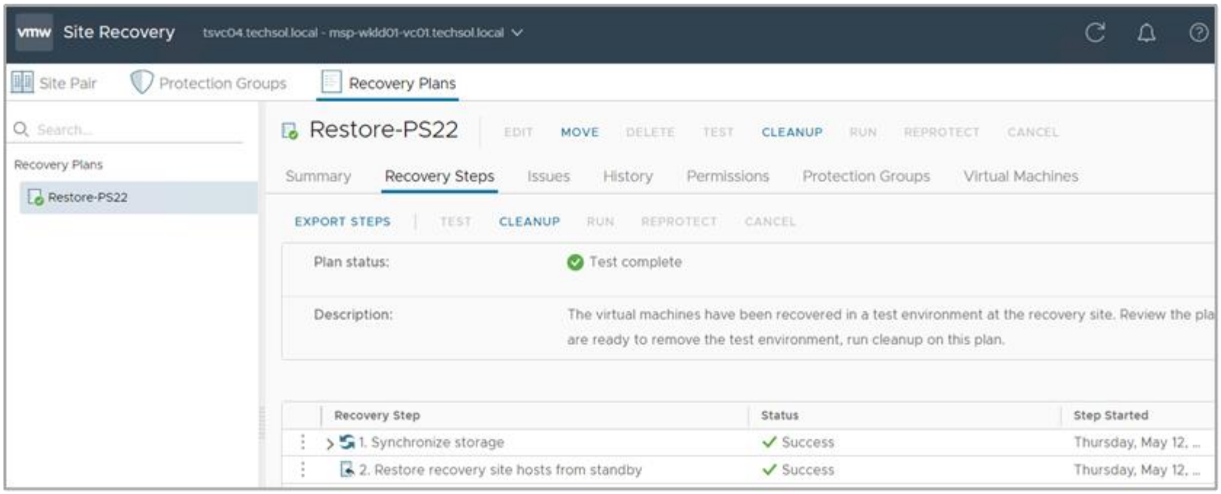
Select fault domain.

	Fault Domain	Description	Status
●	PS-17	PS-17 fault domain	✓ OK

1 domains

Figure 28. **Select vVol replication and Fault Domain**

Note: When using vVols protection groups, SRM checks both the recovery and the protection site and matches the vVols configurations that can be used.



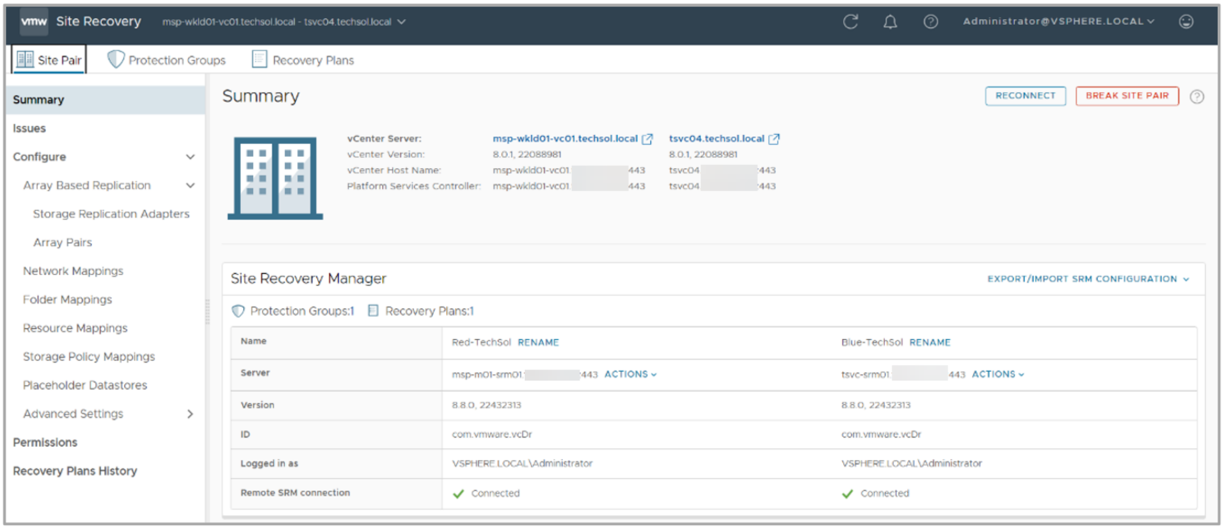
Restore-PS22

Plan status: ✓ Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. Review the pla are ready to remove the test environment, run cleanup on this plan.

Recovery Step	Status	Step Started
1. Synchronize storage	✓ Success	Thursday, May 12, ...
2. Restore recovery site hosts from standby	✓ Success	Thursday, May 12, ...

Figure 29. Testing a recovery plan



Summary

vCenter Server:	msp-wkld01-vc01.techsol.local	tsvc04.techsol.local
vCenter Version:	8.0.1, 22088981	8.0.1, 22088981
vCenter Host Name:	msp-wkld01-vc01.[redacted]443	tsvc04[redacted]443
Platform Services Controller:	msp-wkld01-vc01.[redacted]443	tsvc04[redacted]443

Site Recovery Manager

Protection Groups:1 Recovery Plans:1

Name	Red-TechSol RENAME	Blue-TechSol RENAME
Server	msp-m01-srm01.[redacted]443 ACTIONS	tsvc-srm01.[redacted]443 ACTIONS
Version	8.8.0, 22432313	8.8.0, 22432313
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

Figure 30. Site Recovery Main Screen

PowerStore Metro Volume configuration

Overview

Starting with PowerStoreOS 4.0 and storage replication adapter version 2.1.1.388, Site Recovery Manager supports cross vCenter migration with PowerStore Metro Volume stretched storage. Metro Volume is an active-active synchronous replication that supports Recovery Point Objectives and Recovery Time Objectives of zero in migration or disaster avoidance scenarios. For best practices regarding Metro Volume (uniform/non-uniform configurations, latency, workload mobility, and so on), see the white paper Dell PowerStore: Metro Volume.

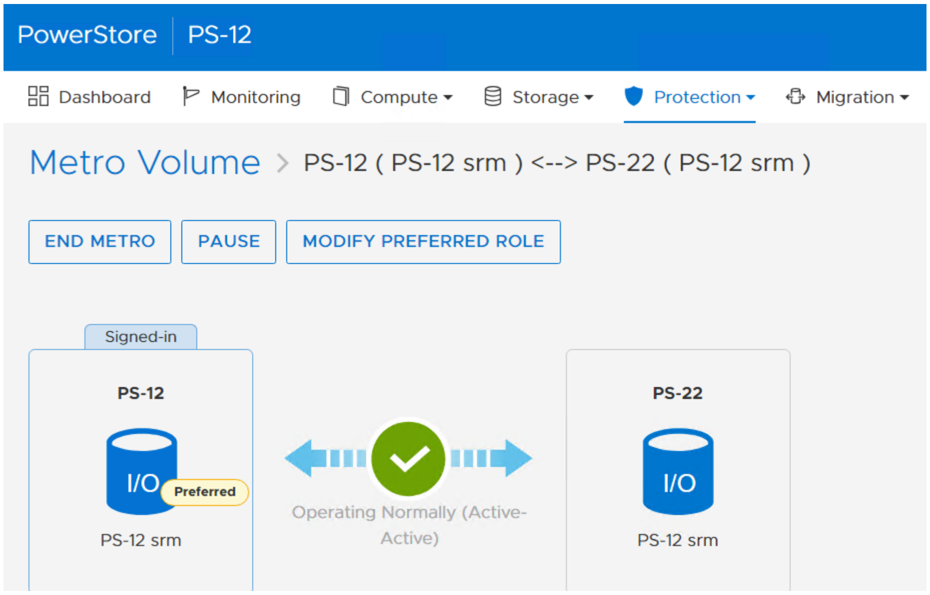
Note: Stretched storage is supported only on vCenter Single Sign-On Enhanced Linked Mode environments.

Metro Volume

Metro Volume uses a symmetric active-active architecture. Read and write I/O can occur directly on either PowerStore cluster hosting the Metro Volume. Bi-directional synchronous replication ensures the volumes on both clusters are synchronized during normal operation. The screenshots below illustrate the workflow steps within SRM to create protection groups, recovery plan, and planned migration with Metro Volume protected workloads.

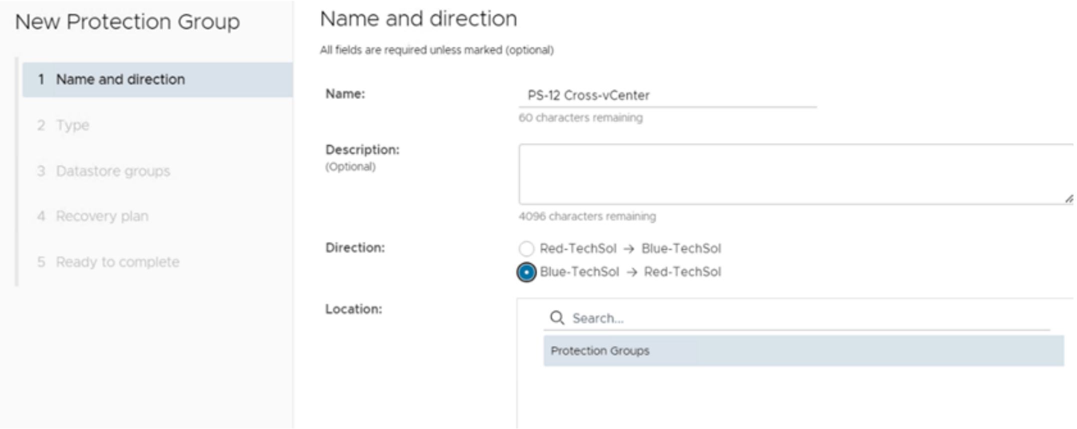
Metro Volume Protection

When a Metro Volume is set up in PowerStore Manager, the Metro Volume appears in Metro overview screen **Protection > Metro**.



Configure Protection Group

Select the source vCenter where the VMs are located, to the target vCenter recovery site, as shown in Figure 31.



Name and direction

All fields are required unless marked (optional)

Name: PS-12 Cross-vCenter

60 characters remaining

Description: (Optional)

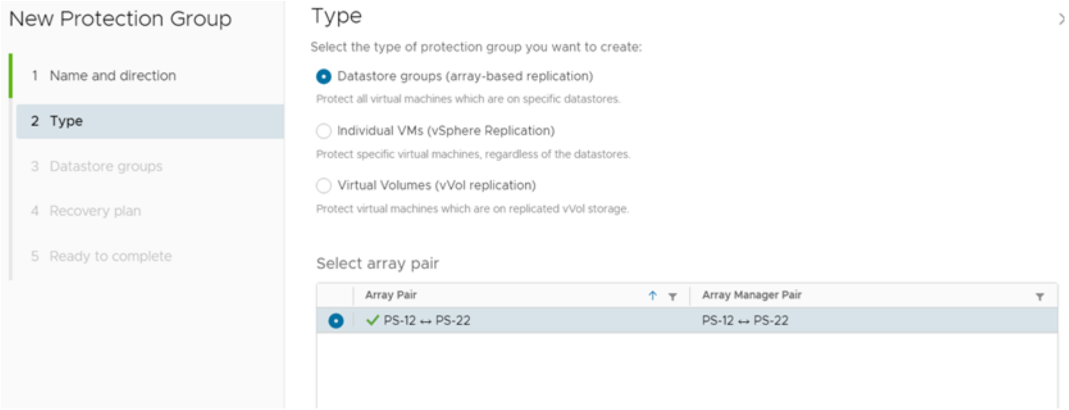
4096 characters remaining

Direction:
○ Red-TechSol → Blue-TechSol
● Blue-TechSol → Red-TechSol

Location:
Search...
Protection Groups

Figure 31. New Protection Group workflow – Name and direction.

Specify the type of protection. Select **Datastore groups** to leverage array-based replication.



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)

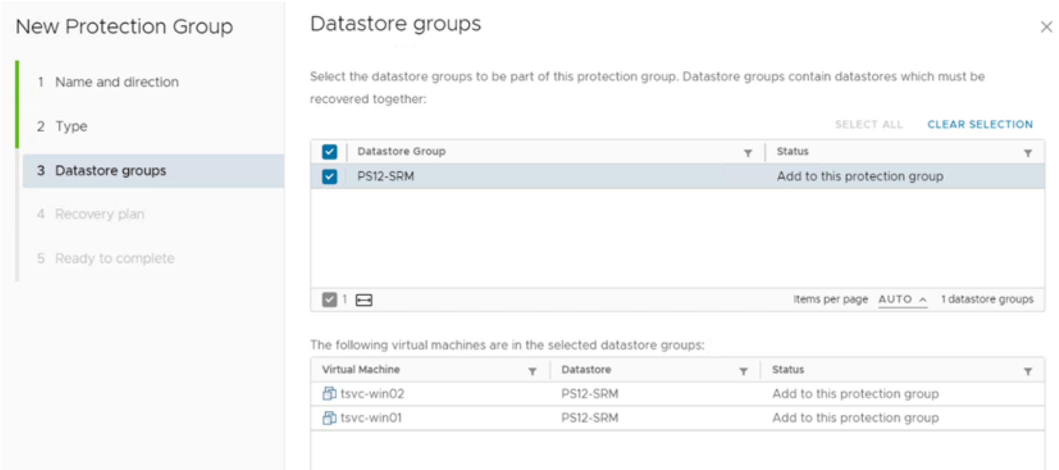
Protect virtual machines which are on replicated vVol storage.

Select array pair

	Array Pair	Array Manager Pair
●	✓ PS-12 ↔ PS-22	PS-12 ↔ PS-22

Figure 32. New Protection Group workflow – Select Type

Select the datastore group that contains virtual machines to be protected.



New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Datastore groups

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

SELECT ALL CLEAR SELECTION

☑	Datastore Group	Status
☑	PS12-SRM	Add to this protection group

☑ 1 Items per page AUTO 1 datastore groups

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
tsvc-win02	PS12-SRM	Add to this protection group
tsvc-win01	PS12-SRM	Add to this protection group

Figure 33. New Protection Group workflow – Select datastore groups

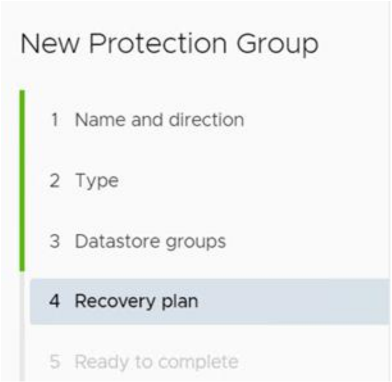
Recovery Plan Testing

Cross vCenter Planned Migration

When testing a recovery plan, the virtual machines will run on a test network and PowerStore does support creating read-write snapshots, allowing Site Recovery Manager to perform a test recovery with the Metro Volume devices.

A recovery operation will attempt a vMotion of the virtual machines in the stretched protection group/recovery plan. The following are two key points during recovery plan testing:

- Test recovery is performed by using the regular test recovery workflow.
- Recovers virtual machines to the recovery site while both sites are running



New Protection Group

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Recovery plan

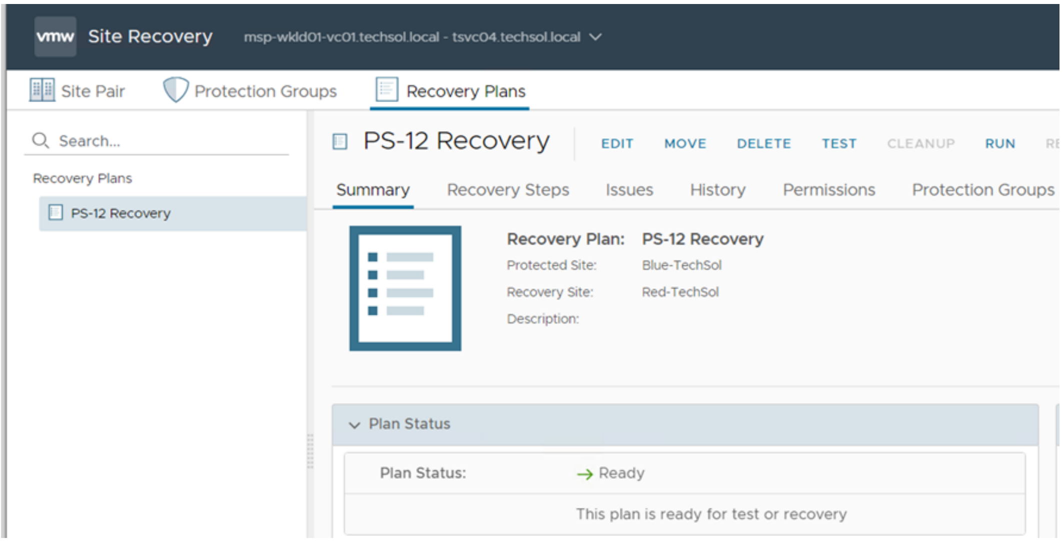
You can optionally add this protection group to a recovery plan.

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

Recovery plan name: PS-12 Recovery

66 characters remaining

Figure 34. Create New Recovery Plan



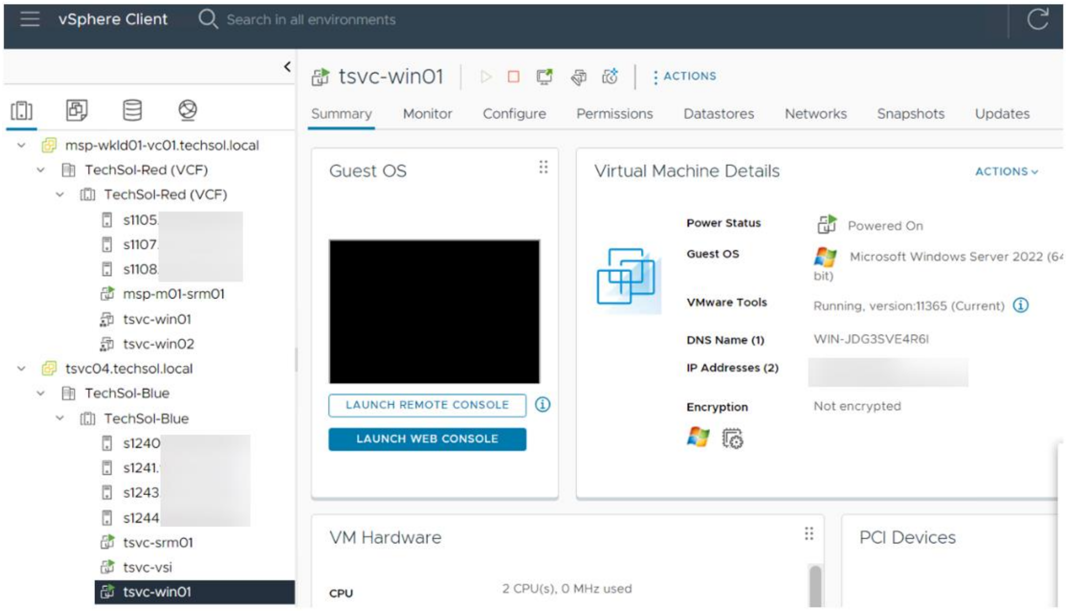
PS-12 Recovery

Recovery Plan: PS-12 Recovery
Protected Site: Blue-TechSol
Recovery Site: Red-TechSol
Description:

Plan Status: → Ready

This plan is ready for test or recovery

Figure 35. PS-12 recovery plan created

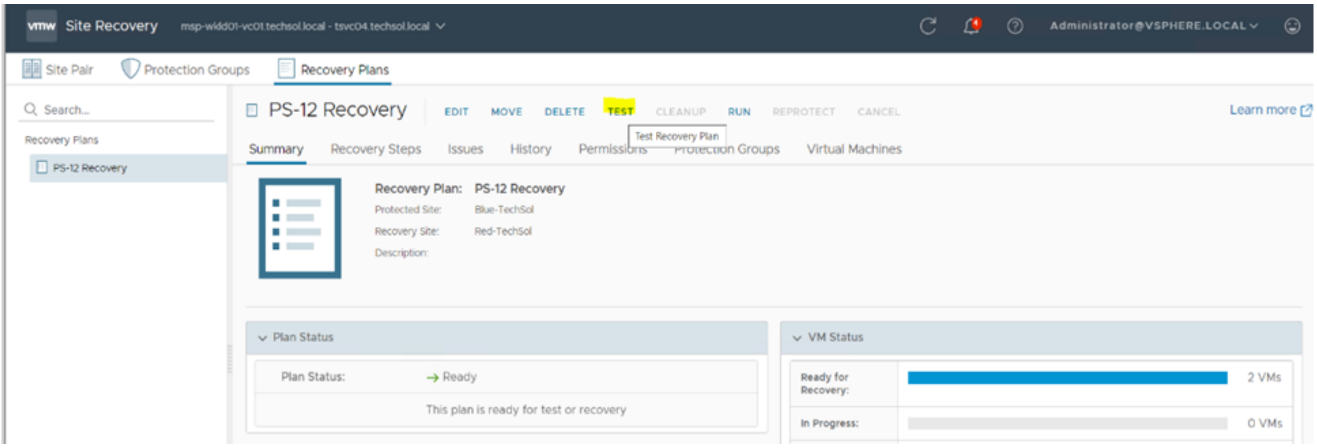


Power Status: Powered On
Guest OS: Microsoft Windows Server 2022 (64 bit)
VMware Tools: Running, version:11365 (Current)
DNS Name (1): WIN-JDG3SVE4R6I
IP Addresses (2): [redacted]
Encryption: Not encrypted

CPU: 2 CPU(s), 0 MHz used

Figure 36. vCenters in linked mode

Note: TechSol Blue is a protected site and TechSol-Red is a recovery site. The test recovery will start the cross-vcenter migration workflow.

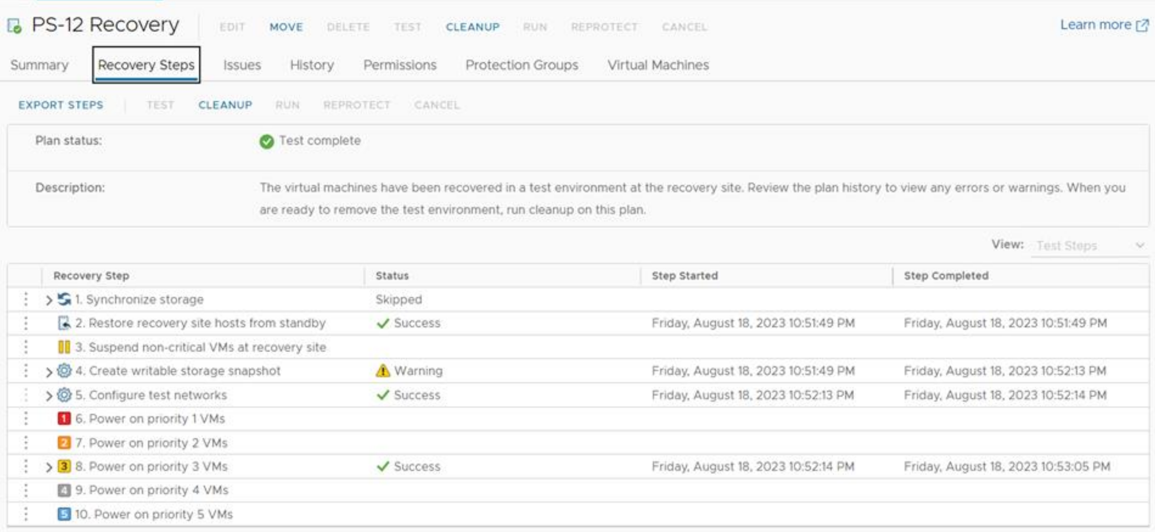


Recovery Plan: PS-12 Recovery
Protected Site: Blue-TechSol
Recovery Site: Red-TechSol
Description:

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

Ready for Recovery: 2 VMs
In Progress: 0 VMs

Figure 37. Select Test from the Recovery Plan page



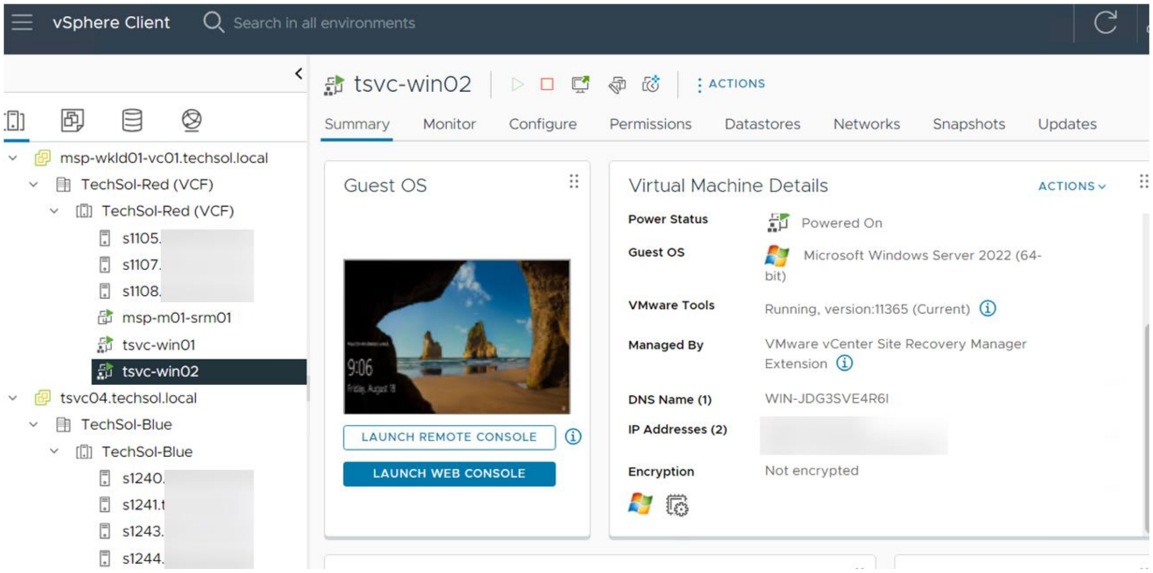
Plan status: ✓ Test complete

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.

View: Test Steps

Recovery Step	Status	Step Started	Step Completed
1. Synchronize storage	Skipped		
2. Restore recovery site hosts from standby	✓ Success	Friday, August 18, 2023 10:51:49 PM	Friday, August 18, 2023 10:51:49 PM
3. Suspend non-critical VMs at recovery site			
4. Create writable storage snapshot	⚠ Warning	Friday, August 18, 2023 10:51:49 PM	Friday, August 18, 2023 10:52:13 PM
5. Configure test networks	✓ Success	Friday, August 18, 2023 10:52:13 PM	Friday, August 18, 2023 10:52:14 PM
6. Power on priority 1 VMs			
7. Power on priority 2 VMs			
8. Power on priority 3 VMs	✓ Success	Friday, August 18, 2023 10:52:14 PM	Friday, August 18, 2023 10:53:05 PM
9. Power on priority 4 VMs			
10. Power on priority 5 VMs			

Figure 38. Test Completed with Recovery Steps



Power Status	Powered On
Guest OS	Microsoft Windows Server 2022 (64-bit)
VMware Tools	Running, version:11365 (Current)
Managed By	VMware vCenter Site Recovery Manager Extension
DNS Name (1)	WIN-JDG3SVE4R6I
IP Addresses (2)	[redacted]
Encryption	Not encrypted

Figure 39. VMs now running in the recovery site, TechSol-Red

Note: The datastores were presented to the recovery host prior to the test recovery and vMotion is enabled. The recovery plan will hang on the step **Prepare stretched storage** if the storage is not presented in the recovery environment.

Conclusion

VMware Site Recovery Manager works in conjunction with Dell PowerStore solutions to automate the process of recovering, testing, migrating and failing-back virtual machine workloads.

References

Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell Technologies storage platforms.

The PowerStore Info Hub provides detailed documentation on how to install, configure, and manage PowerStore systems.

PowerStore snapshot and replication-related resources:

- Replication Technologies
- Snapshots and Thin Clones
- Dell PowerStore: Metro Volume

VMware support

For VMware support, see the following resources:

- VMware.com
- VMware support
- Education and training
- Online documentation
- VMware communities