Technical Report

Deploying VMware vCenter Site Recovery Manager 6 on Clustered Data ONTAP

Kristopher Groh, NetApp

March 2016 | TR-4264-0316

NetApp Best Practices for SRM 6 on Clustered Data ONTAP

This document discusses the implementation of VMware vCenter Site Recovery Manager (SRM) version 6 in an environment that uses the NetApp® clustered Data ONTAP® operating system. It provides a conceptual understanding of what is required in a true disaster recovery scenario, which includes more than just failing over the virtual infrastructure and storage environment.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Solution Architecture

1.1 Overview

This document discusses the implementation of VMware vCenter Site Recovery Manager (SRM) version 6 in an environment that uses NetApp clustered Data ONTAP 8.3 or later.

Note: SRM version 5.8 is also included in the scope of this guide.

Some newer features in SRM and clustered Data ONTAP might not be compatible with previous versions of the NetApp Storage Replication Adapter (SRA). To validate that the exact product and feature versions that are described in this document are supported in your specific environment, see the Interoperability Matrix Tool (IMT) on the NetApp Support site.

This document provides a conceptual understanding of what is required in a true disaster recovery (DR) scenario, a process that typically requires more than just failing over the virtual infrastructure and the storage environment. To architect a DR solution, keep the following factors in mind:

- **The recovery time objective (RTO**). The RTO is how quickly a business can recover from a disaster, or, more specifically, how long it takes to execute the recovery process to make business services available again.
- **The recovery point objective (RPO).** The RPO is how old the recovered data is after it has been made available, relative to the time that the disaster occurred.
- **Scalability and adaptability**. This factor includes the ability to grow storage resources incrementally as demand increases.

An ideal solution has both a low RPO (as measured in minutes) and a low RTO (measured in minutes to hours). One factor that is often overlooked in a DR solution is the ability to test the DR solution efficiently. In physical environments, DR testing might take many hours or even days and requires that replication between sites be stopped while performing the tests.

1.2 Traditional Disaster Recovery Scenario

Failing over business operations to recover from a disaster requires several steps that are manual, lengthy, and complex. Often, custom scripts are written to simplify some of these processes. However, these processes can affect the real RTO that any DR solution can deliver, and most scripts cannot adapt and update as an environment grows or changes.

Consider the following simplified outline of the flow of a traditional DR scenario in a virtual environment. Each of these steps might involve several individual tasks:

1. A DR solution was previously implemented, and replication has occurred.
2. A disaster occurs that requires failover to the DR site. This event might be a lengthy power outage that is too long for the business to withstand without failing over. Or it might be a more severe disaster, causing the loss of data or equipment at the primary site.
3. The DR team takes the necessary steps to confirm the disaster and decides to fail over business operations to the DR site.
4. If data replication is successful and the results are verified, then you must perform the following tasks:
    a. Present the replicated storage to the VMware ESXi hosts at the DR site.
    b. Attach the ESXi hosts to the storage.
    c. Add the virtual machines (VMs) to the inventory of the ESXi hosts.
    d. If the DR site is on a network segment that is different from the primary site, each VM might need to be reconfigured for the new network.
    e. Verify that the environment is brought up properly, with certain systems and services being made available in the correct order.

5. After the DR environment is ready, the business can continue operating at its current capacity.
6. At some point, the primary site becomes available again or the lost equipment is replaced.
7. Changes that were made to the data while the DR site was supporting the business must be replicated to the primary site. Replication must be reversed to accomplish this step.
8. The processes described in step 4 must now be performed again, this time within a controlled outage window, to fail over the environment back to the primary site. Depending on how soon after the original disaster event the DR team was able to engage, this process might take nearly as long as recovering from the DR event.
9. After the primary environment has been recovered, replication must be established in the original direction from the primary site to the DR site.
10. The tests are repeated to verify that the environment is ready for a future disaster.

As previously mentioned, a DR process can be lengthy, complex, and prone to human error. These factors carry risk that is amplified by the fact that the process must be performed again to recover the operations back to the primary site when it is made available. A DR solution is an important insurance policy for any business. Periodic testing of the DR plan is a must to verify its reliability. Because of physical environment limitations and the difficulty of performing DR testing, most environments can test the DR plan only a few times a year at most, and some cannot test it at all.

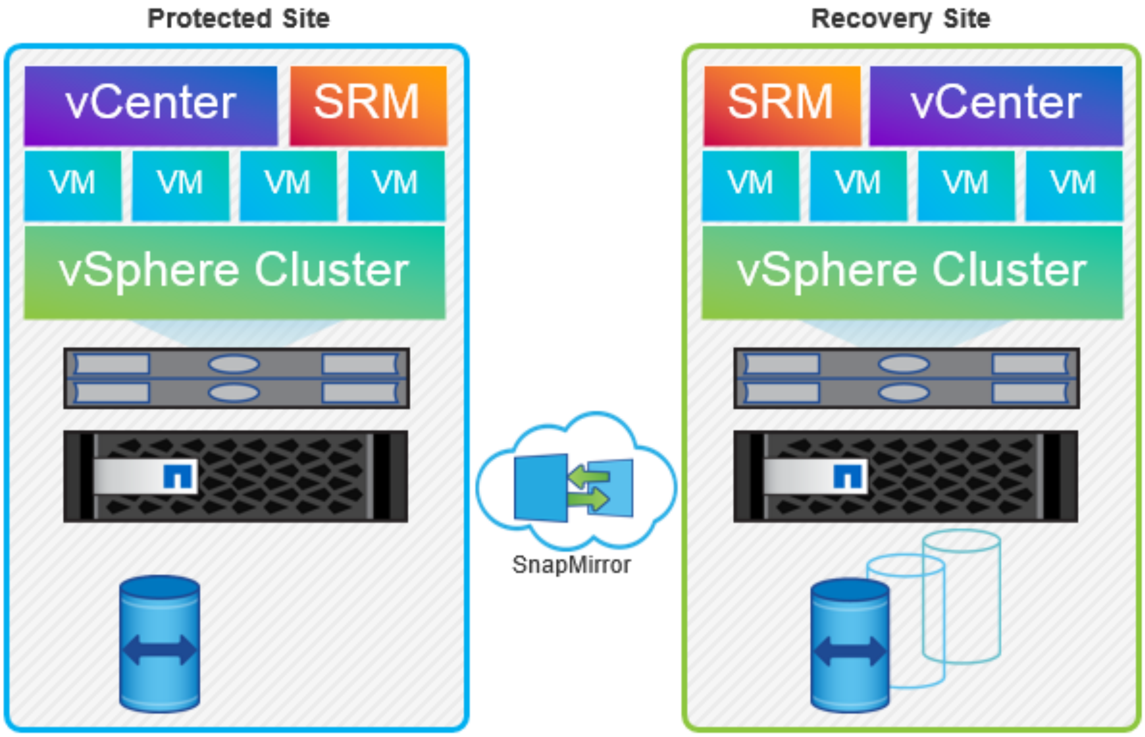
1.3 Site Recovery Manager

One of the most time-consuming parts of a DR failover in a VMware vSphere environment is the execution of the steps necessary to inventory, register, reconfigure, and power up VMs at the DR site. VMware has solved these problems with VMware vCenter Site Recovery Manager. Implementing SRM in an environment that uses NetApp clustered Data ONTAP helps provide business continuity. It also provides a DR solution that helps administrators plan, test, and run the recovery of VMs between a protected vCenter Server site and a recovery vCenter Server site. VMware SRM works in conjunction with NetApp SnapMirror® replication technology through the NetApp SRA. The NetApp SRA is a small software package that is installed on each SRM server and is available to any customer who uses SnapMirror.

1.4 Site Recovery Manager 6 and NetApp Improved Disaster Recovery

A virtualized environment that uses VMware vCenter SRM with NetApp storage provides the infrastructure with superior opportunities to implement real, working DR processes. These processes are quick and easy to test, consume little additional storage, and significantly reduce the RTO and RPO. Figure 1 shows the components of an SRM-protected site and a recovery site.

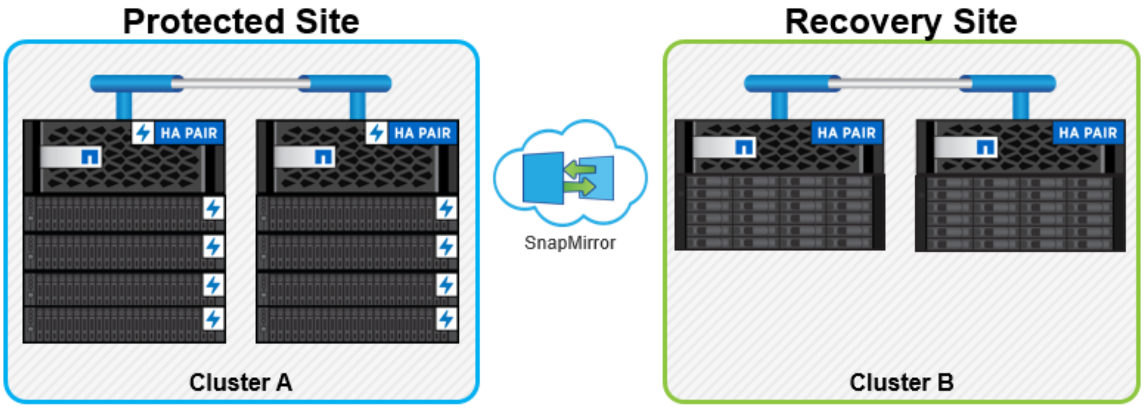
Figure 1) SRM components of protected and recovery sites.



Unified Architecture Flexibility

Starting with clustered Data ONTAP 8.1, SnapMirror can be used between NetApp FAS and NetApp FlexArray® storage systems. Systems with different performance characteristics and different costs can be deployed at the primary and DR sites. For example, depending on the capabilities that are required, the DR site might contain a lower-model storage system, SATA disk instead of FC disk, or the iSCSI or FCoE protocol instead of FC. Figure 2 illustrates the flexibility within a unified architecture.

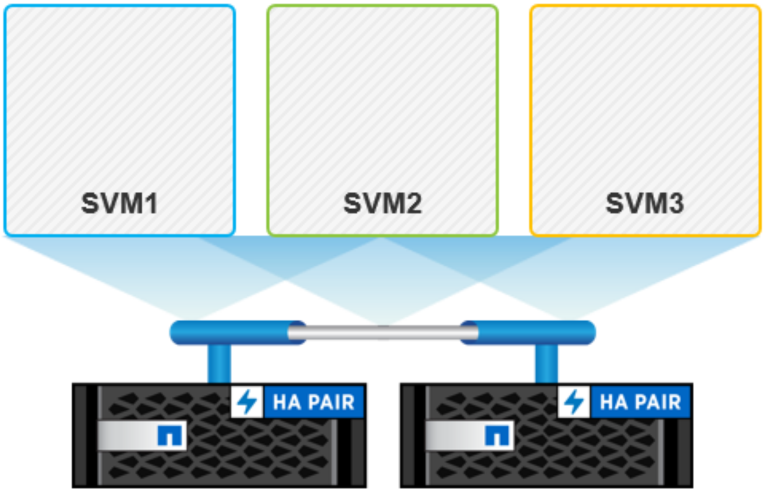
Figure 2) Unified architecture flexibility.



Secure Multitenancy in Clustered Data ONTAP

Clustered Data ONTAP is inherently a multitenant storage operating system and is architected in such a way that all data is accessed through secure virtual storage partitions. It is possible to have a single partition that represents the resources of the entire cluster or to have multiple partitions that are assigned specific subsets of cluster resources. These secure virtual storage partitions, shown in Figure 3, are known as storage virtual machines (SVMs; formerly called Vservers).

Figure 3) Storage virtual machines.



Storage Virtual Machines

An SVM is the secure logical storage partition through which data is accessed in clustered Data ONTAP. A cluster serves data through at least one and possibly multiple SVMs. An SVM is a logical abstraction that represents a set of the cluster's physical resources.

Storage Virtual Machine Pairing with Clustered Data ONTAP

SRM manages DR operations by pairing two SVMs. It offloads all the storage tasks to the NetApp SRA, uses Array Manager to pair the protected site and the recovery site SVMs, and identifies all SnapMirror relationships between the paired SVMs.

In NetApp Data ONTAP operating in 7-Mode, the NetApp SRA pairs physical controllers at the protected site and at the recovery site. However, clustered Data ONTAP pairs SVMs. Therefore, communication is with the SVM, and the SRM is not aware of the individual controllers. Clustered Data ONTAP allows you to pair SVMs in the same cluster, but SRM does not. To successfully complete array configuration, you must pair two SVMs from separate clustered Data ONTAP clusters.

Clustered Data ONTAP allows you to pair multiple SVMs at a protected site to a single SVM at the recovery site and vice versa. This capability provides a many-to-one (x-to-one) site recovery configuration and requires the creation of x array managers at a site with multiple SVMs. You can also pair x SVMs to y SVMs, which similarly requires x or y array managers, respectively, at each site.

NetApp SnapMirror

SnapMirror provides data replication in an SRM and NetApp environment. Built on NetApp Snapshot® technology, SnapMirror replication is extremely efficient because it replicates only the 4KB blocks that have been changed or added since the previous update. SnapMirror is easily configured by using either NetApp OnCommand® System Manager or the clustered Data ONTAP CLI.

For cases in which the primary storage is not completely lost, SnapMirror provides an efficient means of resynchronizing the primary and DR sites. SnapMirror can resynchronize the two sites, transferring only changed or new data back to the primary site from the DR site by simply reversing the SnapMirror relationships.

SnapMirror in clustered Data ONTAP provides asynchronous volume-level replication based on a configured replication update interval. SnapMirror uses NetApp Snapshot technology as part of the replication process.

Clustered Data ONTAP 8.1 or later provides the following replication capabilities:

- **Data protection mirrors** provide replication to create a backup copy within the same cluster (intracluster) or to create a DR copy in a different cluster (intercluster).
- **Load-sharing mirrors** provide replication from one volume to multiple volumes in the same cluster to distribute a read-only workload across a cluster.

  Note: The load-sharing mirror capability is supported only in NetApp SRA 2.1.

Clustered Data ONTAP 8.3 or later provides the following replication capabilities:

- SnapMirror and NetApp SnapVault® backup software can use the same volume baseline copy at the destination, which can reduce secondary storage capacity by 40% and reduce network traffic by 50%.
- NetApp SRA 3.0 uses only the mirror and not the vault Snapshot copies as the source for SRM recovery workflows in unified replication.
- You can replicate from a later release of clustered Data ONTAP to an earlier release, which simplifies upgrade and lifecycle operations at the secondary site.

Note: To implement these capabilities, the secondary site must be running clustered Data ONTAP 8.3 or later.

Basics of NetApp SnapMirror Replication

When the scheduler triggers a replication update, the following operations are performed:

1. A new Snapshot copy is created on the source volume.
2. The block-level difference between the new Snapshot copy and the previous replication Snapshot copy is determined and then is transferred to the destination volume. This transfer includes other Snapshot copies that were created between the previous replication Snapshot copy and the new one.
3. When the transfer is complete, the new Snapshot copy exists on the destination volume.

A SnapMirror destination volume is available for read-only access if it is shared by using the Common Internet File System (CIFS) protocol or is exported by using the Network File System (NFS) protocol. By using NetApp FlexClone® technology, a logical unit number (LUN) in the replicated volume can be made available to a client that supports a connection to read-only LUNs.

Note: Replication occurs at the volume level. Qtrees can be created in clustered Data ONTAP and can be replicated along with the replicated volume. However, individual qtrees cannot be separately replicated.

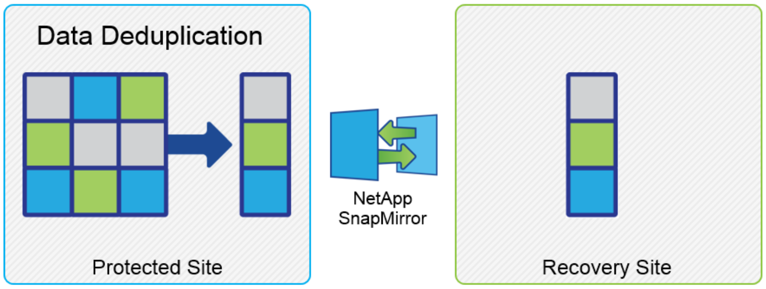
SRM recovery plans can be resynchronized in either direction after a failover without recopying the entire volume. If a relationship is resynchronized in the reverse direction, only new data that was written since the last successful synchronization of the Snapshot copy is sent back to the destination.

Note: For up-to-date technical specifications, see the SnapMirror Data Replication page of the NetApp website.

NetApp Deduplication

Additional efficiency is gained when SnapMirror is combined with data deduplication. As shown in Figure 4, when deduplication is used on the primary storage, only unique data is replicated to the DR site. Additionally, SnapMirror network compression can provide native on-wire compression of data that is sent over the WAN. These technologies result in significant telecommunication and storage capacity savings at the DR site.

Figure 4) Deduplication.

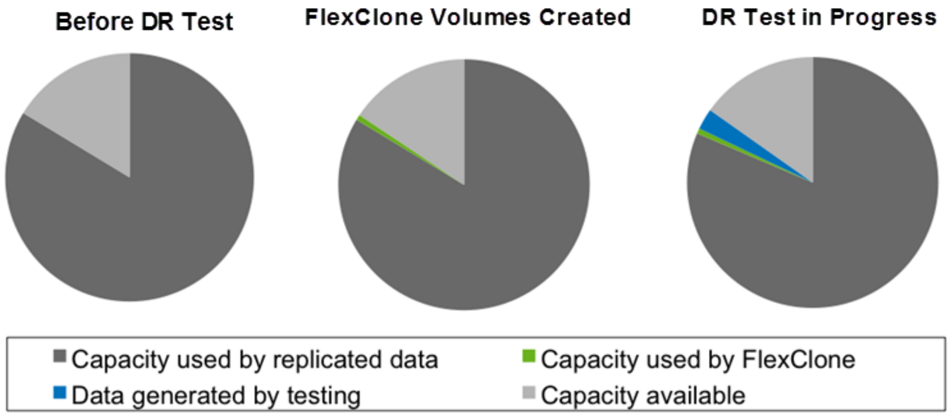


NetApp FlexClone Technology

When FlexClone technology is combined with SnapMirror and SRM, testing the DR solution becomes quick and easy, consumes very little additional storage, and does not interrupt the replication process. FlexClone quickly creates a read-writable copy of a NetApp FlexVol® volume. When this functionality is used, an additional copy of the data is not required. For example, if a read-writable copy of a 10GB LUN is being created, another copy of that 10GB LUN is not required. The only requirement would be the metadata needed to define the LUN. FlexClone volumes only store data that is written or changed after the clone was created.

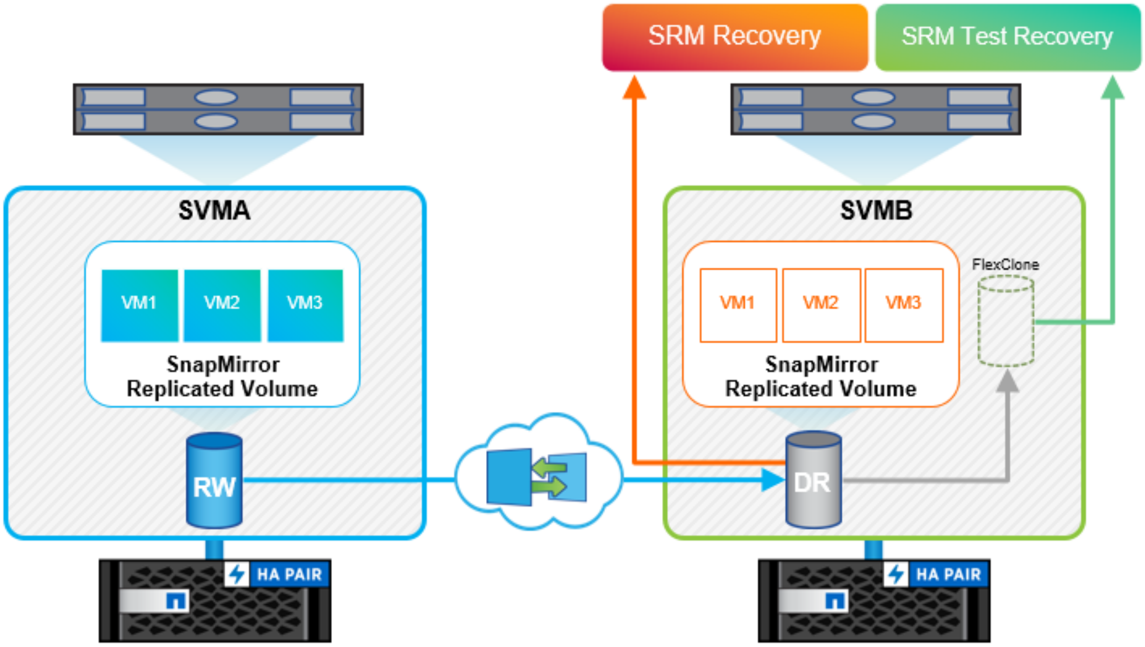
The SRM DR testing component leverages FlexClone functionality to create a copy of the DR data in a matter of seconds. As shown in Figure 5, only a small percentage of additional capacity is required for writes that occur during testing.

Figure 5) Capacity required for FlexClone replication.



FlexClone volumes share common data blocks with their parent FlexVol volumes, but they behave as independent volumes. This feature allows DR testing to be completed without affecting the existing replication processes. Testing of the DR environment can be performed, even for an extended period, while replication to the parent FlexVol volume occurs in the background. Figure 6 depicts an SRM test and recovery workflow that uses FlexVol volumes and FlexClone volumes.

Figure 6) Parent FlexVol volume and FlexClone volumes used for SRM test and recovery workflows.



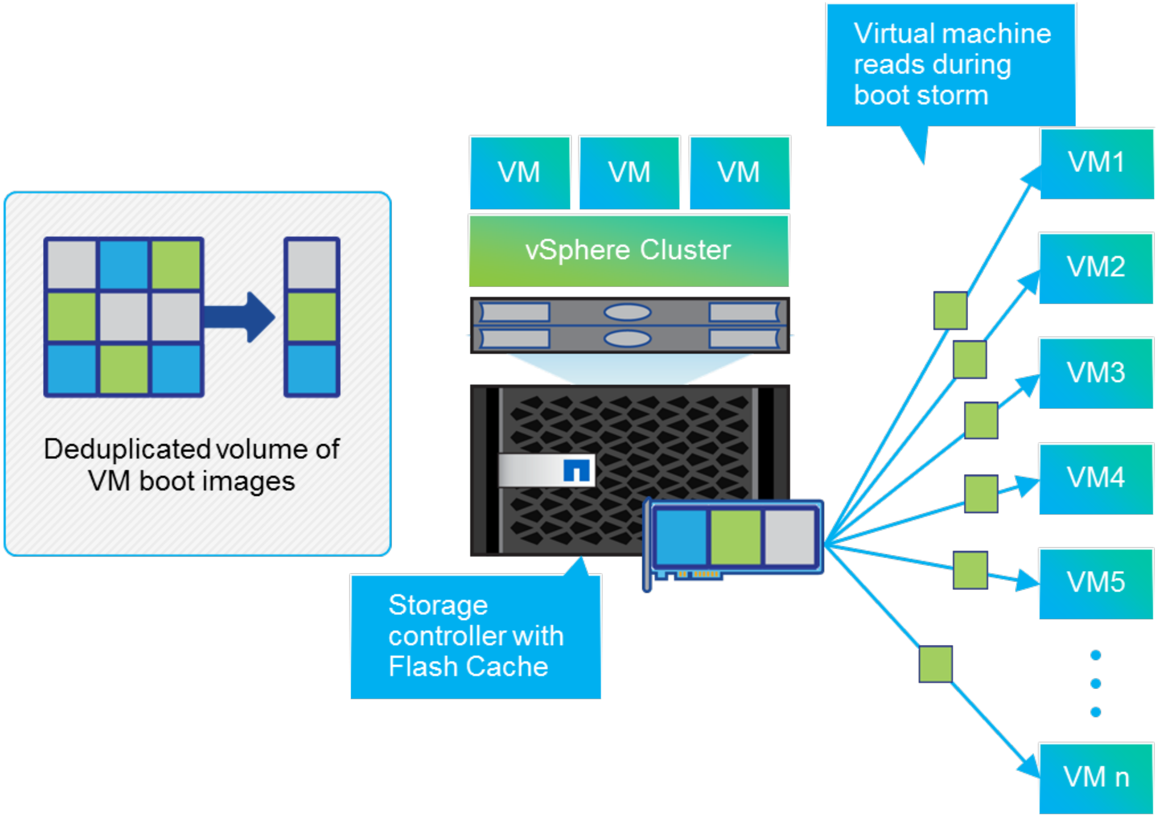
Note: For up-to-date technical specifications, see the Storage Efficiency page of the NetApp website.

NetApp Flash Cache Technology

A DR event is a critical time for any environment. The increase in disk I/O that is generated by booting many VMs can affect the overall performance of the storage array and therefore affect the RTO of the solution. NetApp Flash Cache™ technology reduces the disk I/O requirements for booting multiple VMs simultaneously. This capability allows the solution to be deployed with fewer physical disks, and it provides faster boot time and a significant reduction in recovery time during a DR event. Up to 24TB of read cache can be configured in a storage system by using Flash Cache and Flash Cache 2 modules.

Flash Cache is deduplication aware. That is, it caches a deduplicated block only once and satisfies read requests for all corresponding virtual blocks from cache at least 10 times faster than going to disk. After a master block is cached, then all virtual block duplicates are read at cache speed. Figure 7 depicts the use of Flash Cache during a boot storm.

Figure 7) Flash Cache during a boot storm.


Virtual machine reads during boot storm
VM
VM
VM
vSphere Cluster
Deduplicated volume of VM boot images
Storage controller with Flash Cache
VM1
VM2
VM3
VM4
VM5
VM n

For up-to-date technical specifications for Flash Cache and Flash Cache 2, see the Flash Optimization Features page on the NetApp website.

1.5 New Features and Workflows in Site Recovery Manager

VMware made enhancements to the following versions of vCenter Site Recovery Manager.

Note: For the latest supported configurations and features, see the VMware Site Recovery Manager Documentation.

Site Recovery Manager 6.1

- Support for VMware vSphere 6.0 update 1
- Storage policy-based protection of VMs
- Support for stretched storage clusters
- Support for automapping of stretched VMware NSX networks
- Enhancements to mappings for test networks

Site Recovery Manager 6.0

- Support for VMware vSphere 6.0, including integration with shared infrastructure components such as Platform Services Controller and vCenter Single Sign-On
- Support for vSphere Storage vMotion and Storage DRS on both the protected and the recovery site
- Protection and recovery of VMs in IPv6 environments
- IP customization enhancements to support dual-protocol IP configurations and independent IPv4 and IPv6 configurations

Site Recovery Manager 5.8

- Integration of the SRM UI in vSphere Web Client
- A vCenter Orchestrator plug-in for SRM that allows you to automate certain SRM operations by including them in vCenter Orchestrator workflows
- Increased scale that allows you to use SRM to protect and recover larger numbers of VMs
- Subnet-level IP customization rules that allow you to manage the customization of IP addresses across multiple VMs from the SRM UI
- An optional embedded vPostgreSQL database that you can use with minimal configuration instead of using a dedicated external database
- Improved support for Integrated Windows Authentication when you use Microsoft SQL Server as the SRM database

Unsupported Enhancements

The following enhancements are not supported with NetApp Storage Replication Adapter 3.0 for clustered Data ONTAP:

- Storage policy-based protection of VMs
- Support for stretched storage clusters
- Protection and recovery of VMs in IPv6 environments
- IP customization enhancements to support dual-protocol IP configurations and independent IPv4 and IPv6 configurations

Note: VMware Virtual SAN, NSX, and vSphere replication–specific features are not supported with NetApp SRA.

This document covers SRM versions 5.8, 6.0, and 6.1. It also refers to SRM on clustered Data ONTAP and, therefore, discusses only array-based replication functionality. For detailed information about installing and configuring VMware SRM, see the VMware Site Recovery Manager Documentation.

Site Recovery Manager Workflows

SRM consists of the following workflows:

- Test recovery
- Cleanup operation
- Recovery:
  - Planned migration
  - Disaster recovery
- Reprotect operation
- Failback

The following sections provide a summary of each workflow.

Test Recovery

Test recovery in SRM is an operational procedure that allows VMware administrators to fully validate their recovery plans without disrupting their production environments. SRM incorporates storage replication synchronization as an optional capability in the test recovery operation. This capability allows the VMware administrator to verify that any changes that were recently made in the environment are replicated to the recovery site and thus are present during the test. Such changes include patches to the VM guest operating system.

When the VMware administrator runs a test recovery operation, SRM automates the following tasks:

- **Optional**: Triggering any SnapMirror relationships to update storage at the DR site with any recent changes that were made at the production site.
- Creating NetApp FlexClone volumes of the FlexVol volumes on the DR storage array.
- Connecting the datastores in the FlexClone volumes to the ESXi hosts at the DR site.
- Reconfiguring the storage settings inside the VMs.
- Connecting the VM network adapters to a private bubble test network.
- **Optional**: Reconfiguring the VM guest operating system network settings as defined for the network at the DR site.
- Executing any custom commands that have been stored in the recovery plan.
- Powering on the VMs in the order that is defined in the recovery plan.

To understand how SRM performs a test failover nondisruptively, it is important to understand how the VMs are connected to the network both before and during a test failover operation. Table 1 lists the components that are used in the following recovery scenarios.

Table 1) SRM components.

Component	Protected Site	Recovery Site
Site	Site A	Site B
Network	VM network	VM network
ESXi host	`ESXi-A1.demo.netapp.com`	`ESXi-B1.demo.netapp.com`
Datastore	`Datastore-A1`	`Datastore-B1`
Nonreplicated placeholder database	`Placeholder-A1`	`Placeholder-B1`
VM	`VM-A1`	`VM-B1`

Figure 8 shows a VM-to-network map before the failover test. Note the following items in Figure 8:

- The running `VM-A1` VM is a production VM that belongs to the `Datastore-A1` datastore.
- The running `VM-B1` VM is a production VM that belongs to the `Datastore-B1` datastore.
- Each site has a local datastore that houses placeholder VMs that are created by SRM. The placeholder VMs identify the location in which the protected VM is placed in the recovery site when a test recovery or a recovery operation is performed.
- The placeholder `VM-A1` VM belongs to a nonreplicated placeholder datastore (`Placeholder-B1`) in site B and does not belong to a network.
- The placeholder `VM-B1` VM belongs to a nonreplicated placeholder datastore (`Placeholder-A1`) in site A and does not belong to a network.

Figure 8) VM-to-network map before test failover operation.

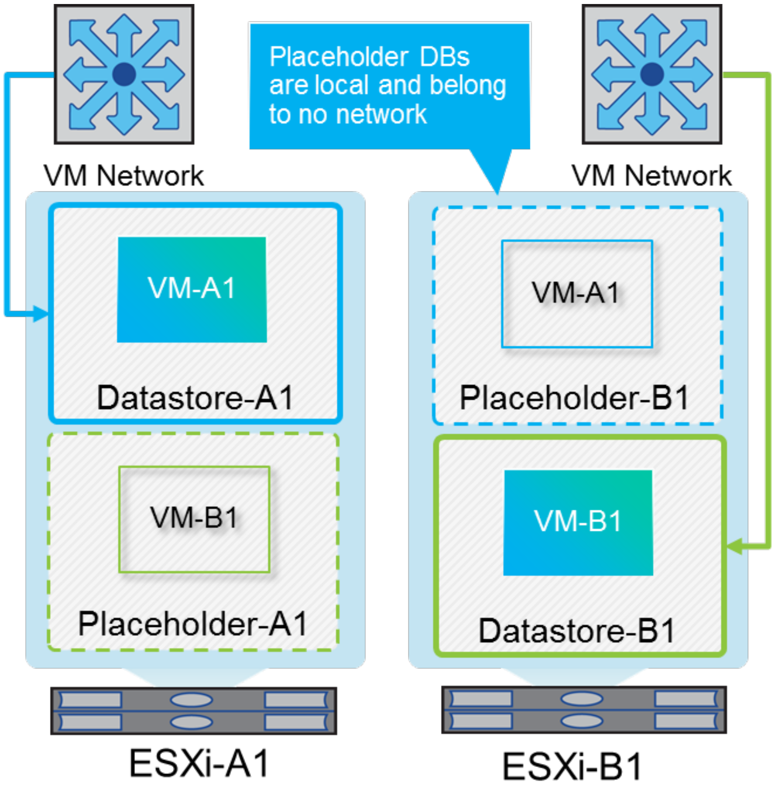
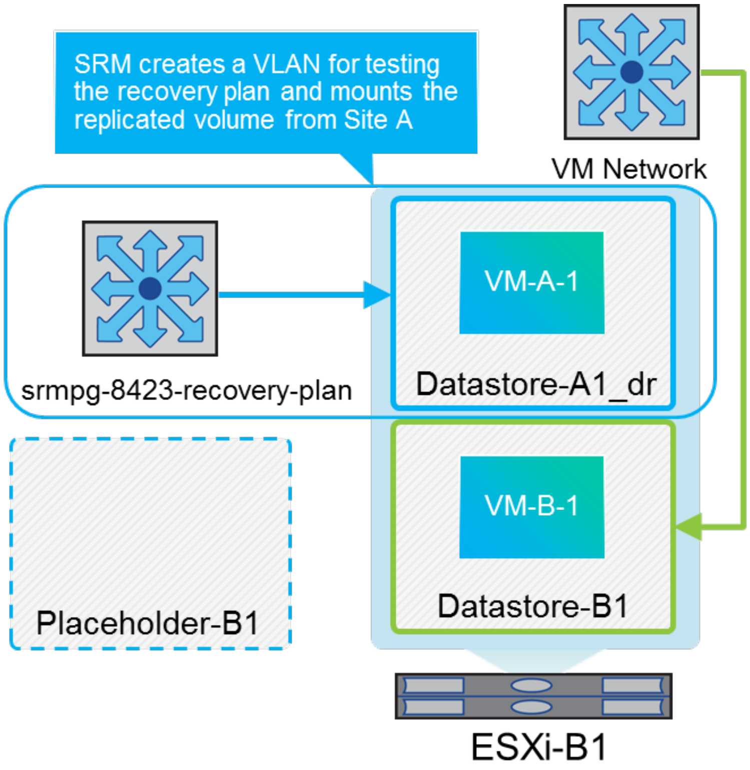


Figure 9 shows the VM-to-network map after the test recovery operation. Note the following items in Figure 9:

- A bubble network (VLAN) has been created (`srmpg-8243-recovery-plan`) that does not interfere with the production network (`VM Network`).
- The recovery site ESXi host has a new datastore (`Datastore-A1_dr`) mounted. This datastore is a FlexClone copy of the replicated volume (`nfs-A1_dr`).
- The nonreplicated placeholder datastore (`Placeholder-B1`) no longer contains a placeholder VM.
- The former placeholder VM (`VM-A1`) has now been replaced by a fully functional, running copy of the protected VM that belongs to the test bubble network (`srmpg-8243-recovery-plan`).

Figure 9) VM-to-network map after a test recovery operation.



Cleanup Operation

The cleanup operation occurs after the recovery plan test has been completed and the VMware administrator responds to the cleanup prompt. This operation returns the protected VMs to their initial state and resets the recovery plan to the ready state.

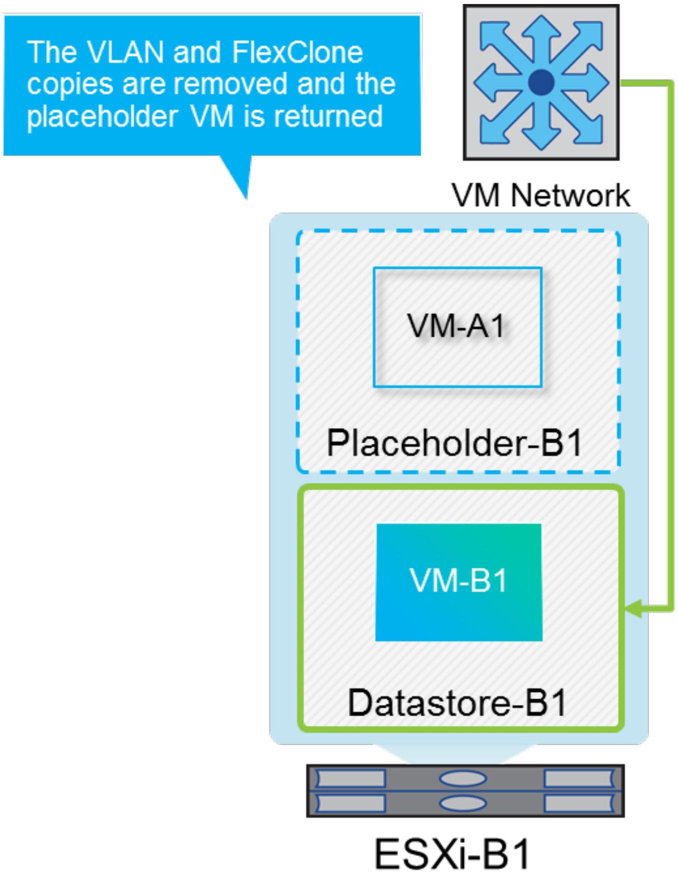
When the VMware administrator performs a recovery operation, SRM completes the following process:

1. It powers off each recovered VM in the FlexClone copy that was used for testing.
2. It replaces the recovered VMs with placeholders, preserving their identity and configuration information.
3. It deletes the FlexClone volume that was used to present the recovered VMs during the test.

Figure 10 shows the map of the network at the recovery site after the cleanup operation has occurred. Note the following changes in Figure 10:

- The bubble test network is gone.
- The recovery site ESXi host does not have a FlexClone volume (`Datastore-A1_dr`).
- The placeholder datastore has a placeholder VM (`VM-A1`) that is not connected to a network.

Figure 10) VM-to-network map after a cleanup operation.

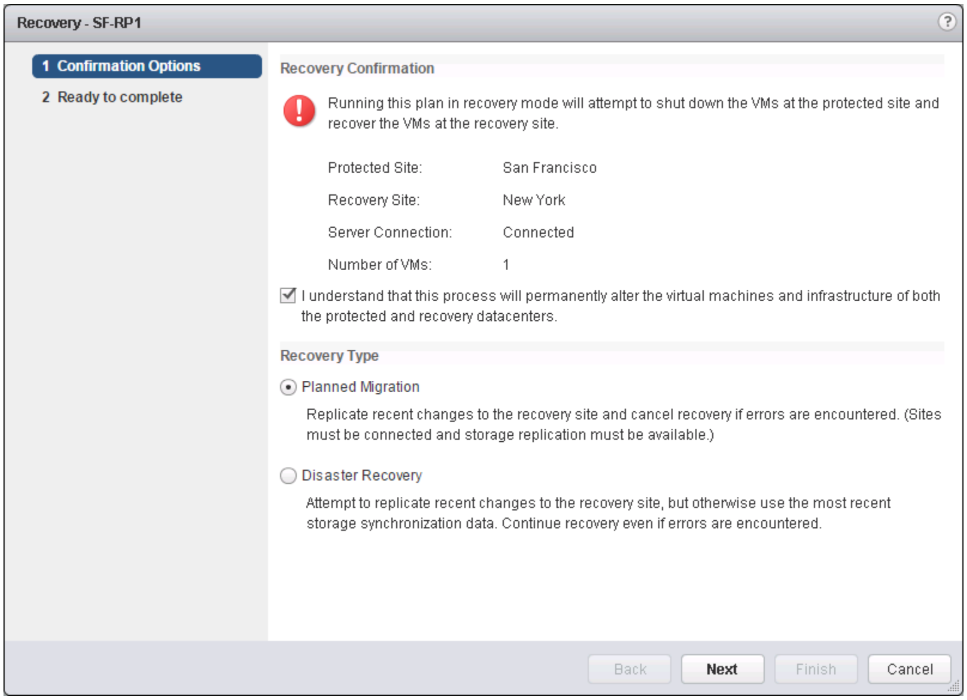

The VLAN and FlexClone copies are removed and the placeholder VM is returned
VM Network
VM-A1
Placeholder-B1
VM-B1
Datastore-B1
ESXi-B1

Planned Migration and Disaster Recovery

SRM has two methods for performing a real failover: planned migration and DR. The first method, planned migration, incorporates VM shutdown and storage replication synchronization into the process to recover or effectively move the VMs to the recovery site. Planned migration requires access to the primary protected site.

The second method, DR, is an unplanned failover in which the VMs are recovered at the DR site from the last storage replication interval that was able to complete. Depending on the RPO that was designed into the solution, some amount of data loss can be expected in the DR scenario. VMware administrators can complete both types of recovery operations through the SRM Recovery Operation wizard. As shown in Figure 11, the VMware administrator selects either planned migration or DR for the recovery operation.

Figure 11) Recovery options.



Recovery - SF-RP1

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:	San Francisco
Recovery Site:	New York
Server Connection:	Connected
Number of VMs:	1

☑ 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.

When the VMware administrator performs a recovery operation, SRM automates the following tasks for a planned migration:

- **Optional:** Trigger the SnapMirror replication relationships to update the storage at the DR site with any recent changes that were made at the production site.
- Gracefully shut down the protected VMs at the primary site.
- Trigger additional storage synchronization to verify that the replicated VMs are in a quiesced state at the recovery site.

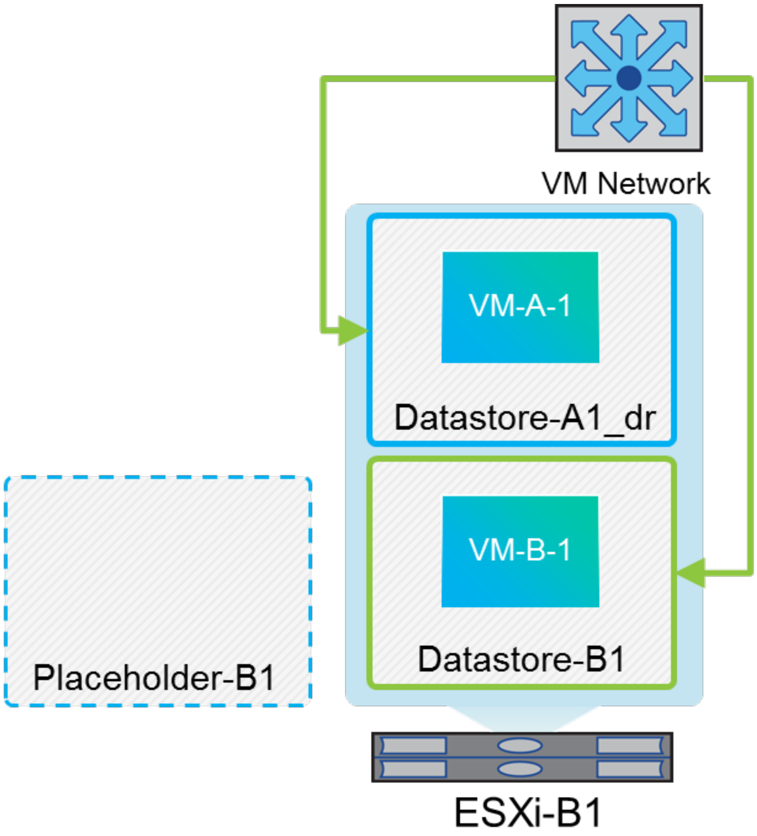
SRM also automates the following tasks for planned migrations and for DR:

- Fail over the NetApp SnapMirror relationships.
- Connect the replicated datastores to the ESXi hosts at the DR site.
- **Optional:** Power off VMs, such as the test/dev instances, at the DR site, thereby freeing compute resources.
- Reconfigure the storage settings inside the VMs.
- Connect the VM network adapters to the appropriate recovery site network.
- **Optional:** Reconfigure the VM guest operating system network settings as defined for the network at the DR site.
- Execute any custom commands that have been stored in the recovery plan.
- Power on the VMs in the order that was defined in the recovery plan.

Figure 12 shows the vSphere Client map of the network at the recovery site after the recovery operation has been completed. Note the following changes in Figure 12:

- The recovery site ESXi host has a new datastore mounted (`Datastore-A1_dr`).
- The protected site VM (`VM-A1`) is now up and running in the recovery site on the VM network.
- The placeholder datastore (`Placeholder-B1`) is empty.

Figure 12) VM-to-network map after recovery operation has been completed.



Reprotect Operation

After a recovery, the recovery site becomes the new production site. Because the recovery operation broke the SnapMirror replication, the new production site is not protected from any future disaster. A best practice is to protect the new production site to another site immediately after a recovery. If the original production site is operational, the VMware administrator can use the original production site as a new recovery site to protect the new production site, effectively reversing the direction of protection.

Reprotection is available only in noncatastrophic failures. Therefore, the original vCenter Servers, ESXi servers, SRM servers, and corresponding databases must be eventually recoverable. If they are not available, a new protection group and a new recovery plan must be created.

Failback

A failback is an optional procedure that restores the original configuration of the protected and recovery sites after a recovery. VMware administrators can configure and run a failback procedure when they are ready to restore services to the protected site. The following scenario provides an example of the failback procedure. In this example, site A was the original protected site and had just failed over to site B. The failback procedure consists of the following steps:

1. Perform a reprotect operation. The former recovery site (site B) becomes the protected site, and all changes in site B are replicated to site A.
2. Perform a planned migration. The VMs are recovered to site A.

   Note: To avoid any potential interruptions in the production VMs, it is important to run a test recovery operation before failing back. If the test identifies errors, resolve these issues before you perform the planned migration.

3. Perform a second reprotect, this time with site A as the protected site and site B as the recovery site.

1.6 Storage Replication Adapter 3.0 for Clustered Data ONTAP

NetApp SRA 3.0 for clustered Data ONTAP is a storage vendor–specific plug-in for VMware vCenter Site Recovery Manager that enables interaction between SRM and the storage controller at the SVM level. The NetApp SRA interacts with the SVM to discover replicated datastores. It also manages failover and test failover of the VMs that are associated with these storage objects.

SRM uses the NetApp SRA to support SAN environments: VMware Virtual Machine File System (VMFS [iSCSI and FC]) and raw device mapping (RDM [iSCSI and FC]). SRM also uses the SRA to support NAS environments: NFS.

The NetApp SRA provides array-specific support by following the SRM input specifications. The adapter enables SRM to execute the following workflows:

- Discovery of arrays and replicated devices
- Test recovery
- Recovery
- Reprotect

NetApp VMware vSphere API for Storage Awareness Provider

Starting with NetApp SRA 3.0, NetApp VMware vSphere API for Storage Awareness (VASA) Provider 6.2 for clustered Data ONTAP is a prerequisite for SRA installation at the protected site and at the recovery site. NetApp SRA 3.0 has been redesigned to leverage the storage capabilities in VASA Provider to perform SRM workflows, such as test recovery, recovery, and reprotect. The use of VASA Provider for all storage intelligence and operations offers several advantages, including:

- Performance and scalability enhancements
- The abstraction of version differences in clustered Data ONTAP
- A robust multithreaded architecture
- A reduced SRA installation footprint

VASA provides the technology to query storage and return a set of storage capabilities to vCenter. VASA vendor providers supply the translation between the storage system APIs and constructs and the VMware APIs that vCenter understands. In the NetApp implementation, the VASA vendor provider is NetApp VASA Provider for clustered Data ONTAP, a virtual appliance that is deployed to vCenter from an OVA file. NetApp VASA Provider is managed through pages and context-sensitive menus in the NetApp Virtual Storage Console (VSC) for VMware vSphere.

Note: NetApp VASA Provider and Virtual Storage Console are designed to work together. As such, VASA Provider 6.2 and VSC 6.2 must be installed before NetApp SRA 3.0 installation.

Replication Topologies Supported in NetApp Storage Replication Adapter 3.0

NetApp SRA 3.0 leverages SnapMirror asynchronous volume replication in clustered Data ONTAP for array-based replication in SRM. Previous versions of SnapMirror in clustered Data ONTAP supported only the data protection (DP) relationship type. In clustered Data ONTAP 8.3 and later, SnapMirror introduces a new extended data protection (XDP) relationship type that delivers feature enhancements such as unified replication and version-flexible replication. SnapVault replication policies and restoring from SnapVault Snapshot copies is not supported with the NetApp SRA.

Table 2) Supported SnapMirror topologies.

Relationship Type	Policy Name	Policy Type
DP	`DPDefault`	`async-mirror`
XDP	`DPDefault, MirrorLatest, MirrorAllSnapShots`	`async-mirror`
XDP	`MirrorAndVault`	`mirror-vault`

Note: NetApp SRA 3.0 also supports custom policy names as long as the policy type matches the types in Table 2.

Storage Virtual Machine Multitenancy

NetApp SRA 3.0 now supports SVM multitenancy with VMware vCenter Site Recovery Manager. This new capability supports the delegation of SRM array manager pairing to SVM administrator credentials in clustered Data ONTAP, which was unsupported in previous releases of SRA.

NetApp SRA 2.x and earlier versions paired two SVM array managers, but required cluster administrator credentials to successfully perform the operation. NetApp VASA Provider enables this functionality by assuming the cluster administrator role and delegating the appropriate privileges to each tenant SVM.

Note: The use of SVM administrator credentials requires that you use role-based access control (RBAC) to create a user with the minimum required permissions. This user can be created manually from the Data ONTAP CLI or by using the NetApp RBAC User Creator tool. NetApp recommends that you use this tool because it simplifies creation of the minimum required permissions by providing prepackaged users with the necessary permissions.

For instructions on how to configure the RBAC user account, see the RBAC User Creator for Data ONTAP page on the NetApp Community site.

SVM multitenancy with SRM enables disaster recovery as a service (DRaaS). Service providers can then build a private cloud infrastructure that provides DRaaS to their internal or external customers (tenants) by leveraging SRM on clustered Data ONTAP. IT organizations (tenants) now have the flexibility to consume centralized DR services and to avoid the necessary capital and operational expenditures.

For example, a service provider can delegate ownership of SVMs at the protected and recovery sites to their tenants while maintaining ownership of the storage and network layers. Tenants would have the ability to configure and customize their own DR environments by using SRM and the underlying infrastructure.

1.7 Site Recovery Manager 6 on the Clustered Data ONTAP Architecture

An SRM environment consists of separate vCenter instances, each with their own installation of SRM Server. Each vCenter instance manages a different set of ESXi hosts. In an SRM environment, the vCenter instance or site in which a VM currently runs is referred to as the protected site for that VM. The site to which the VM's data is replicated is referred to as the recovery site for that VM. When SRM is used to manage failover and DR testing, failover and testing occur at the same granularity as the SnapMirror relationship. That is, if a FlexVol volume has been configured as a datastore, all VMs in that datastore are part of the same SRM protection group and therefore are part of the same SRM recovery plan.

Even though only two instances of vCenter are typically in an SRM environment, SRM supports a shared recovery site model. In this model, multiple protected sites, each with their own vCenter and SRM instances, can be configured to recover VMs on a single vCenter and SRM instance at the recovery site. This configuration requires each SVM at the protected site to be peered with either a single or a dedicated SVM at the recovery site.

VMware also supports multiple SRM instances at the recovery site, which pair to each instance of SRM at the protected site. This configuration is defined as a shared recovery site and requires special configuration during installation of SRM Server.

For more details about installing and configuring SRM in a shared recovery site environment, see the VMware vCenter Site Recovery Manager Documentation.

A typical SRM environment consists of the following components at each site:

- A number of VMware ESX or ESXi hosts that are configured in the high-availability (HA) and Distributed Resource Scheduler (DRS) clusters:
  - Various ESX or ESXi versions are supported, including 4.x, 5.x, and 6.0
- VMware vCenter Server 5.5 and 6.0
- SRM Server 5.8, 6.0, and 6.1

  Note: For up-to-date information about VMware compatibility, see the VMware Product Interoperability Matrixes page on the VMware website.

- A NetApp clustered Data ONTAP cluster to provide storage for VMFS or NFS datastores
- Microsoft SQL Server database or the SRM Server-embedded vPostgreSQL database
- Various servers that provide infrastructure services, such as Active Directory (AD) servers for authentication and DNS servers for name resolution

  Note: Infrastructure services—such as authentication, name resolution, and VMware licensing—must be active and available at both sites.

Figure 13) Typical SRM environment on clustered Data ONTAP.

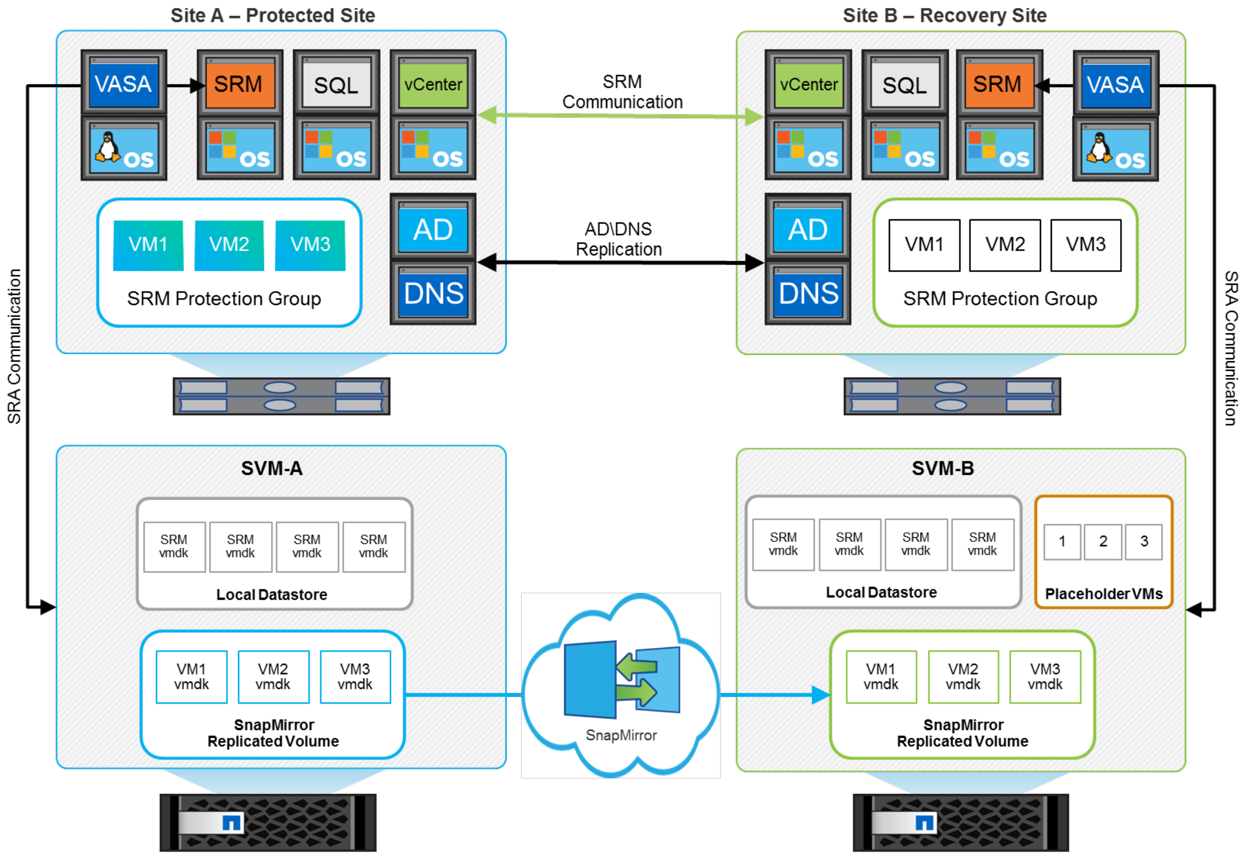


Figure 13 shows VMs from the protected site, site A, replicated to the recovery site, site B. For simplicity, this figure shows replication and protection of VMs going only in one direction, from site A to site B. However, replication and protection of VMs can be performed in both directions, with different VMs in different datastores at each site that are configured to be recovered at the opposite site.

In an SRM environment, communication does not occur directly between the SRM servers. Instead, SRM communication is performed by proxy through the vCenter Server at each site, as is shown by the green arrow in Figure 13. This process also applies to communication with the NetApp SVM. The SRM server in site A never communicates with the SVM in site B. For example, a user is working in the SRM interface at site A and performs an action that requires the SVM to perform an operation at site B. The SRA command is sent by proxy through the vCenter Servers to the SRM server at site B. The SRM server at site B then communicates with the local SVM and sends the response back to the SRM server at site A, again by proxy through the vCenter servers.

With NetApp SRA 3.0, VASA Provider is the communication broker between the SRM servers and the NetApp SVMs at both sites. It also executes all storage operations on behalf of SRA. This interaction is orchestrated in the background and is therefore abstracted from the SRM administrator.

Note: By default, VASA Provider uses SOAP over HTTPS for communication on port 9083.

SnapMirror replicates FlexVol volumes that contain VMFS or NFS datastores from the protected site, site A, to the recovery site, site B.

1.8 Site Recovery Manager 6 Design Considerations

Virtual Machine Network Setting Reconfiguration During Failover

Some environments might be able to use the same network IP addresses at both the primary site and the DR site. This ability is referred to as a stretched virtual LAN (VLAN) or stretched network setup. Other environments might have a requirement to use different network IP addresses (for example, in different VLANs) at the primary site relative to the DR site. VMware vCenter Site Recovery Manager supports both of these scenarios.

SRM 6 can change the network configuration of a VM as it is recovered. This reconfiguration includes settings such as IP addresses, gateway address, and DNS server settings.

Different network settings, which are applied to individual VMs as they are recovered, can be specified in the properties settings of a VM in the recovery plan. To configure SRM to apply different network settings to multiple VMs without having to edit the properties of each one in the recovery plan, VMware provides a tool called the dr-ip-customizer. For directions on how to use this utility, see the “Customize IP Properties for a Group of Virtual Machines” section in the Site Recovery Manager Administration Guide. Dr-ip-customizer takes as input a file that contains a comma-separated value table of IP settings for multiple VMs and generates a unique customization specification for each VM. It then applies that customization specification to the recovery plan for each VM.

NFS Datastore Layout

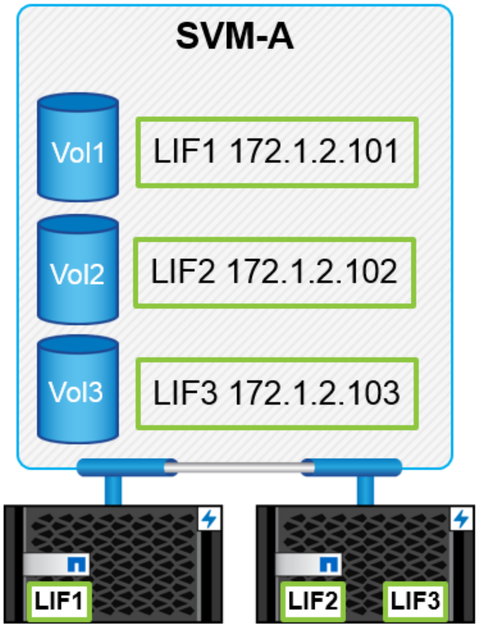
For practical purposes, the NFS protocol does not limit the number of VMs per datastore. It also does not limit the addressable size of an NFS datastore, which means that it automatically supports the current 100TB maximum volume size of clustered Data ONTAP. Therefore, VMs can be grouped according to business requirements, such as organizational (department, tenant, or application) or service level (type of storage, replication requirements, or schedule). Another advantage of having many VMs per datastore, especially with the same guest operating system, is improved space efficiency through the use of NetApp deduplication and VM cloning within the volume.

Datastores and Logical Interfaces

In clustered Data ONTAP, optimal performance is achieved when a volume is accessed by using a network port on the same node that hosts the volume. This approach is called direct data access. Volumes can be migrated to different nodes; therefore, logical interfaces (LIFs) should move with the volumes that are accessed through them to preserve the direct path.

NetApp recommends using a dedicated LIF and associated IP address for each datastore to provide the most flexibility. This task is most easily managed by using the NetApp Virtual Storage Console for VMware vSphere to provision datastores. VSC selects an unused LIF as long as one or more unused LIFs are available on the node in which a datastore is being created. For detailed information and best practices, see TR-4333: VMware vSphere 5 on NetApp Clustered Data ONTAP.

Figure 14) LIF best practices.



Note: When you migrate volumes and LIFs, complete the volume move first and then move the LIF.

Communication Between ESXi Hosts During Disaster Recovery Testing

When a DR test recovery operation is performed, a private test bubble network is created on the ESXi host for the VMs. However, this network is not automatically connected to any physical network adapters and therefore does not provide connectivity between the ESXi hosts. To allow communication among VMs that are running on different ESXi hosts during DR testing, a physical private network is created between the ESXi hosts at the DR site.

To verify that the test network is private, the test bubble network can be separated physically or by using VLANs or VLAN tagging. This network must be segregated from the production network because as the VMs are recovered, they cannot be placed on the production network with IP addresses that could conflict with actual production systems. When a recovery plan is created in SRM, the test network that was created can be selected as the private network to connect the VMs to during the test.

Active Directory and Name Resolution Services

The Active Directory and name resolution (DNS) architecture plays an important role in successful failover, DR testing, and failback scenarios. The Active Directory servers should not be recovered from replicas that were created by unsupported processes because this action can create an update-sequence-number rollback scenario. This type of scenario can occur when an Active Directory server that contains an older version of the Active Directory database is recovered from an unsupported backup method. In this scenario, the Active Directory processes on the recovered server might be unable to process authentication requests or other functions.

For information about supported methods for creating backups of Active Directory servers in virtual server environments, go to the Microsoft Support site. Specifically, see KB 888794: Things to Consider When You Host Active Directory Domain Controllers in Virtual Hosting Environments.

Active Directory and DNS Services for Disaster Recovery Testing

The DR test network is a private network, and the VMware VM console window is used to access the VMs that are running in test mode. To conduct tests inside the VMs, such as verifying that an application server can connect to a database, the login to the application server must be authenticated. The application server must also be able to resolve the network address of the database server.

If authentication and name resolution services are required in the private test network to conduct testing, you can create clones of the required VMs in the test network. One example is when Microsoft Active Directory and DNS services provide user authentication and name resolution services. In that case, you can clone VMs that provide Microsoft Active Directory and DNS services at the DR site before you run the DR test. However, before you power on the cloned VMs, reconfigure the VM network connections to connect the cloned VMs only to the private DR test network. These cloned VMs can then be powered on and can provide name resolution and authentication services in the private test network.

The user must select one of the cloned Active Directory servers that was configured as a global catalog server. Some applications and Active Directory functions require Flexible Single Master Operation (FSMO) roles in the Active Directory forest. For directions on how to seize the roles on the cloned Active Directory server after it has been cloned and connected to the private test network, go to the Microsoft Support site. Specifically, see the procedure described in KB 255504: Using Ntdsutil.exe to Transfer or Seize FSMO Roles to a Domain Controller.

After the roles have been seized, the clone must never be connected to a production VM network. Because these servers cannot replicate their databases with the real servers in the production environment, they should be destroyed after DR testing has been completed. New clones must be created for additional DR tests.

Active Directory and DNS Services for Real Failover

Do not use the cloning process that was described previously in a real DR failover scenario. In a real failover scenario, rely on existing Active Directory and DNS servers at the recovery site to provide those services. In a manner similar to the testing scenario, some applications and Active Directory functions require FSMO roles in the Active Directory forest. If the Active Directory server that is servicing these roles is lost at the protected site, the roles must be seized on an Active Directory server at the recovery site. To accomplish this task and for directions on how to seize the five FSMO roles, go to the Microsoft Support site. Specifically, see the procedures described in KB 255504: Using Ntdsutil.exe to Transfer or Seize FSMO Roles to a Domain Controller.

Site Recovery Manager 6 and NetApp Snapshot Autodelete

NetApp clustered Data ONTAP can be configured to automatically remove Snapshot copies to preserve capacity in a FlexVol volume. The default setting for this capability does not automatically delete the Snapshot copies that are created by SnapMirror. If SnapMirror Snapshot copies are deleted, then the NetApp SRA cannot reverse and resynchronize replication for the affected volume. To prevent clustered Data ONTAP from deleting SnapMirror Snapshot copies, configure the Snapshot autodelete capability to `try`.

```
snap autodelete modify -volume <volname> -commitment try
```

SnapMirror and Clustered Data ONTAP Version Requirements

SRM 6 can change the direction of SnapMirror replication relationships. To reverse replication, the source and destination storage systems must run the correct versions of clustered Data ONTAP. Replication is not possible between storage systems if one system uses Data ONTAP operating in 7-Mode and the other system uses the clustered Data ONTAP operating system.

Starting with clustered Data ONTAP 8.3, SnapMirror version-flexible replication allows different versions of SnapMirror at the source and destination storage systems, which can be upgraded nondisruptively. For example, SnapMirror volume replication is possible from a source system that uses clustered Data ONTAP 8.3.1 to a destination system that uses clustered Data ONTAP 8.3.0. The destination storage system can be upgraded nondisruptively to version 8.3.1 without affecting replication topologies.

Note: A version-flexible relationship cannot be converted back to a default SnapMirror relationship. If a default SnapMirror relationship is needed, a rebaseline action can be performed to a new destination volume.

For detailed information and best practices, see TR-4015: SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP.

Clustered Data ONTAP Volume and Export Best Practices

Nested Junction Paths

A name is assigned to a clustered Data ONTAP volume in an SVM when the volume is created. Volumes that are used for NFS are also given a junction path, which is a mount path within the SVM starting under the root volume. A junction is analogous to a mount in a UNIX system in which a directory serves as an entry point to another file system. It is possible to use junction path names that are different from the volume name or to mount a volume on a junction path that is nested under another nonroot volume. However, these practices should be avoided because they might cause issues with SRM.

Note: For detailed information about using nested junction paths on vSphere, see section 7.4 of TR-4333: VMware vSphere 5 on NetApp Clustered Data ONTAP.

Clustered Data ONTAP does not require a separate NFS export for each volume. A namespace that includes every volume in the SVM is placed under a single NFS export. The export path, `/`, is always the same in every NFS-enabled SVM.

Junctions, a single namespace, and deep mounts eliminate the need for multiple NFS exports in a clustered Data ONTAP NFS SVM. However, these features do not provide the access control that is found in a traditional `/etc/exports` file. A clustered Data ONTAP NFS SVM uses export policies to enforce access control instead. Core differences between traditional NFS export rules and clustered Data ONTAP export policies are as follows:

Traditional NFS export access rules:

- Are defined in the exports file
- Are applied to an entire NFS export
- Cannot be reused for multiple exports
- Are used for NFS only
- Are checked on the initial NFS mount call

A clustered Data ONTAP export policy:

- Is defined by using CLI or GUI tools
- Might differ across flexible volumes in the same namespace

- Can be reused by multiple flexible volumes
- Can be used for both NFS and CIFS
- Is checked on junction traversal to a new flexible volume

  Note: For detailed information about namespaces in clustered Data ONTAP, see TR-4129: Namespaces in Clustered Data ONTAP.

Qtrees

Qtrees (quota trees) are special directories that allow the application of file system quotas for NAS. Clustered Data ONTAP allows the creation of qtrees, and qtrees can exist in volumes that are replicated with SnapMirror. However, SnapMirror does not allow replication of individual qtrees or qtree-level replication. All SnapMirror replication occurs only at the volume level.

NFS allows a volume to be exported, but you should avoid mounting a directory (or qtree) below the root of the volume in vSphere deployments.

Best Practices
• Use VSC to provision datastores because VSC manages junction paths automatically. • If VSC is not being used, mount volumes on junction paths directly on the root volume by using the name of the volume as the junction path. • Do not use junction paths for volumes that contain LUN datastores.

Supported Replication Technologies

NetApp SRA for clustered Data ONTAP supports asynchronous volume SnapMirror data replication technology. However, NetApp SRA does not support SnapVault, asynchronous qtree SnapMirror, or NetApp MetroCluster™ SyncMirror® data replication software.

VASA Provider Considerations

NetApp SRA 3.0 requires preinstallation of NetApp VASA Provider 6.2 for clustered Data ONTAP at both the protected site and the recovery site. VASA Provider is offered as a virtual appliance that is distributed as an OVA file. After the virtual appliance is deployed onto an ESXi host, it must be registered with NetApp Virtual Storage Console (VSC) 6.2 for VMware vSphere.

Because NetApp SRA 3.0 depends on VASA Provider for all SRM workflows, such as recovery and reprotect, it is critical that you maintain this appliance VM in a high-availability vSphere environment.

Note: You can perform maintenance tasks that are associated with VASA Provider from the CLI, including managing network and server issues, managing Secure Shell configurations, generating log bundles, and performing diagnostics.

For detailed information and best practices, see section 3.7 of TR-4400: Applying VMware vSphere Virtual Volumes on NetApp Clustered Data ONTAP 8.3.

Best Practices
• Do not install or migrate VASA Provider or VSC onto a virtual volume (VVol) datastore. Because of the circular nature of VVols, moving these critical infrastructure items to a VVol makes them inaccessible during a catastrophic event such as a power outage. • Back up the VASA Provider VM regularly. At a minimum, create hourly Snapshot copies of the non-VVol datastore that contains VASA Provider. For more information, see NetApp KB 3014620.

1.9 Site Recovery Manager 6 Supported Storage and Replication Layouts

In clustered Data ONTAP, the physical components of a cluster are visible to cluster administrators, but they are not directly visible to the applications and hosts that use the cluster. The physical components provide a pool of shared resources from which the logical cluster resources are constructed. Applications and hosts access data only through SVMs that contain volumes and LIFs.

Each NetApp SVM is treated as an array in VMware vCenter Site Recovery Manager. SRM supports certain array-to-array (or SVM-to-SVM) replication layouts.

A single VM cannot own data—Virtual Machine Disk (VMDK) or RDM—on more than one SRM array for the following reasons:

- SRM sees only the SVM, not an individual physical controller.
- An SVM can control LUNs and volumes that span multiple nodes in a cluster.

Best Practice
To determine supportability, keep this rule in mind: To protect a VM by using SRM and the NetApp SRA, all parts of the VM must exist on only one SVM. This rule applies at both the protected site and the recovery site.

Supported SnapMirror Layouts

Figure 15 through Figure 18 show the SnapMirror relationship layout scenarios that SRM and SRA support. Each VM in the replicated volumes owns data on only one SRM array (SVM) at each site.

Figure 15) Supported storage layout for SRM—scenario 1.

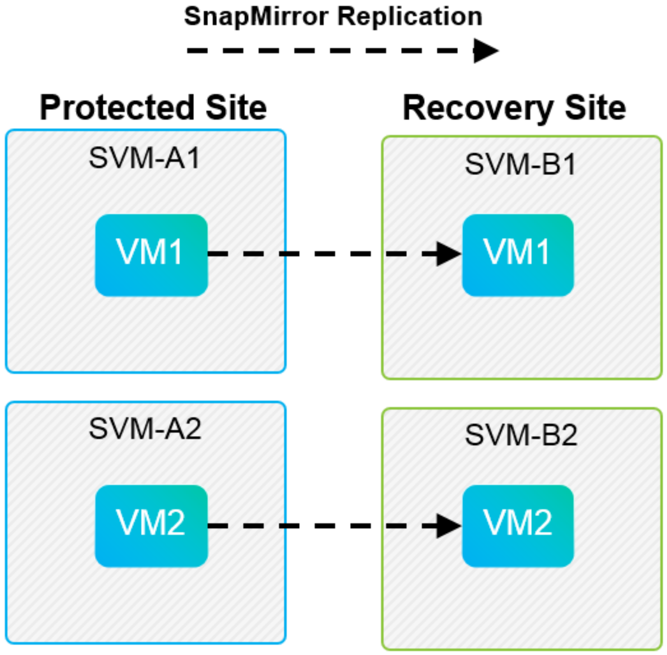


Figure 16) Supported storage layout for SRM—scenario 2.

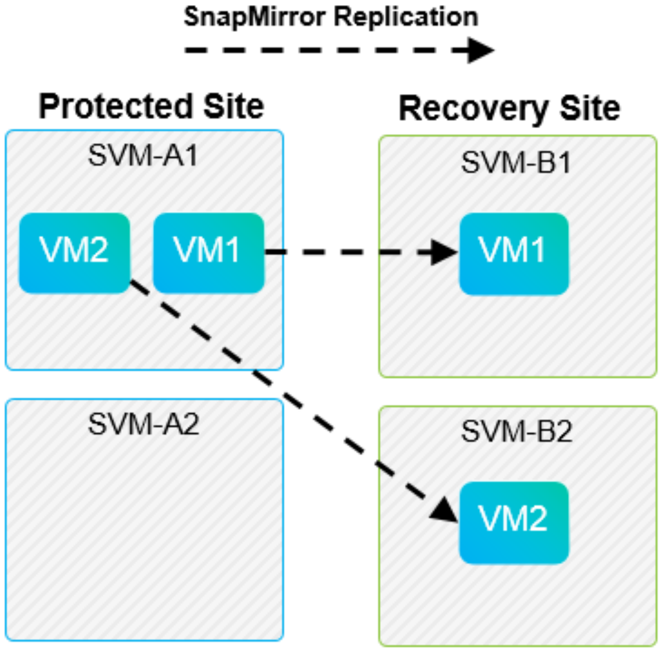


Figure 17) Supported storage layout for SRM—scenario 3.

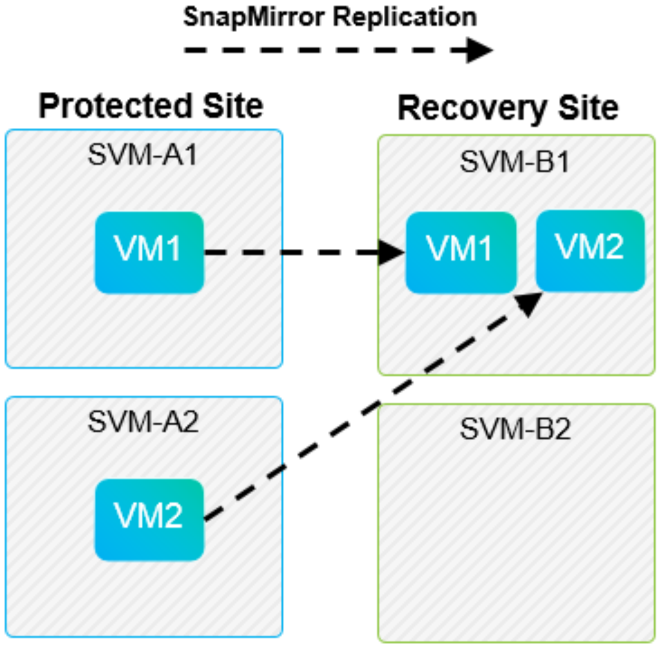
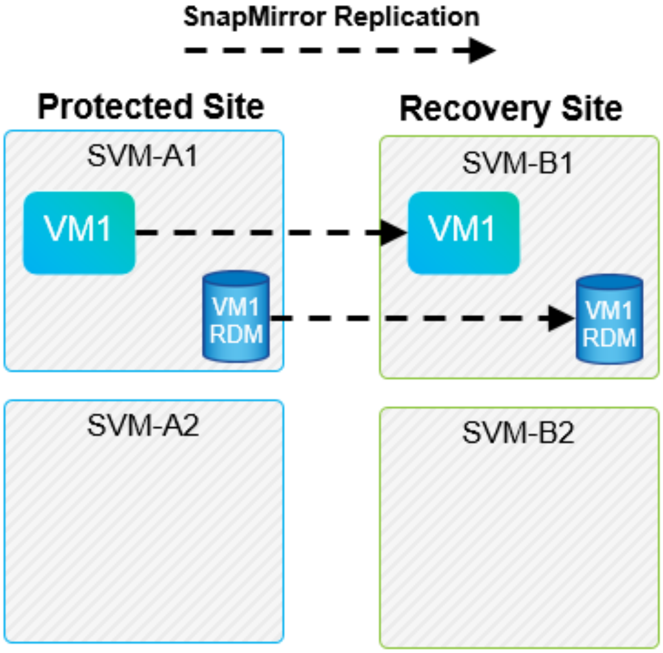
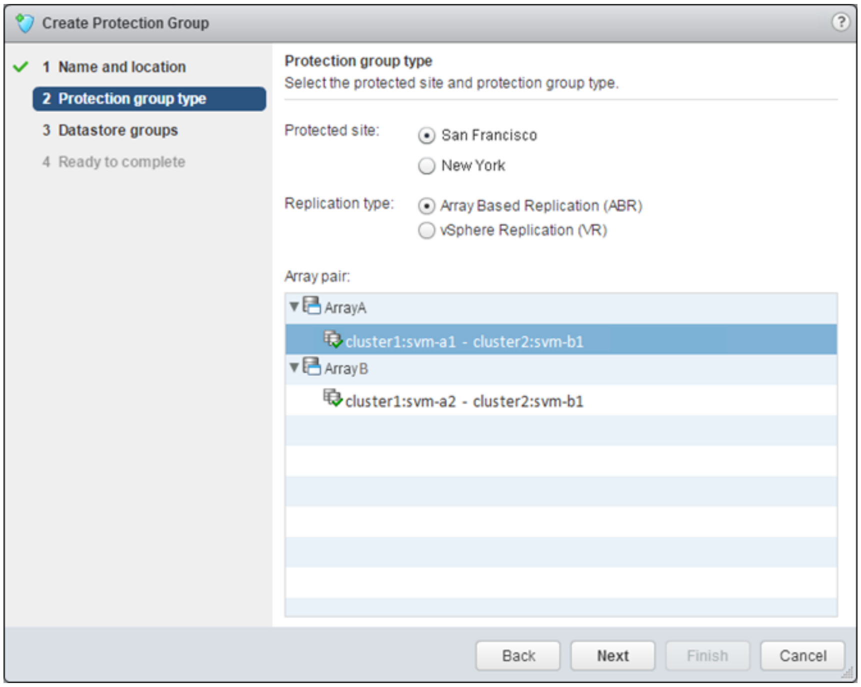


Figure 18) Supported storage layout for SRM—scenario 4.



Supported Array Manager Layouts

When you use array-based replication (ABR) in SRM, protection groups are isolated to a single array pair, as shown in the following screenshot. In this scenario, `SVM-A1` and `SVM-A2` are peered with `SVM-B1` at the recovery site in a fan-in configuration (see Figure 17). However, you can select only one of the two array pairs when you create a protection group.



Protection group type

Select the protected site and protection group type.

Protected site: ● San Francisco ○ New York

Replication type: ● Array Based Replication (ABR) ○ vSphere Replication (VR)

Array pair:

- ArrayA
  - cluster1:svm-a1 - cluster2:svm-b1
- ArrayB
  - cluster1:svm-a2 - cluster2:svm-b1

Unsupported Layouts

Unsupported configurations have data (VMDK or RDM) on multiple SVMs that is owned by an individual VM. In the examples shown in Figure 19 and Figure 20, `VM1` cannot be configured for protection with SRM because `VM1` has data on two SVMs.

Figure 19) Unsupported replication layout—scenario 1.

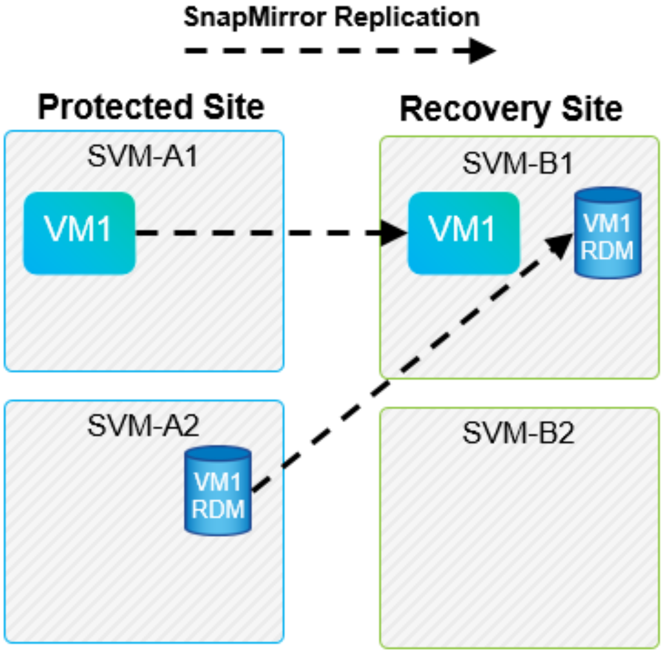
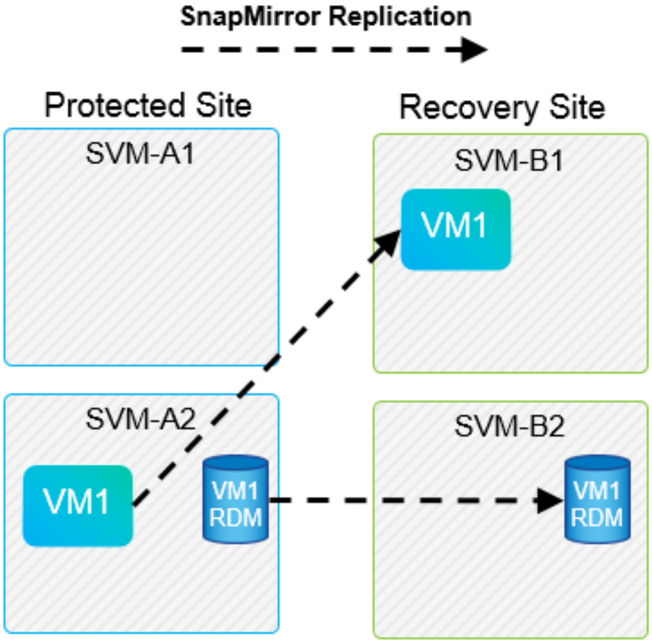
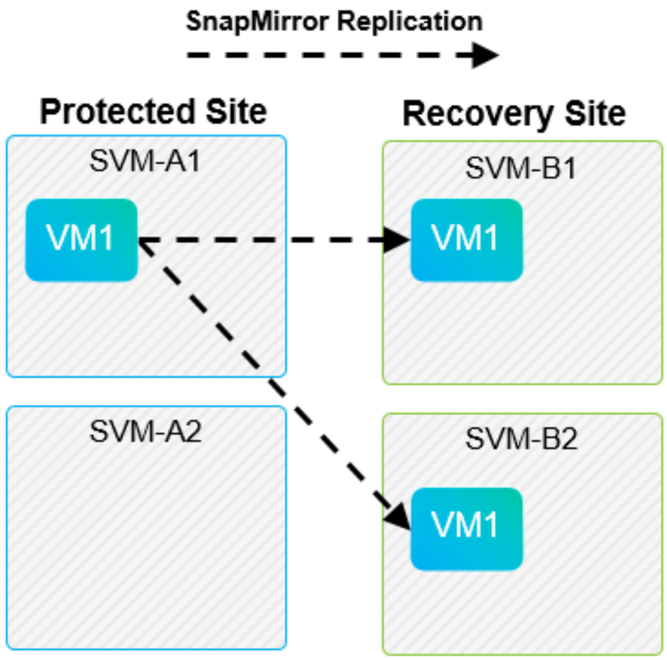


Figure 20) Unsupported replication layout—scenario 2.



Any replication relationship in which an individual NetApp volume is replicated from one source SVM to multiple destinations in the same SVM or in different SVMs is referred to as SnapMirror fan-out. Fan-out is not supported with SRM. In the example shown in Figure 21, `VM1` cannot be configured for protection in SRM because it is replicated with SnapMirror to two different locations.

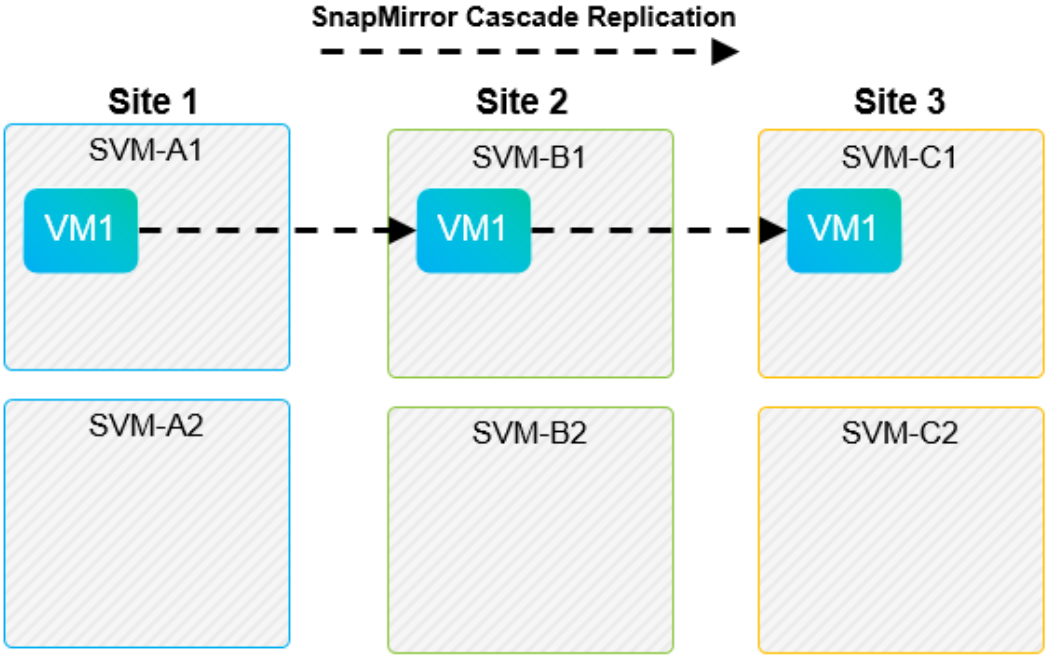
Figure 21) Unsupported replication layout—scenario 3.



SnapMirror Cascade

SRM does not support cascading of SnapMirror relationships, in which a source volume is replicated to a destination volume and that destination volume is also replicated by using SnapMirror to another destination volume. In the scenario shown in Figure 22, SRM cannot be used for failover between any sites.

Figure 22) Unsupported replication layout—scenario 4.



SnapMirror and SnapVault

NetApp SnapVault software enables disk-based backup of enterprise data between NetApp storage systems. SnapVault and SnapMirror can coexist in the same environment; however, SRM supports the failover of only the SnapMirror relationships.

Note: The NetApp SRA supports the `mirror-vault` policy type.

SnapVault was rebuilt from the ground up for its debut in clustered Data ONTAP 8.2. Although former Data ONTAP 7-Mode users should find similarities, major enhancements have been made in this version of SnapVault. One major advance is the ability to preserve storage efficiencies on primary data during SnapVault transfers.

An important architectural change is that SnapVault in clustered Data ONTAP replicates at the volume level as opposed to at the qtree level, as is the case in 7-Mode SnapVault. This setup means that the source of a SnapVault relationship must be a volume, and that volume must replicate to its own volume on the SnapVault secondary system.

In an environment in which SnapVault is used, specifically named Snapshot copies are created on the primary storage system. Depending on the configuration implemented, the named Snapshot copies can be created on the primary system by a SnapVault schedule or by an application such as NetApp OnCommand Unified Manager. The named Snapshot copies that are created on the primary system are then replicated to the SnapMirror destination, and from there they are vaulted to the SnapVault destination.

A source volume can be created in a cascade configuration in which a volume is replicated to a SnapMirror destination in the DR site, and from there it is vaulted to a SnapVault destination. A source volume can also be created in a fan-out relationship in which one destination is a SnapMirror destination and the other destination is a SnapVault destination. However, SRA does not automatically reconfigure the SnapVault relationship to use the SnapMirror destination volume as the source for the vault when SRM failover or replication reversal occurs.

For the latest information about SnapVault for clustered Data ONTAP, including changes for the 7-Mode version of SnapVault, see TR-4183: SnapVault Best Practices Guide for Clustered Data ONTAP.

Best Practice

If SnapVault and SRM are used in the same environment, NetApp recommends using a SnapMirror to SnapVault cascade configuration in which SnapVault backups are normally performed from the SnapMirror destination at the DR site. In the event of a disaster, this configuration makes the primary site inaccessible. Keeping the SnapVault destination at the recovery site allows SnapVault backups to be reconfigured after failover so that SnapVault backups can continue while operating at the recovery site.

In a VMware environment, each datastore has a universal unique identifier (UUID), and each VM has a unique managed object ID (MOID). These IDs are not maintained by SRM during failover or failback. Because datastore UUIDs and VM MOIDs are not maintained during failover by SRM, any applications that depend on these IDs must be reconfigured after SRM failover. An example application is NetApp OnCommand Unified Manager, which coordinates SnapVault replication with the vSphere environment.

Figure 23 depicts a SnapMirror to SnapVault cascade configuration. If the SnapVault destination is at the DR site or at a tertiary site that is not affected by an outage at the primary site, the environment can be reconfigured to allow backups to continue after failover.

Figure 23) SnapMirror to SnapVault cascade configuration.

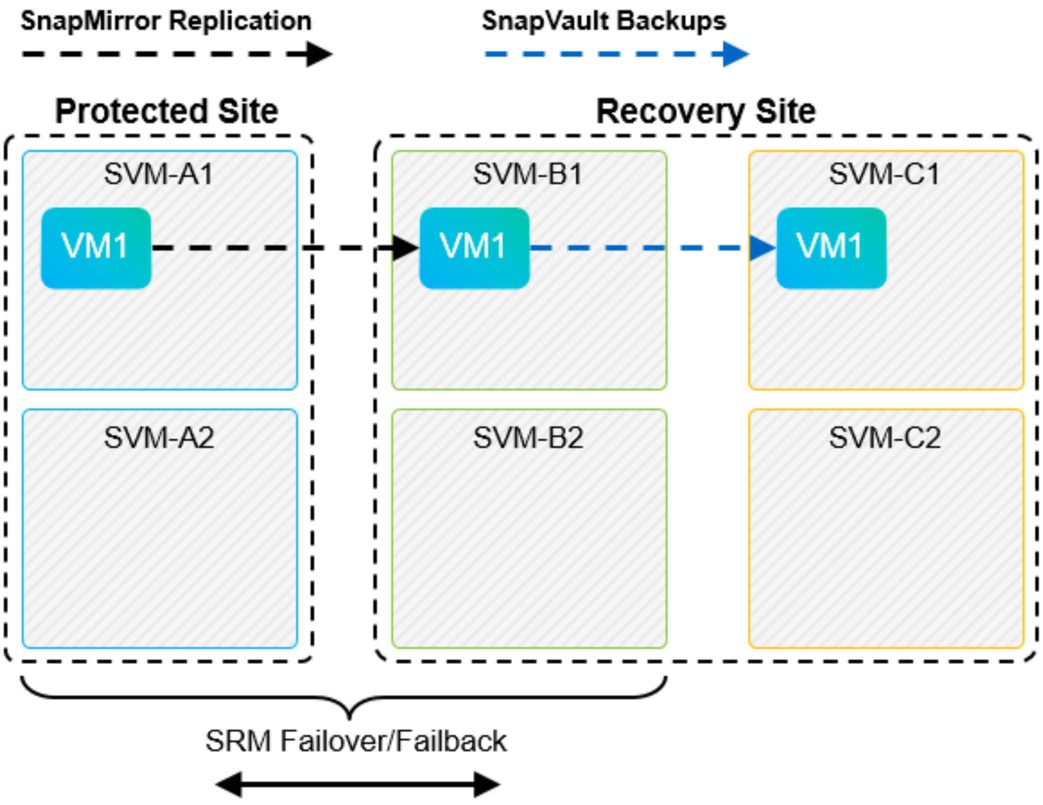
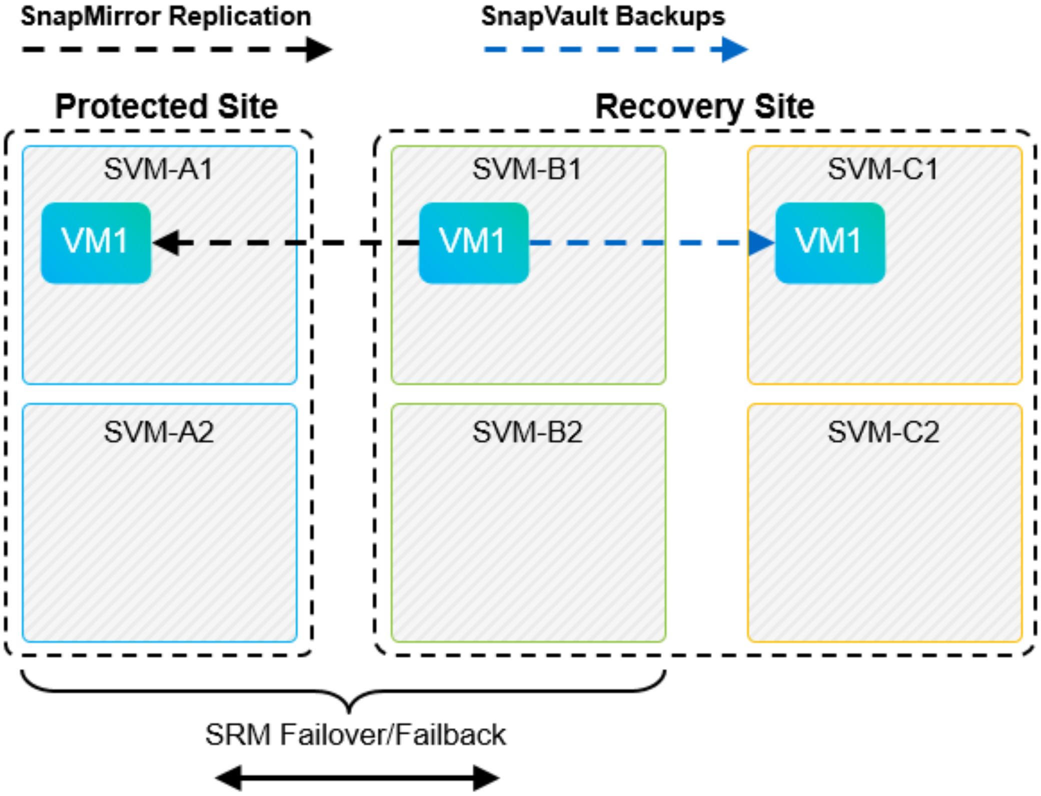


Figure 24 depicts the configuration after SRM has been used to reverse SnapMirror replication back to the primary site. The environment has also been reconfigured such that SnapVault backups are occurring from what is now the SnapMirror source. This setup is a SnapMirror SnapVault fan-out configuration.

Figure 24) SnapMirror SnapVault fan-out configuration.



After SRM performs failback and a second reversal of the SnapMirror relationships, the production data is back at the primary site. This data is now protected in the same way that it was before the failover to the DR site—through SnapMirror and SnapVault backups.

Use of Qtrees in Site Recovery Manager Environments

Qtrees are special directories that allow the application of file system quotas for NAS. Clustered Data ONTAP allows the creation of qtrees, and qtrees can exist in volumes that are replicated with SnapMirror. However, SnapMirror does not allow replication of individual qtrees or qtree-level replication. All SnapMirror replication is at the volume level only. For this reason, NetApp does not recommend the use of qtrees with SRM.

Mixed FC and iSCSI Environments

With the supported SAN protocols (FC, FCoE, and iSCSI), clustered Data ONTAP provides LUN services—that is, the ability to create and map LUNs to attached hosts. Because the cluster consists of multiple controllers, there are multiple logical paths that are managed by multipath I/O to any individual LUN. Asymmetric logical unit access (ALUA) is used on the hosts so that the optimized path to a LUN is selected and is made active for data transfer. If the optimized path to any LUN changes (for example, because the containing volume is moved), clustered Data ONTAP automatically recognizes and nondisruptively adjusts for this change. If the optimized path becomes unavailable, clustered Data ONTAP can nondisruptively switch to any other available path.

VMware SRM and NetApp SRA support the use of the FC protocol at one site and the iSCSI protocol at the other site. It does not support having a mix of FC-attached datastores and iSCSI-attached datastores in the same ESXi host or in different hosts in the same cluster, however.

NetApp clustered Data ONTAP no longer supports a mixed ALUA configuration. ALUA is enabled by default on all igroups and can be disabled only in `diag` mode. A mixed ALUA configuration is one that includes both ALUA-enabled and ALUA-disabled igroups. That is, one ESXi host, or multiple ESXi hosts in the same cluster, has some initiators configured in ALUA-enabled igroups, and the same ESXi host or hosts have other initiators configured in ALUA-disabled igroups. This configuration is not supported with SRM because, during the SRM failover or test failover, SRM includes all FC and iSCSI initiators in the ESXi hosts in the request.

An example of an unsupported ALUA configuration in an ESX or ESXi cluster is one in which the cluster contains ESX 3.5, ESX 4, and ESX 5 hosts. The ESX 3.5 hosts require ALUA to be disabled, and the ESX 4 or ESX 5 hosts have ALUA enabled. Because SRM would include all the initiators from all the hosts in one failover or test failover request, the configuration cannot be supported.

Best Practice
SRM and SRA support mixed FC and iSCSI protocols between the protected and recovery sites. However, each site should be configured with only one protocol, either FC or iSCSI, not both protocols at the same site. If a requirement exists to have both FC and iSCSI protocols configured at the same site, NetApp recommends that some hosts use iSCSI and other hosts use FC. NetApp also recommends in this case that SRM resource mappings be set up so that the VMs are configured to fail over into one group of hosts or the other.

2 Deployment Procedure

To configure SRM to protect the VMs that were replicated by NetApp SnapMirror software, complete the following steps.

Note: You must complete the configuration before you execute the test recovery operation.

1. Ensure that the protected and recovery sites have been peered at both the cluster and the SVM level.
2. Provision storage volumes on the protected site for replication.
3. Use SnapMirror to set up NAS or SAN array-based replication from the protected site to the recovery site.
4. Install SRM 6 Server on both the protected site and the recovery site.
5. Install NetApp VASA Provider 6.2 and Virtual Storage Console 6.2 on both the protected site and the recovery site.
6. Install NetApp SRA 3.0 on each of the SRM 6 servers.
7. Configure SRM to protect the VMs that are replicated by SnapMirror:
    a. Connect the vCenter sites in the SRM interface.
    b. Configure the inventory mappings. This step aligns resources such as hosts, clusters, and networks at the protected site with the resources that are used for recovery at the recovery site.
    c. Pair the protected and recovery site SVMs by using Array Manager. This step enables SRM to communicate with the NetApp SVMs for issuing SnapMirror failover commands, mapping LUNs to igroups, exporting NFS datastores, and so on.
8. Build SRM protection groups. Protection groups define groups of VMs that are recovered together and are restricted to resources within a single array manager.
9. Build SRM recovery plans. Recovery plans identify the start-up priority for the VMs, timeout settings for waiting for recovered VMs to respond, additional custom commands to execute, and so on.

Table 3) Prerequisites for SRM 6 on clustered Data ONTAP.

Description of Prerequisite
Each site must have a vCenter server and an SRM server. These components can be installed on the same server, but it is a best practice to install them on a separate VM.
After installation, the Site Recovery icon appears in the vSphere Web Client on the protected site. In SRM 5.8 and later, there is no plug-in available with the vSphere c# client.
Managing failover of SnapMirror relationships with SRM 6 requires the use of NetApp SRA 3.0 for clustered Data ONTAP. The NetApp SRA can be obtained from the software download section of the NetApp Support site or from the VMware SRM download page.
Intel or AMD x86 processors with at least two 2.0GHz cores are required.
At least 2GB of memory is required.
At least 5GB of disk storage is required.
Network requirements: • 1Gb is recommended for communication between SRM sites. • Use a trusted network to manage ESXi hosts.
Software
VMware vCenter SRM 6.0 or 6.1 and vCenter Server 6.0: • Install the same version of SRM Server and vCenter Server on both sites. • Do not mix SRM and vCenter Server versions across sites.
VMware vCenter SRM 5.8 and vCenter Server 5.5: • Install the same version of SRM Server and vCenter Server on both sites. • Do not mix SRM and vCenter Server versions across sites.
ESX or ESXi: • Review the SRM Compatibility Matrix on the VMware Site Recovery Manager Documentation page of the VMware website. • Make sure that the environment has supported versions of vCenter Server and ESX or ESXi servers.
NetApp Storage Replication Adapter for clustered Data ONTAP: • Version 3.0 is compatible with SRM 5.8, 6.0, and 6.1. The following prerequisites for NetApp SRA 3.0 can be obtained from the NetApp software download site: • NetApp VASA Provider 6.2 for clustered Data ONTAP. • NetApp Virtual Storage Console 6.2 for clustered Data ONTAP.
NetApp clustered Data ONTAP: • Run a supported version of clustered Data ONTAP. • Review the supported versions of the clustered Data ONTAP operating system. Find supported versions in the SRM Storage Partner Compatibility Matrix on the VMware Site Recovery Manager Documentation page of the VMware site and in the Interoperability Matrix Tool (IMT) on the NetApp Support site.
NetApp SnapMirror and FlexClone licenses are required.
NetApp SRA 3.0 installation
A license is required for the storage protocol (NFS, iSCSI, or FC) that is used in the solution.

Description of Prerequisite
NetApp VASA Provider 6.2 and Virtual Storage Console 6.2 must be preinstalled and configured before the NetApp SRA 3.0 installation.
If upgrading from a previous version of SRA, the earlier version of the NetApp adapter must be uninstalled before installing NetApp SRA 3.0.
SRM must be installed.
Connect the protected and recovery sites
SRM must be installed at each site.
The Site Recovery icon must be visible under the Home tab on the protected site's vSphere Web Client.
The vCenter Servers at each site must be able to communicate by HTTP on port 80.
Configure NetApp SRA and discover storage
SRM must be installed on the SRM server at each site.
The source and destination vCenter sites must be paired in the SRM interface.
To support SRM 5.8, 6.0, or 6.1, NetApp SRA 3.0 must be installed.
SnapMirror relationships must be configured and replicated.
Storage discovery
To be able to protect a VM with SRM and the NetApp SRA, all parts of the VM must exist on only one NetApp SVM at both the protected site and the recovery site.
Protection group
NetApp SRA must have been configured at each SRM site.
The SRM array pair must have been enabled, and storage discovery must have been successfully performed by SRM.
To be able to protect a VM with SRM and the NetApp SRA, all parts of the VM must exist on only one NetApp SVM, at both the protected site and the recovery site.

2.1 Verify Storage Setup

Verify that the storage environment is set up correctly before you configure SRA and perform the first SRM test recovery. Before proceeding, ensure that cluster and SVM peering has been established between the protected site and the recovery site.

Verify Storage Setup in a SAN Environment

Verify that the following steps are completed and that the storage setup is successful.

Note: This process is required only for environments that use FC or iSCSI.

1. Connect the protected site's ESXi hosts to LUNs in the protected site storage system.
2. At the protected site, configure the source FC or iSCSI LUNs in igroups that have the `vmware` igroup type. When you use RDM disks with VMware, the igroup type must be set to `vmware`. However, the LUN type can be set to whichever operating system type that the guest VM requires.

   Note: NetApp SRA 3.0 for clustered Data ONTAP automatically creates igroups as needed at the recovery site during recovery and test recovery operations.

3. Replicate the volume that contains the LUNs to the recovery site storage system.
4. Confirm that the ESXi hosts at the recovery site have appropriate FC or iSCSI connectivity to the SVM:
    a. Check whether an existing datastore is connected to the ESXi hosts at the recovery site that is already using the storage network. The existence of such a datastore indicates storage network connectivity.

    b. If existing datastores are not connected on the recovery SVM, verify storage network connectivity by using `the fcp initiator show` or `iscsi initiator show` command on the SVMs.

The following example issues the command at the cluster level:

```
iscsi initiator show -vserver <SVM Name>
```

> **Note:** If iSCSI is used at the recovery site, configure the ESXi iSCSI initiators to connect them to the recovery site SVM. SRM does not configure the connection from an ESXi iSCSI initiator to the NetApp iSCSI target SVM.

Verify Storage Setup in NAS Environments

A clustered Data ONTAP NFS SVM uses export policies to enforce access restrictions and does not require a separate NFS export for each volume. A namespace that includes every volume in the SVM is placed under a single NFS export. The export path, `/`, is always the same in every NFS-enabled SVM.

To discover an exported volume in a NAS environment, verify the following items:

- Volumes are mounted on junction paths.
- Volumes are associated with a valid export policy.
- A rule for the valid export policy that is attached to the volume is created.
- The NFS server is running at the destination SVM.
- The group and user IDs are set to zero.

For detailed information about export policies in clustered Data ONTAP, see TR-4129: Namespaces in Clustered Data ONTAP.

Verify that the following steps were completed and that the storage setup was successful.

Note: This process is required only for environments that use NFS.

1. Register the VMs for the datastores at the protected site with vCenter Server.
2. Mount the NFS exported volumes from the SVM for the ESXi hosts at the protected site.
3. Enter valid addresses (IP address, host name, and FQDN) in the NFS Addresses field when you use the Array Manager wizard to add arrays to SRM.
4. Verify that the ESXi hosts at the recovery site storage system have a VMkernel port that can access the IP addresses that are used to serve NFS exports from the SVM:
    a. Use the `vmkping nfs_ip_address` command on the ESXi shell or ESX service console of each ESXi or ESX host. `nfs_ip_address` is one of the NFS IP addresses on the SVM.

    b. Verify whether access to the ESXi shell is disabled by using the ping `vmkernel_ip_address` command on the console of the SVM. `vmkernel_ip_address` is one of the IP addresses on the VMkernel port that the ESXi host uses to access the SVM.
5. Replicate the volume that contains the exports to the recovery site storage system by using NetApp OnCommand System Manager or by using the Data ONTAP CLI.
6. On the recovery site storage system, enter the command `snapmirror list-destinations` to display a list of replicated destinations and to confirm that the volume is replicated.

7. At the recovery site, verify that proper storage connectivity exists between the NetApp storage array and the ESXi hosts.

Verify Replication

Verify that the following steps were completed and that the replication was successful.

Note: This process is required for both SAN and NAS environments.

1. Use SnapMirror to replicate to the recovery site all the datastores that contain the VMs that are protected with SRM. Note the following issues:
   - SRM does not perform scheduled SnapMirror updates or baseline transfers. Periodic SnapMirror transfers must be managed and scheduled by using NetApp software such as the built-in scheduler in clustered Data ONTAP or OnCommand System Manager.
   - NetApp SRA does not support fan-out replication by using SnapMirror to mirror a datastore to multiple different destinations. This limitation includes cascaded SnapMirror to SnapMirror relationships. Use the `snapmirror list-destinations` command on the source system to display all the destinations for a source. Each source should have only one destination.
   - NetApp SRA ignores SnapVault relationships; a source can be replicated with SnapMirror and with SnapVault. However, SnapVault relationships that are not reconfigured as SnapMirror relationships are failed over and are reversed with SRM.
2. Configure at least one VM in the datastore to enable recovery with SRM. To be discovered by SRM, datastores must contain VMs or virtual disks that are owned by VMs. This VM does not need to be a complete VM and it does not have to be configured with a virtual disk; simply create an empty VM in the datastore.

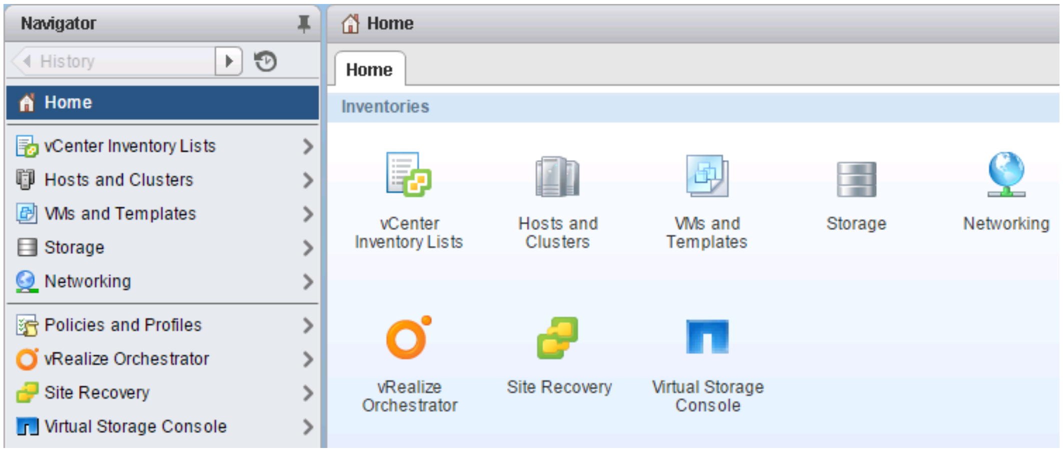
2.2 Install Site Recovery Manager 6

For detailed instructions about installing and configuring SRM, see the [VMware Site Recovery Manager Documentation]().

Verify the vSphere Web Client Plug-In

After SRM has been installed, the Site Recovery vSphere Web Client plug-in becomes visible under the Home tab in the Inventories section. To verify the plug-in, complete the following steps:

1. Open the vSphere Web Client on either the protected site or the recovery site.
2. Click Home.
3. Verify that the Site Recovery icon is present.



Install a Site Recovery Manager License Key

After SRM has been installed, it remains in evaluation mode until the SRM license key is installed. If the license expires, the protection groups that exist must still be protected and can be recovered, but you cannot create new protection groups or add VMs to the existing groups. To obtain SRM license keys, navigate to the SRM Product Licensing Center on the VMware website.

2.3 Install NetApp Storage Replication Adapter 3.0

Install VASA Provider and Virtual Storage Console

To install NetApp SRA 3.0, you must first install NetApp Virtual Storage Console 6.2 and VASA Provider 6.2 for clustered Data ONTAP. These prerequisites must be installed and configured in your vSphere environment before you install NetApp SRA 3.0. Complete the following steps to install VASA Provider and VSC.

Note: If you are upgrading from previous versions of VASA Provider and VSC, first unregister the VASA Provider from VSC before you run the upgrade procedures.

1. Install VSC on a Windows Server (physical or virtual).
2. Register VSC with vCenter.
3. Configure VSC and register your NetApp storage systems.
4. Deploy the VASA Provider OVA file on an ESXi host.
5. Configure the VASA Provider virtual appliance and register with VSC.

For detailed information about installing and configuring VSC, see the Virtual Storage Console for VMware vSphere documentation library.

For detailed information about installing and configuring VASA Provider, see the VASA Provider for Clustered Data ONTAP documentation library.

Upgrade from Site Recovery Manager 5.5 or Earlier to Site Recovery Manager 6

You must uninstall earlier versions of the NetApp SRA for clustered Data ONTAP before you install NetApp SRA 3.0 for clustered Data ONTAP. To upgrade from SRM 5.5 or earlier to SRM 6, complete the following steps for each SRM server that is being upgraded.

Note: NetApp SRA 3.0 can coexist with NetApp SRA 2.1 for 7-Mode on the same SRM server.

1. Uninstall the earlier version of NetApp SRA for clustered Data ONTAP.
2. Uninstall SRM 5.5 or earlier and install SRM 6 Server. Refer to the SRM upgrade procedures listed in the “Site Recovery Manager Administration” section of the VMware Site Recovery Manager Documentation webpage.
3. Install NetApp VASA Provider 6.2 and VSC 6.2 in the vCenter environment. If you are upgrading from previous versions of VASA Provider and VSC, first unregister the VASA Provider from VSC before you run the upgrade procedures.
4. Launch the NetApp SRA 3.0 installer on the SRM 6 server.
5. Accept the license agreement in the Installer wizard.
6. Proceed through the Installer wizard.
7. Complete the SRM upgrade procedures that are listed in the “Site Recovery Manager Administration” section of the VMware Site Recovery Manager Documentation webpage.
8. Repeat this process for the other SRM server.

A user might attempt to uninstall the previous version of the SRA when the SRM 5.5 or earlier software has already been uninstalled. In that case, a message displays that the adapter cannot be uninstalled because the SRM 5.5 or earlier software does not exist. The workaround is to manually uninstall the previous adapter. For instructions on how to manually uninstall the previous adapter, see NetApp KB Article 2016568 on the NetApp Support site.

Complete New Installation of NetApp Storage Replication Adapter 3.0 for Site Recovery Manager 6

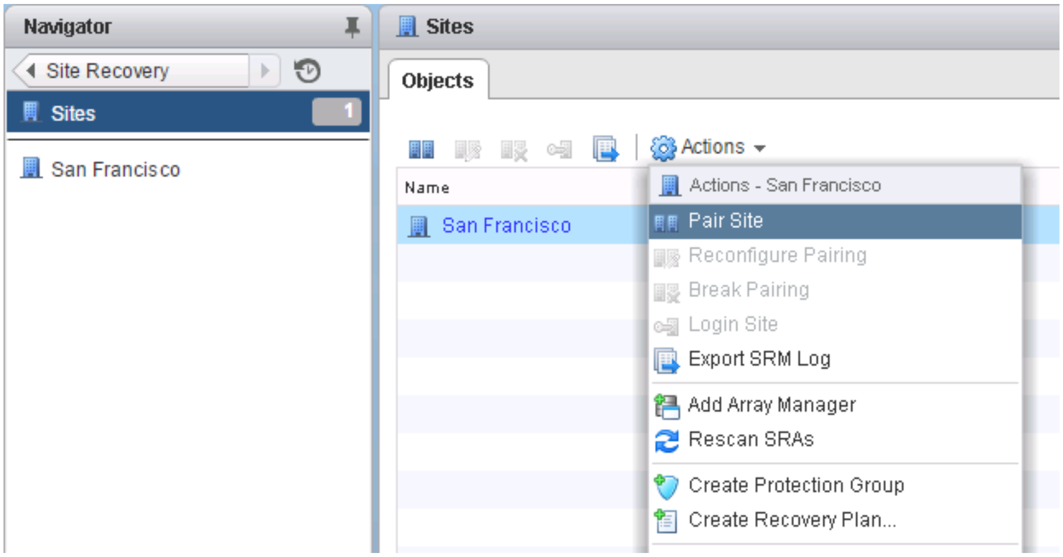
To install the NetApp SRA 3.0 for SRM 6 on a new SRM server, complete the following steps:

1. Install the SRM 6 server. Refer to the SRM installation procedures in the “Site Recovery Manager Administration” section of the VMware Site Recovery Manager Documentation webpage.
2. Install NetApp VASA Provider 6.2 and VSC 6.2 in the vCenter environment.
3. Launch the NetApp SRA 3.0 installer on the SRM server at one site.
4. Accept the license agreement in the Installer wizard.
5. Proceed through the Installer wizard.
6. Repeat this process for the other SRM server.

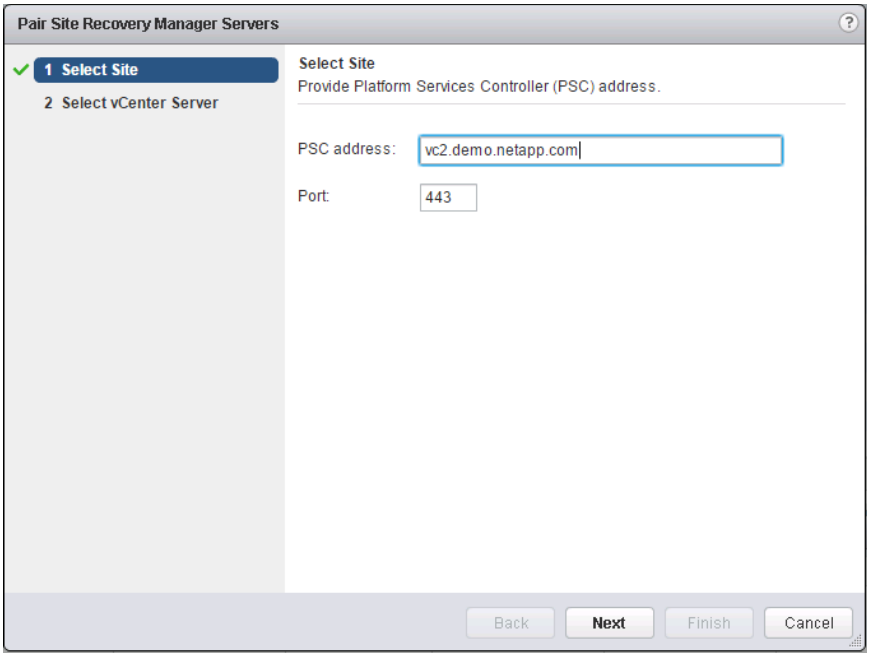
2.4 Connect Protected and Recovery Sites

To connect the protected and recovery sites, complete the following steps from the protected site:

1. Access the Site Recovery home interface from the vSphere Web Client.
2. Click the Sites tab in the left pane.
3. Click Pair Site from the Actions button in the Objects window.



4. Provide the address of the protected site’s Platform Services Controller.



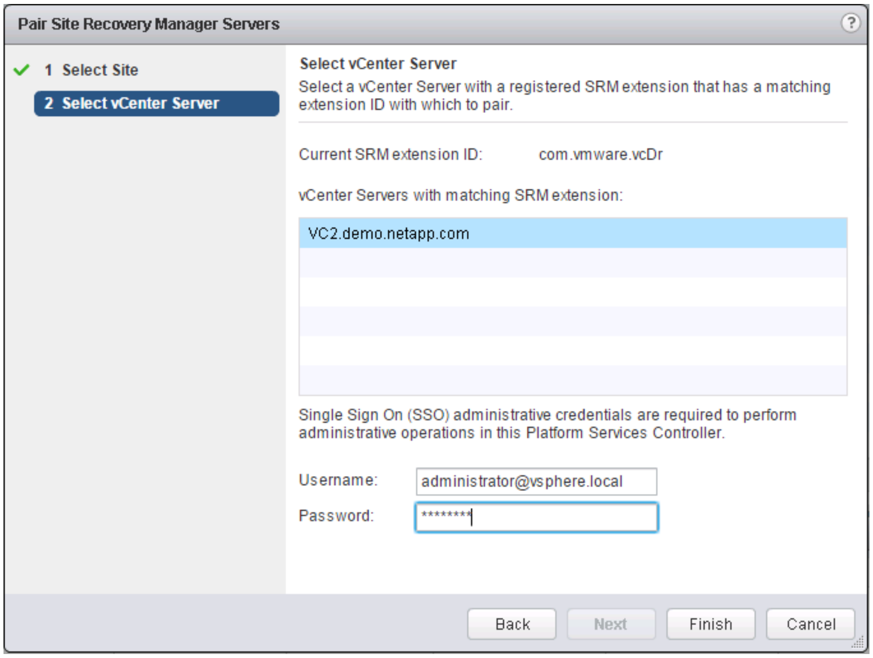
Select Site

Provide Platform Services Controller (PSC) address.

PSC address: vc2.demo.netapp.com

Port: 443

5. Make sure that the protected site's vCenter server appears as a matching candidate to pair, then enter the SSO administrative credentials. Click Finish to complete the wizard.



Select vCenter Server

Select a vCenter Server with a registered SRM extension that has a matching extension ID with which to pair.

Current SRM extension ID: com.vmware.vcDr

vCenter Servers with matching SRM extension:

VC2.demo.netapp.com

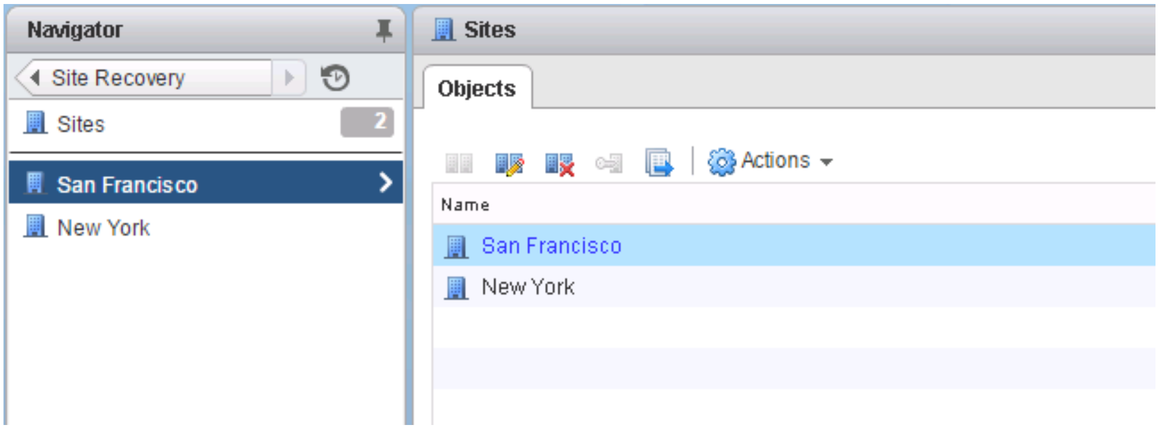
Single Sign On (SSO) administrative credentials are required to perform administrative operations in this Platform Services Controller.

Username: administrator@vsphere.local

Password: ********

6. If prompted, click yes to accept the security certificates.

7. After successfully completing the Pair Site wizard, both the protected site and the recovery site should now appear.



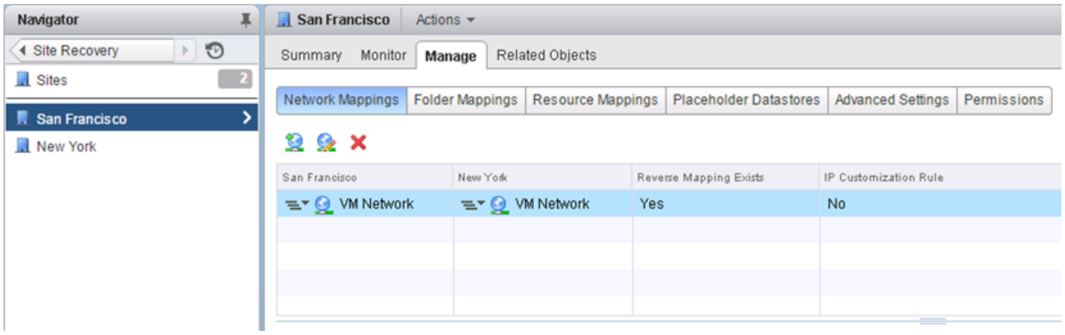
2.5 Configure Inventory Preferences

The VMware environments at the protected and recovery sites have different sets of resources, including different VM networks, ESXi hosts, folders, and so on. In this stage of configuration, a recovery site resource must be identified for each corresponding resource at the protected site.

Configure Network Mappings

To configure network mappings, complete the following steps:

1. In the Site Recovery home interface, expand the Sites tab from the left window pane and select the protected site.
2. Expand the Manage tab from the right window pane and make sure that the Network Mappings tab is selected.
3. Click the icon to create a new network mapping.
4. In the Create Network Mapping wizard, select Automatically Prepare Mappings for Networks with Matching Names and click Next.
5. Prepare the mappings by selecting the data center objects for the protected and recovery sites, and click Add Mappings. After the mapping has been successfully created, click Next.
6. Prepare a reverse mapping by selecting the object that was created in the preceding step. Click Finish to exit the wizard.
7. The Network Mappings page should now display the protected and the recovery site resources.
8. Repeat steps 1 through 6 for the other networks in the environment.

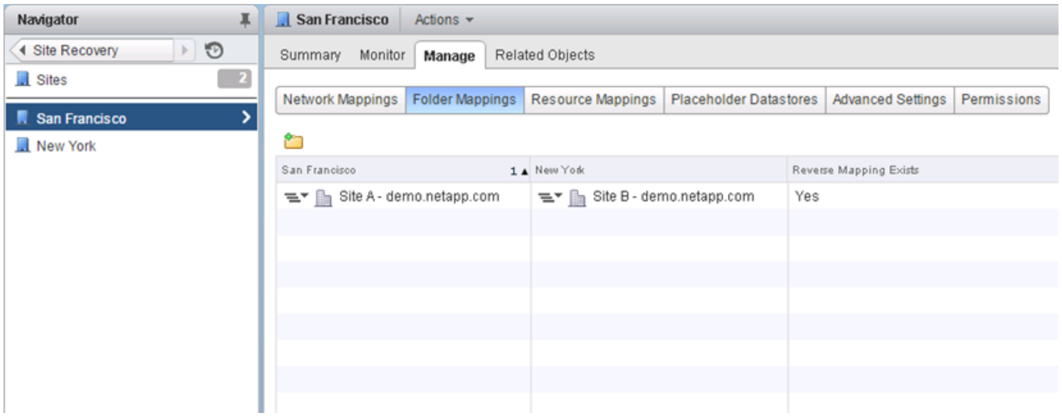


San Francisco	New York	Reverse Mapping Exists	IP Customization Rule
VM Network	VM Network	Yes	No

Configure Folder Mappings

To configure folder mappings, complete the following steps:

1. In the Site Recovery home interface, expand the Sites tab from the left window pane and select the protected site.
2. Expand the Manage tab from the right window pane and make sure that the Folder Mappings tab is selected.
3. Click the icon to create a new folder mapping.
4. In the Create Folder Mapping wizard, select Automatically Prepare Mappings for Folders with Matching Names and click Next.
5. Prepare the mappings by selecting the data center objects for the protected and recovery sites and click Add Mappings. After the mapping has been successfully created, click Next.
6. Prepare a reverse mapping by selecting the object that was created in the preceding step. Click Finish to exit the wizard.
7. The Folder Mappings page should now display the protected and recovery site resources.
8. Repeat steps 1 through 6 for the other folders in the environment.

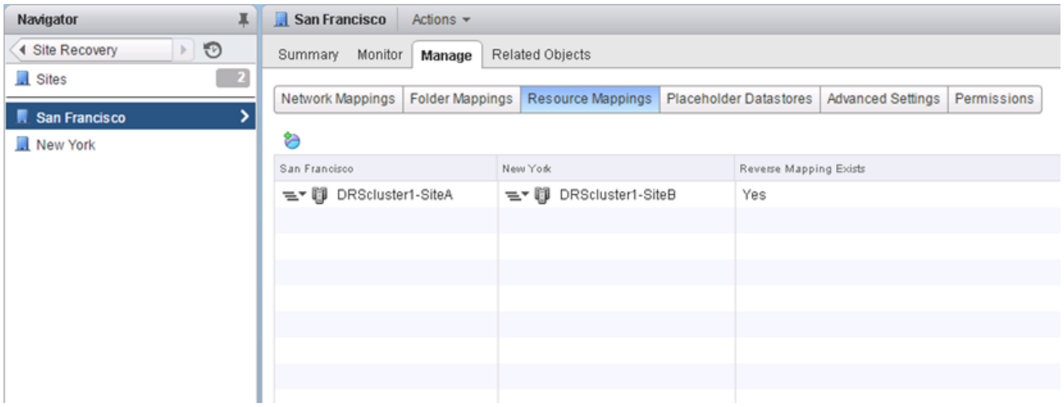


San Francisco 1 ▲	New York	Reverse Mapping Exists
Site A - demo.netapp.com	Site B - demo.netapp.com	Yes

Configure Resource Mappings

To configure the resource mappings, complete the following steps:

1. In the Site Recovery home interface, expand the Sites tab from the left window pane and select the protected site.
2. Expand the Manage tab from the right window pane and make sure that the Resource Mappings tab is selected.
3. Click the icon to create a new resource mapping.
4. In the Create Resource Mapping wizard, prepare the mappings by selecting the vSphere cluster objects for the protected and recovery sites and click Add Mappings. After the mapping has been successfully created, click Next.
5. Prepare a reverse mapping by selecting the object that was created in the preceding step. Click Finish to exit the wizard.
6. The Resource Mappings page should now display the protected and recovery site resources.
7. Repeat steps 1 through 5 for other hosts, clusters, or resource pools in the environment.



San Francisco	New York	Reverse Mapping Exists
DRScluster1-SiteA	DRScluster1-SiteB	Yes

Note: In SRM, resources can be resource pools, ESXi hosts, or vSphere clusters. In this example, a resource mapping was created between two clusters. Configure resource mappings between hosts, clusters, resource pools, or folders as appropriate for the environment.

Best Practice
SRM and the NetApp SRA support mixed FC and iSCSI protocols between the protected site and the recovery site. However, you must configure each site with only one protocol, either FC or iSCSI. Do not use both protocols at the same site. If a requirement exists to have both FC and iSCSI protocols configured at the same site, NetApp recommends that some hosts use iSCSI and others use FC. In addition, configure SRM resource mappings so that the VMs are configured to fail over into one group of hosts or the other.

Configure Placeholder Datastores

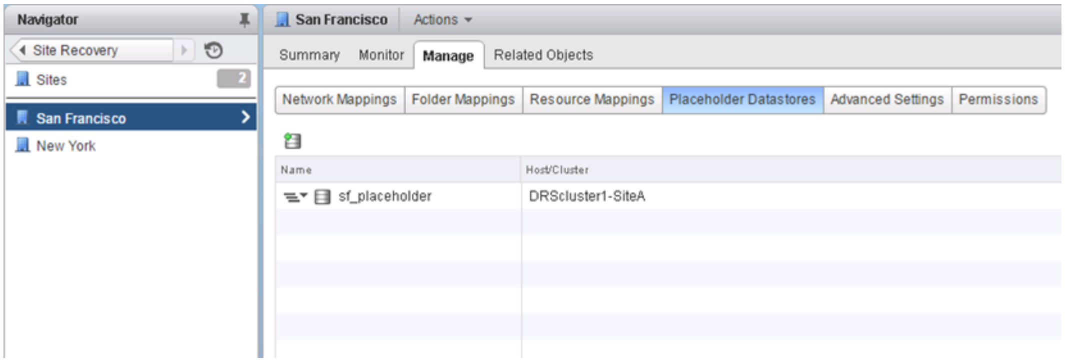
When SRM configures protection of a VM, it creates a placeholder VM with a matching name at the recovery site. This VM does not boot up or consume host resources; it exists primarily to hold a place in the vCenter inventory at the recovery site for the protected VM. A datastore must be specified at the recovery site for storing the placeholder VMs. A large placeholder datastore is not required because placeholder VMs are small and use only a few hundred or fewer kilobytes.

Best Practice
Placeholder VMs are assigned to ESXi hosts when they are added to the vCenter inventory. The host to which the placeholder VM is assigned is determined by how the resource mappings are configured in the environment. The placeholder datastore should be created on a shared storage device so that hosts can access it as required. NetApp recommends creating a dedicated small datastore, named `srm_placeholder`, for example, that is a few gigabytes in size, depending on the number of VMs in the environment.

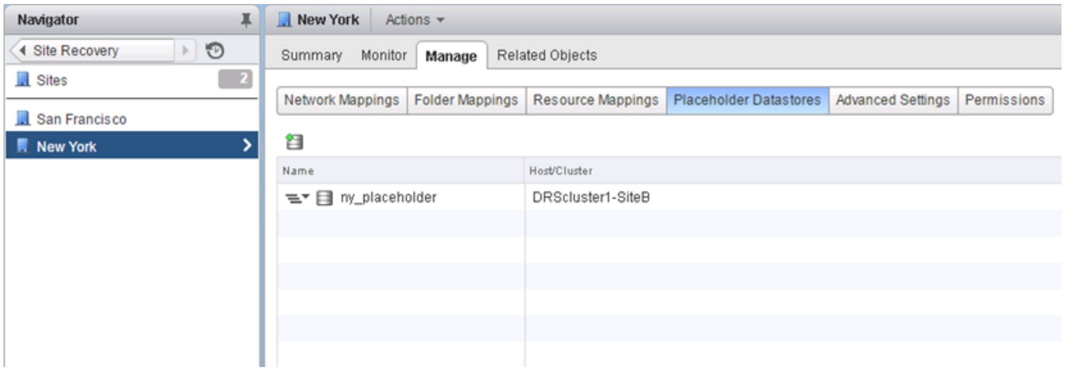
To configure a placeholder datastore at the protected site, complete the following steps:

1. In the Site Recovery home interface, expand the Sites tab from the left window pane and select the protected site.
2. Expand the Manage tab from the right window pane and make sure that the Placeholder Datastores tab is selected.
3. Click the icon to configure a placeholder datastore.
4. Select the appropriate datastore and click OK.

Note: Placeholder datastores can be local or remote and should not be replicated.



5. Repeat the process to configure a placeholder datastore on the recovery site.



2.6 Configure NetApp Storage Replication Adapter 3.0 and Discover Storage

The NetApp SRA is configured in the SRM Array Manager wizard. To configure array managers, the protected and recovery sites must already be paired in SRM, and the SnapMirror relationships must already be configured and replicated.

Configure Array Managers

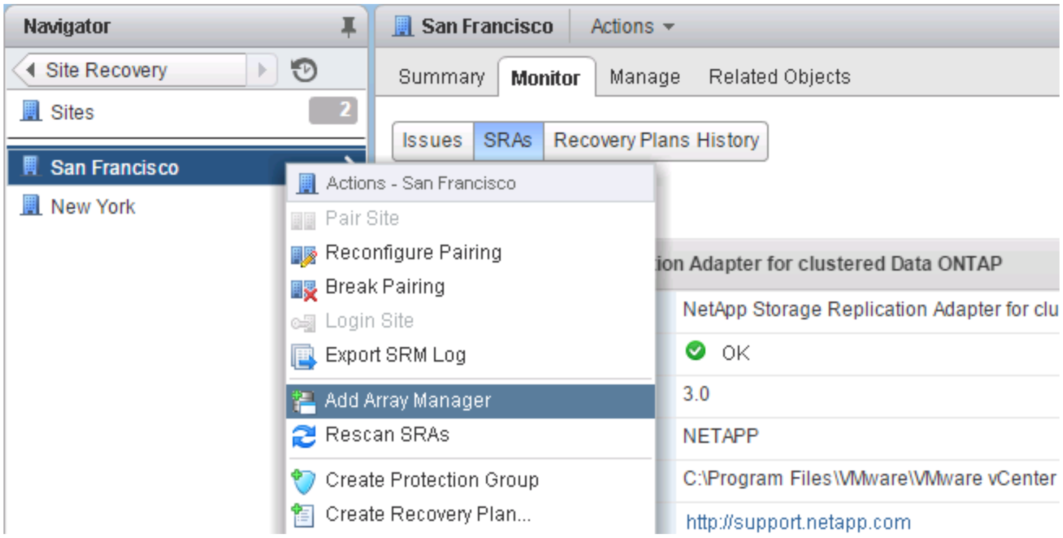
To add a NetApp SVM as an SRM array, complete the following steps on both the protected site and the recovery site. Each SVM is added only once in the vCenter site that is local to that SVM:

1. At the recovery site, check the status of the SnapMirror relationships, noting the name of the source system in the SnapMirror status output.

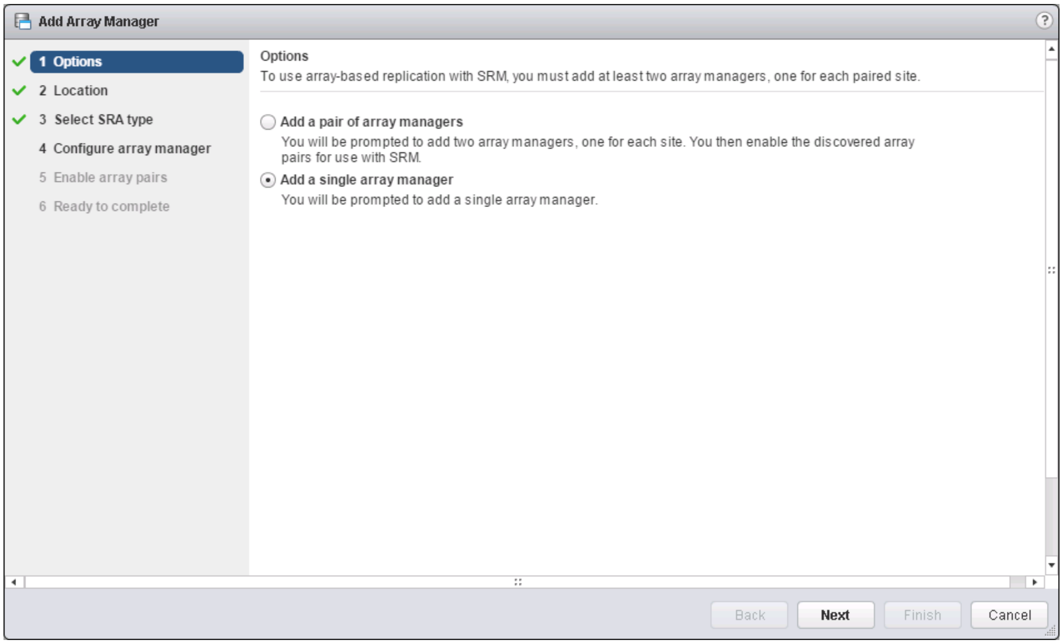
   In the following example, `svm1` is the SVM at the protected site and `svm2` is the SVM at the recovery site. The volume, `sf_nfs1`, is listed under Source Path and is mirrored by using SnapMirror software to the secondary volume, `sf_nfs1_dr`; that is, it is listed under the Destination Path. If the name shown as the source in the SnapMirror relationship at the destination site matches the name of the source volume `<SVM:volume>`, then this SnapMirror relationship can be properly discovered without configuring the SRA. Proceed to the next step to configure the array manager.

```
cluster2::> snapmirror show
                                                                       Progress
Source            Destination   Mirror  Relationship  Total             Last
Path        Type  Path          State   Status        Progress  Healthy Updated
----------- ---- ------------  -------- -------------- --------- ------- ---------
svm1:sf_nfs1   DP   svm2:sf_nfs1_dr  Snapmirrored
                                       Idle           -         true    -
```

2. In the SRM home interface, open the Sites tab from the left window pane. Right-click the protected site and select Add Array Manager.



3. In the Add Array Manager wizard, select Add a Single Array Manager and click Next.



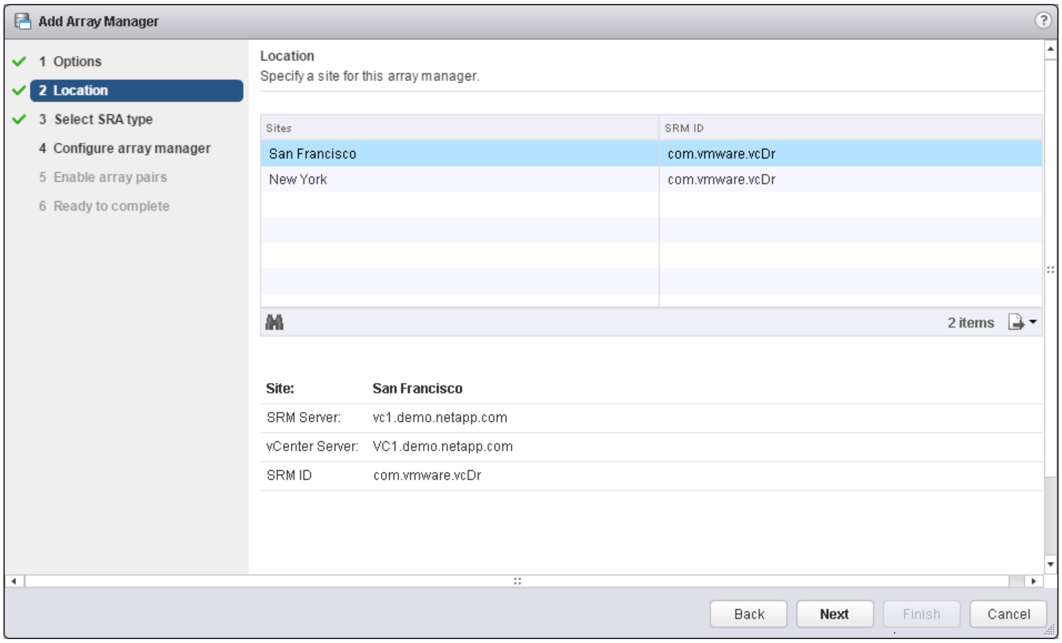
Options

To use array-based replication with SRM, you must add at least two array managers, one for each paired site.

○ Add a pair of array managers
You will be prompted to add two array managers, one for each site. You then enable the discovered array pairs for use with SRM.

● Add a single array manager
You will be prompted to add a single array manager.

4. Select the protected site under the Location window and click Next.



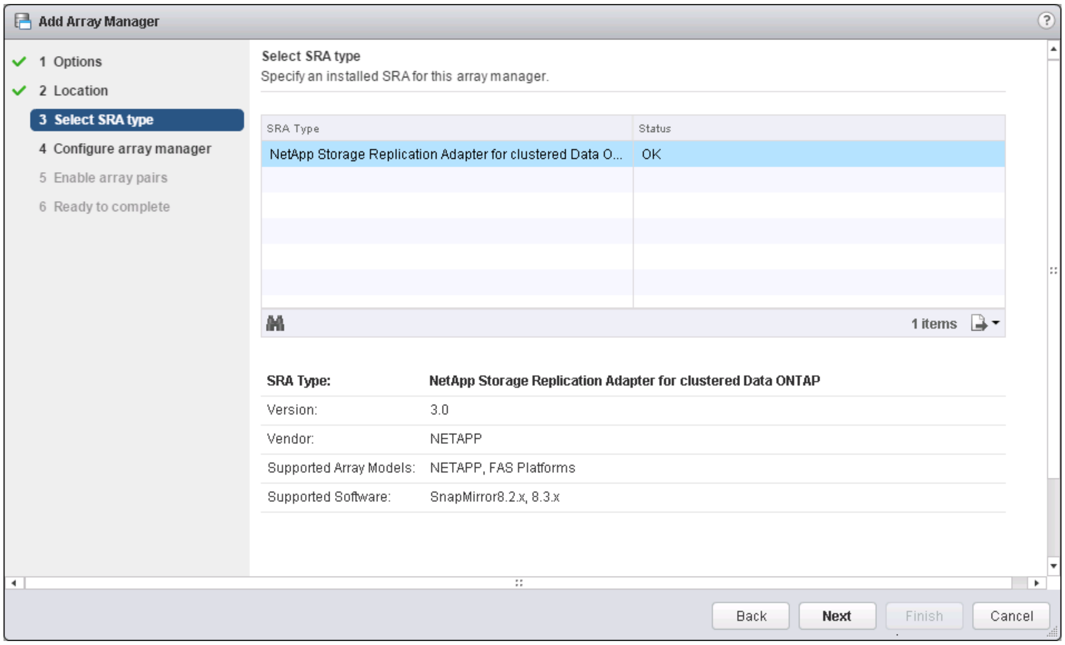
Location

Specify a site for this array manager.

Sites	SRM ID
San Francisco	com.vmware.vcDr
New York	com.vmware.vcDr

Site:	San Francisco
SRM Server:	vc1.demo.netapp.com
vCenter Server:	VC1.demo.netapp.com
SRM ID	com.vmware.vcDr

5. Select NetApp Storage Replication Adapter for Clustered Data ONTAP under SRA Type and click Next.



Select SRA type

Specify an installed SRA for this array manager.

SRA Type	Status
NetApp Storage Replication Adapter for clustered Data O...	OK

SRA Type:	NetApp Storage Replication Adapter for clustered Data ONTAP
Version:	3.0
Vendor:	NETAPP
Supported Array Models:	NETAPP, FAS Platforms
Supported Software:	SnapMirror8.2.x, 8.3.x

6. Configure the protected site's array manager with the following parameters if you are using NFS datastores:
   a. Enter the display name of the array manager. This name is used only in the SRM interface and does not need to match the actual cluster or SVM name.
   b. Enter the SVM management LIF IP address.
   c. Enter all the NFS IP addresses that are assigned to the SVM. Multiple NFS addresses must be separated by commas. Leave this field blank for SAN environments.
   d. Leave the SVM Name field blank if you are using SVM credentials.

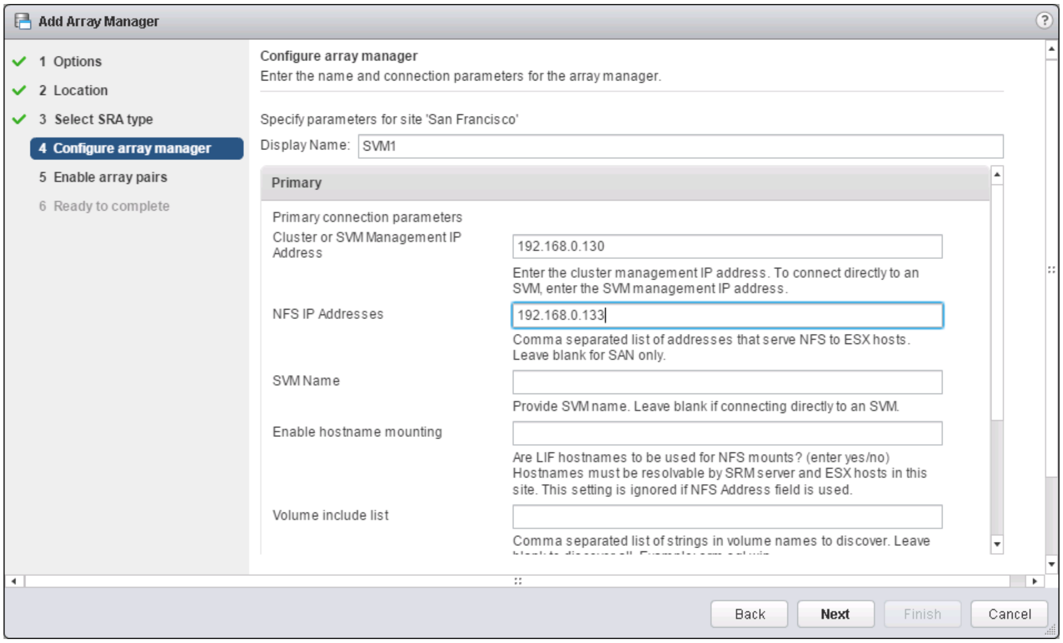
e. Leave the Enable Hostname Mounting field blank if you are using NFS datastores.

f. Leave the Volume Include List field blank to discover all volumes. To discover specified volumes, enter the source and destination names of the replicated volumes. Enter either the full name or a portion of the volume name.

g. Leave the Volume Exclude List field blank to exclude discovery of volumes. To exclude specified volumes, enter the source and destination names of the replicated volumes. Enter either the full name or a portion of the volume name.

h. Enter the SVM administrator user name and password that were created for SRA and click Next.

Note: The SVM management IP addresses and credentials can be used to pair the array managers. This configuration enables the SVM multitenancy feature of NetApp SRA 3.0. If you want the cluster management IP addresses and credentials to pair the array managers, you must provide specific information. Enter the cluster management IP address, the SVM management IP address (for the NFS IP address field if you are using NFS datastores), the SVM name, and a cluster administrator user name and password.



Add Array Manager

✓ 1 Options
✓ 2 Location
✓ 3 Select SRA type
4 Configure array manager
5 Enable array pairs
6 Ready to complete

Configure array manager
Enter the name and connection parameters for the array manager.

Specify parameters for site 'San Francisco'

Display Name: SVM1

Primary

Primary connection parameters

Cluster or SVM Management IP Address: 192.168.0.130
Enter the cluster management IP address. To connect directly to an SVM, enter the SVM management IP address.

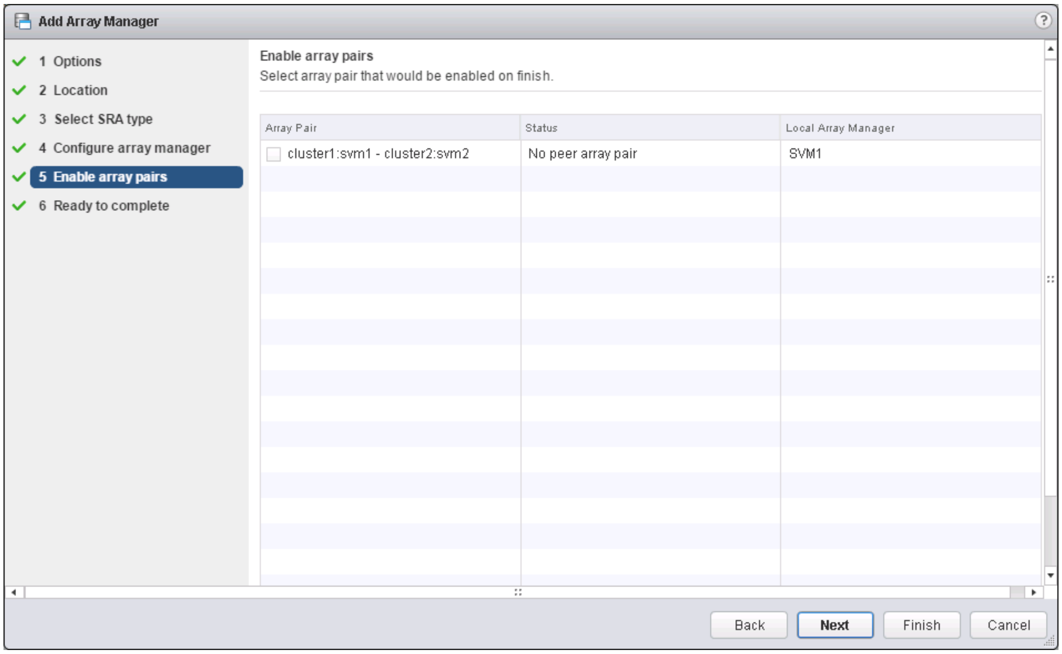
NFS IP Addresses: 192.168.0.133
Comma separated list of addresses that serve NFS to ESX hosts. Leave blank for SAN only.

SVM Name:
Provide SVM name. Leave blank if connecting directly to an SVM.

Enable hostname mounting:
Are LIF hostnames to be used for NFS mounts? (enter yes/no) Hostnames must be resolvable by SRM server and ESX hosts in this site. This setting is ignored if NFS Address field is used.

Volume include list:
Comma separated list of strings in volume names to discover. Leave

7. On the Enable Array Pairs screen, click Next to add the array manager without selecting to enable the array pair at this time. You can enable the array pairs when you create the protected site's array manager.

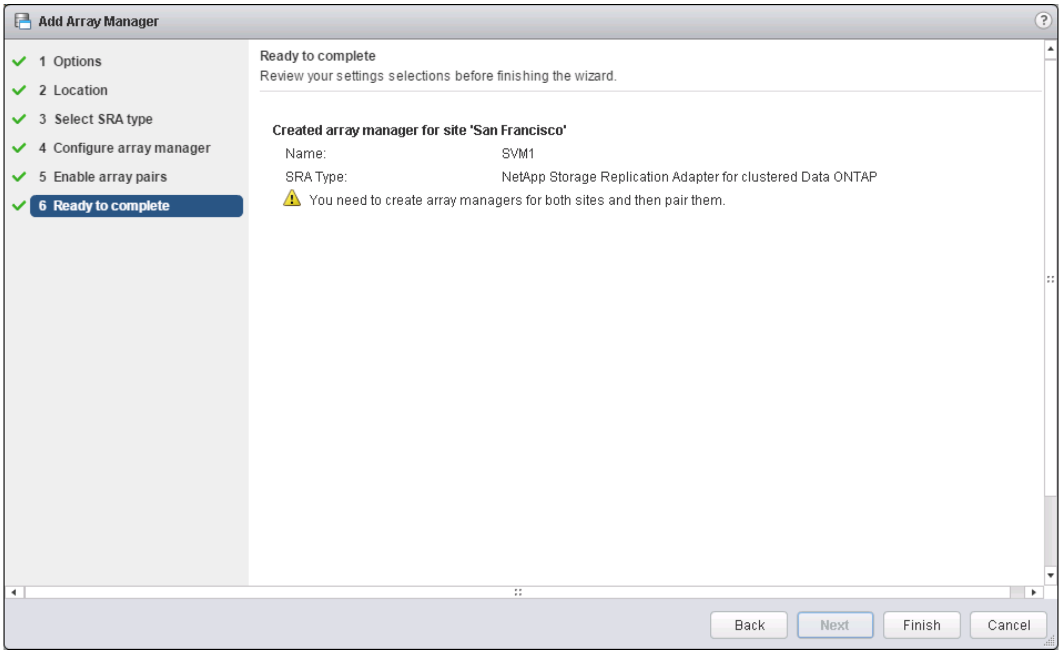


Enable array pairs

Select array pair that would be enabled on finish.

Array Pair	Status	Local Array Manager
□ cluster1:svm1 - cluster2:svm2	No peer array pair	SVM1

8. Complete the Add Array Manager wizard by clicking Finish.



Ready to complete

Review your settings selections before finishing the wizard.

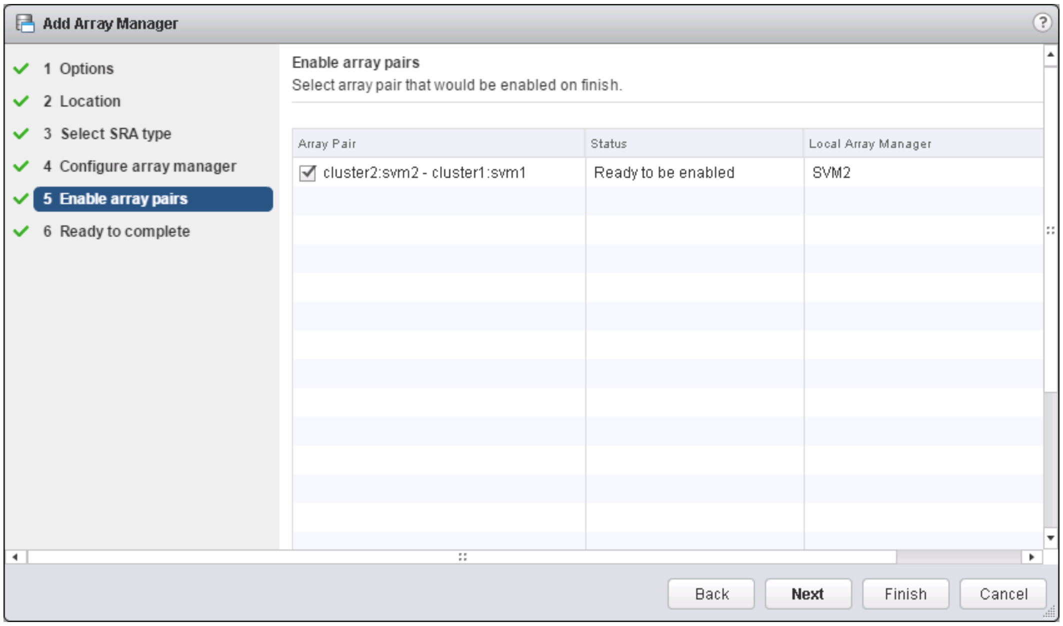
Created array manager for site 'San Francisco'

Name: SVM1

SRA Type: NetApp Storage Replication Adapter for clustered Data ONTAP

⚠ You need to create array managers for both sites and then pair them.

9. After successfully configuring the array manager for the protected site, repeat the process for the recovery site by using the appropriate SVM management IP addresses and credentials. When you reach the Enable Array Pairs screen of the Add Array Manager wizard, ensure that the array pair is selected and that it shows as ready to be enabled. Click Finish to complete the wizard.



Enable array pairs

Select array pair that would be enabled on finish.

Array Pair	Status	Local Array Manager
☑ cluster2:svm2 - cluster1:svm1	Ready to be enabled	SVM2

Best Practice

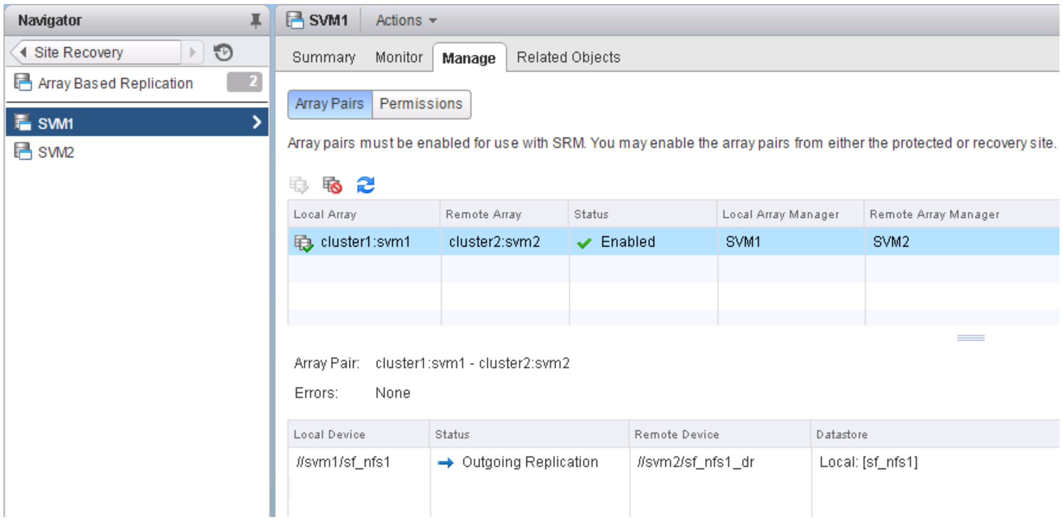
NetApp recommends that you completely configure the array manager by using cluster administrator credentials first and then test SRM functionality. After verifying that SRM is functioning correctly by using the cluster administrator account, reconfigure the array manager to use the RBAC account that was created for the SVM administrator with the RBAC User Creator tool.

This test scenario might not be possible based on the delegation level of the administrator who is installing and configuring SRM. If this scenario is not possible, proceed to directly configuring the array manager with the SVM management credentials.

Verify Replicated Storage

After you configure the array managers, verify that the protected array and the recovery array have been successfully paired and that replicated storage has been discovered at both sites. In SRM 6, discovery is automatic after the array managers have been paired. You can initiate discovery manually if required.

In the following example, the SnapMirror relationship topologies are discovered. The protected site, San Francisco (`SVM1`), has VMs in the NFS volume `//svm1/sf_nfs1`. This volume is being replicated as outgoing to the recovery site. On the recovery site, New York (`SVM2`), the incoming replicated volume is `//svm2/sf_nfs1_dr`.



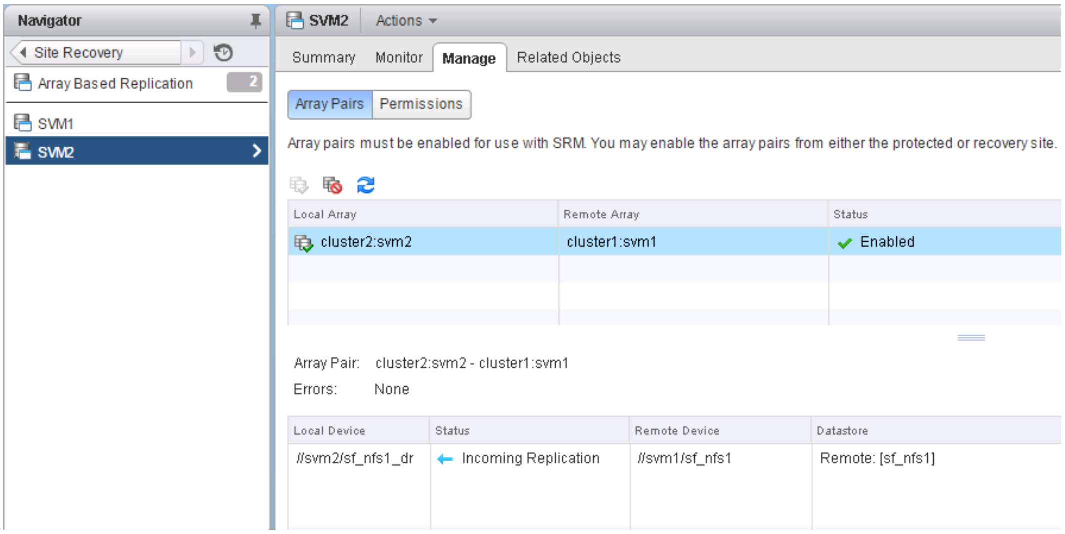
Array pairs must be enabled for use with SRM. You may enable the array pairs from either the protected or recovery site.

Local Array	Remote Array	Status	Local Array Manager	Remote Array Manager
cluster1:svm1	cluster2:svm2	✓ Enabled	SVM1	SVM2

Array Pair: cluster1:svm1 - cluster2:svm2

Errors: None

Local Device	Status	Remote Device	Datastore
//svm1/sf_nfs1	→ Outgoing Replication	//svm2/sf_nfs1_dr	Local: [sf_nfs1]



Array pairs must be enabled for use with SRM. You may enable the array pairs from either the protected or recovery site.

Local Array	Remote Array	Status
cluster2:svm2	cluster1:svm1	✓ Enabled

Array Pair: cluster2:svm2 - cluster1:svm1

Errors: None

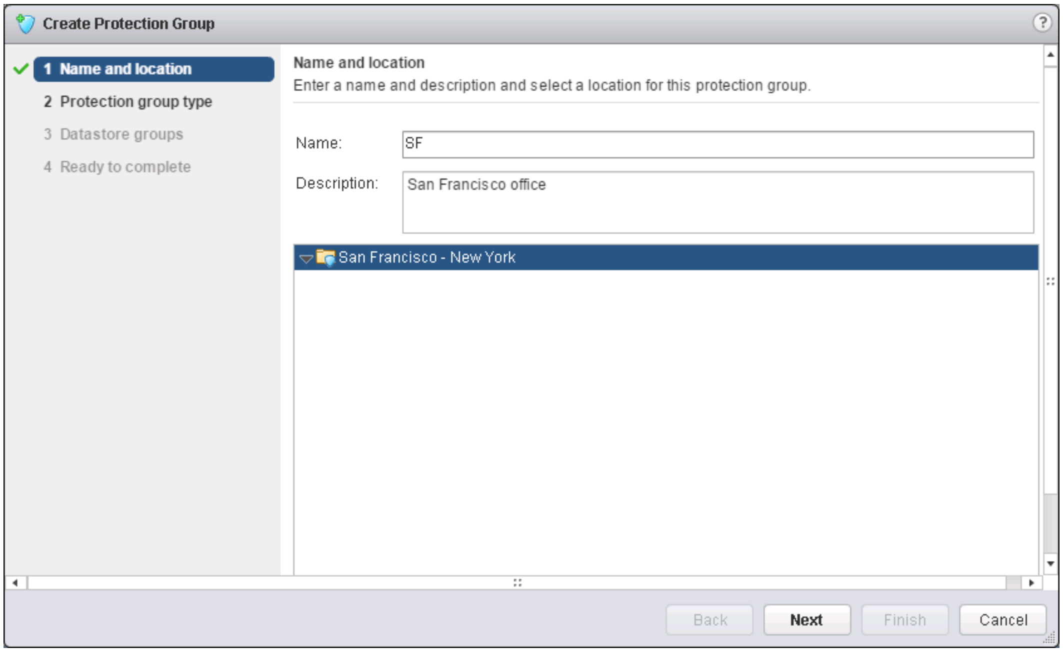
Local Device	Status	Remote Device	Datastore
//svm2/sf_nfs1_dr	← Incoming Replication	//svm1/sf_nfs1	Remote: [sf_nfs1]

2.7 Build Protection Groups

Protection groups define VMs and datastores in groups that are recovered together. In a NetApp environment, replication occurs at the FlexVol volume level with SnapMirror replication.

To create an SRM protection group, complete the following steps:

1. In the Site Recovery home interface, select the Protection Groups tab from the left window pane.
2. Expand the Objects tab on the right window pane, and then click the Create Protection Group icon.
3. In the Create Protection Group wizard, enter a name and a description and click Next.



Create Protection Group

✓ 1 Name and location
2 Protection group type
3 Datastore groups
4 Ready to complete

Name and location
Enter a name and description and select a location for this protection group.

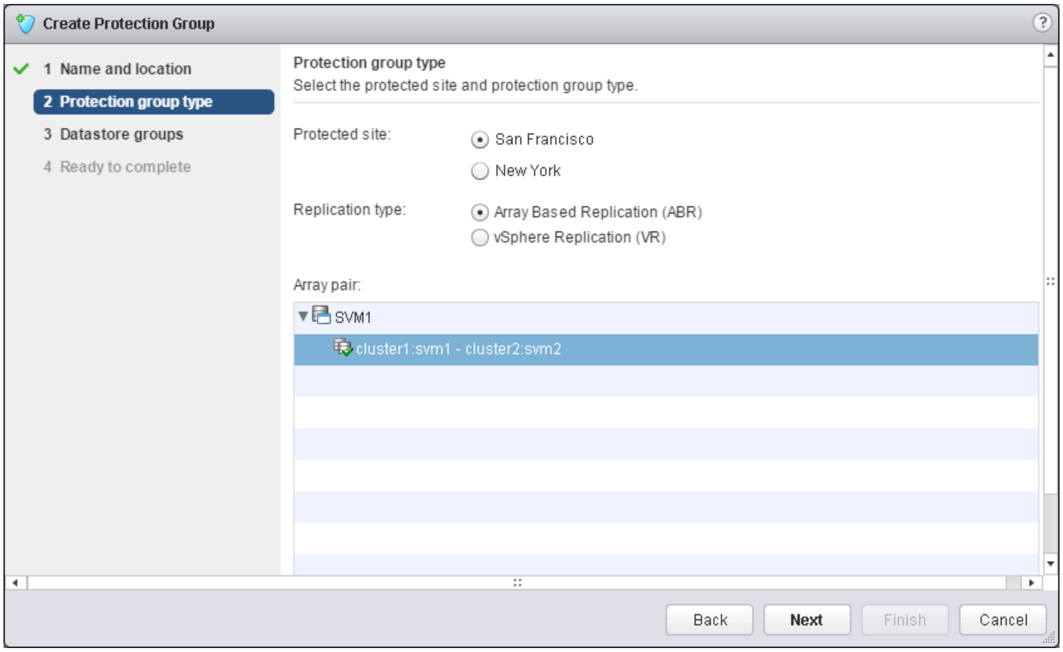
Name: SF

Description: San Francisco office

San Francisco - New York

4. Select the protected site. This site is where the VMs that are configured in this protection group currently exist. Make sure that ABR is selected and then click Next.

   Note: All array managers that have been created are listed in the following window. However, a protection group is limited to one array manager pair and cannot span more than the selected array.



Create Protection Group

✓ 1 Name and location
2 Protection group type
3 Datastore groups
4 Ready to complete

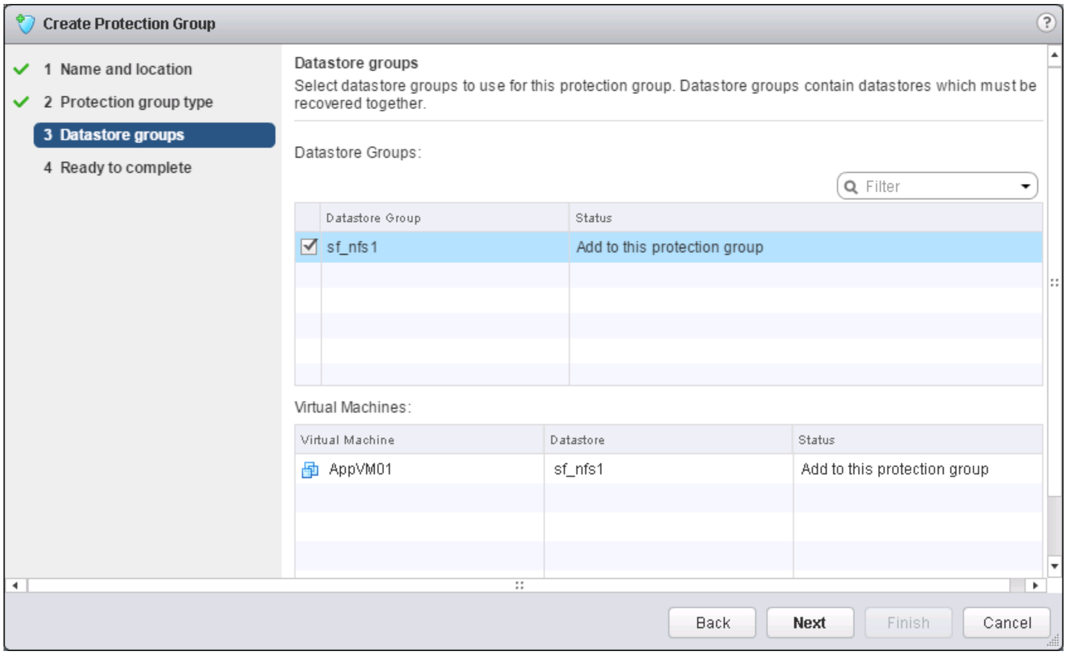
Protection group type
Select the protected site and protection group type.

Protected site: ● San Francisco ○ New York

Replication type: ● Array Based Replication (ABR) ○ vSphere Replication (VR)

Array pair:
SVM1
cluster1:svm1 - cluster2:svm2

5. Select the datastore group or groups to add to this protection group and click Next. All the VMs that are on this datastore are included in the protection group.



Datastore groups

Select datastore groups to use for this protection group. Datastore groups contain datastores which must be recovered together.

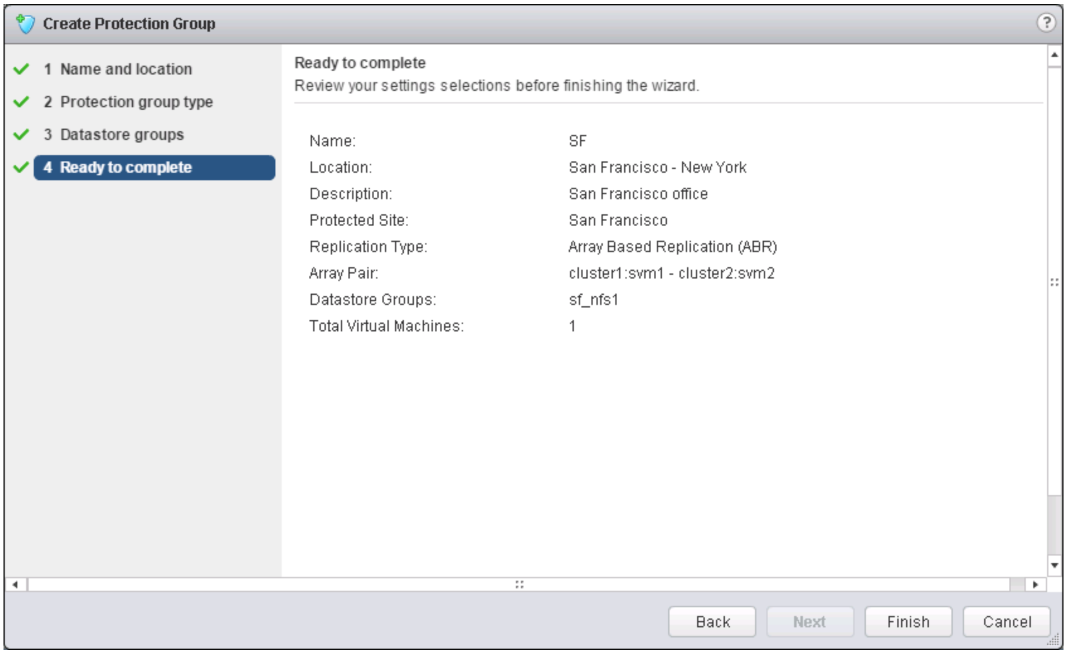
Datastore Groups:

	Datastore Group	Status
☑	sf_nfs1	Add to this protection group

Virtual Machines:

Virtual Machine	Datastore	Status
AppVM01	sf_nfs1	Add to this protection group

6. Review the final page of the Create Protection Group wizard and click Finish.



Ready to complete

Review your settings selections before finishing the wizard.

Name:	SF
Location:	San Francisco - New York
Description:	San Francisco office
Protected Site:	San Francisco
Replication Type:	Array Based Replication (ABR)
Array Pair:	cluster1:svm1 - cluster2:svm2
Datastore Groups:	sf_nfs1
Total Virtual Machines:	1

7. Repeat steps 1 through 6 to create any remaining protection groups that the environment requires.

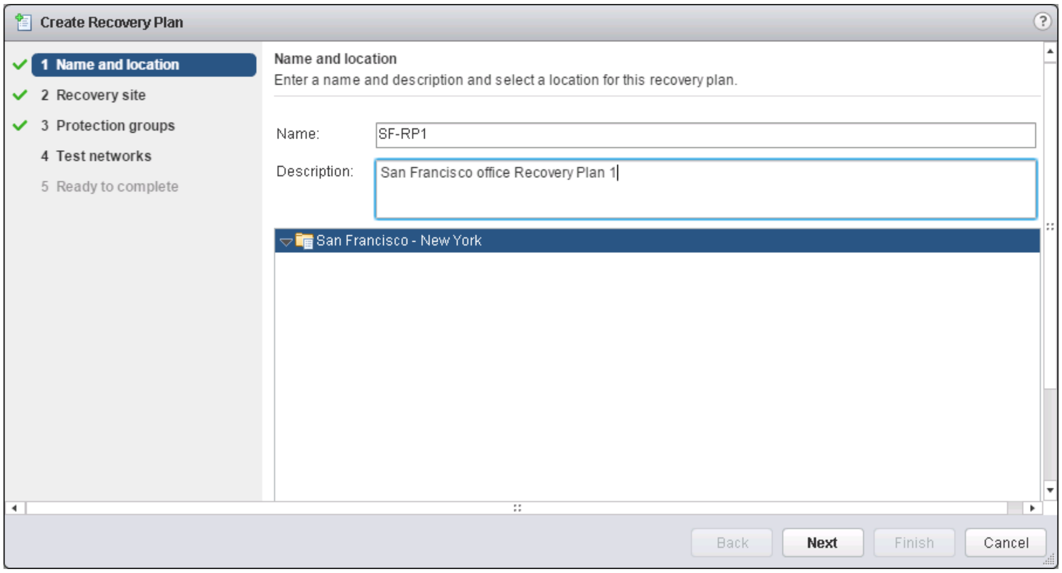
2.8 Create Recovery Plan

Recovery plans define which protection groups are recovered in the same process. Multiple protection groups can be configured in the same recovery plan. Also, to enable more options for the execution of recovery plans, a single protection group can be included in multiple recovery plans.

This procedure assumes that the VMs are recovered at a recovery site that has the same network configuration (IP address, subnet mask, gateway address, DNS settings, and so on) that the protected site uses. If different network settings must be applied to individual VMs as they are recovered, you can specify this requirement in the properties settings of a VM in the recovery plan. To configure SRM to apply different network settings to multiple VMs without having to edit the properties of each VM in the recovery plan separately, VMware provides a tool called the DR IP Customizer. Directions for using this utility are provided in the “Customize IP Properties for Multiple Virtual Machines” section of the [Site Recovery Manager 6.0 Administration Guide](#).

To create a recovery plan, complete the following steps:

1. In the Site Recovery home interface, select the Recovery Plans tab from the left window pane.
2. Under the Objects tab on the right window pane, click the Create Recovery Plan icon.
3. In the Create Recovery Plan wizard, enter a name and a description and then click Next.


Create Recovery Plan

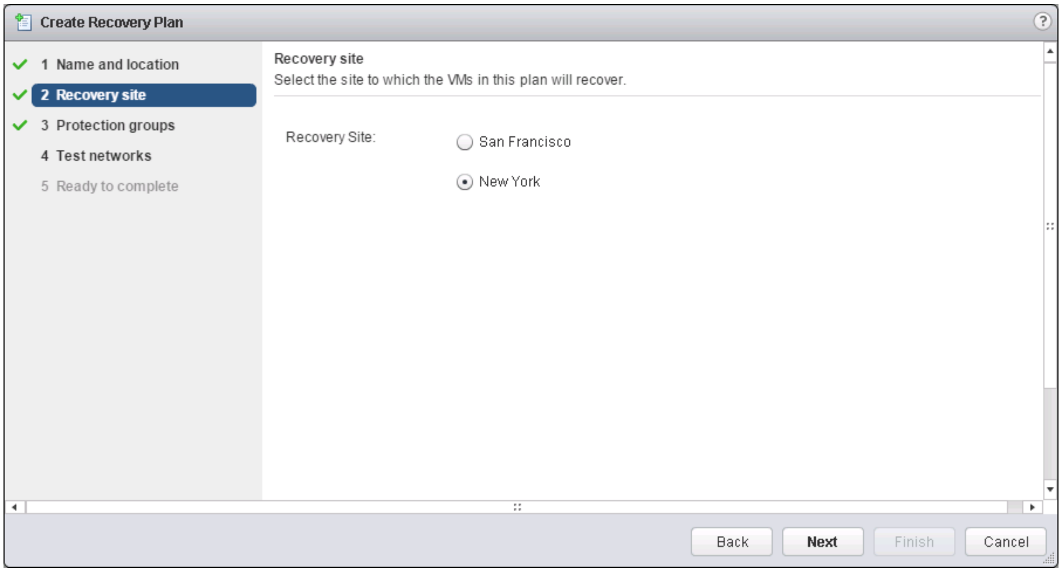
Name and location
Enter a name and description and select a location for this recovery plan.

Name: SF-RP1

Description: San Francisco office Recovery Plan 1

San Francisco - New York

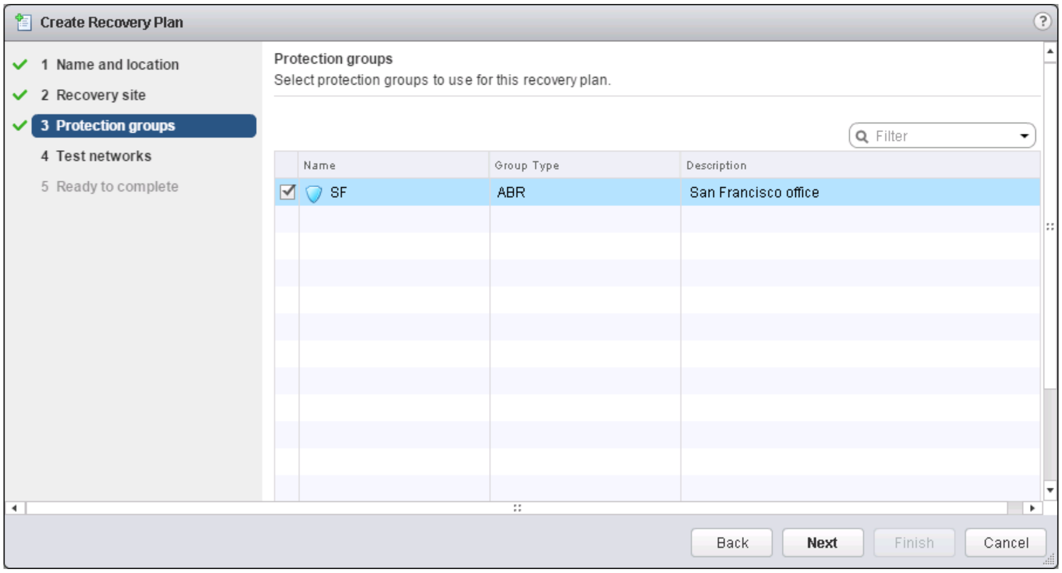
4. Select the recovery site in which to recover the protected VMs and then click Next.


Create Recovery Plan

Recovery site
Select the site to which the VMs in this plan will recover.

Recovery Site: ○ San Francisco ● New York

5. Select the protection groups to use for this recovery plan and click Next.

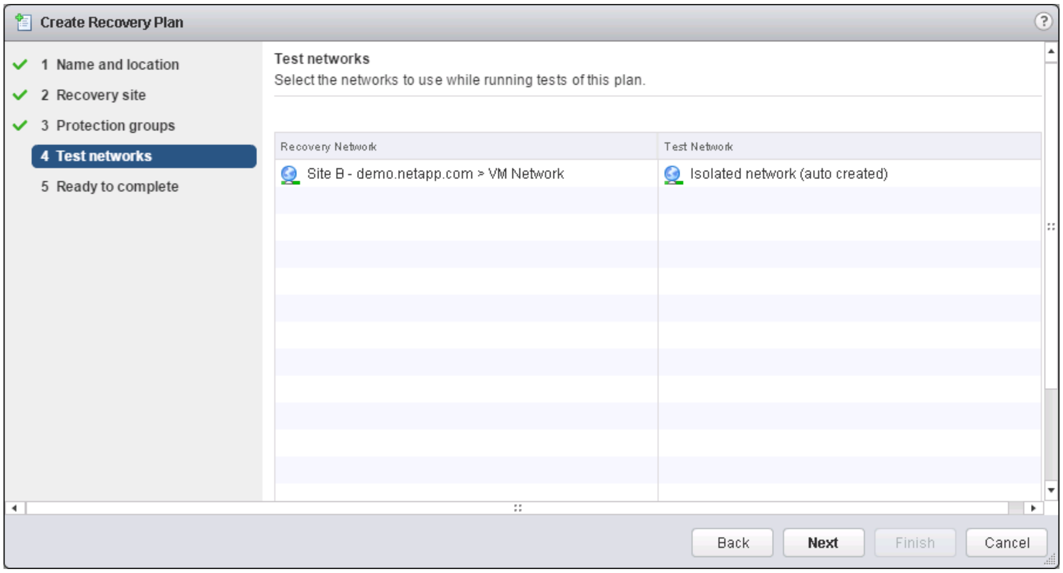


Protection groups

Select protection groups to use for this recovery plan.

	Name	Group Type	Description
☑	SF	ABR	San Francisco office

6. Select the test networks to use when running test recovery operations for this recovery plan and click Next.

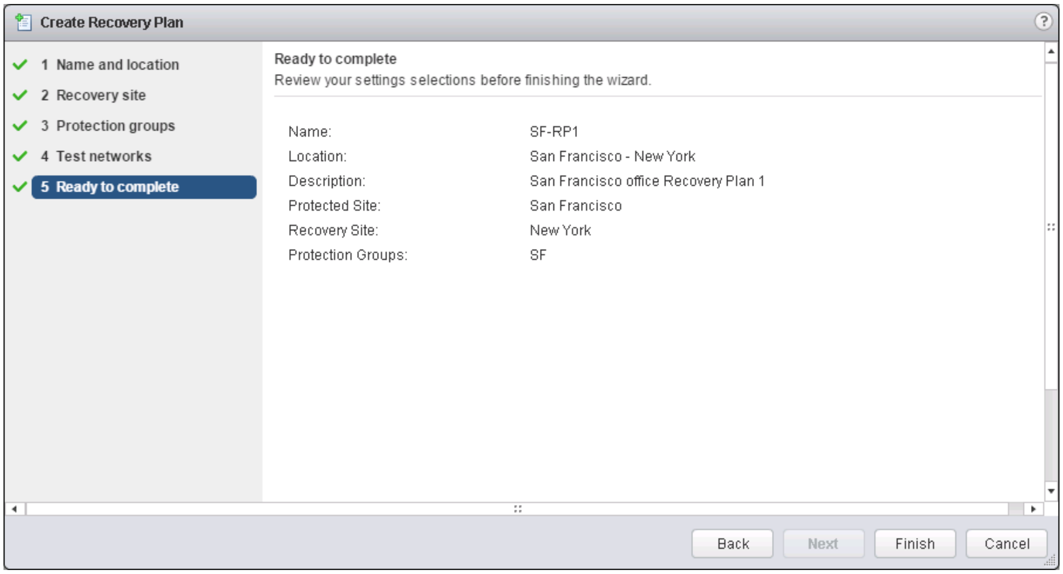


Test networks

Select the networks to use while running tests of this plan.

Recovery Network	Test Network
Site B - demo.netapp.com > VM Network	Isolated network (auto created)

7. Review the final page of the Create Recovery Plan wizard and click Finish.



Ready to complete
Review your settings selections before finishing the wizard.

Name:	SF-RP1
Location:	San Francisco - New York
Description:	San Francisco office Recovery Plan 1
Protected Site:	San Francisco
Recovery Site:	New York
Protection Groups:	SF

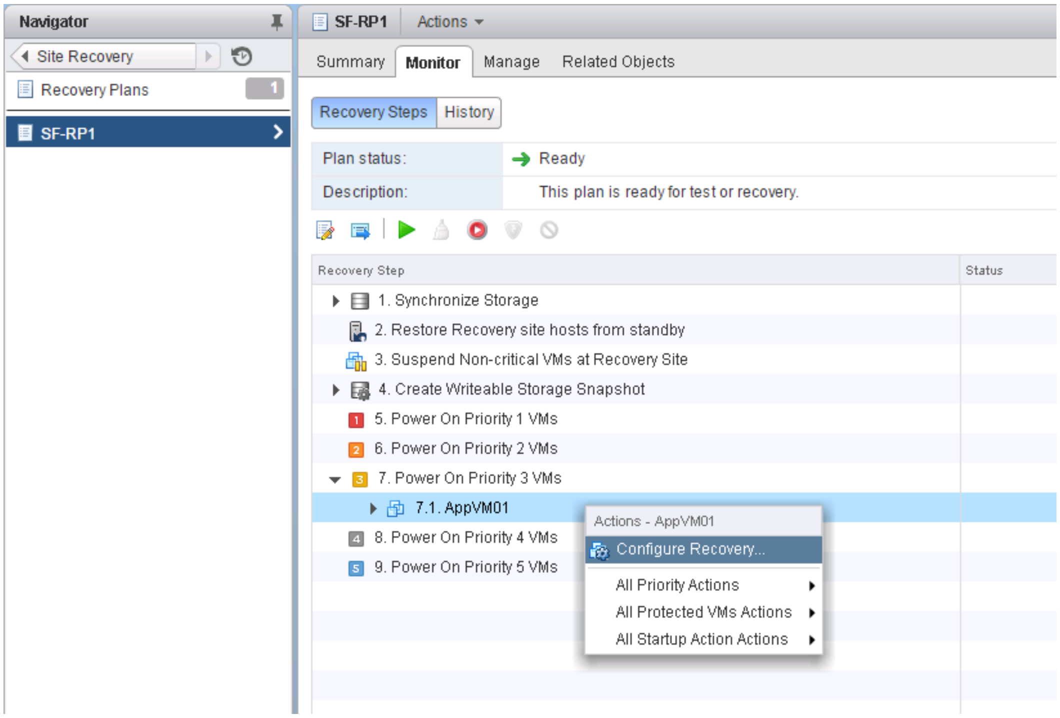
8. Repeat steps 1 through 7 to create any remaining recovery plans that the environment requires.

Optional Recovery Plan Configurations

After the recovery plan has been created, the site is protected and is ready to fail over as needed. At this point, additional options are available to customize the recovery plan.

To customize the recovery plan, complete the following steps:

1. Select the Monitor tab from the right window pane for the recovery plan and then expand the Recovery Steps. Right-click the VM that you want from the default Power On steps and select Configure Recovery.



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 Writeable Storage Snapshot	
5. Power On Priority 1 VMs	
6. Power On Priority 2 VMs	
7. Power On Priority 3 VMs	
7.1. AppVM01	
8. Power On Priority 4 VMs	
9. Power On Priority 5 VMs	

2. Select from the following options:
   a. Under the Recovery Properties tab, you can configure the following properties:
   - **Priority Group.** All VMs within a priority group are started in parallel before proceeding to the next group. The default value is group 3.
   - **VM Dependencies.** Dependencies identify VMs that must be started before others in the group. The default value is set to none.
   - **Shutdown Actions.** This setting allows you to either gracefully shut down the guest operating system (initiated from VMware tools) or simply power off. The default value is guest shutdown.
   - **Startup Actions.** This setting determines whether or not to start the VM on recovery, whether or not to wait for VMware tools, and whether or not to add a delay before running post-power-on steps. The default value is to power on and wait for VMware tools.
   - **Pre and Post Power-On Steps.** These settings allow the addition of scripts to run either before or after the VM is powered on. Scripts can be executed on the SRM server or on the VM itself. The default values are blank.

   b. Under the IP Customization tab, you can select from the following IP customization modes:
   - Auto (default value)
   - The use of IP customization rules if applicable
   - Manual IP customization
   - No IP customization

3 Operational Procedures

After you install and configure your Site Recovery Manager 6 environment, you can perform certain operations. For example, you can nondisruptively test your recovery plan, automate a planned or unplanned recovery, and reprotect your environment after the protected site has been activated. For an overview of SRM use cases and their associated procedures, see Table 4.

Table 4) SRM 6 and clustered Data ONTAP use cases.

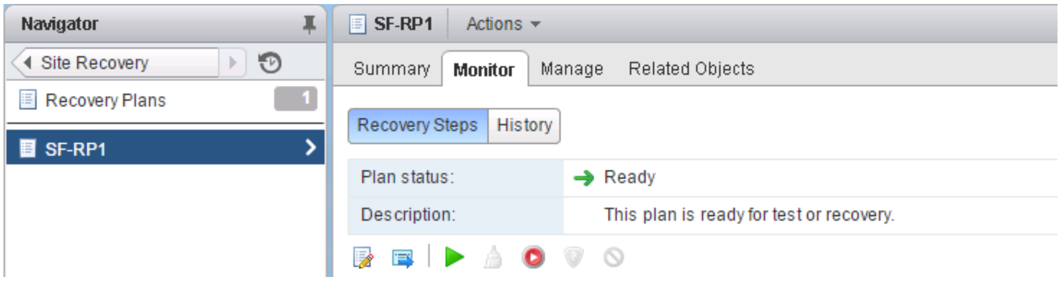
Use Case	Procedure Name
The VMware administrator wants to validate the previously configured SRM recovery plan.	Perform Test Recovery Operation
The VMware administrator wants to clean up the previous test recovery operation.	Perform Cleanup Operation
The VMware administrator wants to perform a planned migration of selected VMs from the protected site (site A) to the recovery site (site B).	Perform Planned Migration
A disaster has occurred at site A, and the VMware administrator must recover the VMs on site B.	Perform Disaster Recovery
After failing over to the recovery site, the VMware administrator must start syncing changes from site B back to site A.	Perform Reprotect Operation

3.1 Perform Test Recovery Operation

To perform a test recovery operation, complete the following steps:

1. In the Site Recovery home interface, select the Recovery Plans tab from the left window pane.

2. Highlight the desired recovery plan from the left window pane and then click the green Play icon to perform the test recovery.



Navigator

Site Recovery

Recovery Plans 1

SF-RP1

SF-RP1 Actions

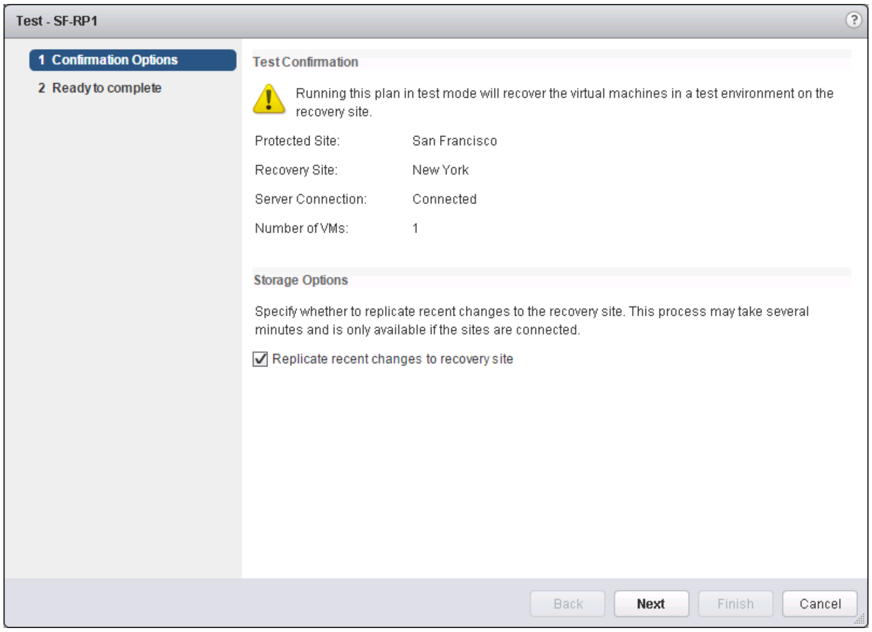
Summary | Monitor | Manage | Related Objects

Recovery Steps | History

Plan status: Ready

Description: This plan is ready for test or recovery.

3. **Optional:** Choose whether or not to replicate changes to the recovery site and click Next.



Test - SF-RP1

1 Confirmation Options

2 Ready to complete

Test Confirmation

Running this plan in test mode will recover the virtual machines in a test environment on the recovery site.

Protected Site: San Francisco

Recovery Site: New York

Server Connection: Connected

Number of VMs: 1

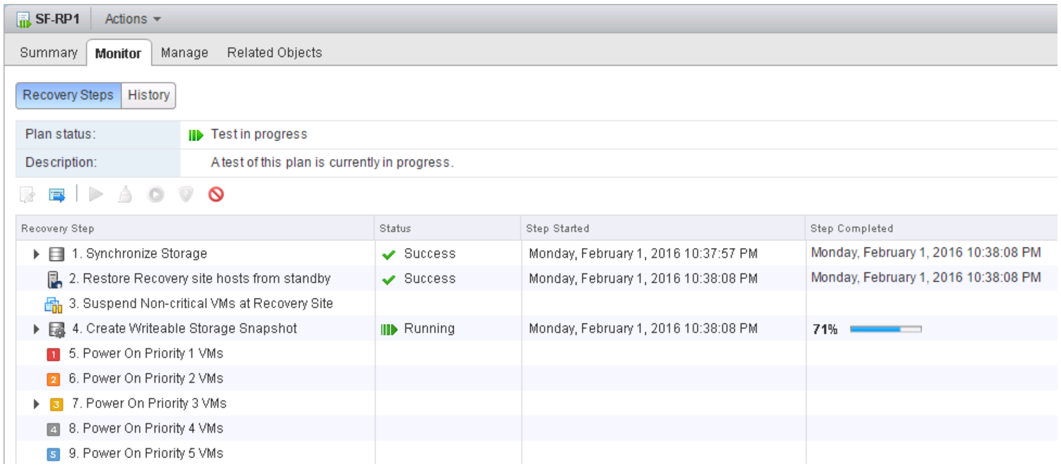
Storage Options

Specify whether to replicate recent changes to the recovery site. This process may take several minutes and is only available if the sites are connected.

☑ Replicate recent changes to recovery site

Back | Next | Finish | Cancel

4. Review the final page of the wizard and click Finish to start the operation.
5. Click the Recovery Steps tab to monitor the progress of the steps in the workflow.



SF-RP1 Actions

Summary | Monitor | Manage | Related Objects

Recovery Steps | History

Plan status: Test in progress

Description: A test of this plan is currently in progress.

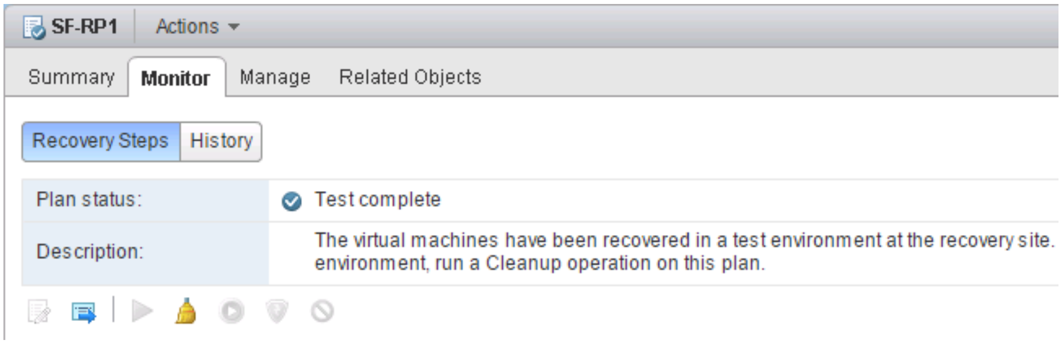
Recovery Step	Status	Step Started	Step Completed
1. Synchronize Storage	✓ Success	Monday, February 1, 2016 10:37:57 PM	Monday, February 1, 2016 10:38:08 PM
2. Restore Recovery site hosts from standby	✓ Success	Monday, February 1, 2016 10:38:08 PM	Monday, February 1, 2016 10:38:08 PM
3. Suspend Non-critical VMs at Recovery Site			
4. Create Writeable Storage Snapshot	Running	Monday, February 1, 2016 10:38:08 PM	71%
5. Power On Priority 1 VMs			
6. Power On Priority 2 VMs			
7. Power On Priority 3 VMs			
8. Power On Priority 4 VMs			
9. Power On Priority 5 VMs			

6. **Optional:** When the test recovery operation has completed, click the History tab to review a detailed report.

3.2 Perform Test Cleanup Operation

After the test has been validated and is no longer required, perform a cleanup operation. Running cleanup returns the protected VMs to their initial state and resets the recovery plan to the Ready state:

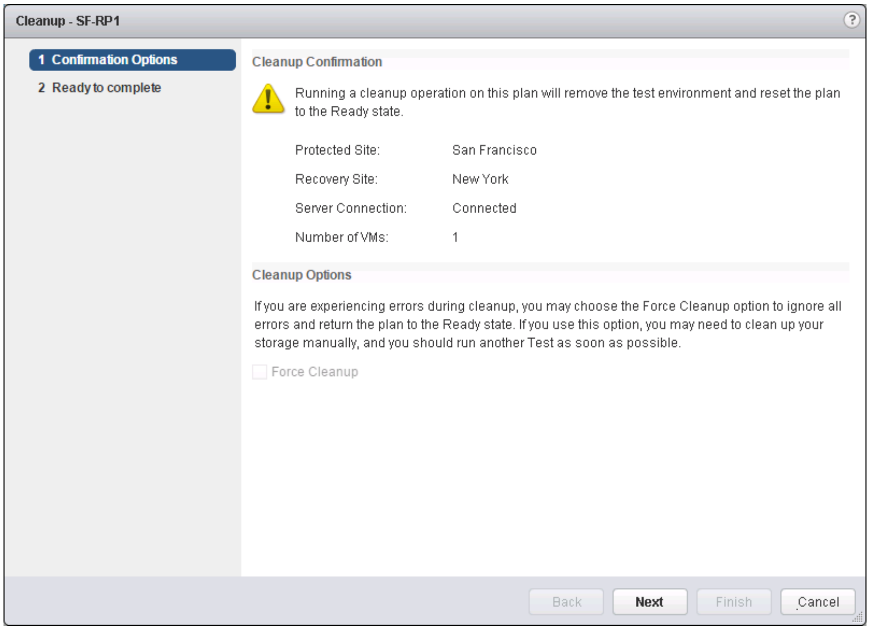
1. In the Site Recovery home interface, select the Recovery Plans tab from the left window pane.
2. Highlight the desired recovery plan from the left window pane and then click the Cleanup Recovery Plan icon to perform the operation.



Plan status: Test complete

Description: The virtual machines have been recovered in a test environment at the recovery site. environment, run a Cleanup operation on this plan.

3. Confirm that you are ready to perform the cleanup and then click Next and Finish to complete the wizard.



Cleanup Confirmation

Running a cleanup operation on this plan will remove the test environment and reset the plan to the Ready state.

Protected Site: San Francisco

Recovery Site: New York

Server Connection: Connected

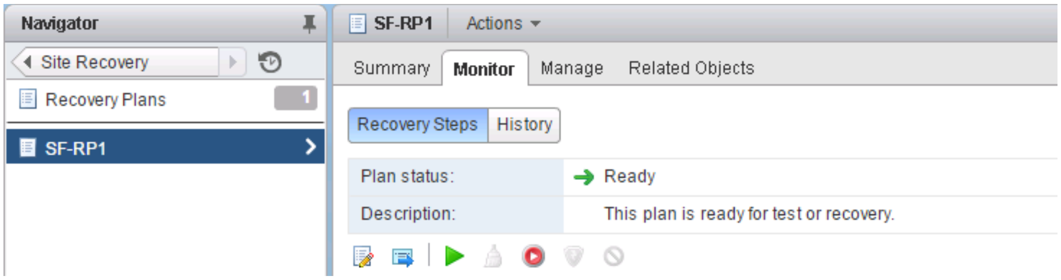
Number of VMs: 1

Cleanup Options

If you are experiencing errors during cleanup, 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 another Test as soon as possible.

□ Force Cleanup

4. After the cleanup is complete, the state of the recovery plan is now ready for another test or recovery operation.



Plan status: Ready

Description: This plan is ready for test or recovery.

5. **Optional:** If the cleanup encounters errors, run cleanup again with the Force Cleanup option selected. The Force Cleanup option cleans up and ignores any errors that might occur. If necessary, run cleanup several times with the Force Cleanup option selected until the cleanup completes successfully.

3.3 Perform Recovery Operation

After successfully completing a test recovery, run the recovery operation to perform a planned migration or disaster recovery. During a recovery operation, all VMs in the recovery plan are migrated to the recovery site. The corresponding VMs in the protected site are shut down.

Note: A recovery operation makes significant changes in the configurations of the protected and recovery sites, and it stops replication. Do not run any recovery plan without testing it first.

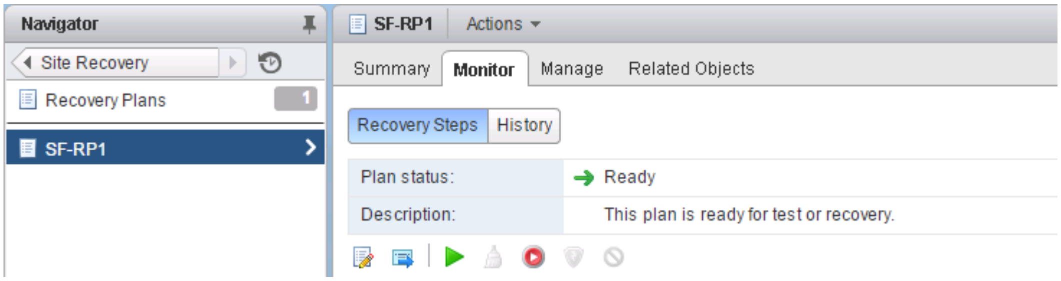
Perform Planned Migration

When a planned migration occurs, SRM completes the following tasks:

1. It replicates all protected VMs.
2. It gracefully shuts down the protected VMs.
3. It replicates the powered-down VMs.
4. It breaks the NetApp SnapMirror replication and makes the recovery datastore writable.
5. It mounts the replicated datastore.
6. It powers on the VMs according to the priority that was configured in the recovery plan.

To run a planned migration of the VMs in the protection group to the recovery site, complete the following steps:

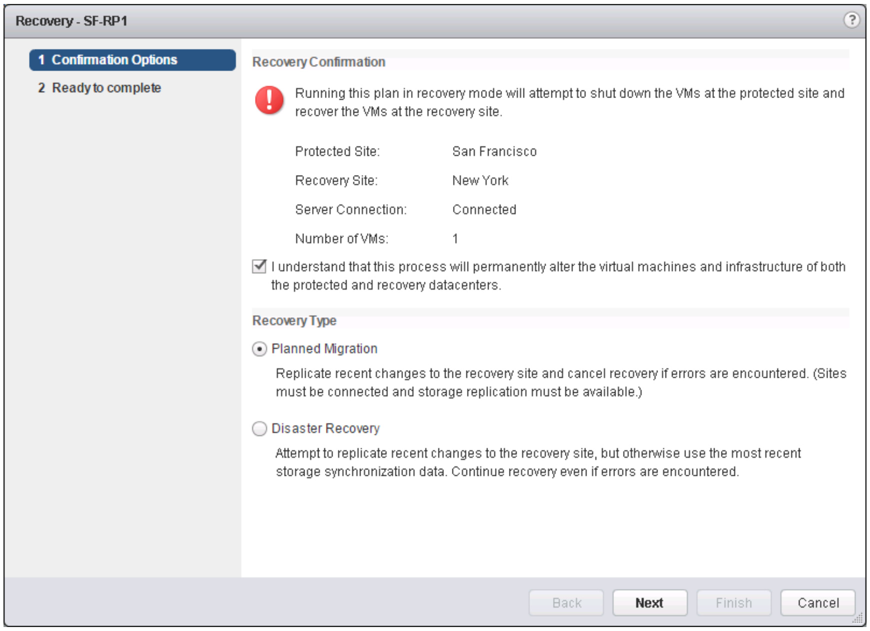
1. In the Site Recovery home interface, select the Recovery Plans tab from the left window pane.
2. Highlight the desired recovery plan from the left window pane and then click the red Play recovery plan icon to perform the operation.



Plan status: Ready

Description: This plan is ready for test or recovery.

3. Select I Understand That This Process Will Permanently Alter the Virtual Machines and Infrastructure of Both the Protected and Recovery Datacenters.
4. Under Recovery Type, select Planned Migration and click Next.



Recovery - SF-RP1

1 Confirmation Options

2 Ready to complete

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:	San Francisco
Recovery Site:	New York
Server Connection:	Connected
Number of VMs:	1

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

Recovery Type

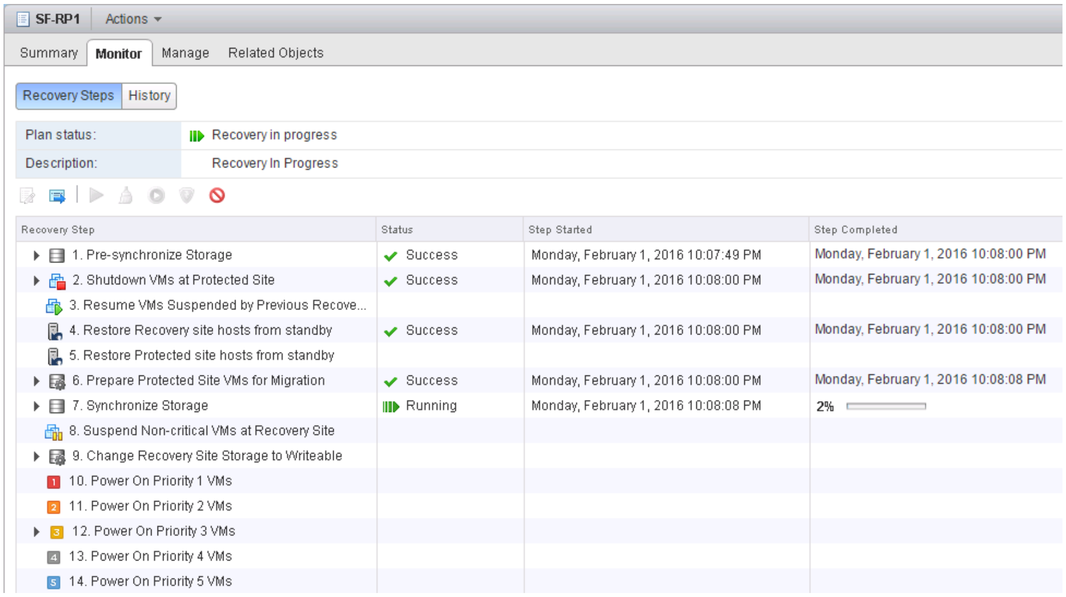
● Planned Migration

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.

5. Click the Recovery Steps tab to monitor the progress of the recovery workflow.



Plan status:	Recovery in progress
Description:	Recovery In Progress

Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize Storage	✓ Success	Monday, February 1, 2016 10:07:49 PM	Monday, February 1, 2016 10:08:00 PM
2. Shutdown VMs at Protected Site	✓ Success	Monday, February 1, 2016 10:08:00 PM	Monday, February 1, 2016 10:08:00 PM
3. Resume VMs Suspended by Previous Recove...			
4. Restore Recovery site hosts from standby	✓ Success	Monday, February 1, 2016 10:08:00 PM	Monday, February 1, 2016 10:08:00 PM
5. Restore Protected site hosts from standby			
6. Prepare Protected Site VMs for Migration	✓ Success	Monday, February 1, 2016 10:08:00 PM	Monday, February 1, 2016 10:08:08 PM
7. Synchronize Storage	Running	Monday, February 1, 2016 10:08:08 PM	2%
8. Suspend Non-critical VMs at Recovery Site			
9. Change Recovery Site Storage to Writeable			
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			

6. **Optional:** After the recovery operation has completed, click the History tab to view a detailed report.

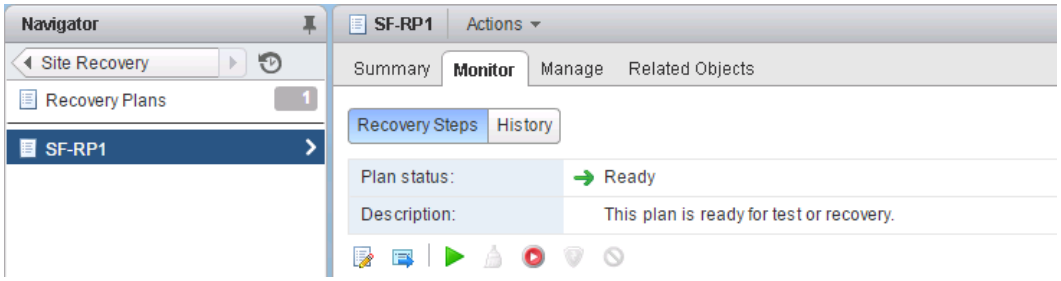
Perform Disaster Recovery

When DR occurs, the protected site might not be reachable. SRM completes the following tasks:

1. It gracefully shuts down the protected VMs (if possible).
2. It replicates the powered-down VMs (if possible).
3. It breaks the SnapMirror replication (if possible).
4. It makes the recovery datastore writable and mounts to the recovery site ESXi host.
5. It powers on the VMs according to the priority that was configured in the recovery plan.

To run a planned migration of the VMs in the protection group to the recovery site, complete the following steps.

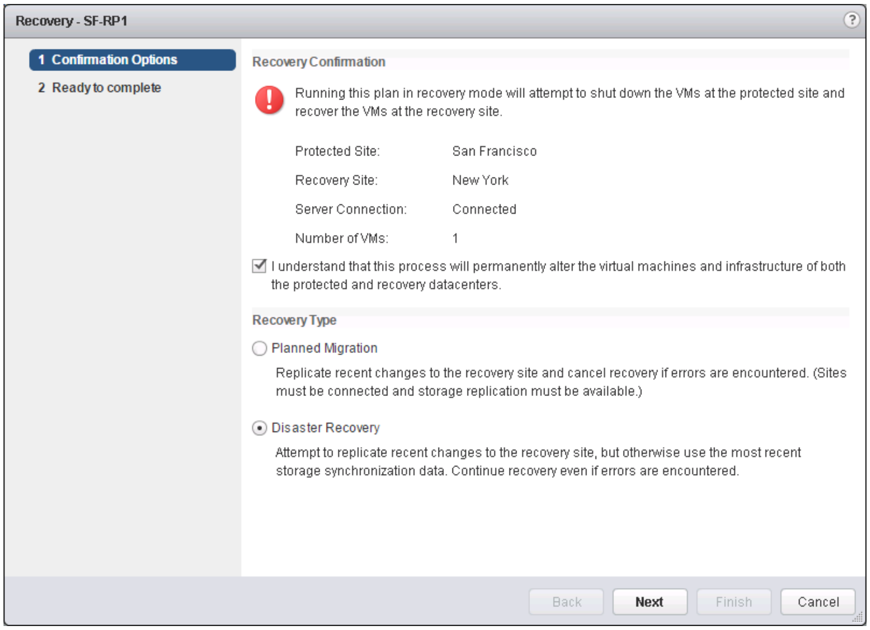
1. In the Site Recovery home interface, select the Recovery Plans tab from the left window pane.
2. Highlight the desired recovery plan from the left window pane and then click the red Play recovery plan icon to perform the operation.



Plan status: Ready

Description: This plan is ready for test or recovery.

3. Select I Understand That This Process Will Permanently Alter the Virtual Machines and Infrastructure of Both the Protected and Recovery Datacenters.
4. Under Recovery Type, select Disaster Recovery and click Next.



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: San Francisco

Recovery Site: New York

Server Connection: Connected

Number of VMs: 1

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

Recovery Type

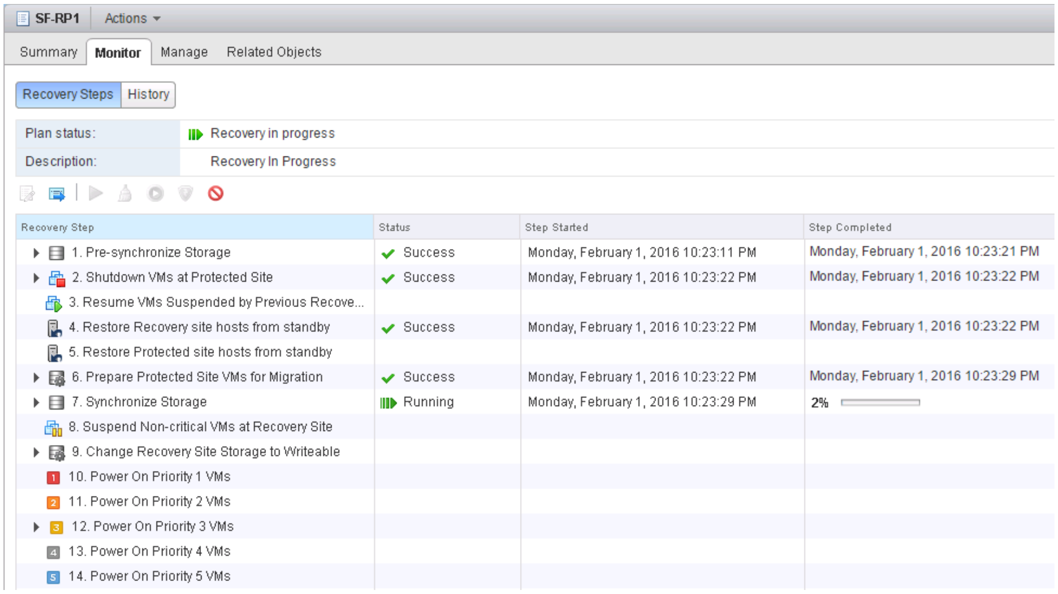
○ Planned Migration

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.

5. Review the final page and click Finish to complete the wizard.
6. Click the Recovery Steps tab to monitor the progress of the recovery operation.



SF-RP1 | Actions

Summary | **Monitor** | Manage | Related Objects

Recovery Steps | History

Plan status: Recovery in progress

Description: Recovery In Progress

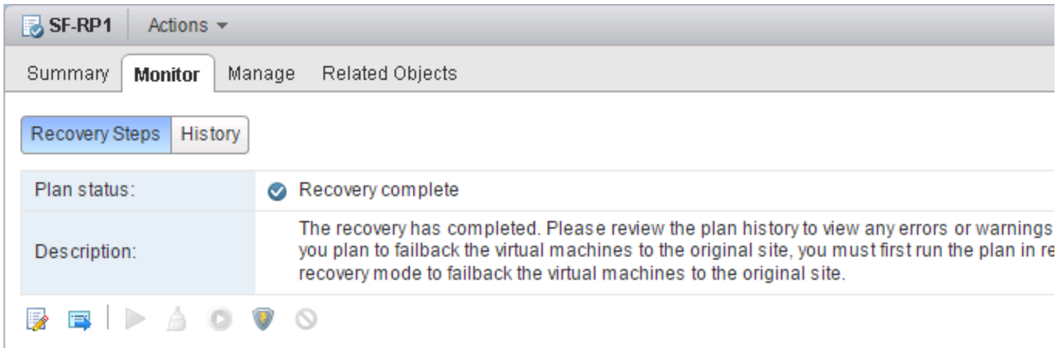
Recovery Step	Status	Step Started	Step Completed
1. Pre-synchronize Storage	✓ Success	Monday, February 1, 2016 10:23:11 PM	Monday, February 1, 2016 10:23:21 PM
2. Shutdown VMs at Protected Site	✓ Success	Monday, February 1, 2016 10:23:22 PM	Monday, February 1, 2016 10:23:22 PM
3. Resume VMs Suspended by Previous Recove...			
4. Restore Recovery site hosts from standby	✓ Success	Monday, February 1, 2016 10:23:22 PM	Monday, February 1, 2016 10:23:22 PM
5. Restore Protected site hosts from standby			
6. Prepare Protected Site VMs for Migration	✓ Success	Monday, February 1, 2016 10:23:22 PM	Monday, February 1, 2016 10:23:29 PM
7. Synchronize Storage	Running	Monday, February 1, 2016 10:23:29 PM	2%
8. Suspend Non-critical VMs at Recovery Site			
9. Change Recovery Site Storage to Writeable			
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			

7. **Optional:** After the recovery operation has completed, click the History tab to view a detailed report.

3.4 Perform Reprotect Operation

To run the reprotect operation, complete the following steps:

1. In the Site Recovery home interface, select the Recovery Plans tab from the left window pane.
2. Highlight the desired recovery plan from the left window pane and then click the Reprotect recovery plan icon to perform the operation.



SF-RP1 | Actions

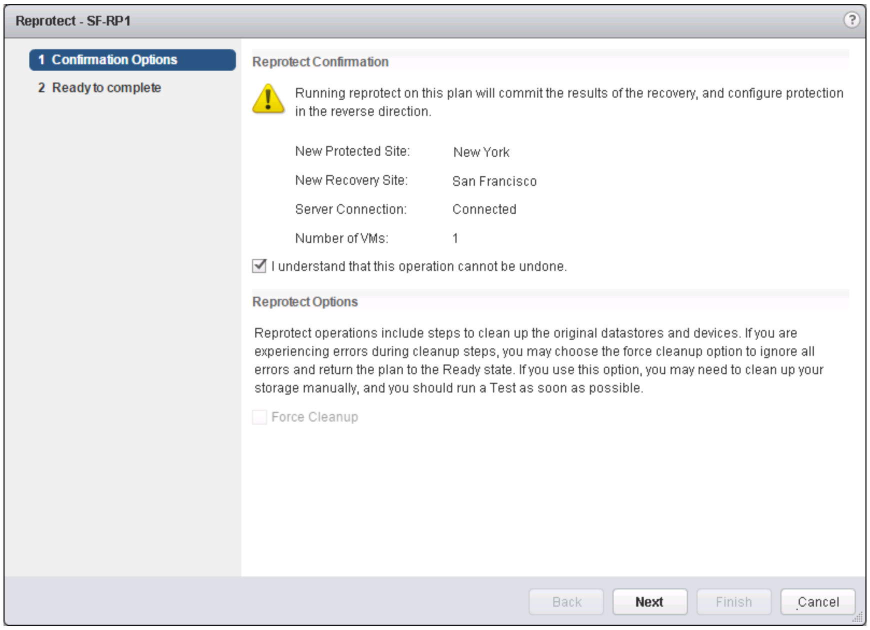
Summary | **Monitor** | Manage | Related Objects

Recovery Steps | History

Plan status: Recovery complete

Description: The recovery has completed. Please review the plan history to view any errors or warnings
you plan to failback the virtual machines to the original site, you must first run the plan in re
recovery mode to failback the virtual machines to the original site.

3. Select I Understand That This Operation Cannot be Undone and click Next and Finish to complete the wizard.



Reprotect - SF-RP1

1 Confirmation Options
2 Ready to complete

Reprotect Confirmation

Running reprotect on this plan will commit the results of the recovery, and configure protection in the reverse direction.

New Protected Site:	New York
New Recovery Site:	San Francisco
Server Connection:	Connected
Number of VMs:	1

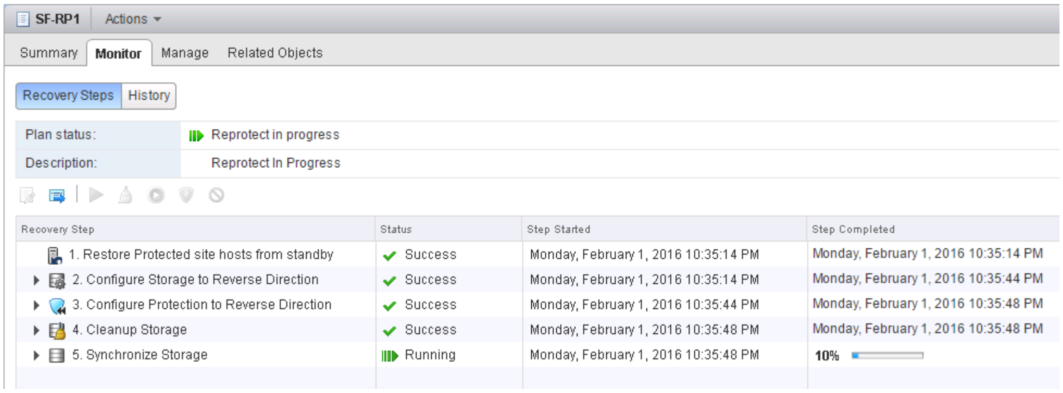
☑ I understand that this operation cannot be undone.

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

4. Click the Recovery Steps tab to monitor the progress of the reprotect operation.



Plan status:	Reprotect in progress
Description:	Reprotect In Progress

Recovery Step	Status	Step Started	Step Completed
1. Restore Protected site hosts from standby	✓ Success	Monday, February 1, 2016 10:35:14 PM	Monday, February 1, 2016 10:35:14 PM
2. Configure Storage to Reverse Direction	✓ Success	Monday, February 1, 2016 10:35:14 PM	Monday, February 1, 2016 10:35:44 PM
3. Configure Protection to Reverse Direction	✓ Success	Monday, February 1, 2016 10:35:44 PM	Monday, February 1, 2016 10:35:48 PM
4. Cleanup Storage	✓ Success	Monday, February 1, 2016 10:35:48 PM	Monday, February 1, 2016 10:35:48 PM
5. Synchronize Storage	Running	Monday, February 1, 2016 10:35:48 PM	10%

5. **Optional:** When the recovery has completed, click the History tab to view a detailed report of the operation.

4 Summary

VMware vCenter Site Recovery Manager 6 is a disaster recovery offering that provides automated orchestration and nondisruptive testing of centralized recovery plans to simplify disaster recovery management for all virtualized applications.

By deploying Site Recovery Manager on NetApp clustered Data ONTAP, you can dramatically lower the cost and complexity of disaster recovery. With high-performance, easy-to-manage, and scalable storage appliances and robust software offerings, NetApp offers flexible storage and data management solutions to support vSphere environments.

The best practices and recommendations that are provided in this guide are not a one-size-fits-all solution. This document contains a collection of best practices and recommendations that provide guidelines to plan, deploy, and manage SRM DR plans. Consult with a local NetApp VMware expert when you plan and deploy VMware vCenter Site Recovery environments onto NetApp storage. NetApp VMware experts can quickly identify the needs and demands of any vSphere environment and can adjust the storage solution accordingly.

References

This report references the following documents and resources:

- TR-4400: Applying VMware vSphere Virtual Volumes on NetApp Clustered Data ONTAP 8.3
  https://www.netapp.com/us/media/tr-4400.pdf
- TR-4333: VMware vSphere 5 on NetApp Clustered Data ONTAP
  http://www.netapp.com/us/media/tr-4333.pdf
- TR-4015: SnapMirror Configuration and Best Practices Guide for clustered Data ONTAP
  https://www.netapp.com/us/media/tr-4015.pdf
- TR-4183: SnapVault Best Practices Guide for Clustered Data ONTAP
  http://www.netapp.com/as/media/tr-4183.pdf
- TR-4129: Namespaces in Clustered Data ONTAP
  http://www.netapp.com/in/media/tr-4129.pdf
- RBAC User Creator for Clustered Data ONTAP community site
  http://community.netapp.com/t5/Virtualization-and-Cloud-Articles-and-Resources/How-to-use-the-RBAC-User-Creator-for-Data-ONTAP/ta-p/86601
- NetApp Virtual Storage Console for VMware vSphere documentation
  http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=30048
- NetApp VASA Provider for Clustered Data ONTAP documentation
  http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=61790
- NetApp Clustered Data ONTAP documentation
  https://mysupport.netapp.com/documentation/productlibrary/index.html?productID=30092
- VMware Site Recovery Manager Documentation
  https://www.vmware.com/support/pubs/srm_pubs.html

Version History

Version	Date	Document Version History
Version 1.1	March 2016	Kristopher Groh: Updated for SRM 6
Version 1.0	March 2014	Peter Flecha: Initial version

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp®

www.netapp.com