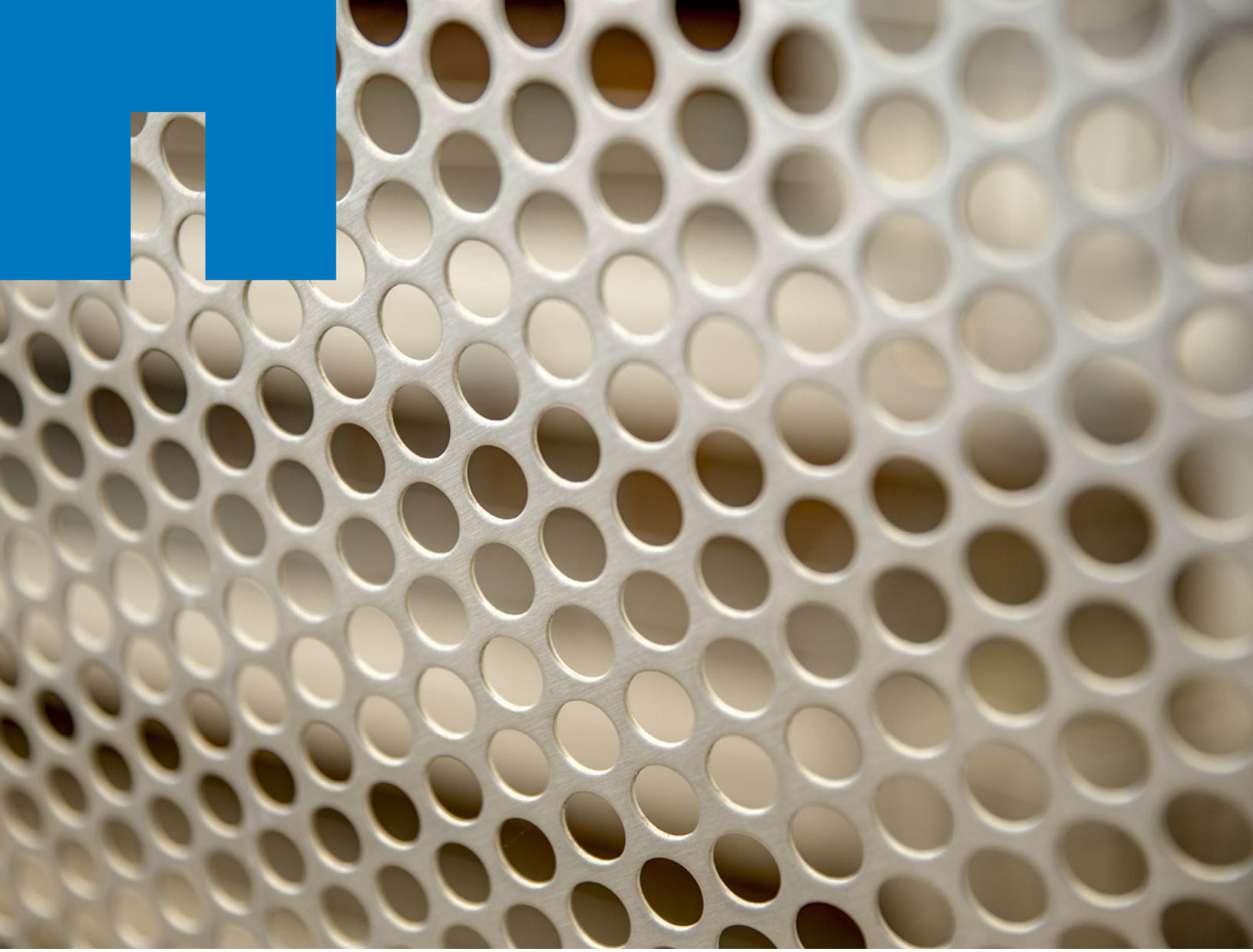


NETAPP UNIVERSITY

ONTAP Data Protection Administration

Student Guide
Content Version 1.0

NetApp®

NETAPP UNIVERSITY

ONTAP Data Protection Administration

Student Guide

Course ID: STRSW-ILT-DATAPROT-REV07
Catalog Number: STRSW-ILT-DATAPROT-REV07-SG

ATTENTION

The information contained in this course is intended only for training. This course contains information and activities that, while beneficial for the purposes of training in a closed, non-production environment, can result in downtime or other severe consequences in a production environment. This course material is not a technical reference and should not, under any circumstances, be used in production environments. To obtain reference materials, refer to the NetApp product documentation that is located at http://now.netapp.com/.

COPYRIGHT

U.S. GOVERNMENT RIGHTS

Commercial Computer Software. Government users are subject to the NetApp, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

TRADEMARK INFORMATION

NetApp, the NetApp logo, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, CyberSnap, Data ONTAP, DataFort, FilerView, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries.

Other product and service names might be trademarks of NetApp or other companies. A current list of NetApp trademarks is available on the Web at http://www.netapp.com/us/legal/netapptmlist.aspx.

TABLE OF CONTENTS

Welcome!

ONTAP Data Protection Administration

- Sign in (classroom sessions only).
- Be sure that you have your Student Guide and Exercise Guide.
- Test your headset and microphone (virtual sessions only).
- Provide yourself with two screens (virtual sessions only).
- Make yourself comfortable—class begins soon.

NetApp

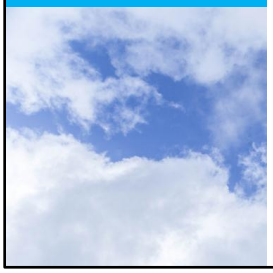
1

ONTAP Data Protection Administration

Course ID: STRSW-ILT-DATAPROT-REV07

NetApp

Welcome



Classroom Logistics

Getting Started

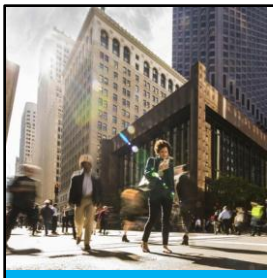
- Schedule (start, stop, breaks, breakout sessions)
- Activities and participation
- Materials
- Equipment check
- Support

Classroom Sessions

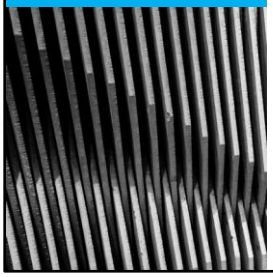
- Sign-in sheet
- Refreshments
- Phones
- Alarm signal
- Evacuation procedure
- Electrical safety

Virtual Sessions

- Collaboration tools
- Ground rules
- Phones and headsets

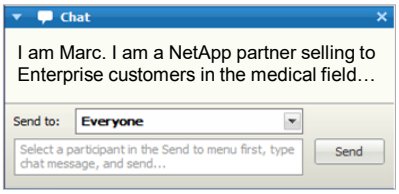


Introductions



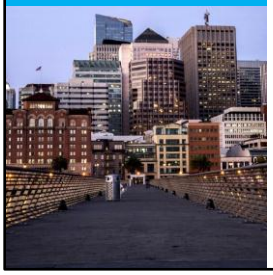
Virtual Sessions

Classroom Sessions



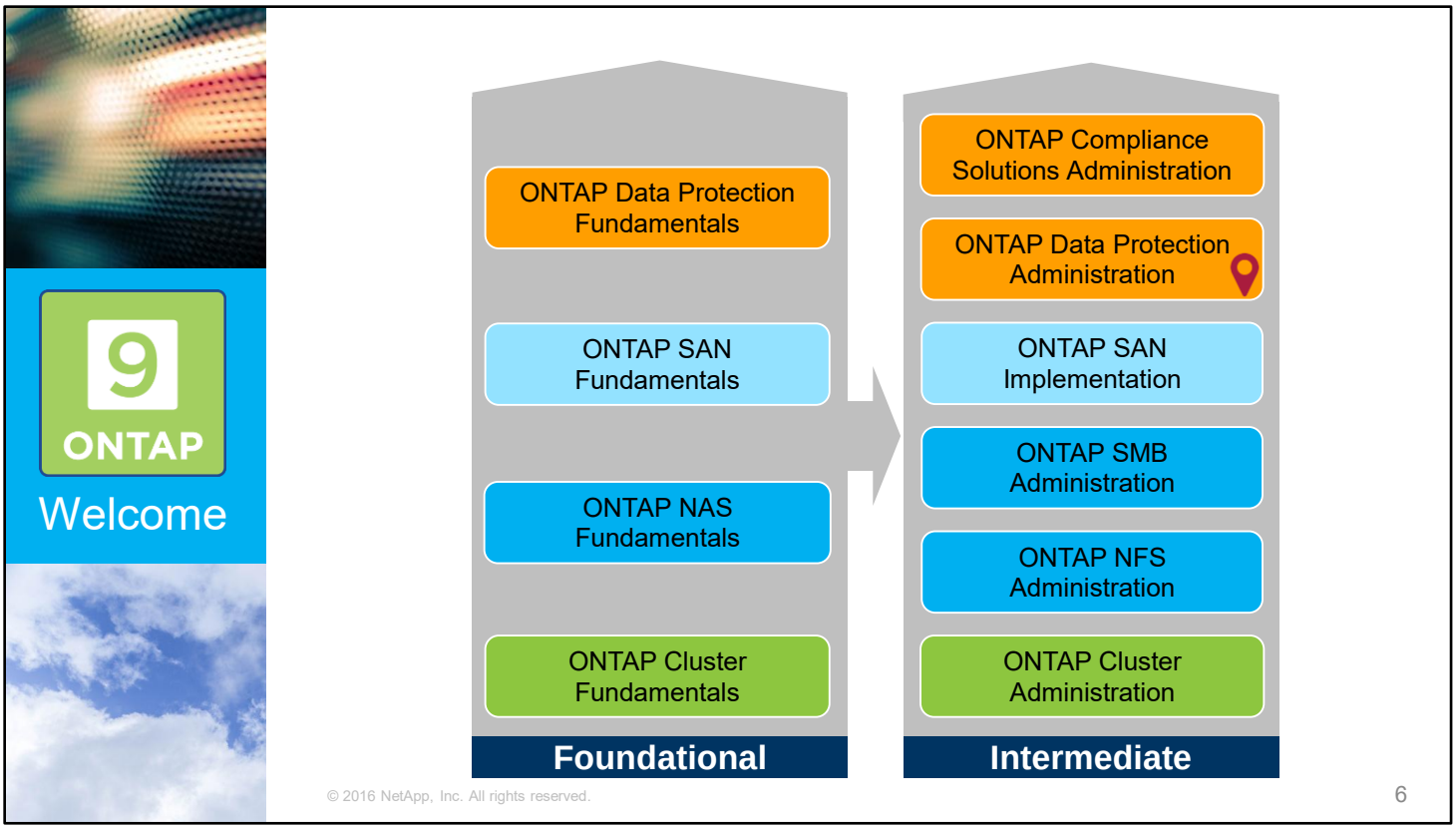
Take time to get to know one another. If you are participating in a NetApp Virtual Live class, your instructor asks you to use the chat window or a conference connection to speak. If you are using a conference connection, unmute your line to speak, and be sure to mute again after you speak.

About This Course



This course focuses on enabling you to do the following:

- Describe the ONTAP 9 data protection features
- Understand the various data mirroring relationships available with ONTAP 9
- Configure and operate SnapMirror and SnapVault data replication
- Demonstrate Storage Virtual Machine data protection
- Explain the components and configuration involved with SyncMirror and MetroCluster
- Describe NDMP protocol operation, configuration and management

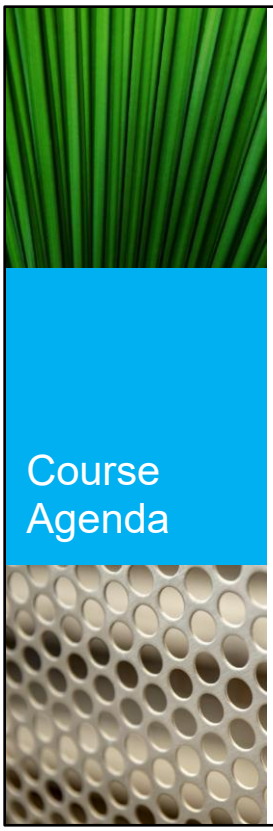


The ONTAP 9 Data Management Software learning path consists of multiple courses that focus on particular topics. Fundamental courses build knowledge as you progress up the foundational column and should therefore be taken in the order shown. Likewise, administration courses also build knowledge as you progress up the intermediate column, but they require the prerequisite foundational knowledge.

You can navigate the learning path in one of three ways:

- Complete all of the fundamental courses and then progress through the administration courses. This navigation is the recommended progression.
- Take a fundamental course and then take its complementary administration course. The courses are color-coded to make complementary courses easier to identify (green=cluster topics, blue=protocol topics, and orange=data protection topics).
- Take the course or courses that best fit your particular needs. For example, if you manage only SMB file shares, you can take ONTAP NAS Fundamentals and then take ONTAP SMB Administration. Most courses require some prerequisite knowledge. For this example, the prerequisites are ONTAP Cluster Fundamentals and ONTAP Cluster Administration.

The “you are here” indicator shows where this course appears in the ONTAP learning path. You should take ONTAP Data Protection Fundamentals in preparation for this course. Also, you should have a working knowledge of ONTAP Cluster Administration. After you complete this course, you might want to take the ONTAP Compliance Solutions Administration course.



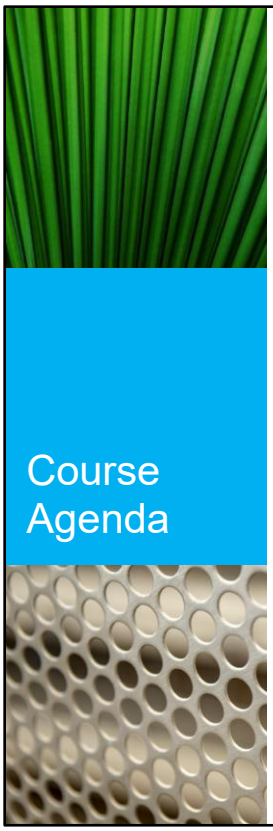
Day One

Morning

- Introduction
- Module 1: ONTAP Integrated Data Protection

Afternoon

- Module 2: NetApp Mirroring Fundamentals
- Module 3: Implement SnapMirror Relationships



Course Agenda

Day Two

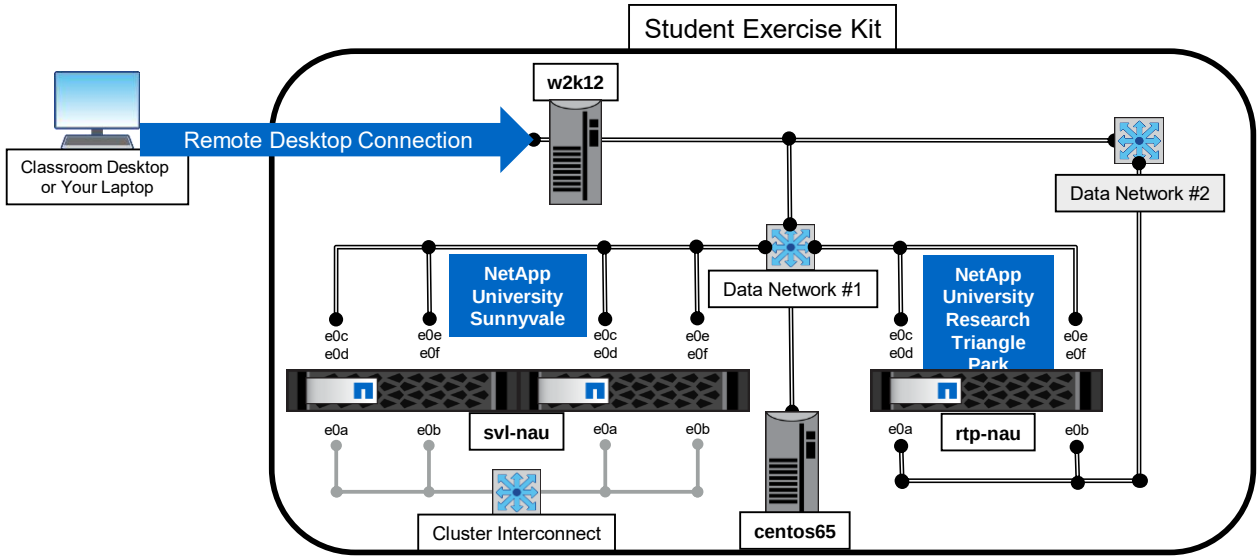
Morning

- Module 4: Disaster Recovery for Storage Virtual Machines
- Module 5: Disk-to-Disk Backup with SnapVault Software

Afternoon

- Module 6: SyncMirror and MetroCluster Software
- Module 7: NDMP and Tape Backup

Class Equipment: Basic Architecture

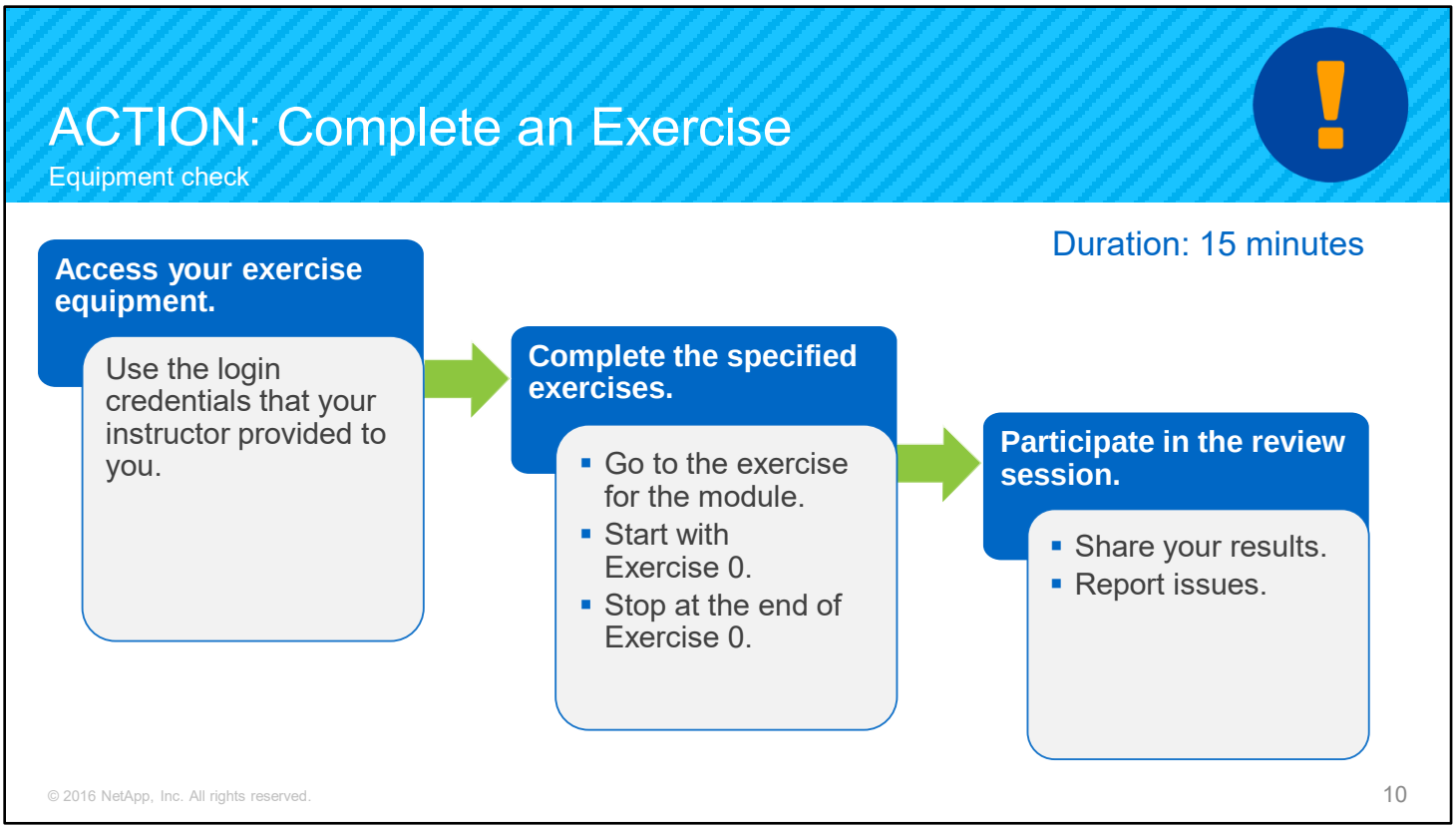


Open your exercise equipment kit from your laptop or from the classroom desktop. To connect to your exercise equipment, use Remote Desktop Connection or the NetApp University portal.

The Windows 2012 Server is your windows domain controller for the LEARN Windows domain. The Windows Server hosts the domain DNS server.

Your exercise equipment consists of several servers:

- One Windows 2012 R2 Server system
- Two CentOS Linux 6.5 Server systems
- One ONTAP 9 two-node cluster (svl-nau)
- One ONTAP 9 single-node cluster (rtp-nau)



See your Exercise Guide.

ACTION: Share Your Experiences

Roundtable questions for the exercise

- Do you have any questions about your equipment kit?
- Do you have any issues to report?

If you encounter an issue, promptly notify your instructor so that the issue can be resolved before you begin the exercise for Module 1.

Your Learning Journey

Bookmark these pages

NetApp University

- NetApp University Overview
  - Find the training that you need.
  - Explore certification.
  - Follow your learning map.
- NetApp University Community
  Join the discussion.
- NetApp University Support
  Contact the support team.

NetApp

- New to NetApp Support Webcast
  Ensure a successful support experience.
- NetApp Support
  Access downloads, tools, and documentation.
- Customer Success Community
  Engage with experts.
- NetApp Knowledgebase
  Access a wealth of knowledge.

The *NetApp University Overview* page is your front door to learning. Find training that fits your learning map and your learning style, learn how to become certified, link to blogs and discussions, and subscribe to the NetApp newsletter *Tech OnTap*.

http://www.netapp.com/us/services-support/university/index.aspx

The *NetApp University Community* page is a public forum for NetApp employees, partners, and customers. NetApp University welcomes your questions and comments.

https://communities.netapp.com/community/netapp_university

The *NetApp University Support* page is a self-help tool that enables you to search for answers to your questions and to contact the NetApp University support team. http://netappusupport.custhelp.com

Are you new to NetApp? If so, register for the *New to NetApp Support Webcast* to acquaint yourself with the facts and tips that help to ensure that you have a successful support experience.

http://www.netapp.com/us/forms/supportwebcastseries.aspx?REF_SOURCE=new2ntapwl-netappu

The *NetApp Support* page is your introduction to all products and solutions support: http://mysupport.netapp.com. Use the *Getting Started* link (http://mysupport.netapp.com/info/web/ECMP1150550.html) to establish your support account and hear from the NetApp CEO. Search for products, downloads, tools, and documentation, or link to the *NetApp Support Community* (http://community.netapp.com/t5/Products-and-Solutions/ct-p/products-and-solutions).

Join the *Customer Success Community* to ask support-related questions, share tips, and engage with other users and experts.

https://forums.netapp.com/

Search the *NetApp Knowledgebase* to apply the accumulated knowledge of NetApp users and product experts.

https://kb.netapp.com/support/index?page=home

Module 1
ONTAP Integrated Data Protection

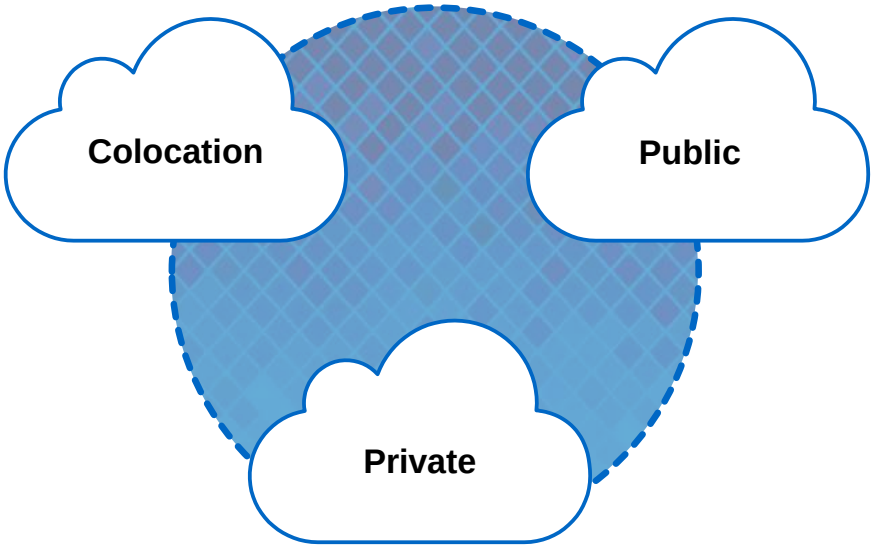
About This Module

This module focuses on enabling you to do the following:

- Describe data protection
- Describe the integrated data protection features in ONTAP 9 software
- Identify the tools and software that are used to manage and monitor the data protection features

Lesson 1
Data Protection Overview

The Data Fabric Powered by NetApp



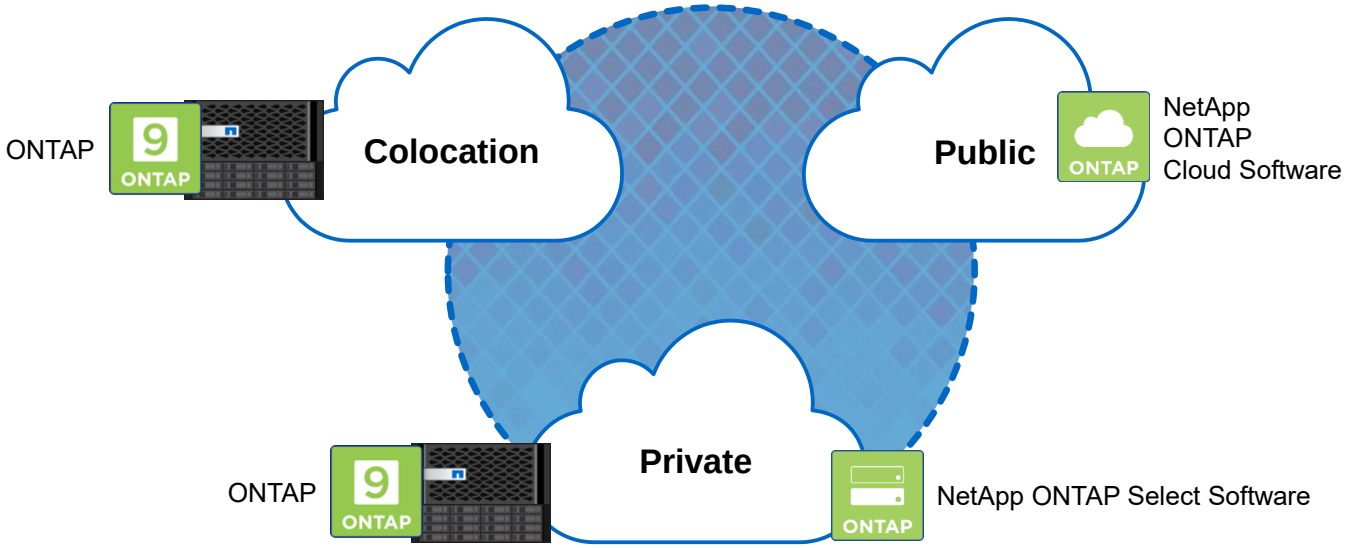
Managing data in hybrid cloud architectures can be a challenge. Sometimes the hybrid architecture becomes a collection of separate, incompatible repositories for data, known as “data silos.” As a solution, the Data Fabric powered by NetApp connects cloud resources. When clouds are connected by the Data Fabric strategy, IT can draw from the resources of each cloud. IT can also move data and applications to new cloud services and place every workload on the most appropriate platform.

Data Fabric is the NetApp vision for the future of data management. Data Fabric is the NetApp architecture for the hybrid cloud.

Data Fabric seamlessly connects multiple data-management environments across disparate clouds into a cohesive, integrated whole. Organizations control the management, security, protection, and access of data across the hybrid cloud, no matter where the data is located. IT has the flexibility to select the right set of resources and the freedom to change the resources whenever necessary.

For more information about Data Fabric, see the Welcome to Data Fabric video: http://www.netapp.com/us/campaigns/data-fabric/index.aspx.

ONTAP Software



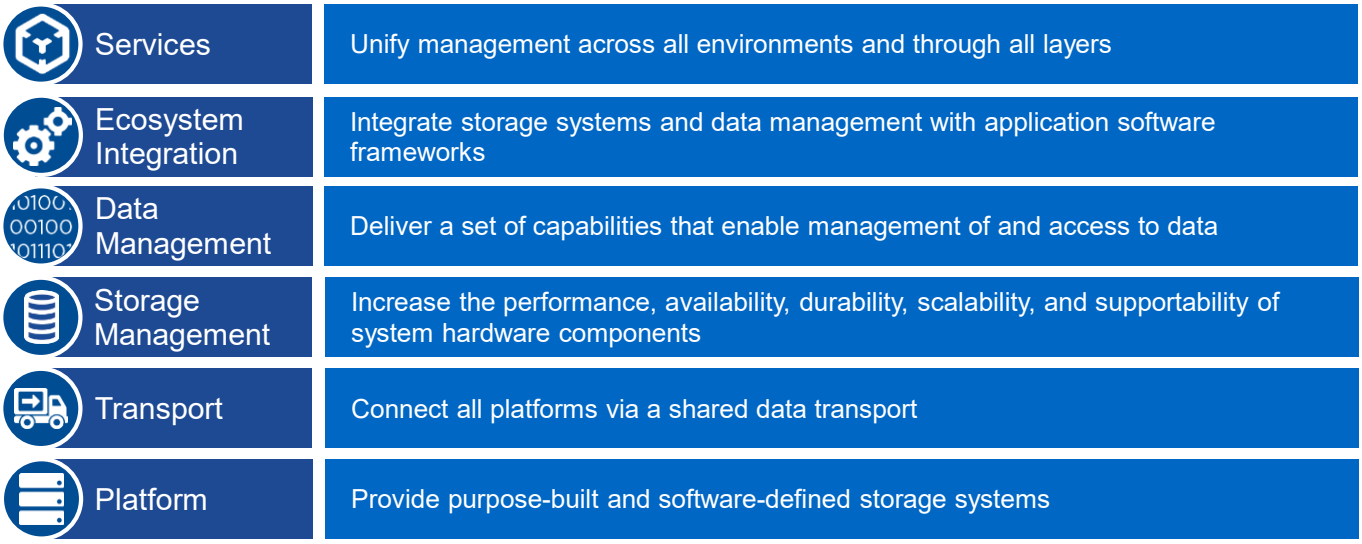
NetApp ONTAP software is known primarily as the storage software that runs on FAS and All Flash FAS controllers. ONTAP software is the foundation of Data Fabric, the NetApp vision for the future of data management.

As part of the Data Fabric vision, ONTAP software can also run in the cloud as a software storage system; for example, NetApp ONTAP Cloud for Amazon Web Services (ONTAP Cloud for AWS).

For remote offices that lack space and resources, NetApp ONTAP Select software can be run as a virtual machine on the VMware vSphere platform. This virtualization enables the distribution of data center management and end-to-end data protection for the remote office environment.

Although this course focuses on ONTAP clusters, the knowledge is also applicable to ONTAP Cloud and ONTAP Select software.

Data Fabric Layers



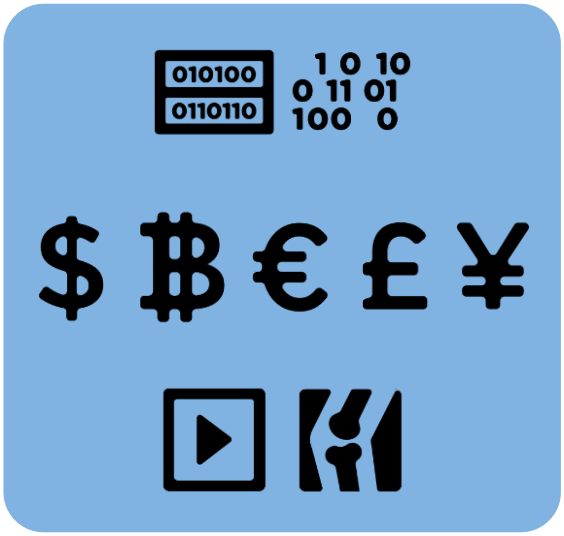
Creators of a data fabric system must take a data-centric view of IT infrastructure in every layer of the environment: platform, transport, storage management, data management, ecosystem integration, and services. The architecture contains the products and solutions that unbind data from underlying systems so that the data can be accessed across the fabric. With Data Fabric powered by NetApp, IT architects have many building blocks to choose from at each layer. These building blocks adhere to the principles of a true Data Fabric strategy.

Data Fabric starts at the platform layer. The platform layer includes the storage systems that are the building blocks for the endpoints of the Data Fabric strategy. The course focuses on ONTAP software, running on FAS or All Flash FAS systems, as the endpoint. The course also discusses the features that the other Data Fabric layers contain.

Data Currency

Data protection SLA terms:

- Recovery point objective (RPO) is the acceptable maximum amount of data loss in the event of a failure.
- Recovery time objective (RTO) is the maximum acceptable time period that is required to make the data available after a failure.



When you consider data and data protection, you must first examine the currency of data. In other words, you need to assign a monetary value to the data, based on the significance of the data to the organization. For example, the video of a child's first steps is important to the child's family but might be of little value outside the family. The medical records of the same child, however, are of great importance to the health of the child, the family, and possibly many other people. These records can be used to identify, heal, or prevent health issues for the child, the family, or possibly other people around the globe. The protection of a video or picture on a cell phone and the protection of records in a health network present different data protection challenges.

Data currency is important when you define the terms of an SLA between the service provider and the customer. The following two terms are frequently used:

- Recovery point objective (RPO): The maximum acceptable amount of data loss in the event of a failure
- Recovery time objective (RTO): The maximum acceptable amount of time that is required to make the data available after a failure

The determination of RTO and RPO helps to define the data protection solution or solutions that are used to meet the particular SLA requirements.

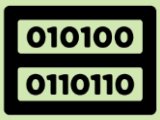
Data Types

Structured Data

Data that is organized

Examples:

- Block-level (SAN) data
- Database application data
- Email
- Server or desktop virtualization



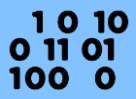
Consistency is typically required.

Unstructured Data

Data that is unorganized

Examples:

- File-level (NAS) data
- Spreadsheets
- Text documents
- PDFs
- Presentations



Consistency is typically not required.

Structured data is organized, typically by a host or host application. Examples include block-level data from a host that uses SAN protocols or the data that is generated by a database and email applications. Also, server or desktop virtualization has many levels of structured data, including the host file system, the guest file system, and the application data.

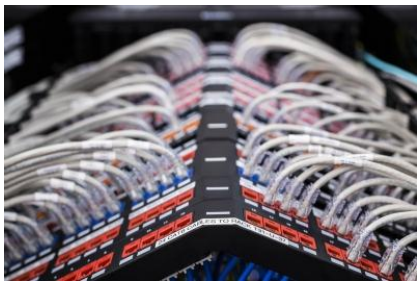
Unstructured data is unorganized. Typically, this data is shared. Examples include folders or shares containing spreadsheets, text documents, PDFs, presentations, and so on.

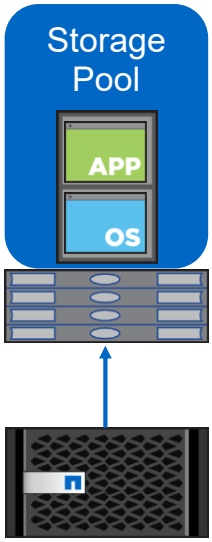
The important point to understand about these two data categories is that structured data usually requires a certain level of consistency. In other words, the host operating system, the application, and the storage system must all be at the same consistency level before a backup is initiated. Unstructured data is contained within a file share, where NetApp ONTAP software controls the file system and the consistency of the data.

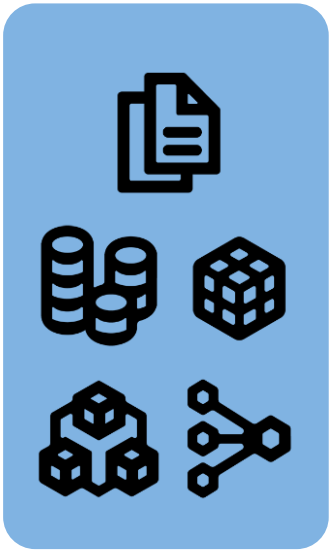
Data Consistency

Consistency types:

- Point-in-time consistency
- Transactional consistency
- Crash consistency
- Application consistency



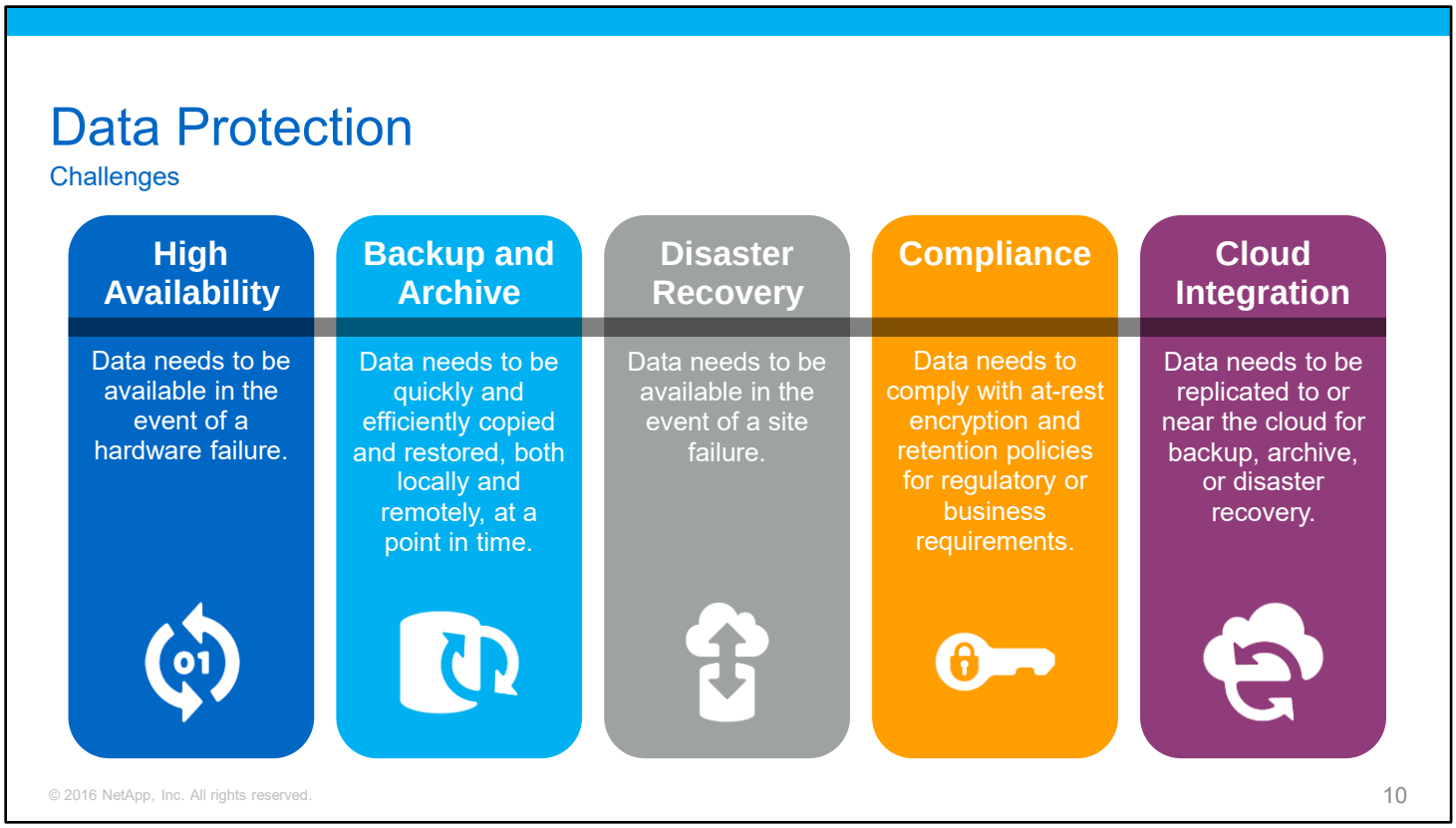




Data consistency requirements vary widely depending on the workload requirements. You can start by examining a single text file on a share or volume. When you back up a file, for example, using a Snapshot copy in ONTAP software, it is consistent in that point in time. In other words, you protect the file at that particular point in time, and if needed, you can restore the file back to that exact point in time. When ONTAP software creates a Snapshot copy, it is at the volume level, and therefore all of the files in a volume are backed up at the same time. As previously stated, for most file shares, this level of consistency is adequate.

For block-level data from a host using SAN protocols, in which the host controls the file system, consistency is required between the host and the storage system. If the host writes data while the storage system is doing a backup, the data consistency between the host and storage system is compromised. This situation would also be true with applications that write structured data, for example, a database application's data. For these workloads, transactional consistency is required. For this level of consistency, transactions must be paused or quiesced while the data is backed up. With ONTAP software, because Snapshot copies are nearly instantaneous, the pause is brief, but the backup must be orchestrated among the host, application, and storage system.

Server and desktop virtualization poses a unique challenge because there are multiple layers of data to protect. The host administrator uses the virtualization software to create storage pools or containers on the storage system. The host administrator uses these storage pools or containers to create virtual machines (VMs) and virtual disks to present to the VMs. Finally, the administrator installs applications on the VMs, which in turn write data to the virtual disks. In a virtualized environment, you need to consider the host and its data, the VMs and their data, and the applications and their data. For the VMs in particular, there are two consistency types: crash consistency and application consistency. The difference between the types is whether only the VM is backup-aware or both the VM and application are backup-aware.



Now that you know more about data, look at the different types or categories of data protection and the challenges that they pose.

High availability: Data needs to be available in the event of a hardware failure. This category includes features that provide for availability or takeover of resources should a component or controller fail. High availability is typically within a data center.

Backup and archive: A point-in-time copy or restore operation can be performed quickly and efficiently. This category includes features that back up or archive data either locally or remotely.

Disaster recovery: Data is made available in the event of a site failure. This category includes features that mirror data either locally or remotely. In the event of a failure at the mirror source (or primary site), the data at the mirror destination (or disaster-recovery site) is made available. Disaster recovery is typically considered a site-level protection because it is usually between two separate data centers.

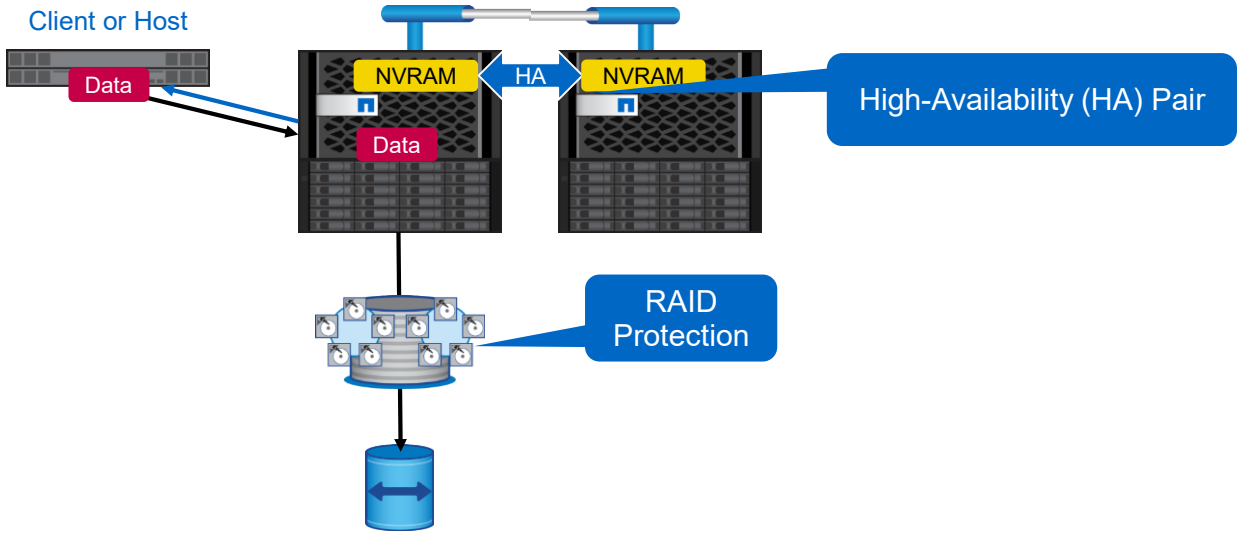
Compliance: Data needs to comply with at-rest encryption and retention policies for regulatory or business requirements. This category includes features that encrypt data or prevent data from being deleted or changed for a specified period. Compliance features are typically used to comply with a regulation or policy requirement, for example, the Sarbanes–Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA).

Cloud integration: Data is replicated to or near the cloud for backup, archive, or disaster recovery purposes. This category includes features that back up, restore, archive, or mirror data to a destination that is either in the cloud or near the cloud.

Lesson 2
Data Protection Solutions

Data Protection Solutions

High availability



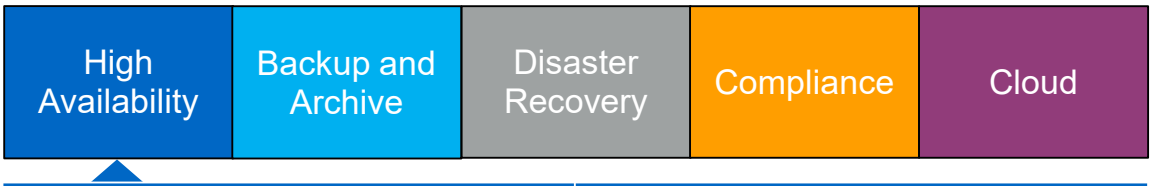
Now that you know the challenges, examine the solutions. ONTAP software starts to protect data that is sent from a client or host when it enters the cluster.

As data enters the system memory of a node in the cluster, it is logged in to NVRAM. The NVRAM is backed up with a battery to prepare for a power failure. The NVRAM logs are also mirrored to the high-availability partner to prepare for a hardware failure. After the data is safely logged in NVRAM and the NVRAM has been mirrored, an acknowledgment is sent to the client or host.

After the data is processed in main memory, along with other incoming data, it is committed to disk. While on disk, RAID protects the data in the event of a drive failure. Also, if the node should fail, the high-availability partner initiates a takeover to continue serving data.

Data Protection Solutions

High-availability features



Feature	Protection
NVRAM	Write acknowledgment before committing to disk
High-availability pairs	Data availability in the event of a controller failure
NetApp RAID DP or RAID-TEC technology	Double-parity or triple-parity protection that prevents data loss if two or three drives fail

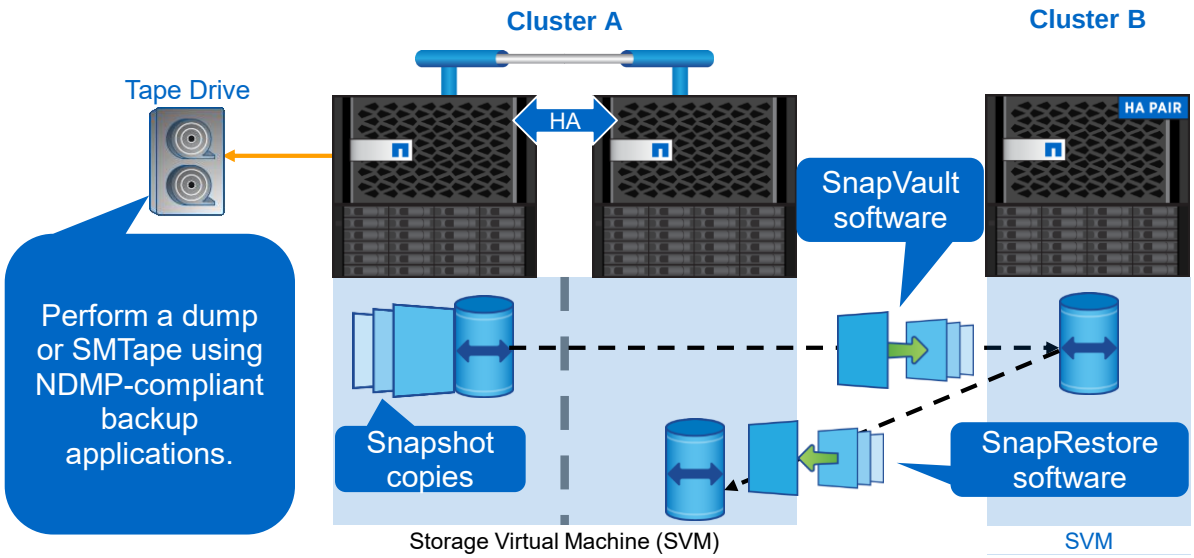
The features that are listed are part of ONTAP software and require no additional licensing.

The fundamentals of high availability are covered in the ONTAP Cluster Fundamentals course and are not discussed in this course.

You can learn more about high-availability administration in the ONTAP Cluster Administration course.

Data Protection Solutions

Backup and archive



When the data is safely on disk, there are various ways to back up and archive the data locally, remotely, or to tape.

Snapshot copies are volume-level, instantaneous, point-in-time local backups. Individual files, LUNs, or the whole volume can be restored.

For backup and archive locally or remotely, SnapVault software can be used. SnapVault software is an efficient, disk-to-disk backup feature that enables the retention of Snapshot copies for archival purposes. Like volume Snapshot copies, individual files, LUNs, or the whole volume can be restored. Also, you can restore to the source, the destination, or to a new location.

Although SnapVault software can be used instead of traditional tape backup, ONTAP software also includes support for tape through NDMP. NDMP enables you to back up data in storage systems directly to tape, resulting in efficient use of network bandwidth. ONTAP software supports both dump and SMTape engines for tape backup. You can perform a dump or SMTape backup or restore by using NDMP-compliant backup applications.

Data Protection Solutions

Backup and archive features

Feature	Protection
Snapshot copy	Point-in-time, volume-level copy
SnapRestore	Snapshot copy recovery
SnapVault	Replication-based, disk-to-disk backup
Dump or SMTape	Tape backup or restore using an NDMP-compliant backup application

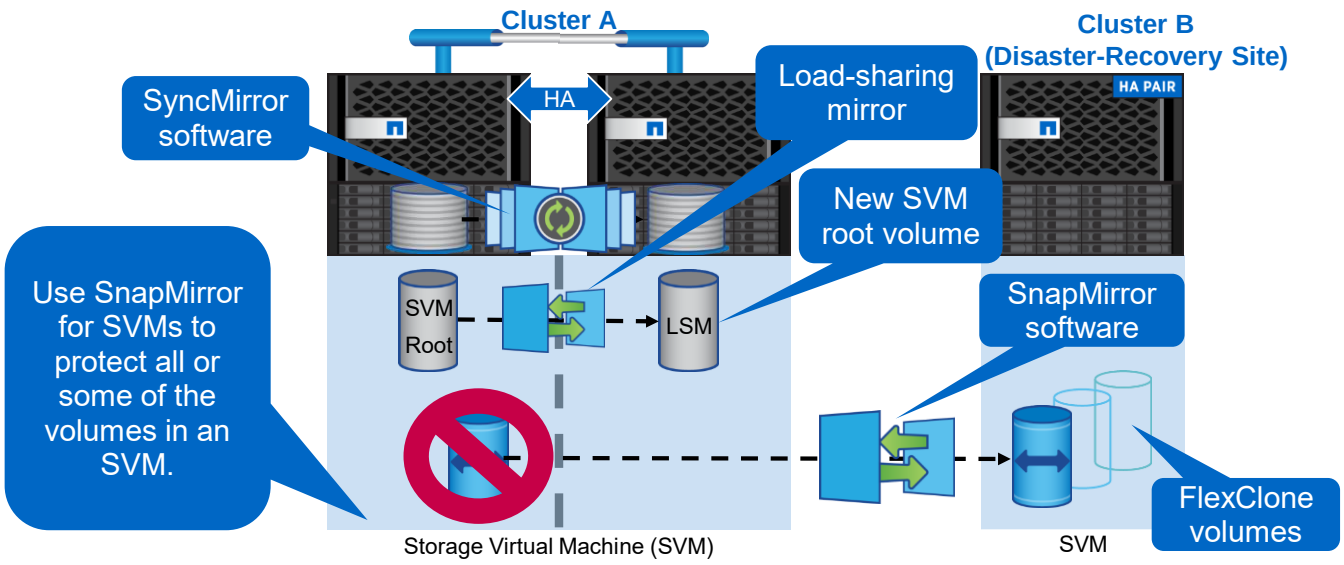
The features that are listed are used to back up and archive data locally, remotely, or to tape. Snapshot copies, NDMP, and SMTape are part of ONTAP software and require no additional licensing. SnapRestore software and SnapVault software require licensing to enable the features.

The fundamentals of Snapshot technology are covered in the ONTAP Cluster Fundamentals course, and only a review is provided in this course. This course focuses on when to use Snapshot copies or restore from a Snapshot copy using SnapRestore software. You also learn how SnapVault software can be used as a disk-to-disk backup solution.

You can learn more about Snapshot and SnapRestore administration in the ONTAP Cluster Administration course. Also, SnapVault administration and tape backups are covered in the ONTAP Data Protection Administration course.

Data Protection Solutions

Disaster recovery



Disaster-recovery solutions are required in the event of a system failure, power failure, or site failure. Disaster-recovery solutions should include the following abilities:

- To test before a failure condition
- To quickly fail over to a disaster recovery site
- To easily return to the previous conditions before the failover occurred

SnapMirror software is an asynchronous volume-level data replication feature that you can use for data movement and disaster recovery. A SnapMirror relationship can be made from a source volume to a destination volume in these locations:

- The same storage virtual machine (SVM)
- Another SVM in the same cluster
- Another SVM in a different cluster

Also, SnapMirror software for SVMs can be used to protect all or just some of the volumes in an SVM.

The destination volume is a read-only copy of the source, which can be cloned using FlexClone software for testing and development.

If a source becomes unavailable, the SnapMirror relationship can be broken, which makes the destination writable. After the issue has been resolved, the relationship can be resynced and then resumed.

A special type of SnapMirror software, called a load-sharing mirror, can also be created for the SVM root volume to protect the namespace in NAS environments. A load-sharing mirror can be created on multiple nodes in the cluster. If the SVM root volume becomes unavailable, a load-sharing mirror can be promoted to become the new SVM root volume.

You can use SyncMirror software for aggregate-level disaster recovery. SyncMirror software uses synchronous mirroring between two aggregates. This technology is used for site-to-site high availability in MetroCluster and the high-availability architecture of NetApp ONTAP Select software.

Data Protection Solutions

Disaster recovery features

Feature	Protection
SnapMirror	Asynchronous, volume-level data replication for data movement and disaster recovery
FlexClone	Instantaneous, space-efficient copies of replicated data
Load-sharing mirrors	Namespace (SVM root volume) protection
SyncMirror	Synchronous, aggregate-level mirror
MetroCluster	Zero RTO and RPO disaster recovery

The features that are listed are used for disaster recovery. Load-sharing mirrors and SyncMirror software are part of ONTAP software and require no additional licensing. SnapMirror software and FlexClone software require licensing to enable the features.

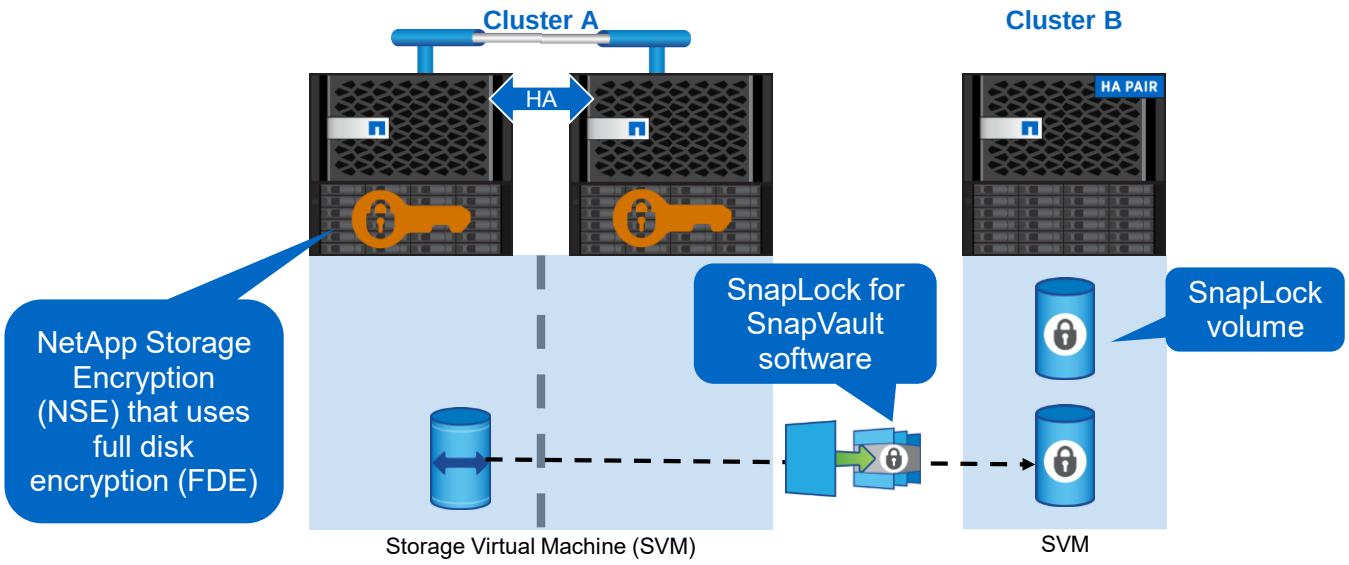
FlexClone volumes and load-sharing mirrors are discussed in the ONTAP Cluster Fundamentals and ONTAP NAS Fundamentals courses but are not discussed in this course.

This course focuses on SnapMirror software, SnapVault software, SVM disaster recovery, NDMP, and tape backup. You also learn how SyncMirror software and MetroCluster software work and where the technology is used.

You can learn more about FlexClone software and load-sharing mirror administration in the ONTAP Cluster Administration course.

Data Protection Solutions

Compliance



Compliance solutions are used when data needs to comply with at-rest encryption or retention policies that are required for regulatory or business reasons.

NetApp Storage Encryption (NSE) uses full disk encryption (FDE), which encrypts all data at rest on the disks. Because this encryption occurs at the disk level, no special configuration of aggregates or volumes is required. All that is required is management of the encryption keys.

SnapLock software is a license-based alternative to optical WORM data on disk. When committed, the data is retained in a locked state until the retention period expires. SnapLock software also works with SnapVault software, enabling the retention of backup and archive data. Although not shown, a SnapLock volume can be mirrored to another SnapLock volume.

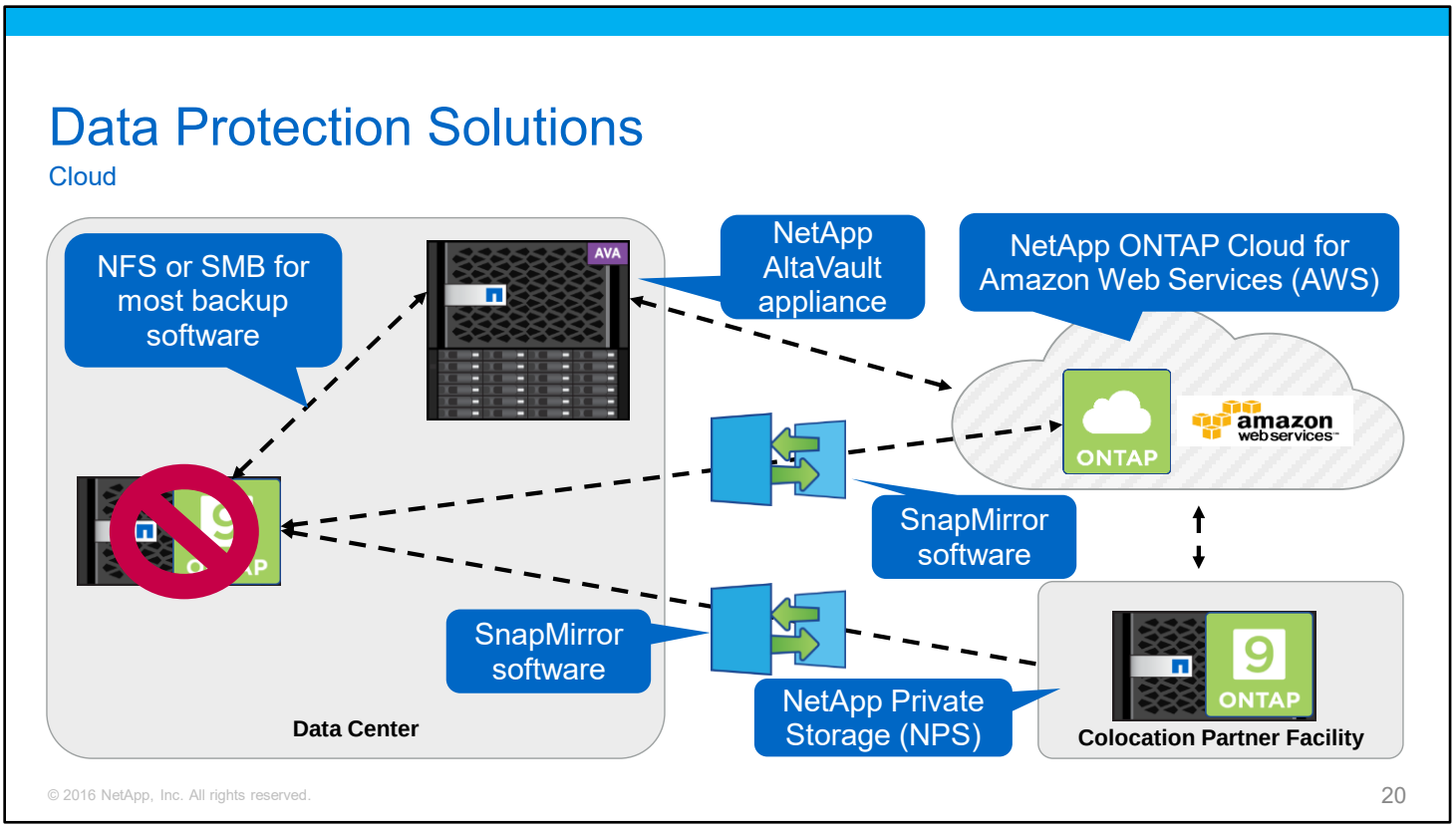
Data Protection Solutions

Compliance features

Feature	Protection
NetApp Storage Encryption (NSE)	FDE using self-encrypting drives
SnapLock	WORM solution to meet external and internal requirements for retaining, protecting, and accessing regulated and reference data

The features that are listed are used for comprehensive encryption and retention of data at rest.

Compliance solutions are not covered in this course. You can learn more about compliance in the ONTAP Compliance Solutions Administration course.



ONTAP software is a part of the Data Fabric and integrates easily with data protection in the cloud.

When you deploy ONTAP software directly in the cloud (for example, with NetApp ONTAP Cloud for Amazon Web Services [AWS]), you can mirror data from ONTAP software in a data center to ONTAP software in the cloud. The NetApp Snap-to-Cloud disaster recovery solution uses SnapMirror software to locate the disaster recovery site in the cloud. If the data becomes unavailable on the primary site, the disaster recovery site in the cloud can be brought online easily.

Alternatively, NetApp Private Storage (NPS) provides a similar solution but locates the disaster recovery site “next to” the cloud. The NPS solution places a storage system that runs ONTAP software in a hyper scale-provider colocation partner facility for the lowest latency and highest bandwidth. When in place, SnapMirror software can be used to mirror data between the primary data center and the colocation partner facility, which provides communication to other cloud providers. In the event of a disaster, the NPS disaster recovery site can be brought online easily. If the data at the NPS site is also mirrored to the NetApp ONTAP Cloud software, the cloud site can be brought online easily instead.

For cloud-integrated backup and recovery, you can use the NetApp AltaVault cloud-integrated storage technology. For primary storage, which can be ONTAP software or another third-party storage system, AltaVault technology connects into any backup software. AltaVault technology uses NFS or SMB for most backup software or Open Storage Technology (OST) for Symantec's Veritas NetBackup. AltaVault uses an optimized replication that gets backups to the cloud of your choice more quickly and with less bandwidth. Data is stored in the cloud, ready to be restored.

Data Protection Solutions

Cloud features

Feature	Protection
NetApp Private Storage for Cloud	Dedicated, private NetApp storage (near-cloud)
NetApp Snap-to-Cloud disaster recovery solution	Cloud-integrated data storage for disaster recovery
AltaVault	Cloud-integrated backup and recovery

The features that are listed are used for backup, archive, or disaster recovery in the cloud.

Although Snap-to-Cloud and NPS are not directly covered in this course, the knowledge that you gain in this course can be transferred easily to these solutions. Also, because this course focuses on ONTAP 9 data management software, AltaVault technology is not discussed. To find AltaVault technology training, search the NetApp LearningCenter.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

Which data protection solution would you use primarily for disaster recovery? (Select one.)

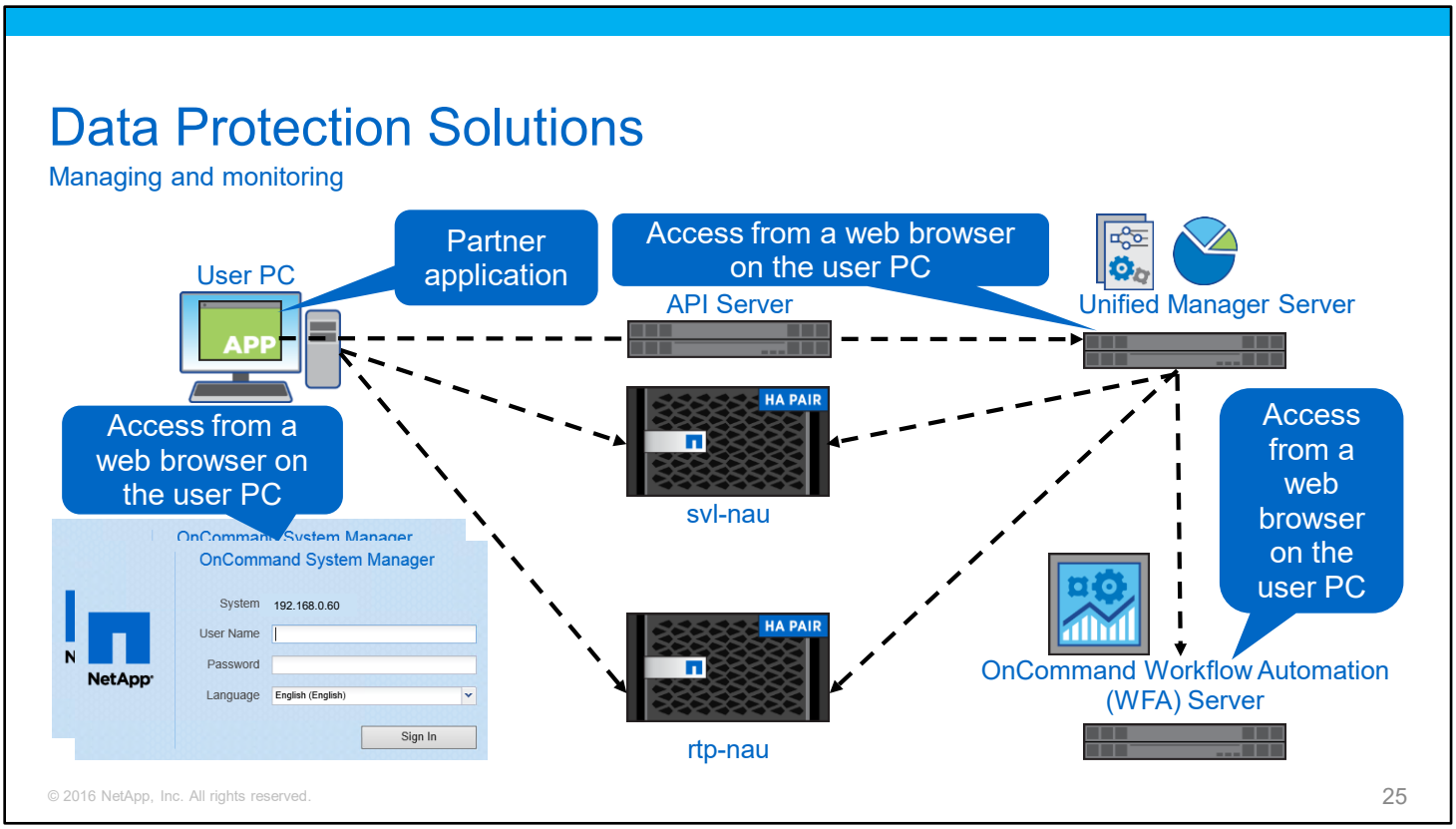
a. SnapVault

b. SnapMirror

c. SnapLock

d. Snapshot

Lesson 3
Monitor and Manage Data Protection Solutions



To manage and monitor a cluster, you use the OnCommand System Manager, which is bundled with ONTAP software. Although you can manage each cluster in a data protection relationship separately through its own System Manager instance, you can configure the cluster peer connection with a remote cluster and set up SnapVault and SnapMirror relationships from either instance. To manage and monitor other protection resources, you need to access each cluster's System Manager instance separately.

With the OnCommand Unified Manager, an administrator can monitor and manage protection from a single URL and single location. The Unified Manager enables you to configure policies and create reports for multiple clusters and their protection relationships.

If you want to use the protection features in the Unified Manager, you must also install OnCommand Workflow Automation (WFA). OnCommand WFA is a software solution that helps to automate storage management tasks, such as data protection. You can use OnCommand WFA to build workflows to complete tasks for your processes and storage service-level tasks.

You can use OnCommand API Services through an API server. APIs enable partner applications to interact with the Unified Manager's monitoring and management operations of ONTAP storage systems. OnCommand API Services also enables you to add a storage system that runs ONTAP software, retrieve storage-related information, and provision storage resources.

Data Protection Solutions

Managing and monitoring software

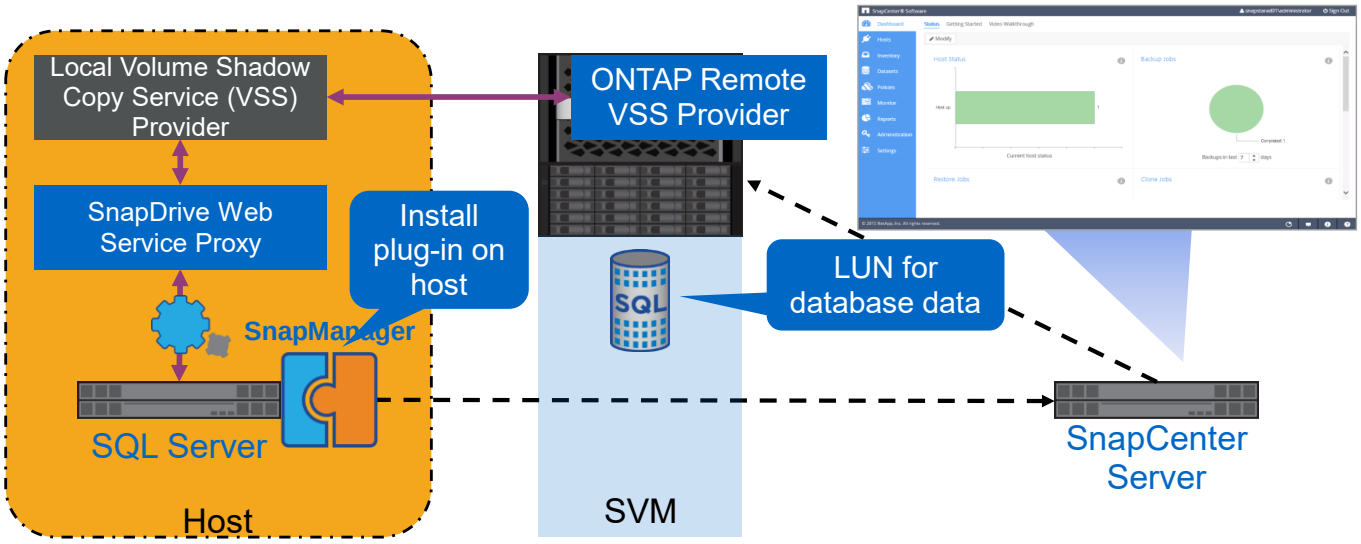
Feature	Description
OnCommand System Manager	Provide fast, simple configuration and management for an ONTAP cluster
OnCommand Unified Manager	Monitor the health and simplify management of multiple ONTAP clusters
OnCommand WFA	Automate storage tasks and data protection processes
OnCommand APIs	Integrate with third-party management solutions

The products that are listed are used to manage and monitor data protection solutions.

This course uses only OnCommand System Manager. To find training for the other products that are listed, search the NetApp LearningCenter.

Data Protection Solutions

Host-level and application-level



From the discussion of structured data and consistency in the first lesson, you recall that transactions must be paused or quiesced while the data is backed up. Performing these steps manually is very time consuming and disruptive. To manage backups, you should use a backup management tool.

In this example we have a SQL Server which is writing data to a LUN on the storage system. SnapManager products such as SnapManager for SQL can initiate backups, restores, and replication operations that are application-aware. To maintain consistency during a backup, a component of the Windows operating system called Volume Shadow Copy (VSS) is used. VSS is typically used to perform local backups from Windows. By using a hardware VSS provider, which is part of SnapDrive for Windows, the backup can be created on the storage system instead of locally. When installed on the SQL Server, SnapDrive creates a web-service proxy to pass requests such as backup and restore operations through the local VSS provider. The local VSS provider communicates with the remote VSS provider, which is part of ONTAP, to create the backup on the storage system. Once the backup is complete, the database software is notified that the shadow copy is done and that it is OK to resumes writes to the database.

In environments with multiple servers and applications, there are will be many instances of SnapDrive and SnapManager to manage. SnapCenter is a data protection and clone management software product that can replace many instances of SnapManager and SnapDrive. SnapCenter is a unified scalable platform that provides consistency and simplicity through a centralized data management GUI. SnapCenter is powered by a SnapCenter server. SnapCenter uses plug-ins that are installed on the host to standardize data management across multiplatform environments.

Data Protection Solutions

Host-level and application-level software

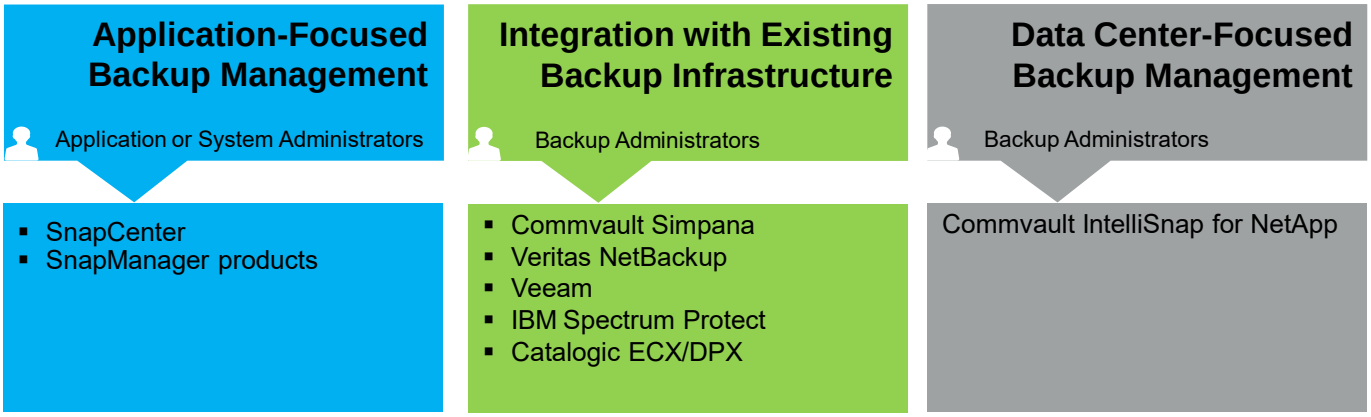
Feature	Description
SnapDrive	Automate storage and data management for physical and virtual environments
SnapManager	Streamline storage management and simplify configuration, backup, and restore for enterprise operating environments
SnapCenter	Centralize data protection and clone management with a single interface across all application environments

The products that are listed are used to simplify data protection management.

These products are not covered in this course. To find training for the products that are listed, search the NetApp LearningCenter.

Data Protection Solutions

Management software solutions

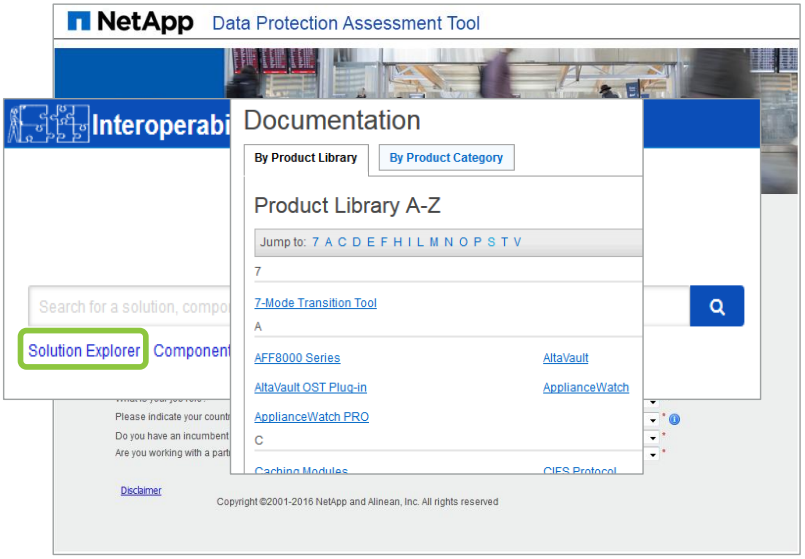


Both NetApp and its partners create data protection management software. NetApp software is written primarily for application or system administrators. Partner software is written primarily for backup administrators.

For details on the partner products listed, visit the NetApp partners website: http://www.netapp.com/partners

Data Protection Tools

- Data Protection Assessment Tool: www.netapp.com/us/products/data-protection
- NetApp Interoperability Matrix Tool (IMT): mysupport.netapp.com/matrix
- Documentation: mysupport.netapp.com



NetApp provides various tools to help decide on a solution and to search for supported configurations.

The data protection assessment tool can help you to discover the NetApp data protection solution or solutions that best fit your requirements. You can find a link to the tool on the data protection products page on the NetApp website.

The NetApp Interoperability Matrix Tool (IMT) is a web-based application that enables you to search for configurations of NetApp products and components that meet the standards and requirements specified by NetApp. To find data protection solutions, click the **Solutions Explorer** link.

You can find documentation for data protections solutions on NetApp Support on the documentation tab.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

Which data protection solution would you use primarily for disk-to-disk backup as a replacement for tape backups? (Select one.)

a. SnapVault

b. SnapMirror

c. SnapLock

d. Snapshot

References

- *ONTAP 9.0 Release Notes*
- *ONTAP Data Protection Fundamentals (web-based training)*

Module Review

This module focused on enabling you to do the following:

- Describe data protection
- Describe the integrated data protection features in ONTAP 9 software
- Identify the tools and software used to manage and monitor the data protection features

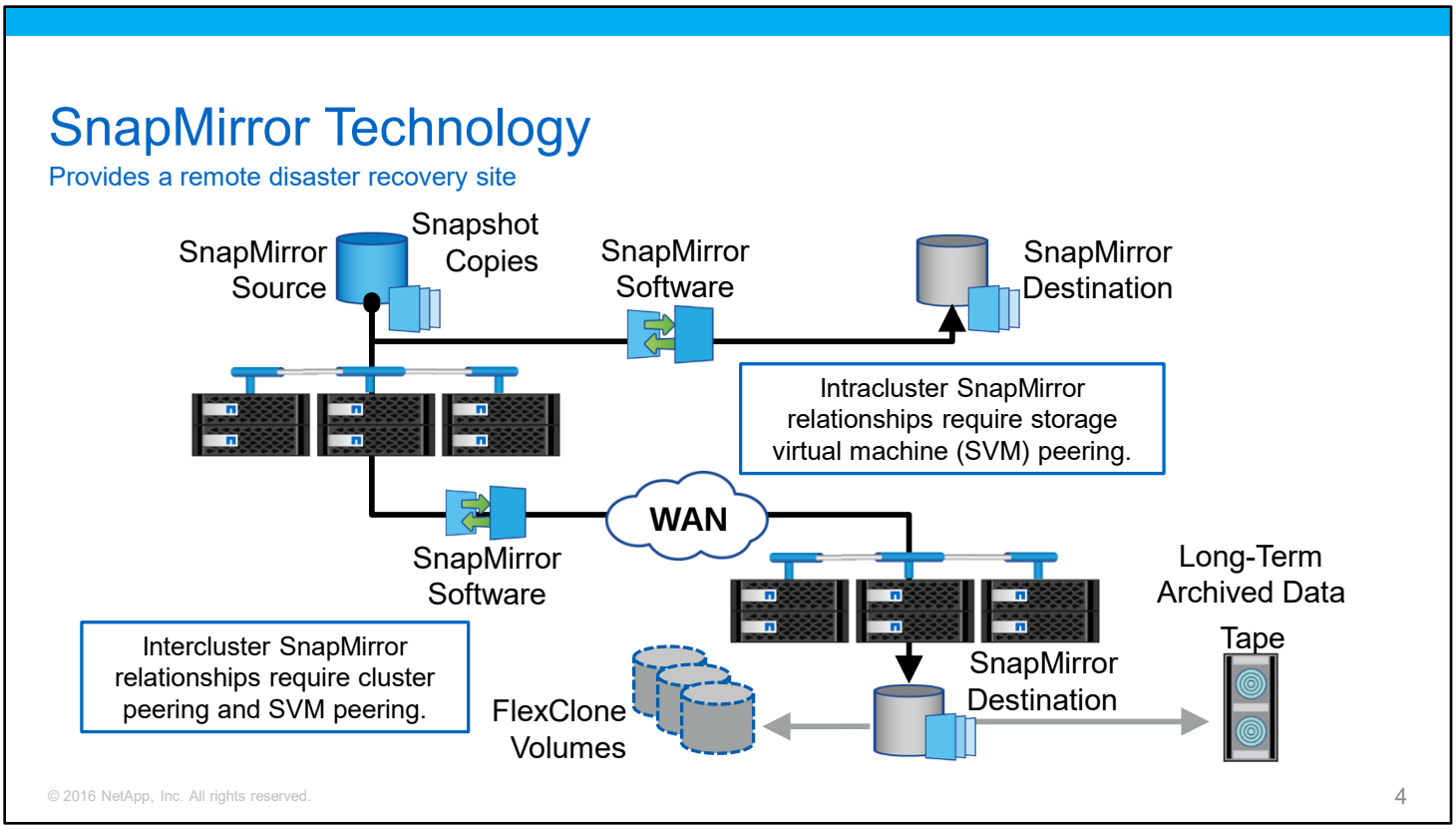
Module 2
NetApp Mirroring Fundamentals

About This Module

This module focuses on enabling you to do the following:

- Explain the different types of mirroring relationships available with ONTAP 9 software
- Describe the required components of each of the ONTAP 9 mirroring relationships
- List the ONTAP features supported by SnapMirror software
- Identify the differences between the cascading replication relationships
- Design a network configuration for intercluster mirroring
- Construct the peer relationships required for intercluster and storage virtual machine (SVM) mirroring

Lesson 1
Components of a NetApp Mirror Relationship



SnapMirror Software Uses and Benefits

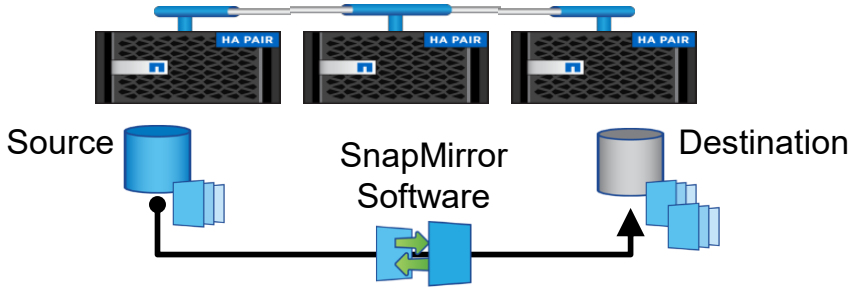
SnapMirror technology in ONTAP software provides asynchronous volume-level replication based on a configured replication update interval. SnapMirror technology uses NetApp Snapshot copy technology as part of the replication process.

SnapMirror relationships consist of source and destination volumes. The SnapMirror source and destination volumes can be in the same cluster (intracluster) or in different clusters (intercluster). Intracluster SnapMirror relationships require that the storage virtual machines (SVMs) be configured as SVM peers (also called Vserver peers). Intercluster SnapMirror relationships require cluster peering and SVM peering.

Instead of leaving the mirrored volume unused in the colocation, SnapMirror technology enables you to use the destination volume to create ONTAP FlexClone volume clones. You can create a clone of the destination volume without affecting performance on the source volume. You can also use the destination volume to offload to tape.

Data Protection Mirror Relationships

- Mirror relationships between FlexVol volumes
- Mirror relationships for SVM data volumes and configuration

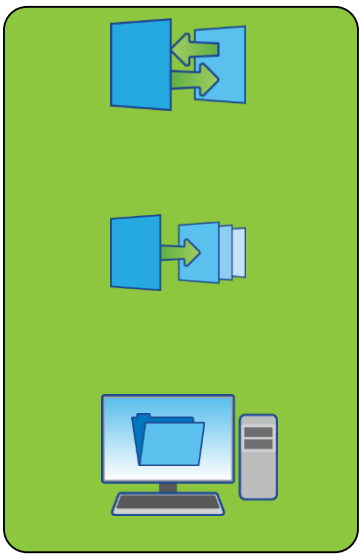


SnapMirror technology in ONTAP software provides asynchronous volume-level replication based on a configured replication update interval. SnapMirror software uses NetApp Snapshot technology as part of the replication process.

Data Protection Relationships

Types

- Data protection: For data protection mirror copies (the default)
- Extended data protection: For SnapVault and version-flexible SnapMirror relationships
- Load-sharing (LS): For SVM root volume protection (primarily)



There are different types of SnapMirror relationships, which are used for different purposes.

Data protection relationships are used for data protection mirror copies. When you create a mirror relationship, if you do not specify a type, the default is the data protection type.

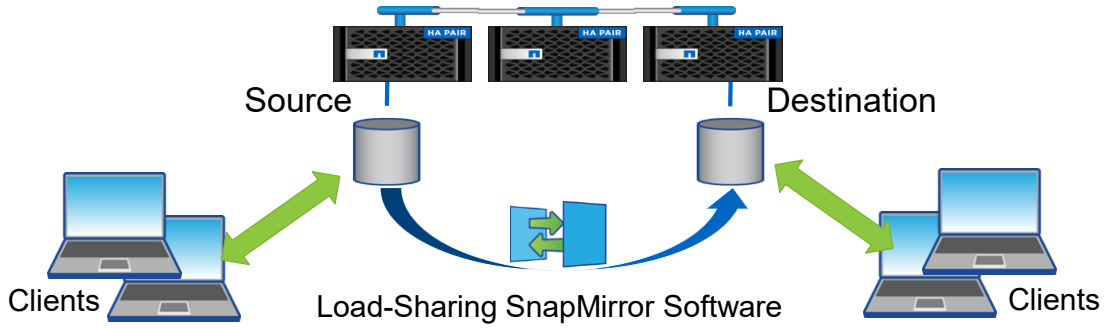
Extended data protection relationships are used for SnapVault backups. SnapVault backups also contain retention rules, which are defined in the SnapMirror policy.

SnapMirror relationships using type XDP and policy async-mirror or mirror-vault, also known as version-flexible SnapMirror software, are available. Such a relationship can be built only from source and destination volumes on controllers running ONTAP 8.3 or later software.

Load-sharing (LS) relationships are used to protect SVM root volumes, also known as namespace protection.

Load-Sharing Mirror Relationships

- SnapMirror load-sharing mirror copies can support only NAS (CIFS and NFSv3).
- Load-sharing mirror copies do not support NFSv4 clients or SAN client protocol connections (FC, FCoE, or iSCSI).



How should you deploy load-sharing mirror relationships?

SnapMirror load-sharing mirror copies increase performance and availability for NAS clients. Load-sharing mirrors distribute an SVM namespace root volume to other nodes in the same cluster. By distributing data volumes to other nodes in the cluster, performance for large read-only workloads is improved.

Key points to remember:

- LS mirrors are asynchronous. Therefore, data served from a mirror is accurate at the time of the update, but the mirror remains unchanged until the next update. Therefore, data that becomes stale is a poor candidate for LS mirrors.
- The blocks are replicated, not shared. You can have one LS mirror per node, so it is possible to have the read/write (RW) volume and 24 individual copies of that volume, each consuming space. If the RW volume is going to be large, the use of LS mirrors could become expensive.
- The mirrors are read-only. If most users need to be able to write to the volume, they all go to the RW volume, and never use the mirror volumes.

Generally, you should use LS mirrors for the root volume of the SVM. The root volume is usually the mount point, and the mirrors protect the mount point by the fact that they are read-only. The mount point cannot be filled or corrupted. Remember that the root volume and its mirrors are not replicated when using SVM data recovery (SVM-DR).

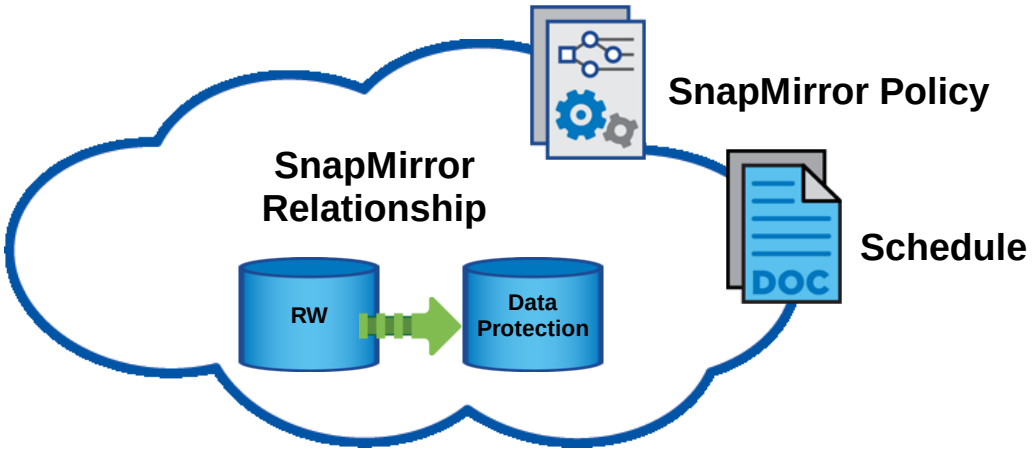
A small, read-only volume that contains static data might be a good candidate for LS mirroring.

NOTE: SnapMirror load-sharing mirror copies support only NAS (CIFS/NFSv3). Load-sharing mirror copies do not support NFSv4 clients or SAN client protocol connections (FC, FCoE, or iSCSI). ONTAP software routes NFSv4 clients to the source of the load-sharing mirror for direct read and write access.

The configuration methods for NFS and CIFS clients' access to load-sharing mirrors is different. See the CIFS and NFS administration courses for more information.

SnapMirror and SnapVault Configuration

SnapMirror or SnapVault relationships must be assigned a policy and an optional schedule.



The SnapMirror relationship, policy, and schedule work together to provide an automated data protection solution.

Default SnapMirror Policies

Pre-configured policies for SnapMirror and SnapVault relationships

Feature	Policy Name	Policy Type	Comment
Mirror	DPDefault	Async-mirror	Default policy for a data protection relationship
Vault	XDPDefault	Vault	Default policy for an extended data protection relationship with daily and weekly rules
Version-Flexible Mirror	MirrorLatest	Async-mirror	Policy to mirror the latest active file system (default)
Version-Flexible Mirror (with all source Snapshot copies)	MirrorAllSnapshots	Async-mirror	Policy to mirror all Snapshot copies and the latest active file system
Mirror and Vault	MirrorAndVault	Mirror-vault	A unified SnapMirror and SnapVault policy to mirror the latest active file system and daily and weekly Snapshot copies

ONTAP 9 software has pre-configured SnapMirror policies for both SnapMirror and SnapVault relationships. The default policies can be used without any changes or modified for your needs. You can always create a policy.

If no policy is assigned to a relationship, a default policy is assigned. If it is a data protection mirror relationship, the DPDefault policy is assigned. If it is a SnapVault relationship, the XDPDefault policy is assigned.

A SnapMirror policy can be used cluster-wide, or be assigned to a specific SVM. If the `vserver name` is configured to use the cluster name, the policy is a cluster-wide policy and can be used for SnapMirror relationships with any SVM in the cluster. If the `vserver name` is configured to use the SVM name, then the policy is specific to that SVM and can be used for only SVM relationships.

SnapMirror Policy Configuration

Shared configuration attributes

Attribute	Description
`-type`	▪ Async-mirror (data protection, disaster recovery) ▪ Vault (extended data protection, backup, and archive) ▪ Mirror-vault (extended data protection, unified data protection)
`-tries`	The maximum number of times to attempt each manual or scheduled transfer
`-transfer-priority`	`Normal` or `low`. Normal-priority transfers are scheduled before low-priority transfers.
`-restart (DP only)`	`Always`, `never`, or `default`. By default, transfers always resume from the restart checkpoint.

Policy Attributes

You can use the `snapmirror policy modify` command to modify policy attributes. For example, use the `comment` attribute (not shown) to enter details about the policy. Other attributes include the maximum number of times to attempt a failed transfer, the transfer priority, whether to record file access time (not shown), or whether to restart an interrupted transfer.

All SnapMirror policies have a field `create-snapshot`. This field specifies whether SnapMirror software creates a Snapshot copy on the primary volume at the beginning of a SnapMirror update or SnapMirror resync operation. Currently, a user cannot set or modify this field. It is set to true for SnapMirror policies of type async-mirror and mirror-vault at the time of creation. SnapMirror policies of type vault have `create-snapshot` set to false at the time of creation.

SnapMirror Policy Parameters

-type

Specifies the SnapMirror policy type. The supported values are async-mirror, vault, and mirror-vault. Data protection relationships support only async-mirror policy type, whereas extended data protection relationships support all three policy types.

If the type is set to async-mirror, the policy is for disaster recovery. When the policy type is associated with extended data protection relationships, SnapMirror update and SnapMirror resync operations transfer selected Snapshot copies from the primary volume to the secondary volume. The rules in the policy govern the selection of Snapshot copies. However, SnapMirror initialize and SnapMirror update operations on data protection relationships ignore the rules in the policy. These operations transfer all Snapshot copies of the primary volume which are newer than the shared Snapshot copy on the destination.

If the type is set to vault, the policy is used for backup and archive. The rules in this policy type determine which Snapshot copies are protected and how long they are retained on the secondary volume. This policy type is supported by only extended data protection relationships.

If the type is set to mirror-vault, the policy is used for unified data protection which provides both disaster recovery and backup on the same secondary volume. This policy type is supported by only extended data protection relationships.

-tries

Determines the maximum number of times to attempt each manual or scheduled transfer for a SnapMirror relationship. The value of this parameter must be a positive integer or unlimited. The default value is 8.

-restart

Applies to only data protection relationships. It defines the behavior of SnapMirror software if an interrupted transfer exists. The supported values are always, never, or default. If the value is set to always, an interrupted SnapMirror transfer always restarts if both these conditions are met:

- It has a restart checkpoint
- The conditions are the same as they were before the transfer was interrupted

Also, a new SnapMirror Snapshot copy is created and then transferred. If the value is set to never, an interrupted SnapMirror transfer never restarts, even if a restart checkpoint exists. A new SnapMirror Snapshot copy is still created and transferred.

-transfer-priority

Specifies the priority at which a transfer runs. The supported values are normal or low. The normal transfers are scheduled before the low-priority transfers. The default is normal.

See the ONTAP 9.0 Commands: Manual Page Reference for complete details of the `snapmirror policy create` command options.

SnapMirror Policy Configuration

Shared configuration rules

`-keep`	Specifies the maximum number of Snapshot copies that are retained on the SnapMirror vault secondary volume for a rule
`-preserve`	Specifies the behavior when the Snapshot copy retention count is reached on the SnapMirror vault secondary volume. If the number specified is reached, the update fails. The value can be `true` or `false`. The default value is `false`.
`-snapmirror-label`	Specifies the rule to modify in a SnapMirror policy. Used for Snapshot copy selection for extended data protection relationships
`-schedule`	Specifies the name of the Snapshot copy schedule associated with a rule

Policy Rules

A SnapMirror policy can be applied to a data protection mirror relationship or a SnapVault relationship. Whether the SnapMirror policy has rules determines whether the policy is applied to a SnapVault relationship or applied to a data protection mirror copy. If the policy has rules that define which Snapshot copies are protected, that policy can be applied to only SnapVault relationships. If the policy does not have rules, the policy can be applied to only data protection mirror copies.

SnapMirror policy rules can be used to modify the retention count, preserve setting, warning threshold count, schedule, and prefix for a rule in a SnapMirror policy. Modifying a rule to add a schedule enables creation of Snapshot copies on the SnapMirror destination. Snapshot copies on the source that have a SnapMirror label matching this rule are not selected for transfer. A SnapMirror policy with rules must have at least one rule without a schedule.

The rules in SnapMirror policies of type async-mirror cannot be modified.

SnapMirror Policy Configuration Rules

-keep

Specifies the maximum number of Snapshot copies that are retained on the SnapMirror destination volume for a rule. The total number of Snapshot copies retained for all the rules in a policy cannot exceed 251. For all the rules in SnapMirror policies of type async-mirror, this parameter must be set to 1.

-preserve

Specifies the behavior when the Snapshot copy retention count is reached on the SnapMirror vault destination for the rule. The default value is false. False means that the oldest Snapshot copy is deleted to make room for new ones only if the number of Snapshot copies exceeds the retention count specified in the "keep" parameter.

Snapshot copies are no longer created on the SnapMirror destination if the following conditions are all met:

- You set the value to true.
- The Snapshot copies have reached the retention count.
- An incremental SnapMirror vault update transfer fails or the rule has a schedule.

For all the rules in SnapMirror policies of type async-mirror, this parameter must be set to the value false.

-snapmirror-label

This parameter specifies the rule to modify in a SnapMirror policy.

-schedule

This optional parameter specifies the name of the schedule associated with a rule. You can use this parameter for only rules associated with SnapMirror policies of type vault or mirror-vault. When this parameter is specified, Snapshot copies are directly created on the SnapMirror destination. The Snapshot copies created have the same content as the latest Snapshot copy already present on the SnapMirror destination. Snapshot copies on the source that have a SnapMirror label matching this rule are not selected for transfer. The default value is -.

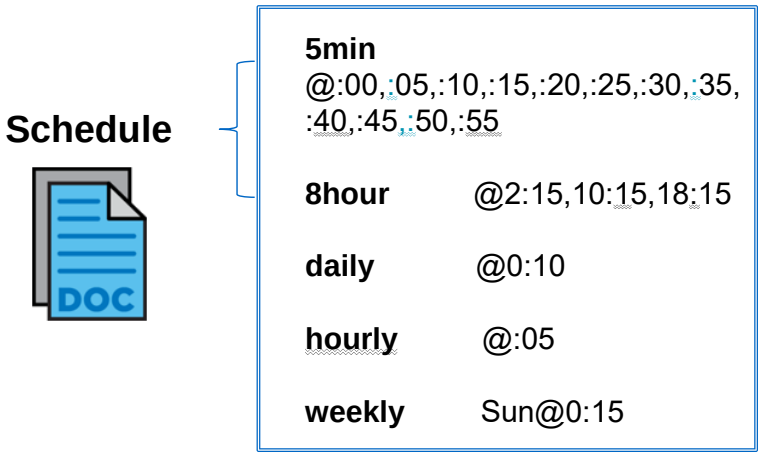
NOTE:

You define and name a schedule using the `job schedule cron create` command.

See the ONTAP 9.0 Commands: Manual Page Reference for complete details of the `snapmirror policy modify-rule` command options.

Schedule Automatic Transfers

To automate data protection SnapMirror or SnapVault transfers, you must assign a schedule to the relationship.



When a SnapMirror and SnapVault relationship is created, an optional update schedule is applied. The cron job schedule is normally created to control the frequency of the SnapMirror or SnapVault update.

Cron job schedules are schedules that run at a specific time. You can use a preconfigured schedule, modify a preconfigured schedule, or create a schedule.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

You have a four-node ONTAP 9.0 cluster. You want to protect the root volume associated with an SVM. What would you do? (Select one.)

a. Create a clone of the root volume using the latest Snapshot copy.

b. Create a load-sharing mirror relationship for the root volume with every node of the cluster.

c. Create a script that copies the data to a non-root volume.

d. Nothing. The ONTAP 9.0 cluster automatically protects SVM root volumes.

Lesson 2
Configuration Guidelines for Intercluster SnapMirror Software

Intercluster Network Connectivity

IP address and subnet setup

Before cluster peering can be established, network connectivity between the clusters must be set up correctly.

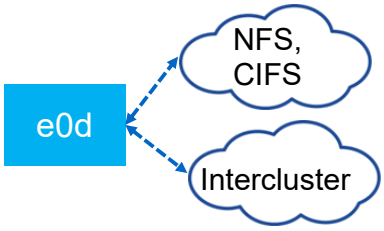
- The subnet must belong to the broadcast domain containing the ports used for intercluster communication.
- The IP addresses used for the intercluster logical interfaces (LIFs) should be in the same subnet.
- The subnet must have one intercluster LIF per node in the cluster.
- The intercluster network must have full-mesh connectivity.
- Cluster LIFs can use either IPv4 or IPv6 addresses.

Before cluster peering is set up, network connectivity must be established so the intercluster logical interfaces (LIFs) can communicate with each other reliably. There are several details to remember concerning the subnet, broadcast domain, IP addresses, and network ports.

Intercluster Network Connectivity

Port setup for intercluster communication

- The ports do not have to be in the default IPspace.
- Ports added to a broadcast domain can be physical ports, virtual LANs (VLANs), or interface groups.
- The maximum transmission unit (MTU) settings of all ports must be identical.
- The ports can be used (shared) with data communications.




```
Node: svl-nau-02
                                                          Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   1500  auto/1000  healthy
e0b       Cluster      Cluster          up   1500  auto/1000  healthy
e0c       Default      Default          up   1500  auto/1000  healthy
e0d       Default      Default          up   1500  auto/1000  healthy
e0e       Default      Default          up   1500  auto/1000  healthy
e0f       Default      Default          up   1500  auto/1000  healthy
```


To determine whether sharing a data port for intercluster replication is the correct intercluster network solution, you should consider configurations and requirements such as the following:

- LAN type
- Available WAN bandwidth
- Replication interval
- Change rate
- Number of ports

Intercluster network ports can be shared with data communications, but it is recommended that these ports are dedicated to the SnapMirror function to avoid contention between user data and SnapMirror data.

ACTION: Try This Task

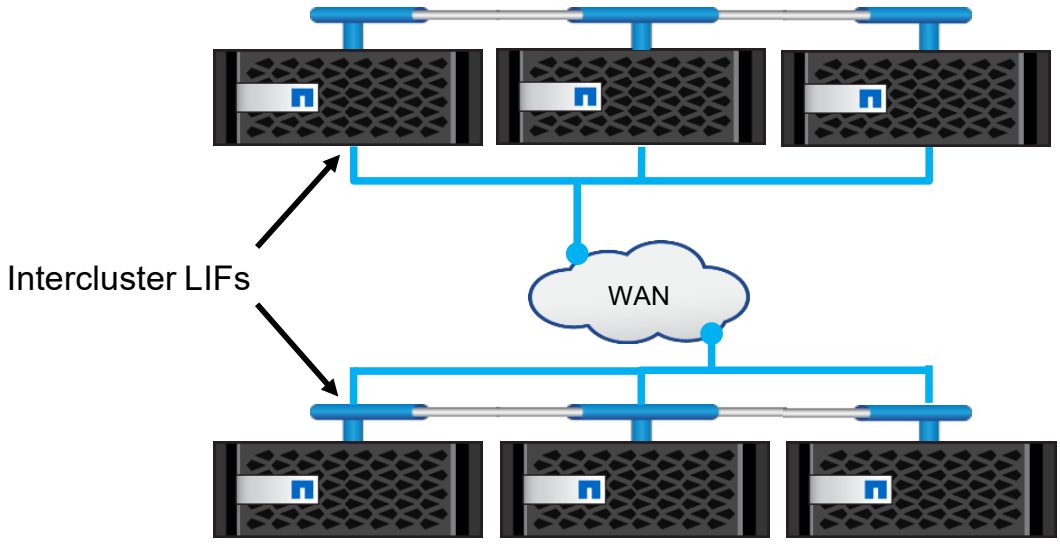
Using cluster svl-nau on your exercise kit, follow these steps:

1. Enter the `network interface show` command.
2. Enter the `network subnet show` command.
3. Enter the `network port show` command.

Answer these questions:

- Are any LIFs set up for intercluster connectivity?
- Is there a subnet that can be used for an intercluster network?
- Do all the network ports have the same maximum transmission unit (MTU) settings?

The Intercluster Network

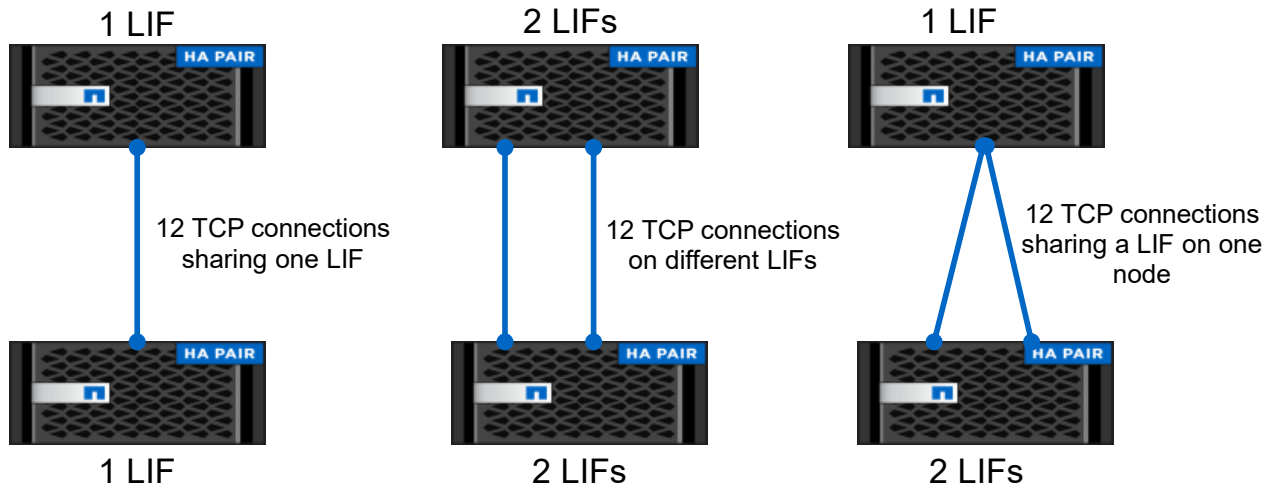


An intercluster network is a network that enables communication and replication between two different clusters operating ONTAP software. This network might be a network of dedicated physical ports but could also be a network sharing ports with data or management networks.

NOTE: Intracluster data protection mirror relationships use the cluster interconnect, which is the private connection used for communication between nodes in the same cluster.

Network Connections for Intercluster Replication

TCP connections



In ONTAP software, the number of intercluster LIFs determines the number of TCP connections established between the source and destination node for SnapMirror. TCP connections are not created per volume or per relationship.

Starting in the ONTAP 8.2 software, ONTAP establishes at least 12 intercluster TCP connections to send data. A minimum of 12 TCP connections are created to send data. These connections exist even in the following situation:

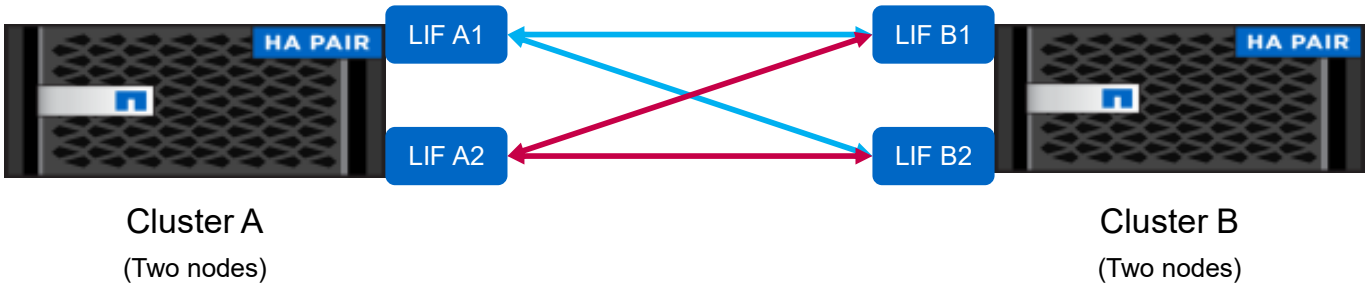
- Both the source and destination nodes have only one intercluster LIF.
- Enough connections are created so that all intercluster LIFs on both the source and destination nodes are used.

If the source node, destination node, or both nodes are configured with two intercluster LIFs, ONTAP software establishes 12 TCP connections to send data. However, instead of both connections using the same LIFs, one connection uses one LIF pair, and the other connection uses the other LIF pair. This example shows different combinations of intercluster LIFs that produce 12 intercluster TCP connections. It is not possible to select a specific LIF pair to use for a certain TCP connection. ONTAP software automatically manages the pairs.

After scaling past 12 intercluster LIFs on a node, ONTAP software creates additional intercluster TCP connections, so that all intercluster LIFs are used.

The creation of additional intercluster TCP connections continues as more intercluster LIFs are added to either the source or the destination node. A maximum of 24 intercluster connections are currently supported for SnapMirror on a single node in ONTAP software.

Intercluster Networking Between Two Clusters



Cluster A
(Two nodes)

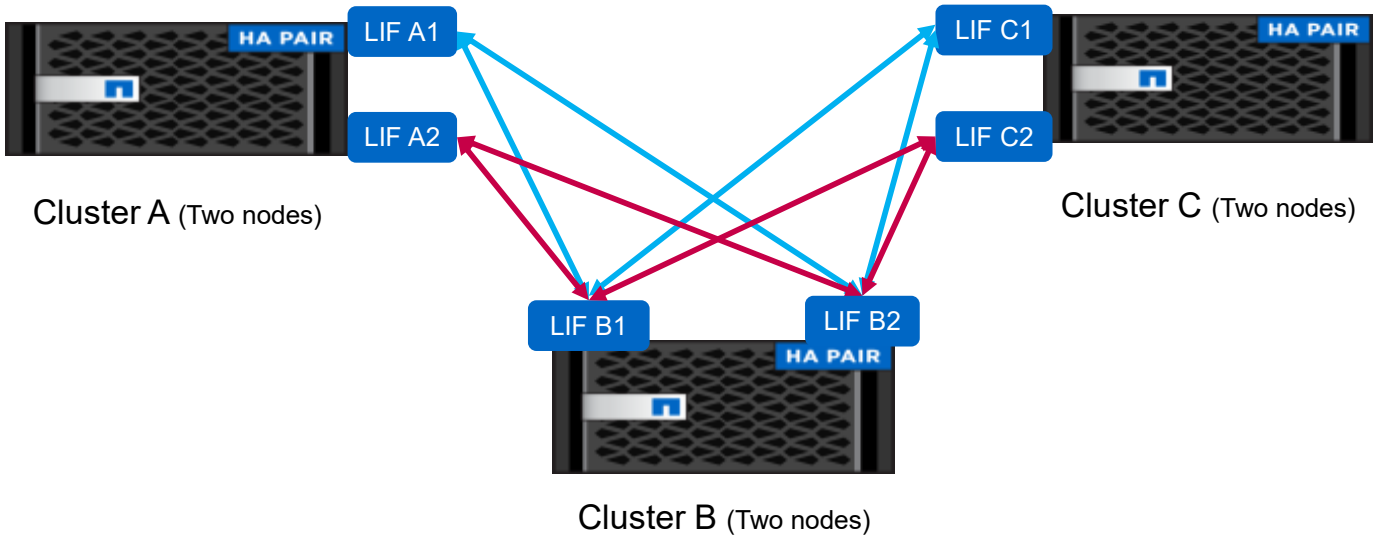
Cluster B
(Two nodes)

Creating an intercluster network between two clusters is the basic cluster peer configuration. For example, you want to create an intercluster network between two clusters, Cluster A and Cluster B.

Cluster A has two intercluster LIFs, A1 and A2, in its Default IPspace. Cluster B has two intercluster LIFs, B1 and B2, in its Default IPspace.

Intercluster Networking in a Cluster Cascade

Part 1 of 2

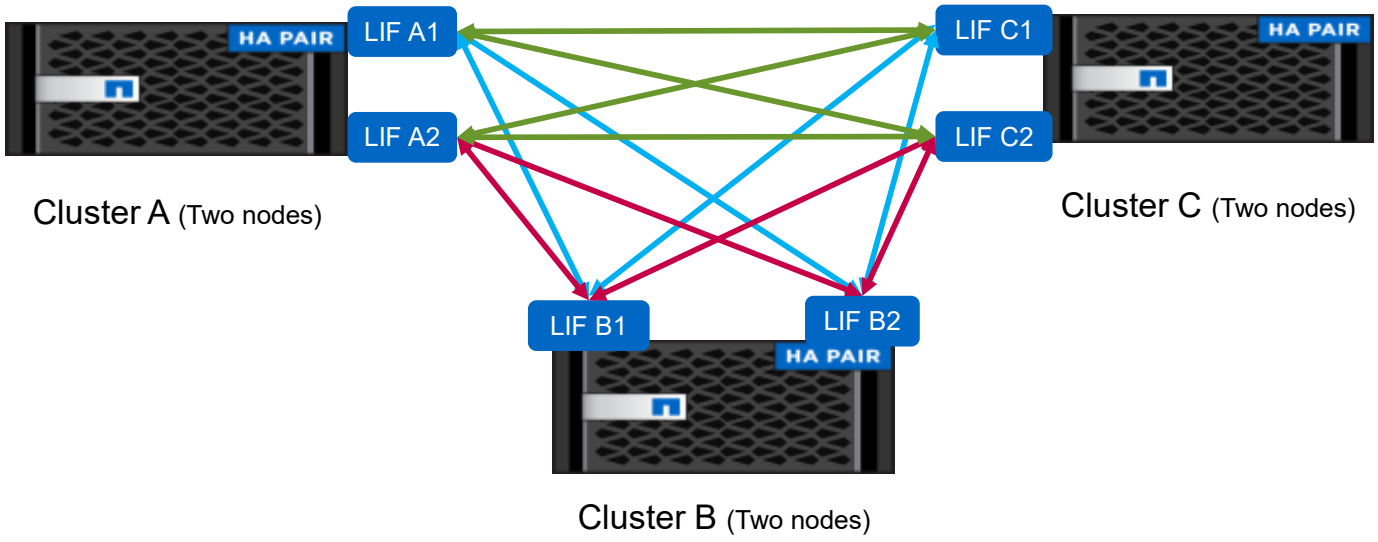


When you connect three clusters in a cascade, all of the intercluster LIFs of the primary cluster must be able to communicate with all of the intercluster LIFs of the secondary cluster. Likewise, all of the intercluster LIFs of the secondary cluster must be able to communicate with all of the intercluster LIFs of the tertiary cluster. You do not need to create an intercluster network between the primary cluster and the tertiary cluster if you do not want to connect the two clusters in a cluster peer relationship.

The figure shows an intercluster network between Cluster A and Cluster B and an intercluster network between Cluster B and Cluster C. Cluster A has two intercluster LIFs, A1 and A2, in its Default IPspace. Cluster B has two intercluster LIFs, B1 and B2, in its Default IPspace. Cluster C has two intercluster LIFs, C1 and C2, in its Default IPspace.

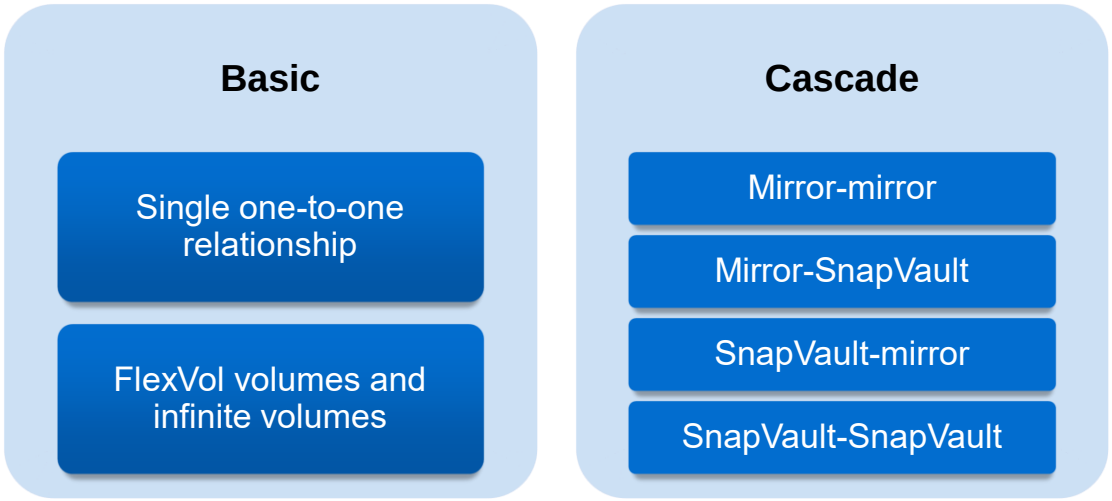
Intercluster Networking in a Cluster Cascade

Part 2 of 2



A cluster cascade could be configured in which the tertiary cluster connects to the primary cluster if something happens to the secondary cluster. If this configuration is required, the intercluster LIFs of the tertiary cluster must be able to communicate with all of the intercluster LIFs of the primary cluster.

Data Protection Deployment Configurations



Basic

Basic data protection configuration (for FlexVol volumes and infinite volumes).

- A FlexVol volume or infinite volume is in a single relationship with another volume as the source or the destination of mirror replication operations.
- A FlexVol volume is in a single relationship with another volume as the primary or the secondary of SnapVault operations.

Cascade (one-to-one-to-one relationship)

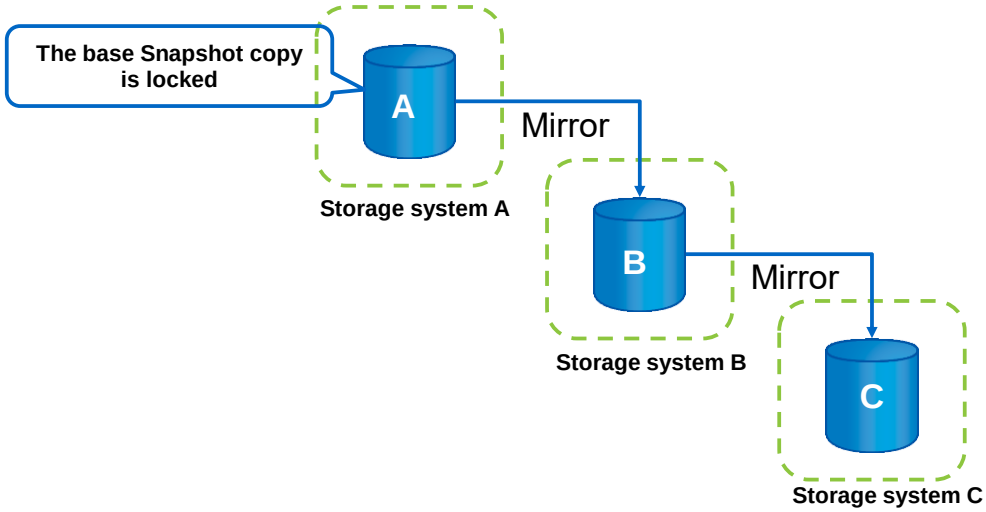
The four types of cascade chain relationships that you can configure are as follows:

1. Mirror-mirror cascade (for only FlexVol volumes)
   A chain of at least two mirror relationships. A volume is the source for replication operations to a secondary volume, and the secondary volume is the source for replication operations to a tertiary volume.
2. Mirror-SnapVault cascade (for only FlexVol volumes)
   A chain of a mirror relationship followed by a SnapVault relationship. A volume is the source for replication operations to a secondary volume, and the secondary volume is the primary for SnapVault operations to a tertiary volume.
3. SnapVault-mirror cascade (for only FlexVol volumes)
   A chain of a SnapVault relationship followed by a mirror relationship. A volume is the primary for SnapVault operations to a secondary volume, and the secondary volume is the source for replication operations to a tertiary volume.
4. SnapVault-SnapVault cascade (for only FlexVol volumes)
   In a chain of two SnapVault relationships, the primary volume creates the Snapshot copies and plans the scheduled transfers to secondary and tertiary volumes.

SnapMirror Cascade Deployments

Data protection deployment configurations

A mirror-mirror cascade



A mirror-mirror cascade deployment is supported on FlexVol volumes. The cascade consists of a chain of mirror relationships in which a volume is replicated to a secondary volume and the secondary is replicated to a tertiary volume. This deployment adds one or more additional backup destinations without degrading performance on the source volume.

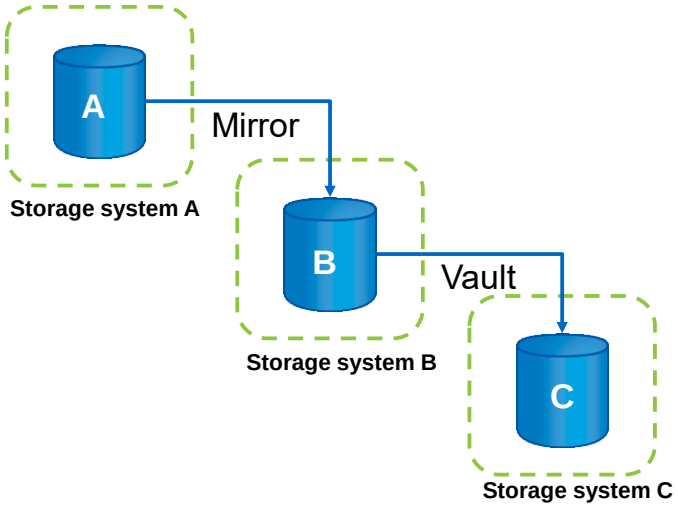
By replicating source A to two different volumes (B and C) in a series of mirror relationships in a cascade chain, you create an additional backup. The base for the B-to-C relationship is always locked on A to ensure that the backup data in B and C always stay synchronized with the source data in A.

If the base Snapshot copy for the B-to-C relationship is deleted from A, the next update operation from A to B fails. An error message is generated that instructs you to force an update from B to C. The forced update establishes a new base Snapshot copy and releases the lock, which enables subsequent updates from A to B to finish successfully.

If the volume on B becomes unavailable, you can synchronize the relationship between C and A to continue protection of A without performing a new baseline transfer. After the resynchronize operation finishes, A is in a direct mirror relationship with C and bypasses B. Before you perform a resynchronization operation in a cascade, know that a resynchronization operation deletes Snapshot copies and might cause a relationship in the cascade to lose its shared Snapshot copy. If the relationship loses its shared Snapshot copy, the relationship requires a new baseline.

SnapMirror and SnapVault Cascade Deployments

A SnapMirror and SnapVault cascade



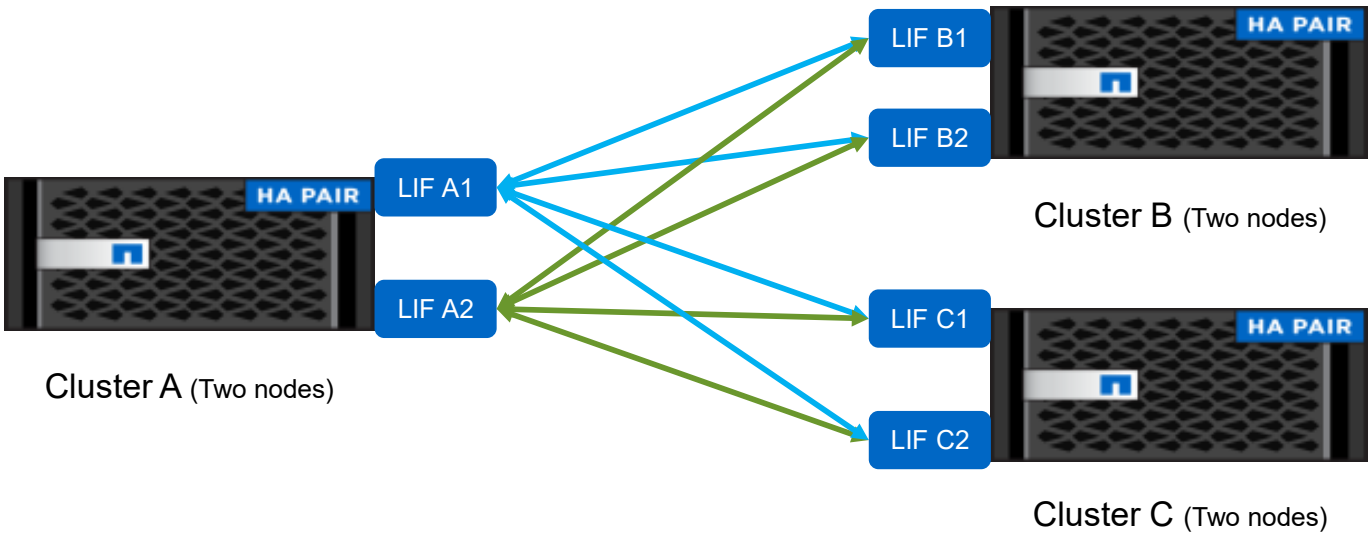
A SnapVault and SnapMirror cascade deployment is supported on only FlexVol volumes. The first leg of the cascade consists of a SnapVault backup. A cascade chain in which the first leg is a SnapVault relationship behaves in the same manner as does a single leg SnapVault relationship. The updates to the SnapVault backup include the Snapshot copies that are selected in conformance with the SnapVault policy assigned to the relationship. In a typical SnapVault and SnapMirror cascade, all Snapshot copies up to the latest one are replicated from the SnapVault backup to the SnapMirror destination.

The SnapVault-SnapVault Cascade

The SnapVault-SnapVault cascade relationship enables you to retain more than 255 backup Snapshot copies combined.

A backup administrator keeps most of the daily Snapshot copies and a few weekly Snapshot copies on volume B and keeps many weekly Snapshot copies on volume C. The Snapshot policy attached to volume A must create both daily and weekly Snapshot copies and retain them for a scheduled transfer. These Snapshot copies can transfer the backups to volume B. If volume B is lost, the A to C SnapVault relationship can be established by using the SnapMirror resync command.

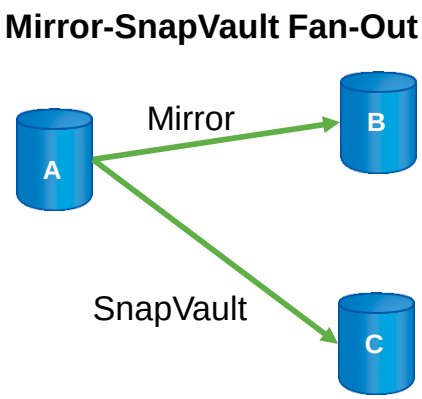
Intercluster Networking in a Cluster Fan-Out or Fan-In

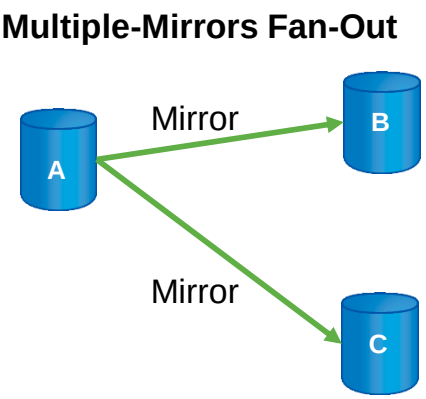


When you connect clusters in a fan-out or fan-in configuration, the intercluster LIFs of each cluster that connect to the primary cluster must be able to communicate with all of the intercluster LIFs of the primary cluster. There is no need to connect intercluster LIFs between the remote clusters if the remote clusters do not need to communicate with each other.

The figure shows an intercluster network between Cluster A and Cluster B and an intercluster network between Cluster A and Cluster C. Cluster A has two intercluster LIFs, A1 and A2, in its Default IPspace. Cluster B has two intercluster LIFs, B1 and B2, in its Default IPspace. Cluster C has two intercluster LIFs, C1 and C2, in its Default IPspace.

Types of Fan-Out Relationships





Fan-Out (one-to-many relationship)

In a fan-out relationship structure, the source is replicated to multiple destinations, which can be mirror or SnapVault destinations. Only one SnapVault relationship is possible in a fan-out replication.

Mirror-SnapVault fan-out (for only FlexVol volumes)

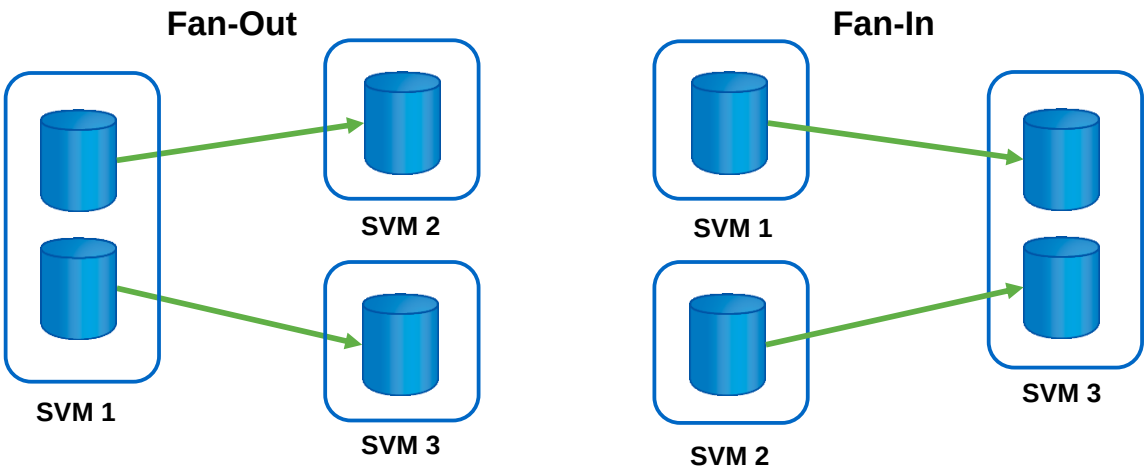
A volume is the source for replication operations to a secondary volume and also the source for SnapVault operations to a different secondary volume.

Multiple-mirrors fan-out (for FlexVol volumes and infinite volumes)

A volume is the source for replication operations to a destination volume and also the source for replication operations to another, different destination volume.

Fan-Out and Fan-In Replication

SVM and volume fan-out and fan-in replications



SVM Fan-Out and Fan-In Replications

It is possible to fan out or fan in volumes between different SVMs. In a fan-out replication, multiple different volumes from a single SVM in the source cluster can be replicated, with each volume replicating into a different SVM in the destination cluster. In a fan-in replication, multiple different volumes can be replicated, each existing in a different SVM in the source cluster, to a single SVM in the destination cluster.

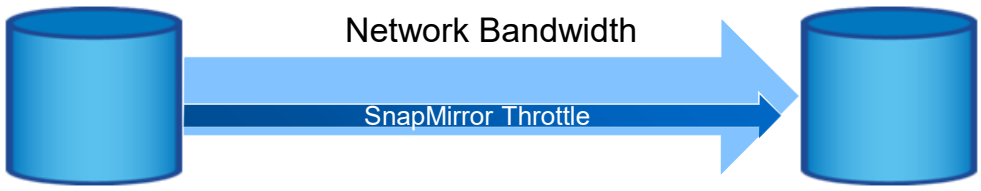
Volume Fan-Out and Fan-In Replications

In volume fan-out replication, for SnapMirror data protection relationships, a single NetApp FlexVol volume can be replicated to up to five different destination volumes. Each destination volume can exist in a different SVM, or all can exist in the same SVM. Volume fan-in, which is replication of multiple different volumes into the same destination volume, is not possible.

Intercluster SnapMirror Throttle

Conserving network bandwidth

To limit the amount of bandwidth that is used by intercluster SnapMirror transfers, apply a throttle to intercluster SnapMirror relationships.



To limit the amount of bandwidth that is used by intercluster SnapMirror transfers, apply a throttle to intercluster SnapMirror relationships.

- After you create a relationship, you can use the CLI to set a throttle. Use the `snapmirror modify` command with the `-throttle` option and a value in kilobytes.
- NetApp OnCommand System Manager 3.0 does not currently support SnapMirror throttle management.

In the following example, a 10-MB throttle is applied to an existing relationship by using the `snapmirror modify` command:

```
cluster02::> snapmirror modify -destination-path cluster02://vs1/vol1 -throttle 10240
```

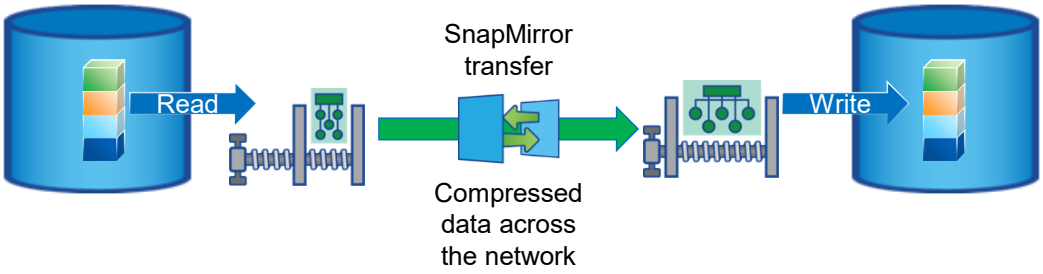
To change the throttle of an active SnapMirror relationship, terminate the existing transfer and restart it to use the new value. The SnapMirror feature restarts the transfer from the most recent restart checkpoint by using the new throttle value, rather than restarting from the beginning.

Starting with ONTAP 8.2.1 software, both intracluster throttle and intercluster throttle are supported and are both configured with the `-throttle` variable.

SnapMirror Network Compression

Conserving network bandwidth

SnapMirror network compression enables data compression over the network for SnapMirror transfers.



You can enable or disable SnapMirror network compression by using the `-is-network-compression-enabled` option in the SnapMirror policy.

SnapMirror network compression enables data compression over the network for SnapMirror transfers. It is an ONTAP feature that is built into the SnapMirror software. SnapMirror network compression is not the same as volume compression. With SnapMirror network compression, data is not compressed on the source or destination system SVMs. The data blocks that need to be sent to the destination system are handed off to the compression engine, which compresses the data blocks.

The compression engine on the source system creates several threads, depending on the number of CPUs available on the storage system. These compression threads help to compress data in a parallel fashion. The compressed blocks are then sent over the network.

On the destination system, the compressed blocks are received over the network and are then decompressed. The destination compression engine also has several threads to decompress the data in a parallel fashion. The decompressed data is reordered and is saved to the disk on the appropriate volume.

In other words, when SnapMirror network compression is enabled, two additional steps are performed:

- Compression processing occurs on the source system before data is sent over the network.
- Decompression processing occurs on the destination system before the data is written to the SnapMirror destination.

You can enable or disable the SnapMirror network compression by using the `-is-network-compression-enabled` option in the SnapMirror policy.

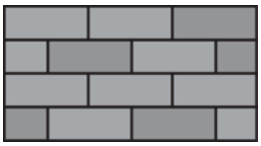
Cluster and Firewall Requirements

Cluster Requirements

- Each cluster must have a unique name.
- The time on the clusters must be within 300 seconds (5 minutes).
- Clusters can be in different time zones.

Firewall Requirements

- ICMP service
- TCP to the IP addresses of all intercluster LIFs over ports 10000, 11104, and 11105
- HTTPS



Firewalls and the intercluster firewall policy must allow the following:

- ICMP service
- TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105
- HTTPS

Although HTTPS is not required when you set up cluster peering, HTTPS is required later if you use the OnCommand System Manager to configure data protection. However, if you use the CLI to configure data protection, HTTPS is not required to configure cluster peering or data protection.

The default intercluster firewall policy enables access through the HTTPS protocol and from all IP addresses (0.0.0.0/0), but the policy can be altered or replaced.

ACTION: Try This Task

Using cluster svl-nau and cluster rtp-nau on your exercise kit, follow these steps:

1. Enter the `date` command.
2. Enter the `timezone` command.
3. Enter the `system services firewall policy show` command.

Answer these questions:

- Is the time on the clusters within 300 seconds?
- Are both clusters in the same time zone?
- What protocols do the firewalls permit?

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

You want to establish a peer relationship between two ONTAP clusters. You are concerned about the network connectivity. What would you do? (Select three.)

a. Use or create a subnet that has one intercluster LIF per node in each cluster.

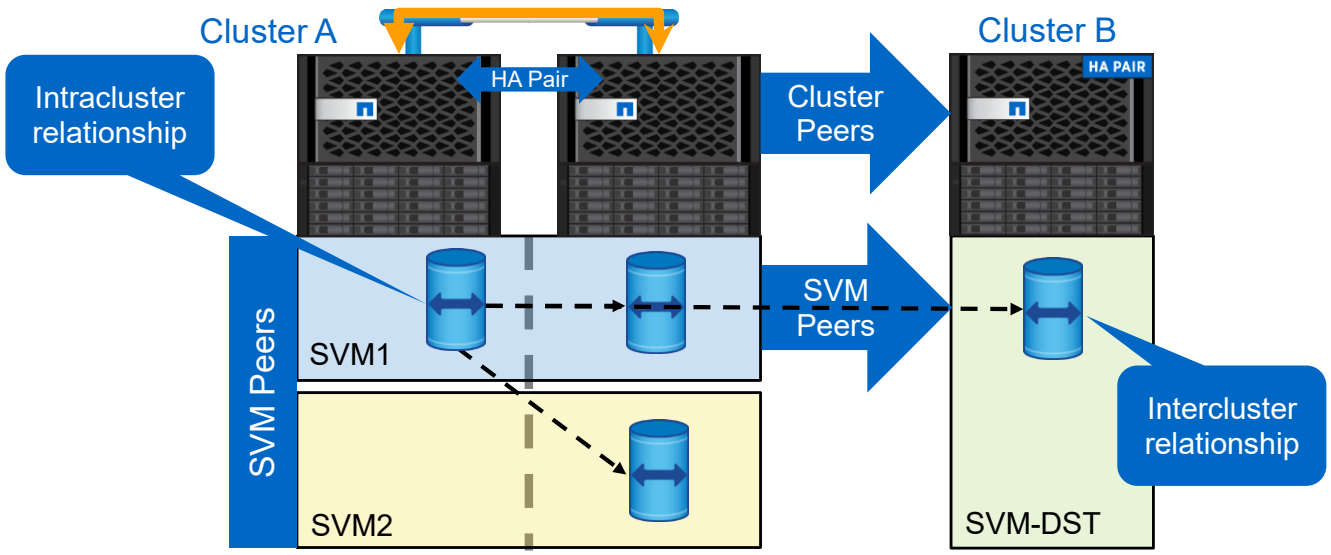
b. Check that the subnet belongs to the broadcast domain containing the ports used for intercluster communication.

c. Check that the intercluster network has full-mesh connectivity between cluster nodes.

d. Make sure that all network ports are using the default IPspace.

Lesson 3
Cluster and SVM Peering

Peer Relationships



When the intercluster LIFs have been created and the intercluster network configured, cluster peers can be created. To enable clusters to replicate, a cluster peer relationship must be established.

Establishing cluster peering is a one-time operation performed by cluster administrators.

A cluster can be in a peer relationship with up to eight clusters to enable multiple clusters to replicate among one another.

SVM peering is the act of connecting two SVMs to enable replication to occur between them (starting in the ONTAP 8.2 software). In ONTAP 8.1 software, any SVM could replicate data to any other SVM in the same cluster or any cluster peer. Control of replication security could be maintained at only a clusterwide level.

Starting in the ONTAP 8.2 software, more granularity in SnapMirror security is provided. Replication permission must be defined by peering SVMs together.

Create Cluster Peer Relationships

Peer relationships can be authenticated or unauthenticated.

A passphrase can be used to complete the cluster peer.

A cluster peer offer can be extended beyond the default of one hour.

Cluster peers can use the default or a custom IPspace.

When you create a cluster peer relationship, a passphrase is used by the administrators of the two clusters to authenticate the relationship. This passphrase ensures that the cluster to which you send data is the cluster to which you intend to send data.

A part of the cluster peer creation process is to use a passphrase to authenticate the cluster peers to each other. The passphrase is used when creating the relationship from the first cluster to the second and again when creating the relationship from the second cluster to the first. The passphrase is not exchanged on the network by ONTAP software, but each cluster in the cluster peer relationship recognizes the passphrase when ONTAP software creates the cluster peer relationship.

The passphrase that you use is not displayed as you type it.

If you created a nondefault IPspace to designate intercluster connectivity, you use the `ipspace` parameter to select that IPspace.

Manage Cluster Peer Relationships

Use this command…	If you want to…
`cluster peer create`	Create an authenticated cluster peer relationship
`cluster peer ping`	Initiate an intercluster connectivity test
`cluster peer show`	Display information about the cluster peer relationship
`cluster peer connection show`	Display TCP connection information for a cluster peer
`cluster peer health show`	Display health information of the nodes in a cluster peer
`cluster peer offer show`	Display information about outstanding authentication offers
`cluster peer offer cancel`	Cancel an outstanding authentication offer to a peer cluster
`cluster peer modify`	Modify a cluster peer relationship
`cluster peer delete`	Delete a cluster peer relationship

See the ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology guide for more information.

SVM Peer Relationships

Enable volume-level SnapMirror relationships to exist between SVMs.	One SVM can be peered with multiple SVMs within a cluster or across clusters.
	Only SnapMirror data protection and SnapVault extended data protection relationships can be set up.
	Both clusters must be peered with each other before you create the SVM peer relationship.
	The SVM names in any peered clusters must be unique across the clusters.

See the ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology guide for more information.

The SVM peer relationship enables volume-level SnapMirror relationships to exist between SVMs either within a cluster or in peered clusters. One SVM can be peered with multiple SVMs within a cluster or across clusters.

Only SnapMirror data protection and SnapVault extended data protection relationships can be set up by using the SVM peer infrastructure.

To create an intercluster SVM peer relationship, both clusters must be peered with each other. The SVM peering commands and procedures are similar to the cluster peering commands and procedures.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

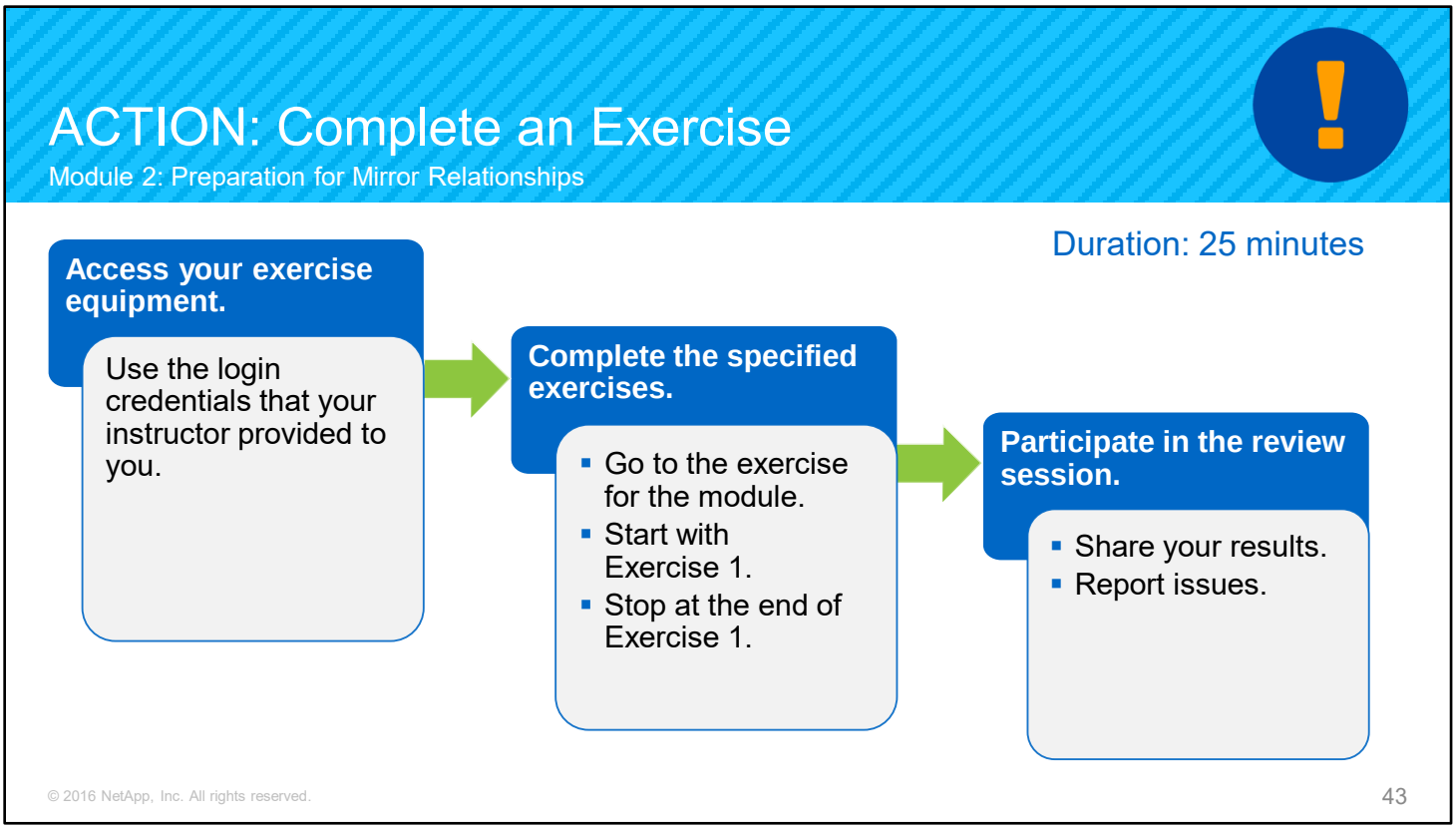
You are tasked with establishing a peer relationship with another cluster. You need to configure the cluster peer offer now, but the other cluster's administrator will not be available to complete the peer authentication for several hours. What would you do? (Select two.)

a. Run multiple cluster peer create commands from your cluster.

b. Extend the cluster peer offer beyond the default time.

c. Use the cluster peer create –offer expiration command.

d. Wait until the other cluster administrator is available, then proceed to establish the peer relationship.



In this exercise, you perform the following tasks:

1. Create intercluster LIFs on each node of each cluster.
2. Configure cluster peering.
3. Configure SVM peering.
4. Review the existing exercise configuration.

ACTION: Share Your Experiences

Roundtable questions for the exercise

- To which IPspace were the intercluster LIFs assigned?
- Which two SVMs were peered together?
- What command was necessary to be entered on the rtp-nau cluster to accept the peer offer from the svl-nau cluster?

References

- *ONTAP 9.0 Release Notes*
- *ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology*
- *NetApp Technical Report TR-4015: SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP*
- *ONTAP 9.0 Cluster Peering Express Guide*

Module Review

This module focused on enabling you to do the following:

- Explain the different types of mirroring relationships available with ONTAP 9 software
- Describe the required components of each of the ONTAP 9 mirroring relationships
- List the ONTAP features supported by SnapMirror software
- Identify the differences between the cascading replication relationships
- Design a network configuration for intercluster mirroring
- Construct the peer relationships required for intercluster and storage virtual machine (SVM) mirroring

Module 3
Implement SnapMirror Relationships

About This Module

This module focuses on enabling you to do the following:

- Construct the required configuration to replicate data using SnapMirror software
- Demonstrate a SnapMirror baseline transfer
- Perform a manual SnapMirror update
- Produce regularly scheduled SnapMirror updates
- Describe data recovery methods using SnapMirror software

Lesson 1
Creating and Initializing the SnapMirror Relationship

Creating a Mirror Copy for FlexVol Volumes

The SnapMirror source volume is online and writable.

The SnapMirror destination volume is online and read-only.

A basic data protection deployment consists of two volumes, either FlexVol volumes or infinite volumes, in a one-to-one, source-to-destination relationship. This deployment backs up data to one location, which provides a minimal level of data protection.

Source volumes are the data objects that need to be replicated. Typically, users can access and write to source volumes.

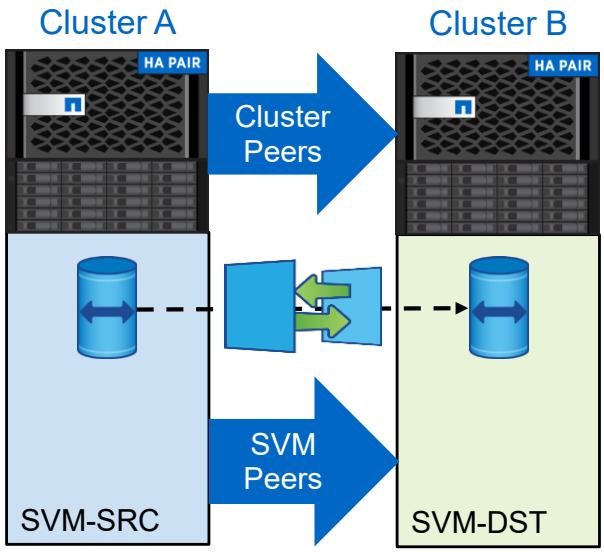
Destination volumes are data objects to which the source volumes are replicated. Destination volumes are read-only.

- Destination FlexVol volumes are placed on a different storage virtual machine (SVM) from the source SVM.
- Destination infinite volumes must be placed on a different SVM from the source SVM.
- Users can access destination volumes in case the source becomes unavailable.
- Administrators can use SnapMirror commands to make the replicated data at the destination accessible and writable.

Steps to Configure SnapMirror Relationships

To create a protection relationship using SnapMirror software, follow these steps:

1. Verify that SnapMirror licenses have been applied on both the source and the destination clusters.
2. Establish cluster and SVM peering.
3. Select the destination cluster and SVM.
4. Create a data protection volume on the destination.
5. Select or create a mirror policy.
6. Select or create a schedule.
7. Create the relationship.
8. Initialize the relationship.



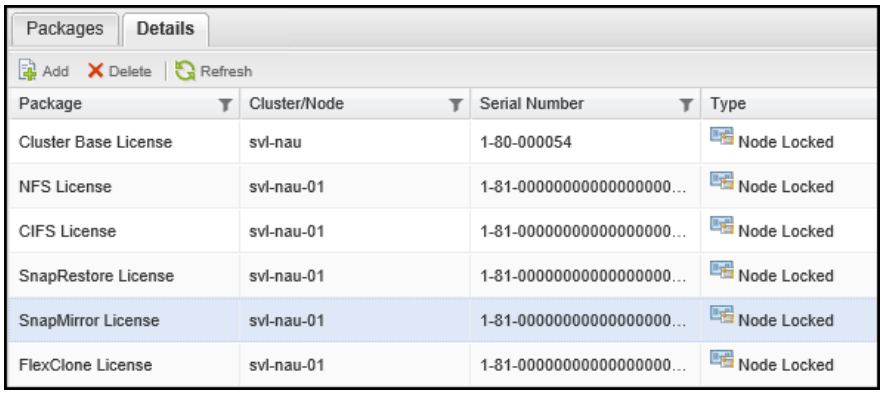
Before you create a SnapMirror relationship, verify that the SnapMirror license has been applied to both the source and destinations clusters. Also, a peering relationship between the clusters and SVMs must be established. After you verify that peering is healthy, on the destination SVM, you create a destination volume. The destination volume must be created as a data protection volume in OnCommand System Manager or volume type `DP` in CLI.

Now that you have created the resources, you need a policy and schedule to create the mirror relationship. The destination of a mirror relationship contains a copy of all data and Snapshot copies. Unlike the vault policy, the mirror policy does not contain rules to specify the number of Snapshot copies that are retained on the destination volume. Like vault relationships, the schedule configures the frequency at which the relationship updates. You can either use the default policies and schedules or create your own.

After you create the SnapMirror relationship, you initialize the relationship, which will start the baseline transfer.

Licensing

- SnapMirror or SnapVault license
  - The SnapMirror license enables SnapVault.
- Other licenses
  - SnapRestore license
  - FlexClone license



Beginning with ONTAP 9.0 software, you can use either a SnapMirror or SnapVault license to enable SnapVault. In previous releases, you could use only a SnapVault license.

A SnapMirror license is required on both the source and destination cluster.

Language Settings

The source and destination FlexVol volumes or infinite volumes of a mirror relationship must have the same language setting; otherwise, NFS or CIFS clients might not be able to access data.

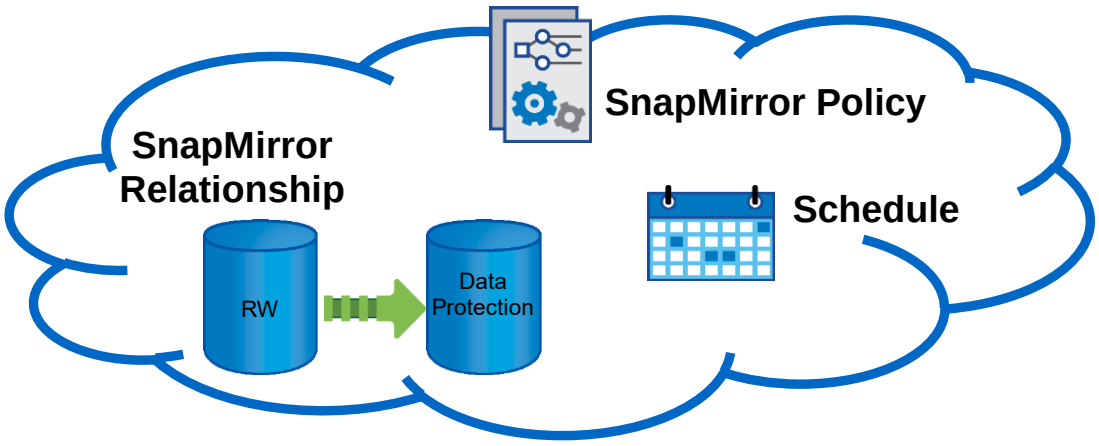

```
svl-nau::> volume show -volume yellow_thinvol -fields language
vserver    volume         language
---------- -------------- --------
svm_yellow yellow_thinvol C.UTF-8
```


The source and destination FlexVol volumes or infinite volumes of a mirror relationship must have the same language setting; otherwise, NFS or CIFS clients might not be able to access data.

For FlexVol volumes, it is not a problem if the source and destination volumes are on the same Storage Virtual Machine (SVM) because the language is set on the SVM. For FlexVol volumes and infinite volumes with mirror relationships between volumes on two different SVMs, the language setting on the SVMs must be the same.

Creating a SnapMirror Policy and Job Schedule

To manage a data protection mirror or SnapVault relationship, you must assign a policy and a schedule to the relationship.



When a SnapMirror and SnapVault relationship is created, an optional update schedule is applied. The cron job schedule is normally created to control the frequency of the SnapMirror or SnapVault update.

You use a policy to maximize the efficiency of the transfers to the backup secondaries and to manage the update operations.

Selecting a Job Schedule

- Select or modify an existing job schedule.
- Create a job schedule.

```
svl-nau::> job schedule show
Name                Type                Description
-----------         ---------           ----------------------------------------------
5min                cron                @:00,:05,:10,:15,:20,:25,:30,:35,:40,:45,:50,:55
8hour               cron                @2:15,10:15,18:15
daily               cron                @0:10
Hourly              cron                @:05
weekly              cron                Sun@0:15
```


If the default Snapshot copy schedule does not meet your needs, you can create a schedule that does.

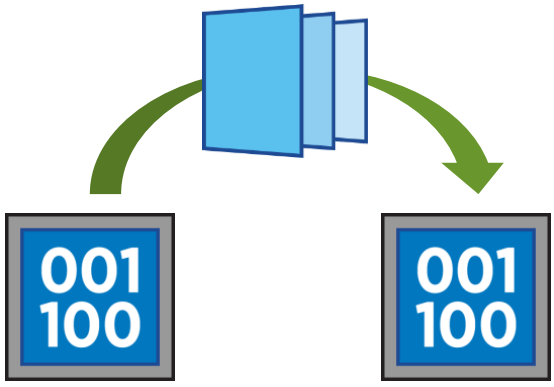
Create a Snapshot copy schedule by using the `job schedule cron create` command or the `job schedule interval create` command. The command you use depends on how you want to implement the schedule.

Apply the schedule to the mirror relationship by using the `-schedule` option of the `snapmirror modify` command.

See the man page for each command to determine the command that meets your needs.

Performing the Initial Transfer

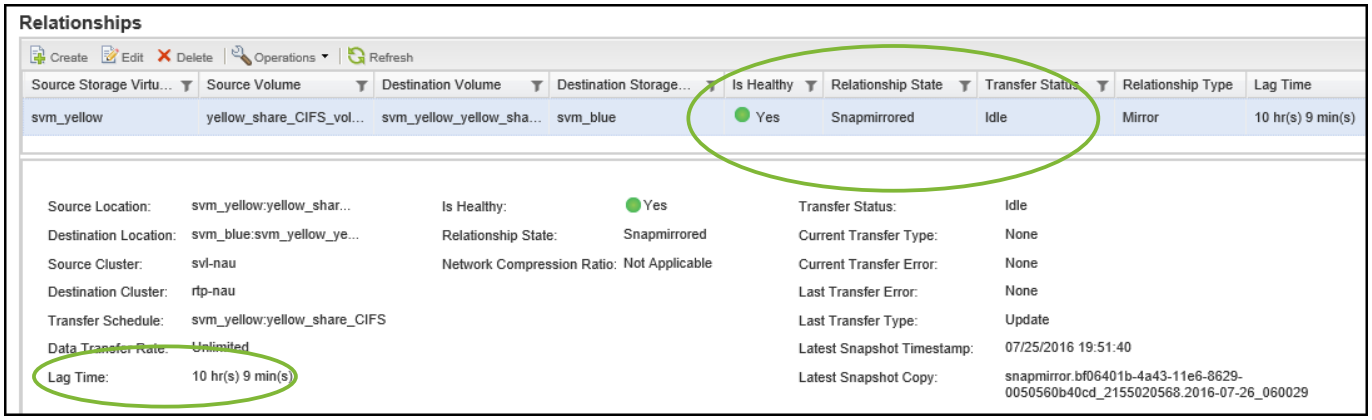
To initialize the data protection mirror copy, use the `snapmirror initialize` command.



The initial transfer (also referred to as a baseline transfer) is a complete backup of a primary storage volume to a volume on the secondary system.

After the initial transfer successfully finishes, subsequent transfers contain only the changes that were made to the primary data since the previous transfer.

Monitoring the Relationship



An easy way to check your SnapMirror and SnapVault relationships is to use the OnCommand System Manager. Check the Relationships window on the destination cluster for Is Healthy, Relationship State, Transfer Status, and Lag Time.

The relationship should be healthy and the relationship state should be shown as Snapmirrored. The transfer status indicates whether a transfer is in progress or where there is an idle period.

The lag time is the difference between the current time and the timestamp of the Snapshot copy that was most recently successfully transferred to the destination system. The lag time is always at least as much as the duration of the most recent successful transfer, unless the clocks on the source and destination systems are not synchronized. The lag time can be negative if the time zone of the destination system is behind the time zone of the source system.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

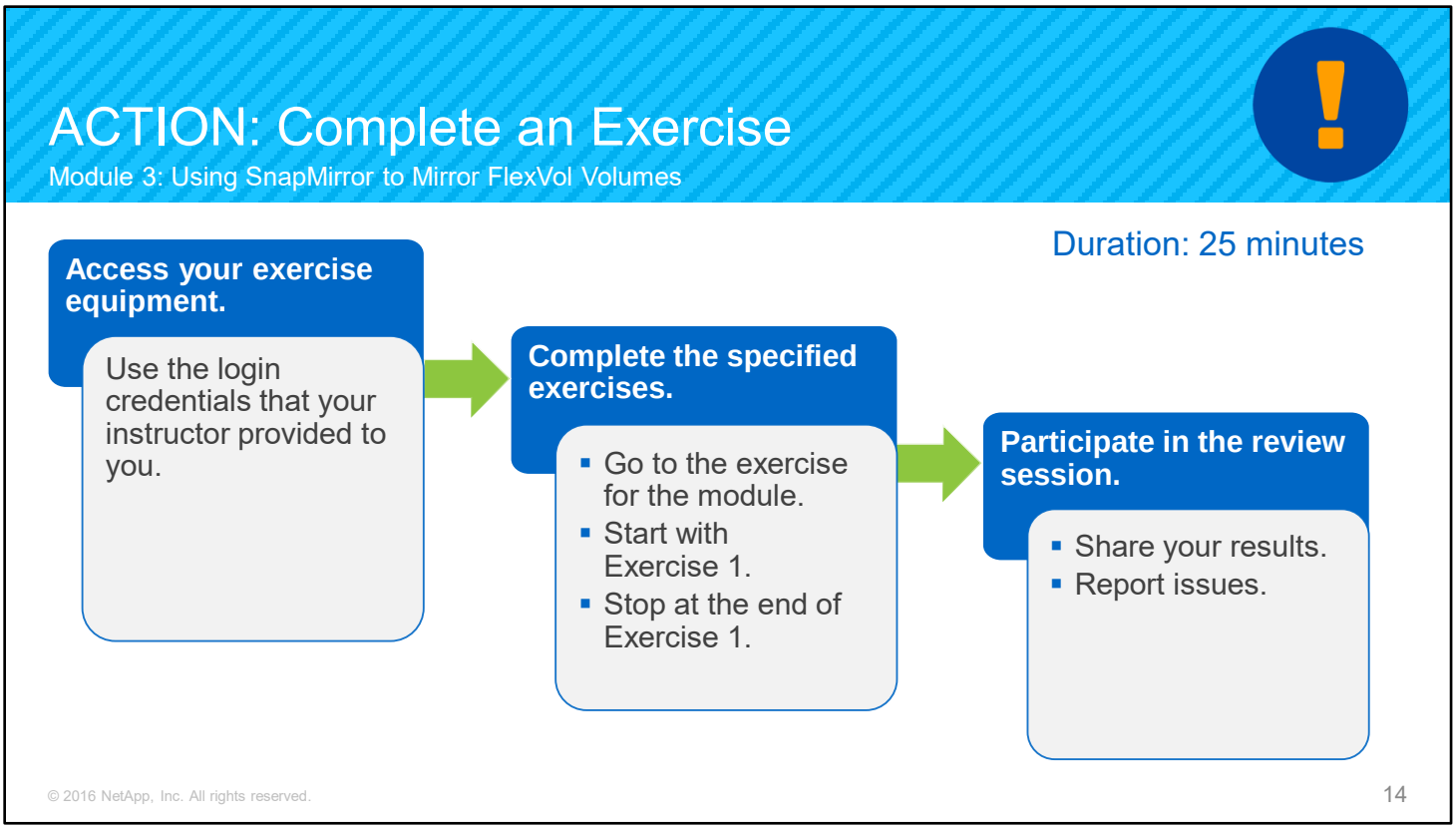
You recently set up a SnapMirror relationship with a daily update schedule. You want to check that the updates are being performed daily. What would you do? (Select two.)

a. In the OnCommand System Manager Relationships window, make sure that the lag time is less than the most recent scheduled transfer time.

b. Use the OnCommand System Manager to check the Relationships window and make sure that the Relationship State is Acceptable.

c. Use the OnCommand System Manager to check the Relationships window and make sure that the Relationship State is SnapMirrored.

d. Reboot the destination cluster so that a new SnapMirror transfer begins.



In this exercise, you perform the following tasks:

1. Create a SnapMirror policy.
2. Create a cron job schedule.
3. Apply the cron job schedule to the SnapMirror policy.
4. Set up a mirror relationship between FlexVol volumes on two different clusters.
5. Perform the SnapMirror initial transfer and verify the data transfer.
6. Perform a manual SnapMirror update and verify the data transfer.
7. Review the existing exercise configuration.

ACTION: Share Your Experiences

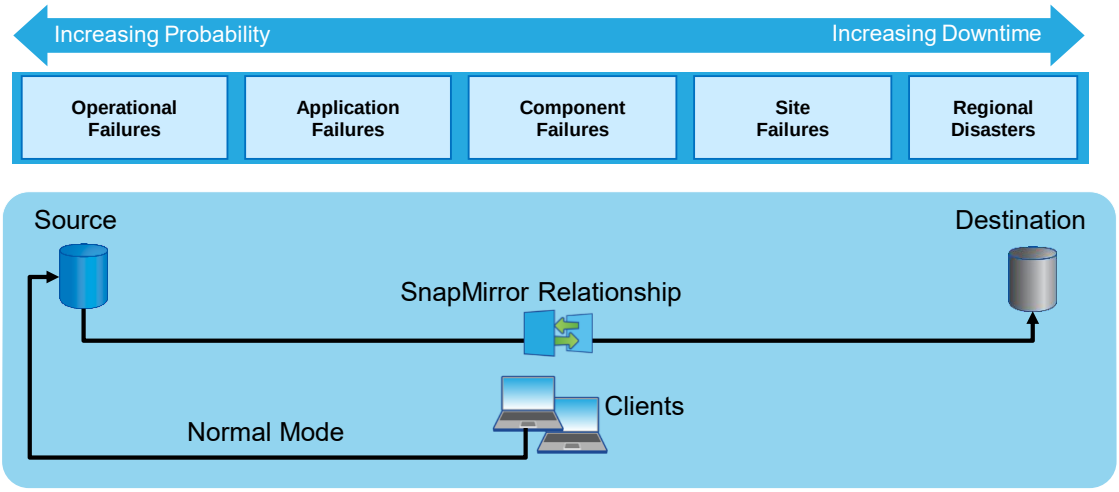
Roundtable questions for the exercise

- What is the name of the destination volume that was created automatically in Task 1?
- What did you have to do to verify data transfer on the destination volume after you performed the initial transfer?

Lesson 2
Disaster Recovery Using SnapMirror Software

SnapMirror Technology in a Normal Operation

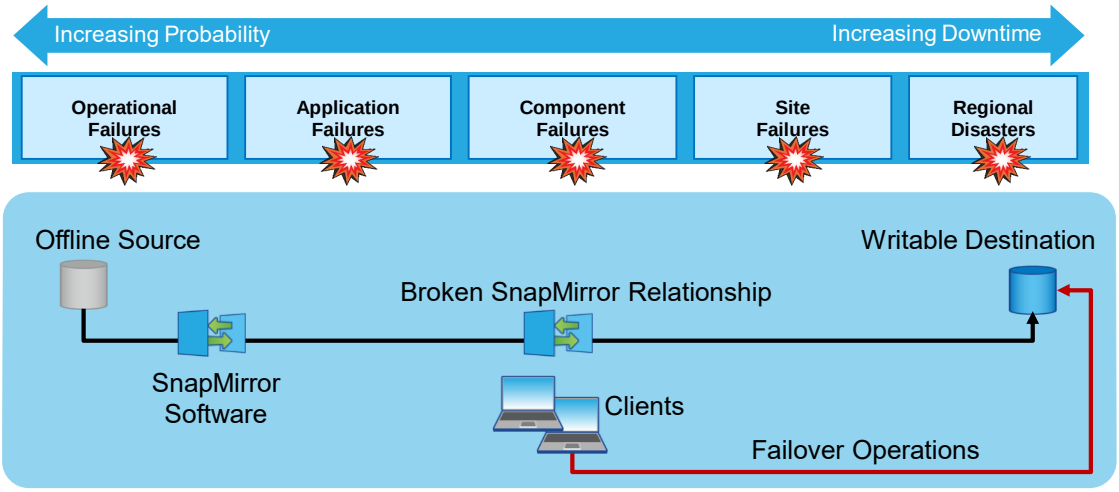
Clients have normal read/write permission to the source volume.



In normal operation, clients have read/write permission to the source volume. The destination volume in the SnapMirror relationship is read-only and is available to clients in RO mode.

SnapMirror Technology in Failover Mode

Clients have normal read/write permission to the destination volume.

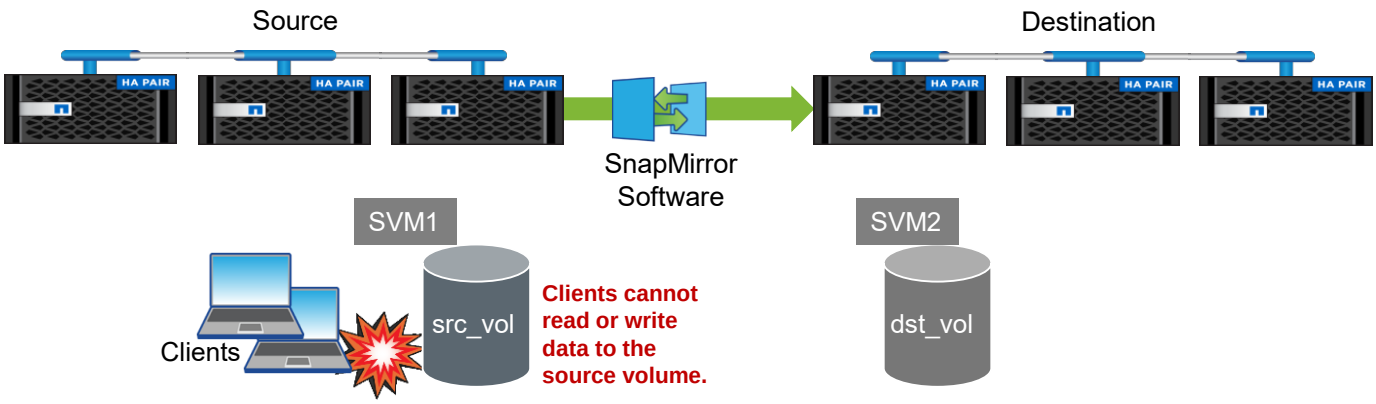


If the source volume goes offline or is unavailable for any reason, the SnapMirror relationship can be broken, which makes the destination volume writable for the clients.

Disaster Mode

Source unavailable

Disaster strikes

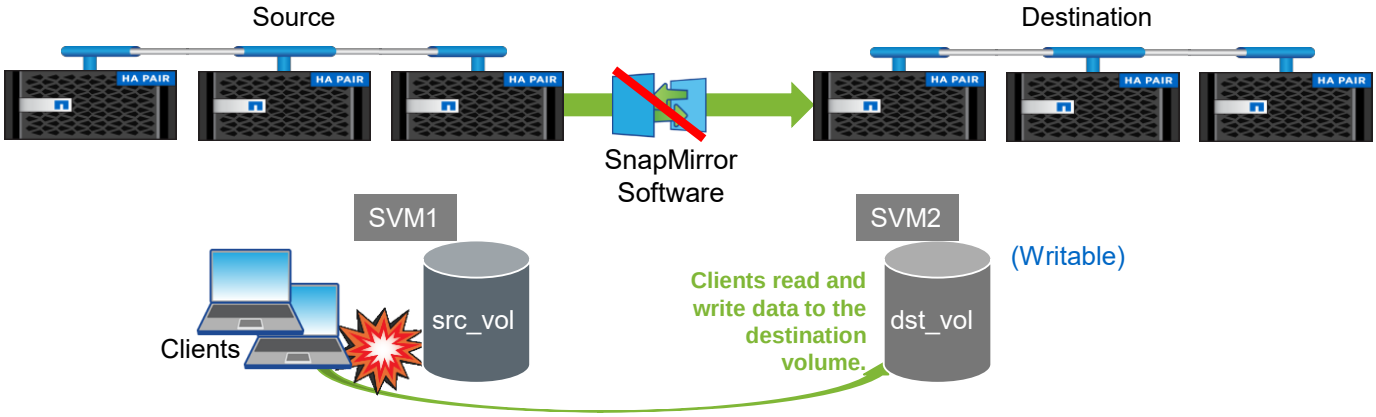


Disaster strikes. For this example, the data center volume (src_vol) becomes unavailable.

Disaster Mode

Clients fail over to the destination volume

From the destination node, break the SnapMirror relationship and direct clients to the destination volume.



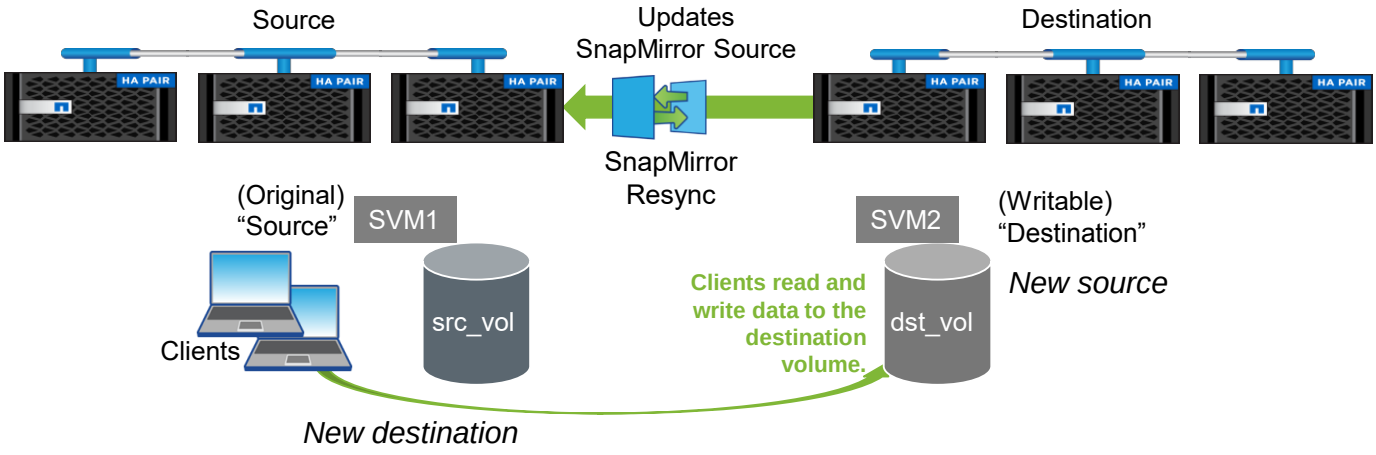
From the destination node, you break the SnapMirror relationship. When the SnapMirror relationship is broken, SnapMirror updates are interrupted, and the SnapMirror replica becomes writable. Then you direct clients to the writable destination volume (dst_vol), and clients continue reading and writing their data.

Because the source volume is offline, its data is becoming out of date. However, the most recent shared Snapshot copy is preserved, ready, and waiting for the reestablishment of the SnapMirror relationship.

Resumption of Normal Operations: Part 1

Write new data from the destination to the source

To update the source from the destination, run the snapmirror resync command from the original source SVM.



To return from failover mode to normal mode, you first need to capture the data that was written to the destination volume while the source volume was offline. To update the original source volume with the new data that was written to the destination volume, you run the `snapmirror resync` command from the original source SVM. The resync command, run from the source, reverses the direction of the SnapMirror relationship.

When you use the OnCommand System Manager to manage SnapMirror software, you use the Reverse Resync tool. Until the source volume is updated with the data that was written to the destination, the original destination becomes the source. To update the source when you use the CLI, ensure that you run the `snapmirror resync` command from the original source. Data written to the destination is reverse synchronized to the original source.

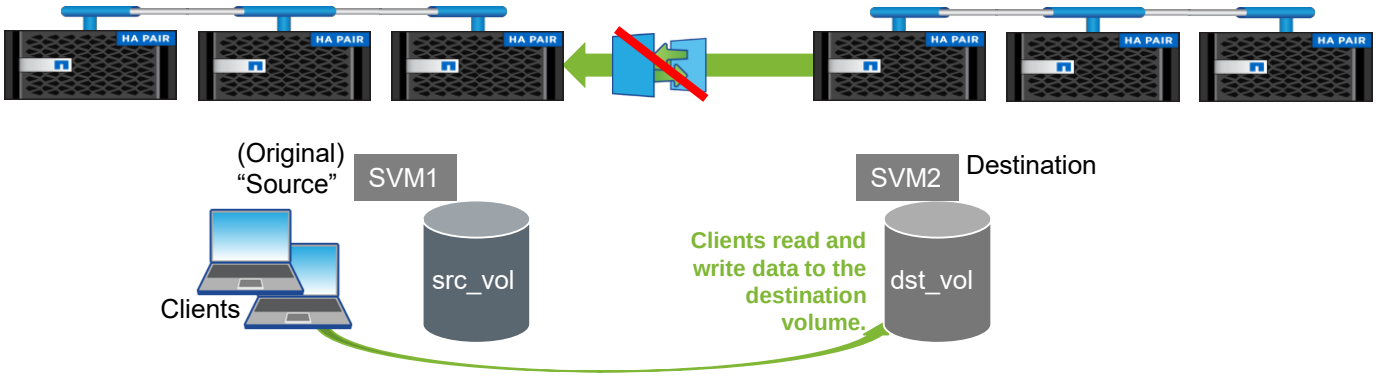
Before you run the `snapmirror resync` command, check the size of the secondary volume compared to the primary volume. It is possible that, when the primary volume was offline, the automatic resizing feature or the administrator increased the size of the secondary volume. The secondary volume could have become larger than the primary volume.

Increase the size of the primary volume if necessary.

Resumption of Normal Operations: Part 2

Breaking the temporary mirror relationship

To reverse the direction of the SnapMirror relationship, break the SnapMirror relationship from the original source system.



After the `snapmirror resync` command is run from the original source SVM (src_vol), the SnapMirror relationship is updated with the data that was written in disaster mode, when clients wrote to the destination volume. In this temporary, reversed SnapMirror relationship, the original source is now the destination and the original destination is the source.

To reverse the temporary relationship, you must break the temporary relationship from the temporary destination. Run the `snapmirror break` command from the original source. The syntax of the `snapmirror break` command is:

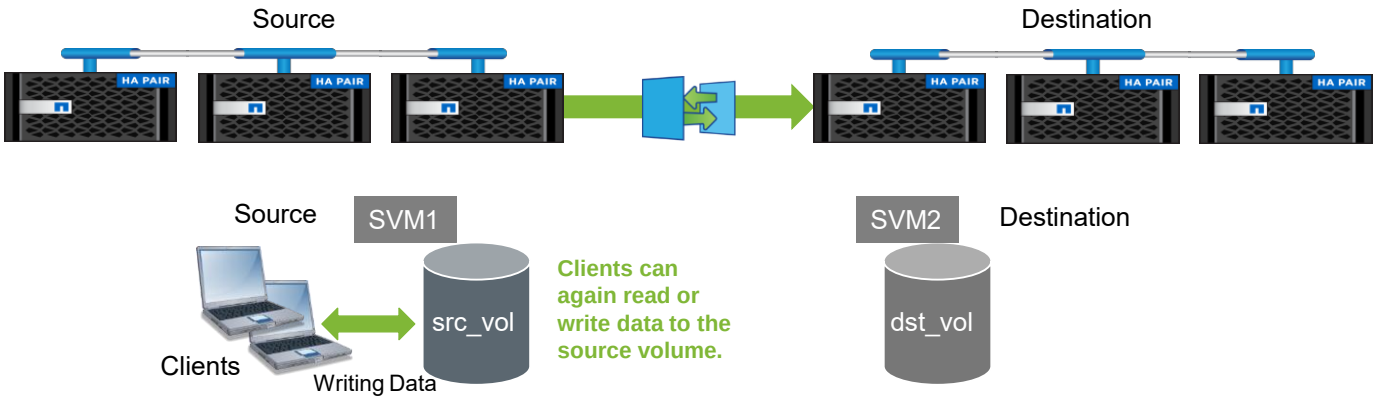
```
destination>snapmirror break destination_vol
```

In this slide, the temporary SnapMirror relationship is now broken. However, clients are not yet writing to the original source volume.

Resumption of Normal Operations: Part 3

Breaking the temporary mirror relationship

Resynchronize the SnapMirror relationship, and redirect users to the original source volume.



After the problem is repaired and you want to return to normal operations, you use the `snapmirror resync` command. The `snapmirror resync` command establishes or reestablishes a SnapMirror relationship between the source and destination volumes. The `snapmirror resync` command must be run from the destination node CLI.

If it is run from the wrong node, the `snapmirror resync` command can cause data loss on the destination volume. The data loss occurs because the command removes the newest Snapshot copies and written data on the destination volume.

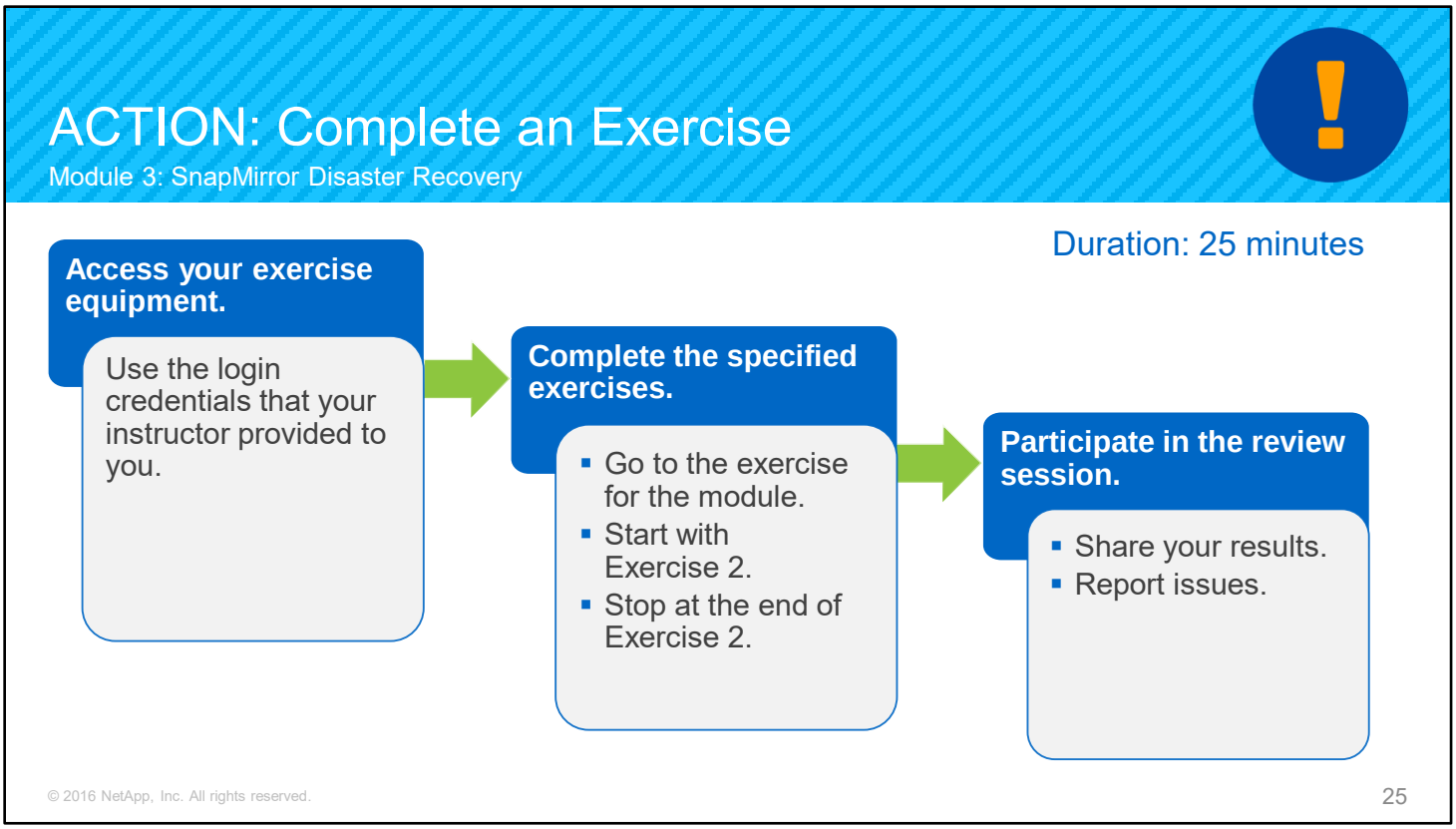
The `snapmirror resync` command first finds the most recent shared Snapshot copy between the source and destination volumes. The command next removes Snapshot copies on the destination volume that are newer than the shared Snapshot copy on the source volume. Finally, the command mounts the destination volume as a data protection volume, retaining the shared Snapshot copy.

Next, ONTAP `snapmirror resync` creates a Snapshot copy of the source volume and calculates to determine what data is newer than the shared Snapshot copy. The source transfers newer data to the destination volume.

With these actions, the original SnapMirror relationship is reestablished, and the test data that was written to the destination volume is gone.

ACTION: Topic for Discussion

Why is it necessary to break the SnapMirror relationship as the first step when a disaster strikes and the source data is unavailable?



In this exercise, you perform the following tasks:

1. Simulate a disaster scenario by taking the source volume offline.
2. Break the SnapMirror relationship and activate the destination volume.
3. Verify data access.
4. Review the existing exercise configuration.
5. Reactivate the original source volume.
6. Perform a reverse resync operation.
7. Review the existing exercise configuration.
8. Restore the original SnapMirror relationship.
9. Review the existing exercise configuration.

ACTION: Share Your Experiences

Roundtable questions for the exercise

- Before you performed the SnapMirror break operation, what did you check for first?
- What happens when you do a quiesce operation on a SnapMirror relationship?
- When the SnapMirror relationship was broken, what happened to the SVM peer relationship?

Lesson 3
SnapMirror and ONTAP Feature Interaction

SnapMirror Relationships and ONTAP Versions

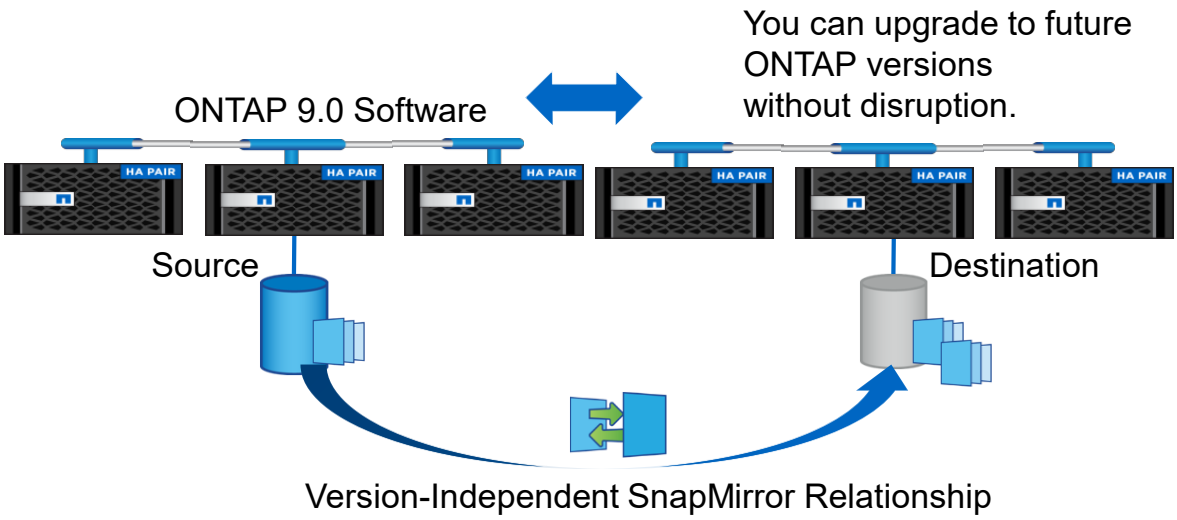
In SnapMirror relationships using type `DP` and policy async-mirror, the relationship can be built from an ONTAP release no more than two releases later.

Source volume ONTAP version	Destination volume can reside on a system running one of the following releases			
	8.1.x	8.2.x	8.3.x	9.0
8.1.x	Yes	Yes	Yes	No
8.2.x	No	Yes	Yes	Yes
8.3.x	No	No	Yes	Yes
9.0	No	No	No	Yes

The ONTAP versions to support a SnapMirror relationship depend on the relationship type and policy defined for that SnapMirror relationship.

Replication for relationship type `DP` or `DR` is not possible between systems operating in 7-Mode and ONTAP software. In addition, the Data ONTAP 8.1 implementation of SnapMirror is not compatible with the Data ONTAP 8.0 implementation. Replication between systems running clustered Data ONTAP 8.0 and 8.1 operating systems is not possible.

Version-Independent SnapMirror Technology



In earlier versions of Data ONTAP, the destination controller required the same version or a later version of Data ONTAP as the source controller. Because of this limitation, you had to upgrade your SnapMirror destination before you upgraded your SnapMirror source. If you had a complex or bidirectional replication topology, you might have been required to take a disruption at upgrade time.

Beginning with Data ONTAP 8.3, you can upgrade without disruption. Data ONTAP 8.3 introduces a new type of SnapMirror relationship that is no longer tied to the ONTAP version. Now, even with complex replication topologies, you can perform nondisruptive upgrades without having to do the upgrades concurrently across source and destination and without having to resynchronize the relationship.

Before you create version-independent SnapMirror relationships, you should consider some guidelines.

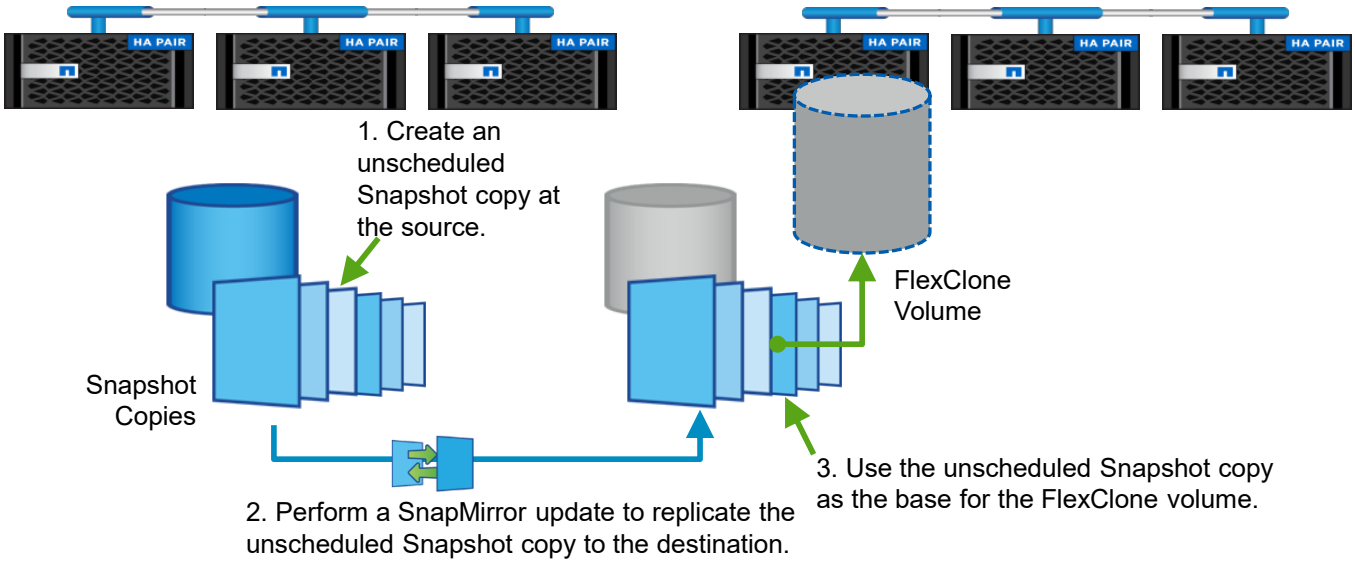
SnapMirror Relationships and ONTAP Versions

SnapMirror relationships using type `XDP` and policy async-mirror or mirror-vault (version-flexible SnapMirror software), are available with ONTAP 8.3 and later software.

Source volume ONTAP version	Destination volume can reside on a system running one of the following releases			
	8.1.x	8.2.x	8.3.x	9.0
8.1.x	No	No	No	No
8.2.x	No	No	No	No
8.3.x	No	No	Yes	Yes
9.0	No	No	Yes	Yes

SnapMirror relationships using type `XDP` and policy async-mirror or mirror-vault, also known as version-flexible SnapMirror software, are available with only ONTAP 8.3 and later releases. Such a relationship can be built only from source and destination volumes running an ONTAP 8.3 or later release. The version-flexible SnapMirror feature is not available before ONTAP 8.3 software.

SnapMirror and FlexClone Technology

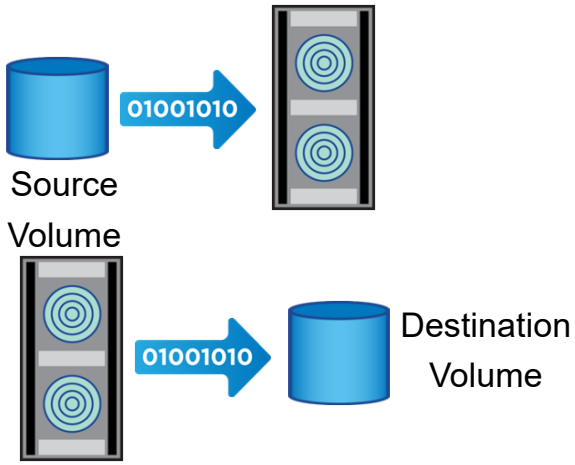


A NetApp FlexClone volume is a writable point-in-time clone of a FlexVol volume. A FlexClone volume shares data blocks with the parent volume and stores only new data or changes that are made to the clone.

FlexClone technology also enables you to create a writable volume from a read-only SnapMirror destination without interrupting the SnapMirror replication process or production operations.

SnapMirror to Tape Backup

Typically, you create a populated secondary volume when you copy a primary volume to a secondary volume by using tape. This process is called tape seeding.



Tape seeding is an SMTape functionality that helps you to initialize a destination FlexVol volume in a data-protection mirror relationship.

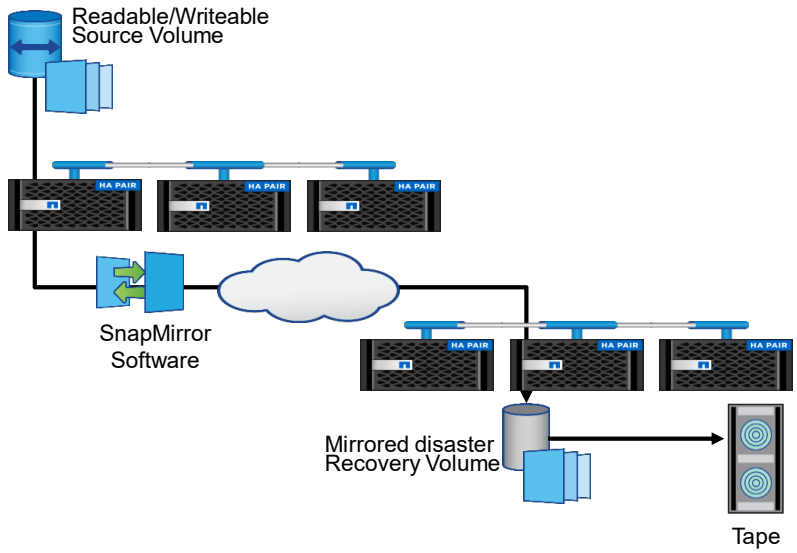
Tape seeding enables you to establish a data protection mirror relationship between a source system and a destination system over a low-bandwidth connection.

Incremental mirroring of Snapshot copies from the source to the destination is feasible over a low-bandwidth connection. However, an initial mirroring of the base Snapshot copy takes a long time over a low-bandwidth connection. In such cases, you can perform an SMTape backup of the source volume to a tape and use the tape to transfer the initial base Snapshot copy to the destination. You can then set up incremental SnapMirror updates to the destination system using the low-bandwidth connection.

For more information, see the ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology guide.

SnapMirror and NDMP

NDMP backups can be performed from the source or destination volumes.

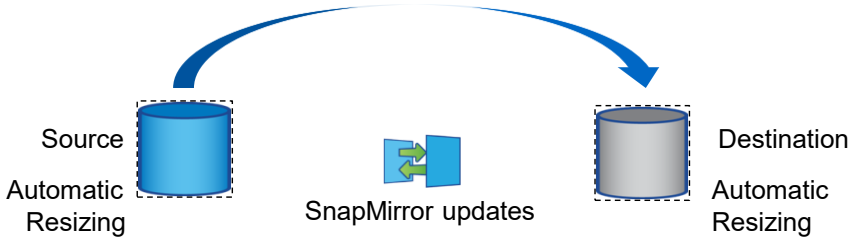


Performing NDMP backups from SnapMirror destination volumes rather than from source volumes includes the following advantages:

- SnapMirror transfers can happen quickly and with less effect on the source system than NDMP backups. Use NetApp Snapshot copies and perform SnapMirror replication from a primary system as a first stage of backup to significantly shorten or eliminate backup windows. Then perform NDMP backup to tape from the secondary system.
- SnapMirror source volumes are more likely to be moved using volume move capability for performance or capacity reasons. When a volume is moved to a different node, the NDMP backup job must be reconfigured to back up the volume from the new location. If backups are performed from the SnapMirror destination volume, these volumes are less likely to require a move, and it is less likely that the NDMP backup jobs need to be reconfigured.

SnapMirror Software and Volume Automatic Resizing

When the source volume automatically grows, the destination volume also grows.

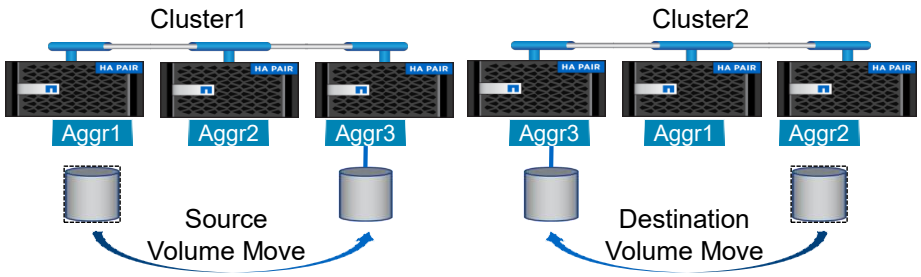


You can manage data growth in the primary volume by configuring volume automatic resizing. As source data grows, ONTAP software automatically increases the size of the source volume based on size thresholds that you configure on that volume.

When the source volume size automatically increases, the size of the destination volume automatically increases. ONTAP software has several types of volumes, including FlexVol volumes and infinite volumes. The automatic resizing feature is available with only FlexVol volumes, not infinite volumes.

SnapMirror Software and Volume Move

A data protection source or destination volume can be moved nondisruptively to another node in the cluster without the need to reconfigure the SnapMirror relationship.



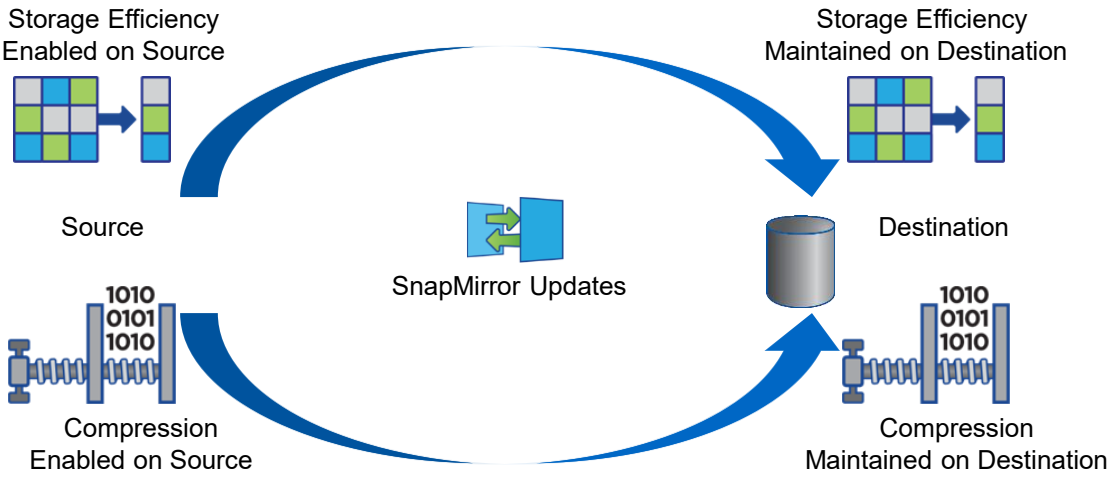
With ONTAP software, you can nondisruptively move a SnapMirror source volume or destination volume to another aggregate on the same node or to an aggregate on a different node within a cluster.

You might want to move a volume from FC to SATA disks, or you might want to free disk space without affecting the SnapMirror relationship. SnapMirror configurations, and even storage efficiency configurations, are revised automatically and do not need to be manually changed.

To nondisruptively move a volume, even a volume that is a part of a SnapMirror configuration, use the `volume move` command.

Enabling Storage Efficiency

If a SnapMirror source volume is in a deduplicated or compressed state, the destination volume remains so.



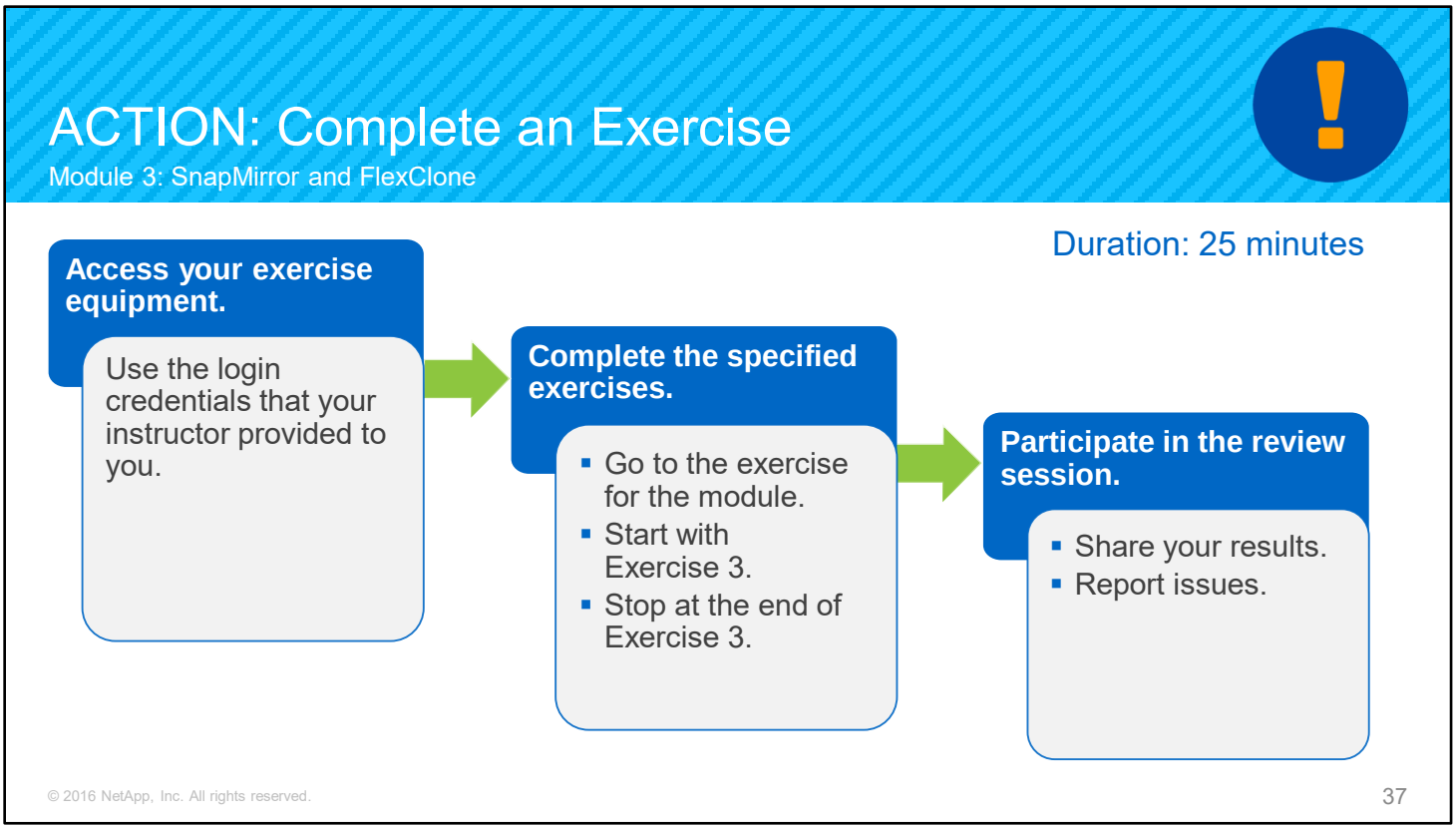
SnapMirror technology supports NetApp deduplication and compression storage efficiency technologies.

If you implement storage efficiency and a SnapMirror source volume is in a deduplicated state, the destination volume remains in a deduplicated state. Along with storage efficiency, you have network efficiency because SnapMirror software does not inflate the deduplicated data during the transfer from primary to secondary storage.

Likewise, if a SnapMirror source volume is in a compressed state, the destination volume remains compressed. SnapMirror software does not decompress the source data before or during the transfer to the destination volume. Data is replicated in a compressed state.

NOTE: It is not possible to have different configurations of storage efficiency enabled between the source and destination volumes.

When you configure volume SnapMirror relationship software and compression and deduplication, consider the compression and deduplication schedule and the time you want to start a volume SnapMirror relationship initialization. As a best practice, start volume SnapMirror relationship initialization of a compressed and deduplicated volume after compression and deduplication are complete. Doing so prevents sending data that is decompressed and not deduplicated and additional temporary metadata files over the network. If the temporary metadata files in the source volume are locked in Snapshot copies, they also consume extra space in the source and destination volumes.



In this exercise, you perform the following tasks:

1. Create an unscheduled Snapshot copy on the SnapMirror source volume.
2. Perform a manual SnapMirror update.
3. Use the unscheduled Snapshot copy on the destination volume as a base for a FlexClone.
4. Write data to the FlexClone volume.
5. Destroy the FlexClone and the original Snapshot copy.

ACTION: Share Your Experiences

Roundtable questions for the exercise

- When you created the FlexClone, what was the warning message that appeared?
- Why would it be OK to ignore the warning message?
- Why is it a good idea to delete the Snapshot copy you created manually on the SnapMirror source volume?

References

- *ONTAP 9.0 Release Notes*
- *ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology*
- *ONTAP 9.0 Volume Disaster Recovery Preparation Express Guide*
- *ONTAP 9.0 Volume Disaster Recovery Express Guide*
- *NetApp Technical Report TR-4015: SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP*
- *NetApp Technical Report TR-4476: NetApp Data Compression and Deduplication: Data ONTAP 8.3.1 and Later*

Module Review

This module focused on enabling you to do the following:

- Construct the required configuration to replicate data using SnapMirror software
- Demonstrate a SnapMirror baseline transfer
- Perform a manual SnapMirror update
- Produce regularly scheduled SnapMirror updates
- Describe data recovery methods using SnapMirror software

Module 4
Disaster Recovery for Storage Virtual Machines

About This Module

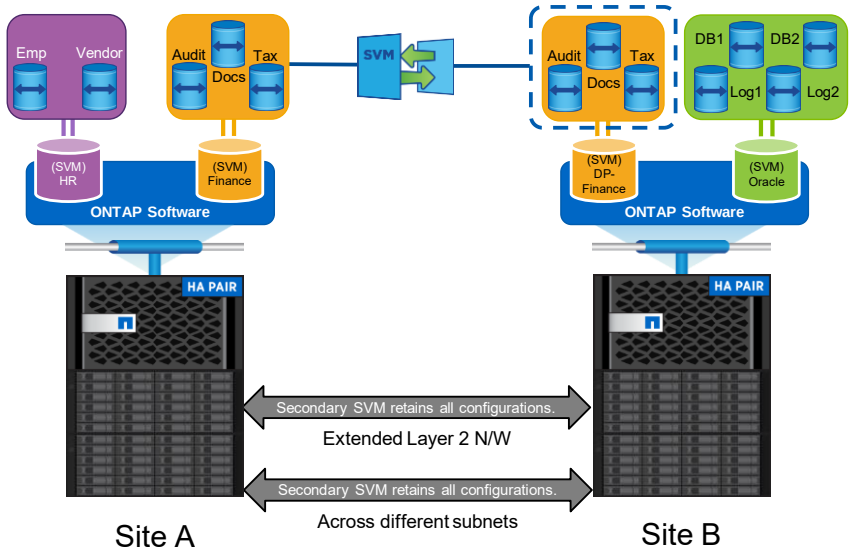
This module focuses on enabling you to do the following:

- Summarize the requirements and options to replicate storage virtual machine (SVM) data
- Prepare a storage virtual machine for data protection
- Perform a storage virtual machine initial data transfer
- Demonstrate a manual storage virtual machine update
- Manually update a storage virtual machine disaster-recovery relationship
- Produce regularly scheduled storage virtual machine updates

Lesson 1
Introduction to SVM Disaster Recovery

SnapMirror for Storage Virtual Machines

SVM disaster recovery is available in ONTAP 8.3.1 and later software.



- Simple pre-defined steps to fail over
- Ease of management with automation
- Assured protection for SVM data

- Protected SVM namespace, not just volumes
- Automated setup and provisioning
- Automated change management
- Familiar SnapMirror CLI commands

4

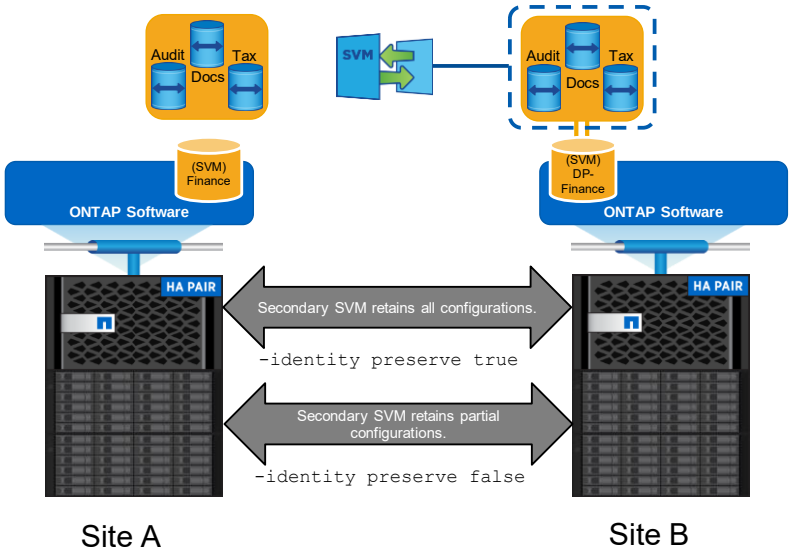
SnapMirror for storage virtual machines (or storage virtual machine disaster recovery) is designed to mirror not just the data inside an SVM, but the configuration of the SVM. This mirroring includes the SVM's namespace, quality of service (QoS) policies, name mapping configurations, and other aspects of the SVM.

The goal of SnapMirror software for SVMs is simplicity. When a replication relationship is configured between SVMs, SnapMirror software eliminates the need to maintain replication relationships for each individual volume inside the SVMs. Change management between the two SVMs is managed automatically.

SnapMirror software for SVMs can be configured in two different modes, depending on the business requirements: `identity preserve true` and `identity preserve false`.

Options to Replicate Configurations in SVM Disaster Recovery

Using the `-identity preserve` option



- Easily preserve the SVM identity across networks.
- Replicate all configurations except logical interfaces (LIFs).
- Start the destination SVM to provide read-only access to clients.

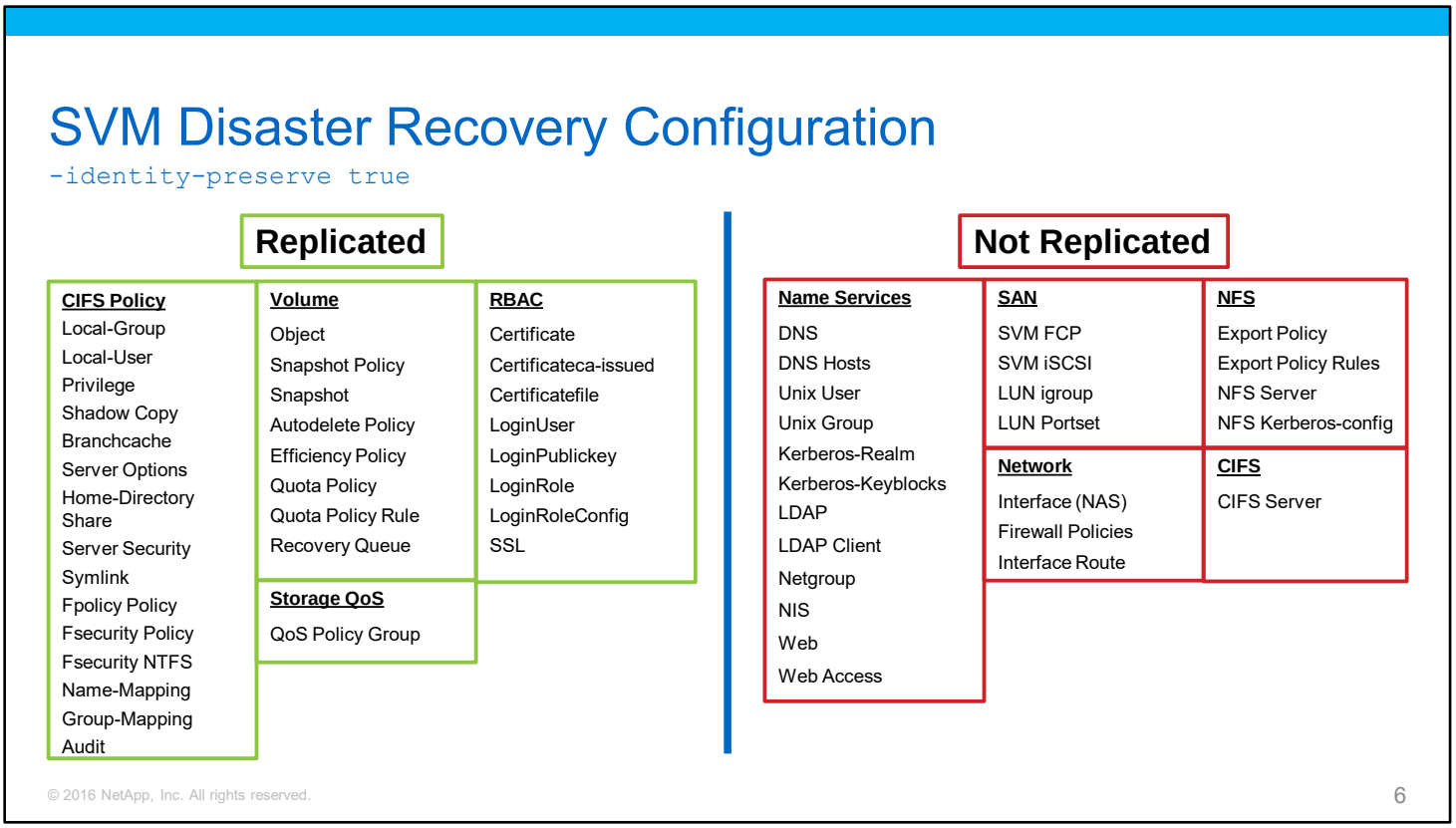
When you create the SVM disaster recovery relationship, the value that you select for the `-identity-preserve` option of the snapmirror create command determines the configurations that are replicated in the destination SVM.

For both `-identity-preserve` settings, all volumes and data are replicated. The difference between the two options is in the configuration data that is replicated.

If you set the `-identity-preserve` option to true, all the configuration details except the SAN configuration are replicated. If the source cluster and destination cluster are in different network subnets, you can decide not to replicate the NAS logical interfaces (LIFs) on the destination SVM.

If you set the `-identity-preserve` option to false, only a subset of the configuration details—those details that are not associated with the network configuration—is replicated.

For complete details, see the NetApp Data Protection Using SnapMirror and SnapVault Technology guide.



When you use `-identity-preserve true`, the CIFS server identity is maintained, as is the network configuration. The destination SVM is offline until the SnapMirror relationship is broken and the source SVM is offline. Here are a few use cases for this option:

- The source and destination SVMs remain in the same Layer-2 network.
- The source and destination SVMs are in different Layer-2 networks but have access to the same active directory structure.
- You want to move an SVM from one cluster to a different cluster and maintain the CIFS server configuration and possibly network configuration.

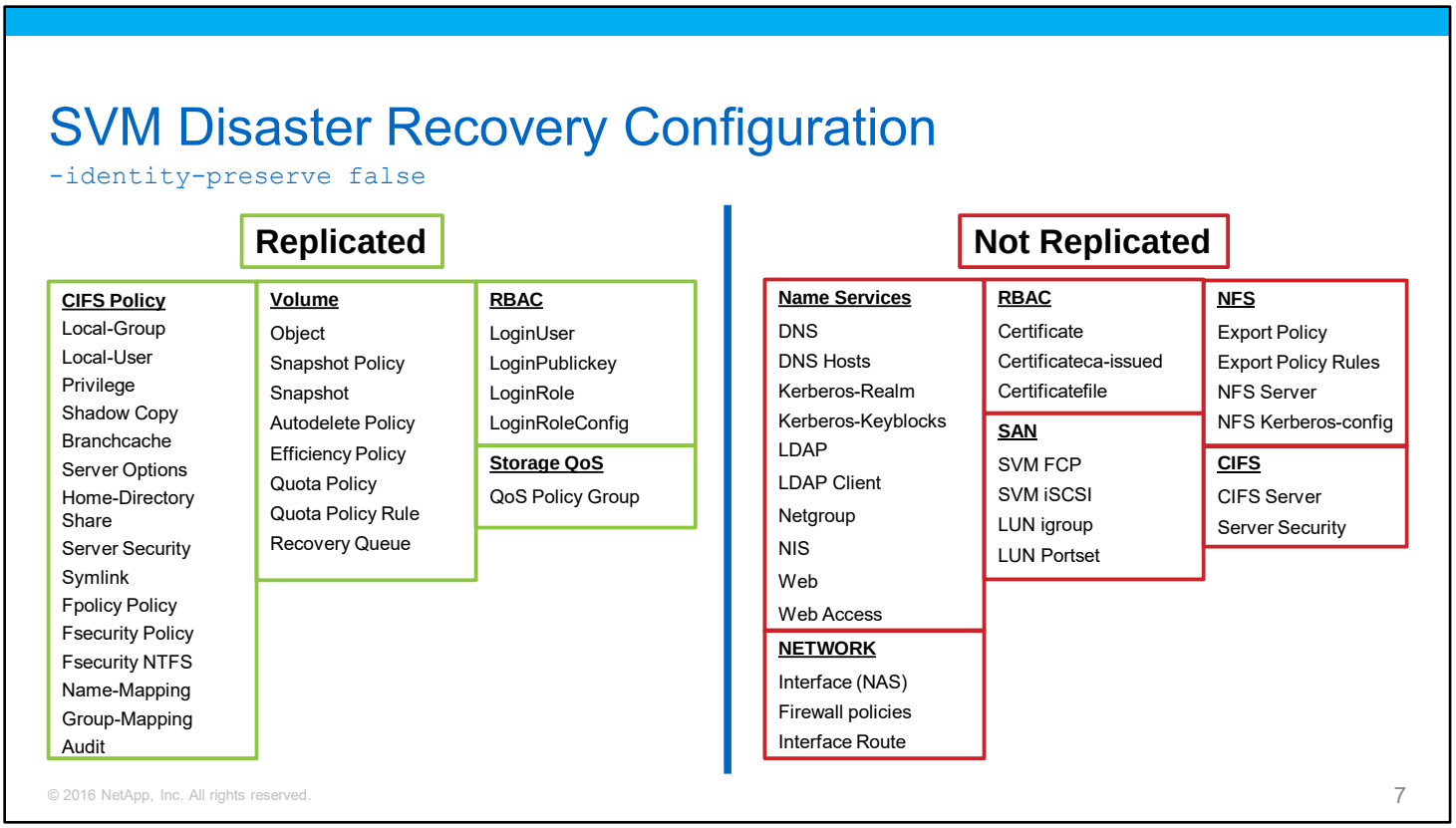
The first use case listed is for customers who have two clusters in the same Layer-2 network. The clusters could be in the same data center or in an extended Layer-2 network across data centers. The cutover from the source to destination cluster does not require any additional SVM configuration changes to bring the SVM online.

In the second use case, because the network configuration is maintained but the SVM is moving into a different network, you must make some configuration changes.

- The IP addresses on the data LIFs on the SVM after the cutover need to change.
- The routing table of the SVM itself has to change. Each SVM has a unique routing table that determines the default gateway for the network.

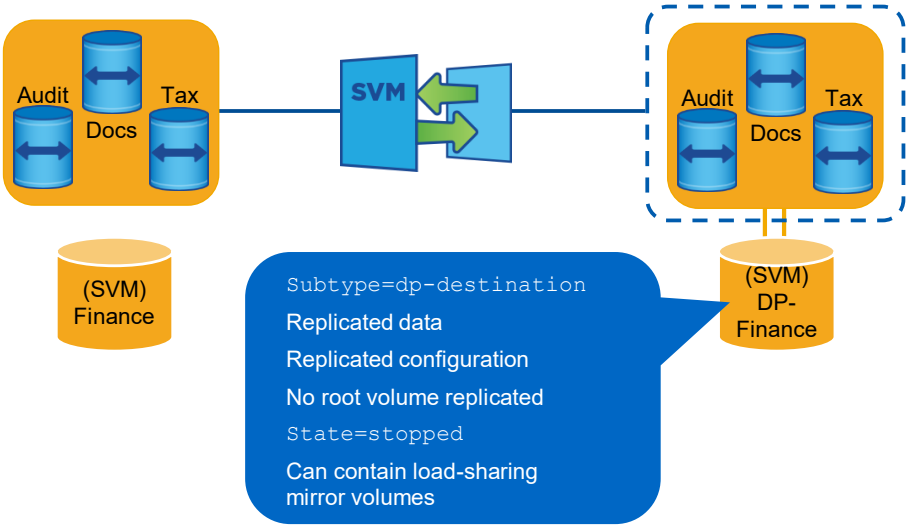
Usually, only these two changes are required. If the DNS server that is configured for the SVM is not reachable on the network, the DNS settings have to change. No other changes should be required for CIFS environments. For NFS environments, if the NFS clients also change their IP addresses (think whole site failover), ensure that export policies are updated to use the new IP addresses of those hosts.

The third example is more a move of an SVM rather than to use it for SVM disaster recovery. For example, the SVM is in the cloud and it is moved back to on-site premises. Use SVM disaster recovery to establish a whole SVM relationship between clusters and move the SVM from one cluster to another. After the cutover to the new cluster, make the necessary changes to the network, route, DNS, and exports as needed, delete the SnapMirror relationship, and continue serving data.



There is one primary use case for `-identity-preserve false`. Because the network configuration, the CIFS server configuration, or any of the export policies are not being maintained, the destination SVM can be in an active read-only environment.

SVM Disaster Recovery Requirements



Create the destination SVM with the `dp-destination` subtype. The destination SVM is normally in a stopped state until it is activated. The activation enables the destination SVM to start serving data if there is a disaster causing the source SVM to become unavailable. When you activate the destination SVM, it becomes writable and the subtype changes from `dp-destination` to default. This change causes all volumes to enable read/write permission.

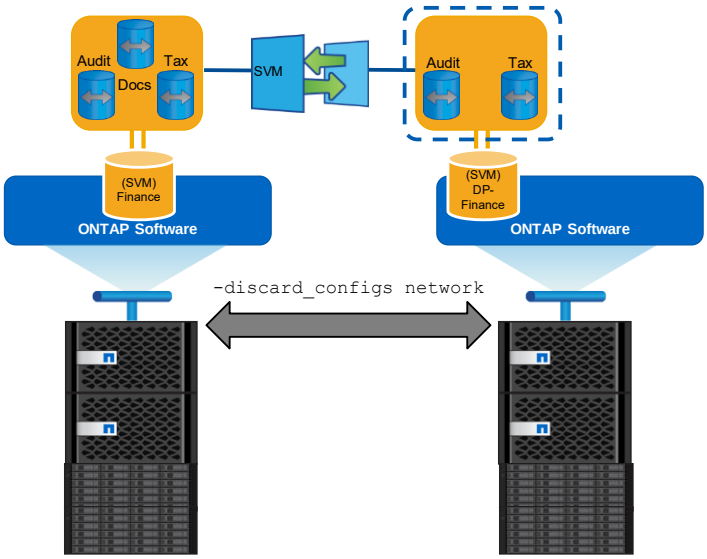
The destination SVM can also be started to provide read-only access to clients if the option `-identity-preserve` is set to `false`.

When the disaster-recovery SVM is initially created, no corresponding SVM root volume is created. The SVM root volume is created later, when the SnapMirror SVM relationship is initialized. The volumes that are created during the SnapMirror initialization process are mounted into the disaster-recovery namespace identically to the source namespace.

The destination SVM can contain load-sharing mirror volumes that are created for only the root volume.

Replicate Configuration Without LIFs

`-identity-preserve=true` and `-discard_configs network`



Use cases:

- Move an SVM from a cloud environment back to on-site premises.
- Move an SVM from one cluster to another.
- The destination SVM operates in an active read-only environment.

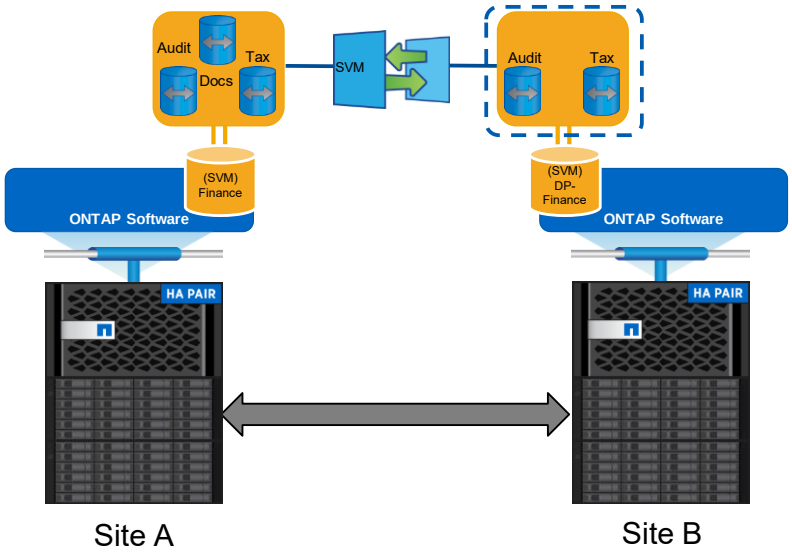
For an example, you have an SVM that is in the cloud, and you want to move it back to your premises.

You can use SVM disaster recovery to establish a whole SVM relationship between clusters and move the SVM from one cluster to another. After the cutover to the new cluster, you make the necessary changes to the network, route, DNS, and exports as needed; delete the SnapMirror relationship; and continue serving data.

Because you are not maintaining the network configuration, the CIFS server configuration, or any of the export policies, you can have the destination SVM in an active read-only environment.

Selective Protection in SVM Disaster Recovery

Per-volume protection



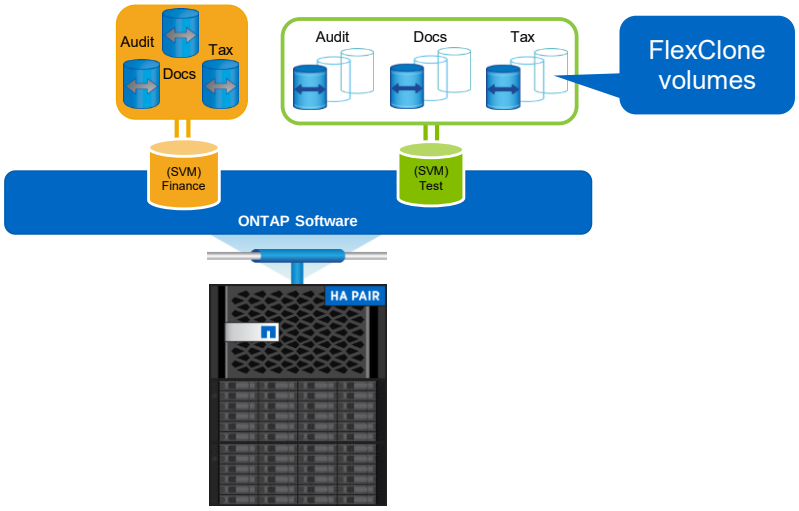
- Save capacity by excluding volumes from disaster recovery.
- Specify one or more volumes for exclusion.
- Retain all the benefits applicable for whole SVM disaster recovery.

If the `-vserver-dr-protection` option of the volume is set to `unprotected`, the SVM disaster recovery does not replicate this volume at the destination SVM. All the unprotected volumes and their namespace child volumes and clone child volumes are excluded from replication. Existing volumes and newly created volumes on the source SVM are protected by default.

You cannot exclude a volume that, if excluded, would break the junction path in the namespace. For example, if vol1 is mounted to the root of the namespace, vol2 is mounted to vol1, and vol3 is mounted to vol2 (root-vol1-vol2-vol3), you cannot exclude vol2 from SVM disaster recovery protection. This exclusion would break the path to vol3 in the namespace.

Test and Dev in SVM Disaster Recovery

Volume clones at the destination

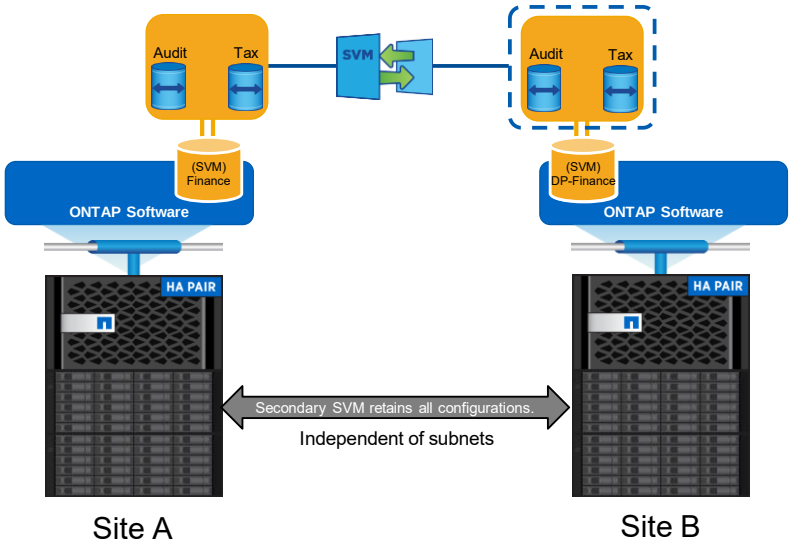


Destination Cluster

- Create clones of data protection volumes in the test SVM.
- Manually set up test SVM configuration.
- Volumes are ready to use in SVM disaster recovery if there is a disaster.

The `-vserver-dr-protection` option can also be set to `protected` or `unprotected` on a FlexClone volume. This setting optionally specifies whether the volume is protected by SVM disaster recovery. By default, the clone volume inherits this value from the parent volume.

Convert a Volume SnapMirror Relationship to SVM Disaster Recovery



- Requires peered SVMs in a SnapMirror relationship
- Easy conversion of SnapMirror relationship into SVM disaster recovery relationship

If there are volume-level SnapMirror relationships between two SVMs, you can create a SnapMirror relationship between the SVMs to convert the volume-level SnapMirror relationships to an SVM disaster recovery relationship.

All the volumes except the root volume on the destination SVM must be in a volume-level SnapMirror relationship with the corresponding volumes on the source SVM.

1. Ensure that the names of the source volume and destination volume (including the root volume) are the same.
2. Resynchronize all the volume-level SnapMirror relationships between the source and destination volumes by using the `snapmirror resync` command. For successful resynchronization, a shared Snapshot copy must exist between the primary volume and the secondary volume.
3. Verify that the resynchronization operation is complete and that all the SnapMirror relationships are in the `Snapmirrored` state by using the `snapmirror show` command.
4. Create an SVM disaster recovery relationship between the source SVM and destination SVM by using the `snapmirror create` command with the `-identity-preserve` option set to `true`.
5. Resynchronize the destination SVM from the source SVM by using the `snapmirror resync` command.
6. Verify that the resynchronization operation is complete and that the SnapMirror relationship is in the `Snapmirrored` state by using the `snapmirror show` command.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

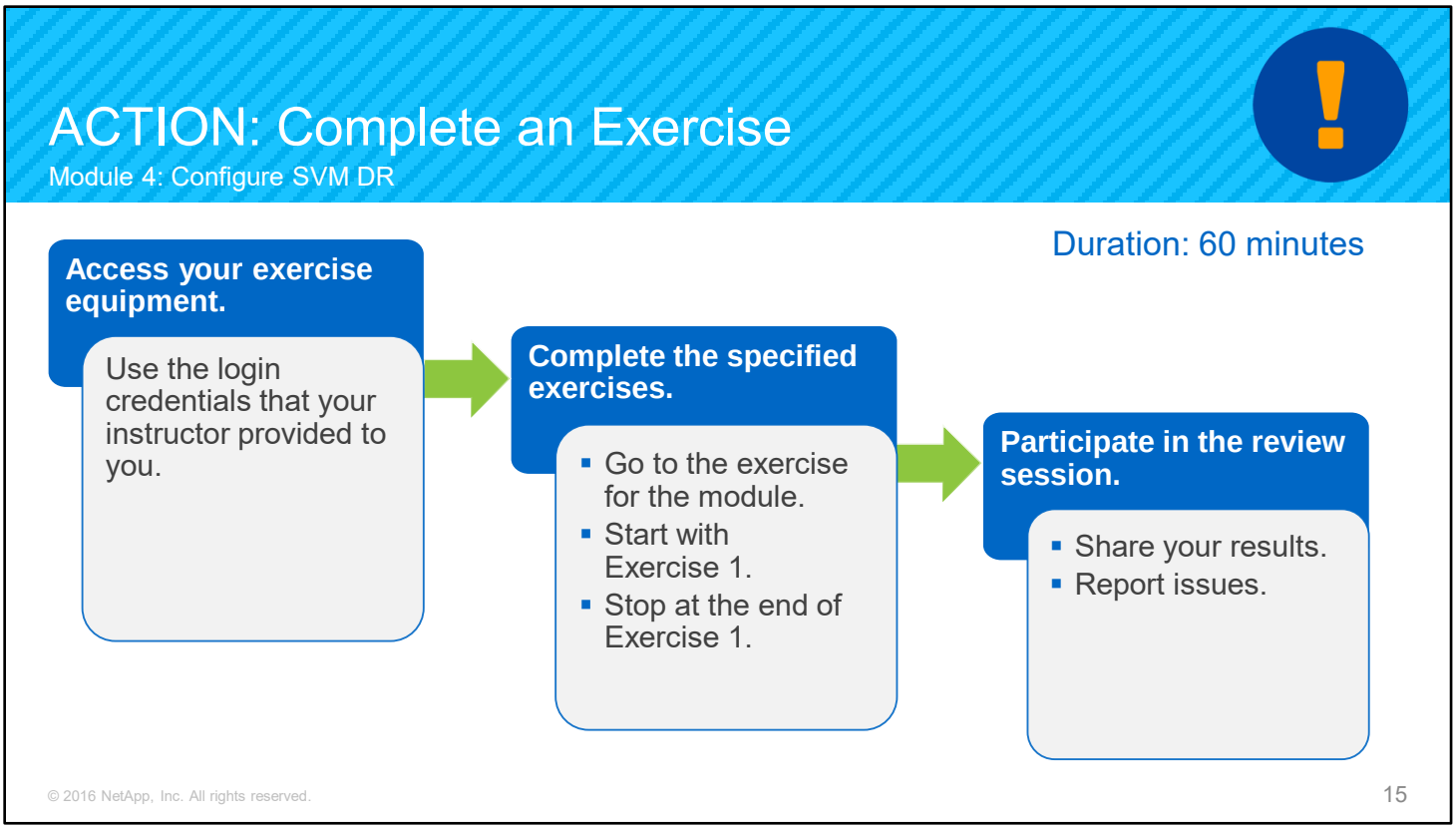
You have an SVM in a cloud environment (same layer-2 network). You want to move the SVM back to your on-site premises. What would you do? (Select two.)

a. Use the –identity-preserve true option in the snapmirror create command.

b. Use the –identity-preserve false option in the snapmirror create command.

c. Break the SVM peer relationship that was set up previously.

d. Use SVM disaster recovery to establish the SVM relationship between clusters. After cutover to the new cluster, make the necessary changes to network, route, DNS, and exports.



In this exercise you perform the following tasks:

1. Check the space requirements.
2. Create the disaster-recovery SVM.
3. Create the SVM peer relationship.
4. Create the SVM SnapMirror relationship.
5. Fail over to the disaster-recovery SVM and verify data access.
6. Reverse the SnapMirror relationship.
7. Recover the primary SVM.

ACTION: Share Your Experiences

Roundtable questions for the exercise

- When a disaster-recovery SVM is created, is there a corresponding SVM root volume?
- In the source SVM (svm_yellow), how many of the eight volumes were mirrored as part of the SVM SnapMirror relationship?

References

- *ONTAP 9.0 Release Notes*
- *ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology*
- *ONTAP 9.0 SVM Disaster Recovery Preparation Express Guide*
- *ONTAP 9.0 SVM Disaster Recovery Express Guide*
- *NetApp Technical Report TR-4015: SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP*
- *NetApp Technical FAQ: SnapMirror for SVM (SVM DR)*

Module Review

This module focused on enabling you to do the following:

- Summarize the requirements and options to replicate storage virtual machine data
- Prepare a storage virtual machine for data protection
- Perform a storage virtual machine initial data transfer
- Demonstrate a manual storage virtual machine update
- Manually update a storage virtual machine disaster-recovery relationship
- Produce regularly scheduled storage virtual machine updates

Module 5
Disk-to-Disk Backup with SnapVault Software

About This Module

This module focuses on enabling you to do the following:

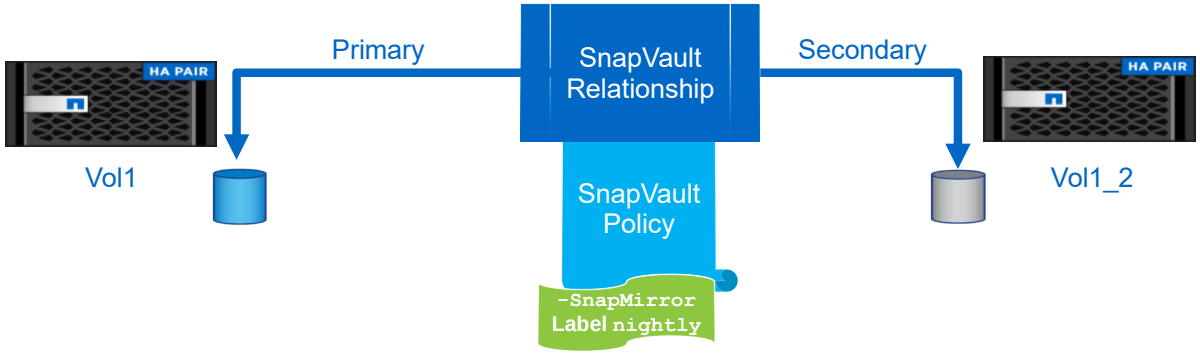
- Construct the required configuration to replicate data using SnapVault software
- Demonstrate a SnapVault initial transfer
- Perform a manual SnapVault update
- Produce regularly scheduled SnapVault updates
- Understand how to restore data using SnapVault software

Lesson 1
Implementing a SnapVault Relationship

Components of the SnapVault Solution: Part 1

SnapVault relationship, Snapshot copy policies, and the SnapMirror label

A SnapVault policy is the component of the SnapVault relationship that determines schedule and retention rules.



A SnapVault configuration is controlled from the SnapVault secondary storage virtual machine (SVM). The SnapVault configuration components on the secondary SVM consist of the following:

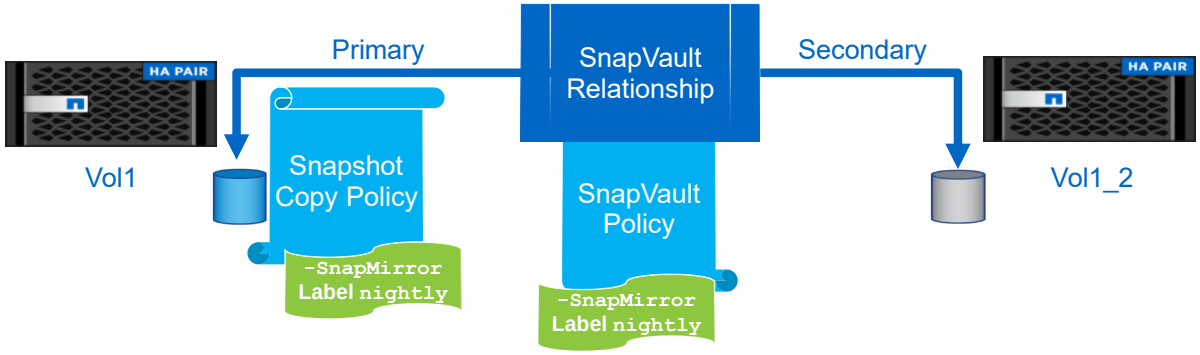
- A SnapVault relationship that specifies the primary and secondary volumes
- A SnapVault policy that specifies the retention rules
- A SnapMirror label that specifies the update schedule

You can configure a SnapVault solution by creating a SnapVault relationship and then assigning the default SnapVault policy with the default retention rules and SnapMirror label.

Components of the SnapVault Solution: Part 2

SnapVault relationship, Snapshot copy policies, and the SnapMirror label

A SnapVault policy is the component of the SnapVault relationship that determines schedule and retention rules.



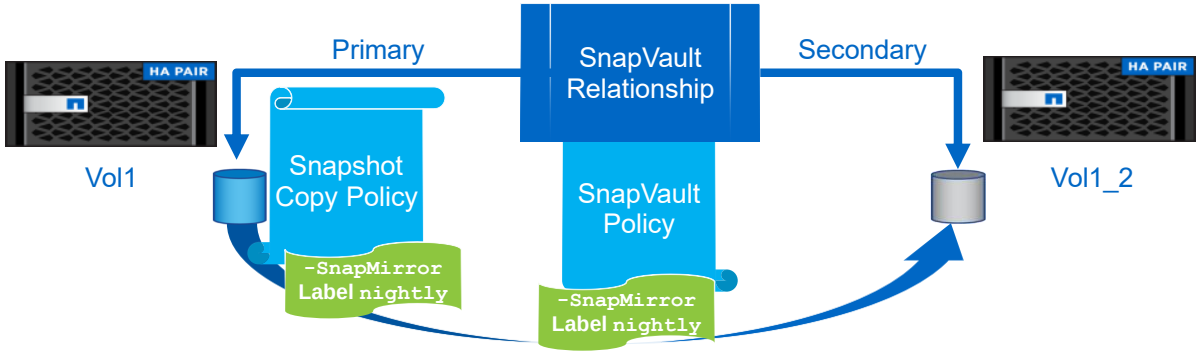
The SnapMirror label specified in the SnapVault policy on the secondary SVM matches the SnapMirror label configured in the Snapshot copies on the primary SVM.

The matching SnapMirror label identifies the Snapshot copy to transfer to the secondary SVM.

Components of the SnapVault Solution: Part 3

SnapVault relationship, Snapshot copy policies, and the SnapMirror label

A SnapVault policy is the component of the SnapVault relationship that determines schedule and retention rules.



SnapVault Software Updates Based on SnapMirror Label

Default SnapMirror labels are `weekly`, `nightly`, and `hourly`, with set schedule and retention rules that apply. The SnapVault policy specifies the weekly, nightly, or hourly SnapMirror label and sets the schedule and retention rules for SnapVault updates.

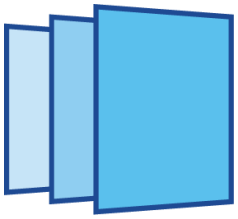
You can customize the SnapVault backup intervals by creating a customized Snapshot copy policy, a customized schedule, or a customized SnapVault label.

The Snapshot Copy Policy

Requirements

- Must have the `snapmirror-label` attribute enabled
- Must match the `snapmirror-label` attribute in the SnapVault policy

You must decide whether to use a preconfigured Snapshot copy policy or to create a policy.



The Snapshot copy policy sets the Snapshot schedule for volumes. For SnapVault updates, the default SnapVault policy uses the daily and weekly `snapmirror-label` attribute specified by the default Snapshot copy policy. You can use the preconfigured Snapshot copy policy or, if you need a different schedule, you can create a Snapshot copy policy.

If you create a Snapshot copy policy, you must modify the `snapmirror-label` attribute to match the `snapmirror-label` attribute in the SnapVault policy.

Verifying the Snapshot Copy Policy

Check for the SnapMirror label attribute on the primary SVM.

Following is the command to determine whether a Snapshot copy policy has the `snapmirror-label` attribute:

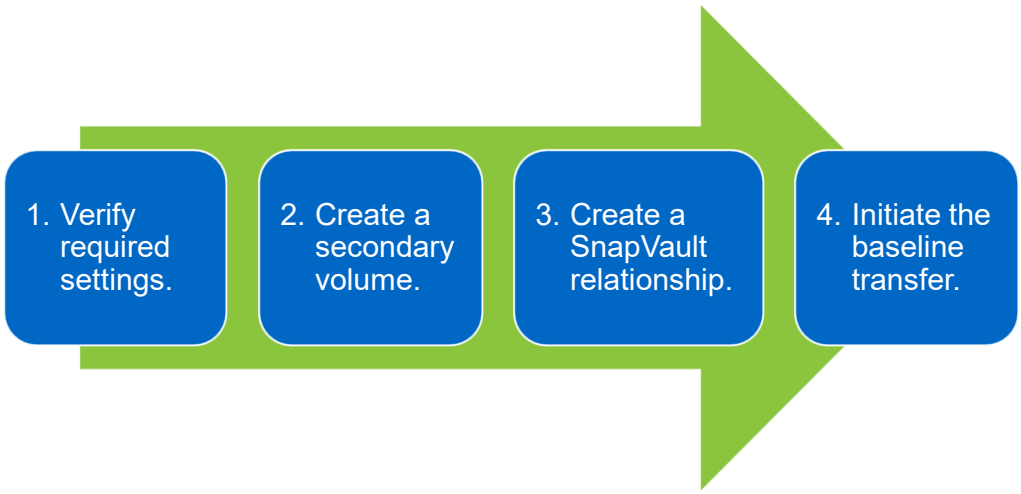
```
svl-nau::> volume snapshot policy show
Vserver: svl-nau
                          Number of Is
Policy Name               Schedules Enabled Comment
------------------------- --------- ------- ---------------------------------
default                           3 true    Default policy with hourly, daily & weekly schedules.
    Schedule                Count     Prefix                SnapMirror Label
    ----------------------- -----     ----------------------- ------------------
    hourly                      6     hourly                -
    daily                       2     daily                 daily
    weekly                      2     weekly                weekly

default-1weekly                 3     true    Default policy with 6 hourly, 2 daily & 1 weekly schedule.
    Schedule                Count     Prefix                SnapMirror Label
    ----------------------- -----     ----------------------- ------------------
    hourly                      6     hourly                -
    daily                       2     daily                 -
    weekly                      1     weekly                -
```

The `default-1weekly` policy does not have a SnapMirror label.

The Snapshot copy policy controls the Snapshot copy schedule and retention rules for all volumes. For SnapVault relationships, the Snapshot copy policy on the primary volume should have the `snapmirror-label` attribute. The `snapmirror-label` attribute controls the SnapVault update schedule and the retention rules for the primary and secondary volumes.

As a prerequisite check, verify that the Snapshot copy policies on the primary volume are using the `snapmirror-label` attribute. If your ONTAP cluster has been upgraded several times, you might have to modify the Snapshot copy policy by adding the `snapmirror-label` attribute.

Steps to Implement SnapVault Backups



If you are using the CLI to implement the SnapVault solution, follow these steps:

1. To ensure that the required preconfigurations are performed, create a checklist.
2. Create a secondary volume.
3. Create a SnapVault relationship.
4. Initiate the baseline transfer.

1. SnapVault Preconfiguration Checklist

Planning a SnapVault deployment

- Install SnapVault license codes.
- Verify that language setting requirements are met.
- Verify that firewall settings permit SnapVault transfers.
- Verify that cluster and SVM peer relationships are healthy.
- Estimate the amount of time required to complete the baseline transfer.
- Verify that the Snapshot copy policy on the primary volume has the `snapmirror-label` attribute.

Before you begin to implement your SnapVault backups, make a checklist of the required preconfigurations and then verify that preconfigurations are set correctly.

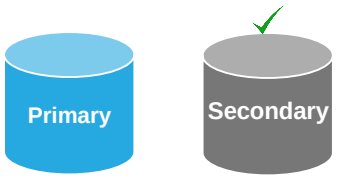
Careful planning is also recommended. Plan which primary volumes you are protecting and what SnapVault topography you are deploying. The amount of data and network congestion make it necessary to plan for the amount of time required to complete the baseline transfer.

2. Create a SnapVault Destination Volume

Required volume settings

The SnapVault secondary volume must have the following configurations:

- FlexVol volume: –type DP (data protection)
- Sizing management: automatic resizing
- Space efficiency: enabled
- Using the OnCommand System Manager, you can automatically create a volume on the destination SVM.



After you verify that the prerequisite configurations are set, you create the SnapVault secondary volume. If you are using the OnCommand System Manager, the OnCommand Unified Manager, NetApp SnapProtect management software, or another backup management solution, the secondary volume is created automatically. If you are setting up SnapVault software on the CLI, you create the SnapVault secondary volume manually.

When you create a FlexVol volume and use the `-type DP` option, the volume is created with settings that reflect best practices for secondary volumes. The volume settings are different from the default settings used for read/write (RW) volumes.

Space setting	RW volume	DP volume
Space guarantee	volume	volume
autosize	false	true
autosize-mode	off	grow_shrink
autosize-growthreshold-Percent	85 (percent)	85 (percent)
autosize-shrinkthreshold %	50 (percent)	80(percent; autosize-growthreshold-percent -5)
min-autosize	Initial volume size	Initial volume size
max-autosize	120% of volume size	Maximum aggregate size
Snap reserve	5 (percent)	0 (percent)
fractional-reserve	100 (percent)	0 (percent)

3. Create a SnapVault Relationship

Assign a default SnapVault policy and Snapshot copy schedule.

Use the snapmirror create command for the following:

- To create a SnapVault relationship (SnapMirror type XDP)
- To assign the default SnapVault policy

```
rtp-nau::> snapmirror create -source-path svl-nau://svm_red/red_share_CIFS_volume
-destination-path rtp-nau://svm_blue/svm_red_red_share_CIFS_volume_vault -type XDP
-policy XDPDefault
```

The default SnapVault policy

SnapVault type of SnapMirror relationship

12

On the destination SVM, create a SnapVault relationship and assign an XDP policy by using the `snapmirror create` command with the `-type XDP` parameter and the `-policy` parameter. The `snapmirror create` command with the `-type XDP` specified creates the SnapVault relationship between the primary and secondary volumes.

The `-source-path` specifies the primary SVM and volume.

The `-destination-path` specifies the secondary SVM and volume.

The `-policy XDPDefault` specifies the default SnapVault policy.

In the example command, the default SnapVault policy was specified. If no policy is specified, ONTAP software automatically selects the default SnapVault policy.

You cannot change the default SnapVault policy. However, you can create your own SnapVault policy.

4. Initiate the Baseline Transfer

Copy primary data to the secondary volume.

Command to start the baseline transfer:

```
rtp-nau::> snapmirror initialize
-destination-path rtp-nau://svm_blue/svm_red_red_share_CIFS_volume_vault
```

Verify the SnapVault status:

```
rtp-nau::> snapmirror show
```


After the SnapVault relationship is created, you must start the baseline transfer by using the `snapmirror initialize` command.

The `snapmirror initialize` command creates a Snapshot copy on the primary volume that is transferred to the secondary volume. The initial Snapshot copy is used as a baseline for subsequent incremental Snapshot copies. The command does not transfer any Snapshot copies that currently exist on the primary volume.

Scheduled updates do not succeed until the SnapVault relationship finishes initialization.

You do not have to initialize the SnapVault relationship when you create it. You can initialize the relationship from the secondary SVM at a time that can better accommodate the baseline transfer.

Managing SnapMirror and SnapVault Updates

To Do This	Use This Command
Get the SnapVault status	`snapmirror show`
Manually update a SnapVault relationship	`snapmirror update`
Modify SnapVault relationship properties	`snapmirror modify`
Modify a mirror policy or SnapVault policy	`snapmirror policy modify`
Modify an existing rule in a SnapVault policy	`snapmirror policy modify-rule`
Remove a rule in a SnapVault policy	`snapmirror policy remove-rule`
Delete a mirror policy or SnapVault policy	`snapmirror policy delete`

SnapMirror commands are used to manage SnapMirror and SnapVault relationships.

Commands for Managing Mirror and SnapVault Policies

Cluster administrators can use the `snapmirror policy` commands to create and manage all data protection mirror and SnapVault policies. SVM administrators can use the same commands to create and manage all data protection mirror and SnapVault policies within SVMs.

- All policy-management commands (except for the `snapmirror policy show` command) must be run on the SVM that contains the secondary volume.
- Only FlexVol volumes support commands for SnapVault policies.

ACTION: Try This Task

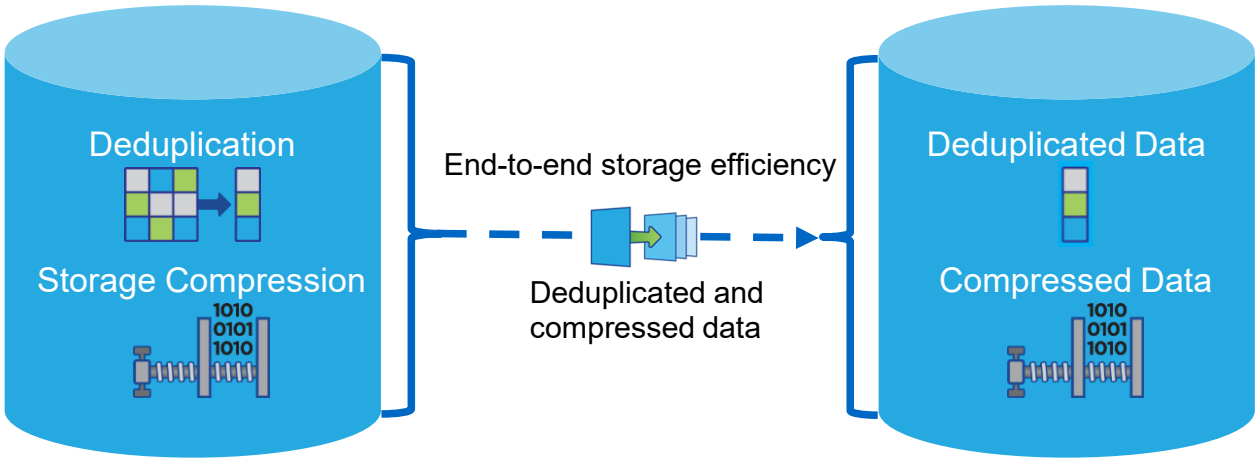
Using clusters svl-nau and rtp-nau on your exercise kit, do the following:

- Using the svl-nau cluster, enter the `volume snapshot policy show` command.
- Using the rtp-nau cluster, enter the `snapmirror policy show` command.

Answer these questions:

- Do any Snapshot copy policies have a SnapMirror label?
- Which SnapMirror policies have a SnapMirror label rule?
- Do any of the SnapMirror policies on rtp-nau have a SnapMirror label that matches a SnapMirror label in a Snapshot copy policy on svl-nau?

SnapVault End-to-End Storage Efficiency



If the primary volume in a SnapVault relationship is enabled for storage efficiency, all data backup operations preserve the storage efficiency.

In this configuration, the deduplication and compression processes are running on the source volume, not the destination. The data transfer savings over the network are retained.

If you have compression or deduplication enabled on the destination, the process starts automatically after the transfer completes. You cannot change when this process runs. However, you can change the volume efficiency priority that is assigned to the volume.

Following are some recommendations for SnapVault destinations when the source has compression enabled:

- If you require compression savings on the destination and your source has compression enabled, then do not enable compression on the SnapVault destination. The savings are already inherited on the destination.
- If you enable compression on the SnapVault destination, the savings are lost during the transfer, and you have to redo the savings on the destination.
- If you ever enable compression on the destination, even if you later disable it, you never retain the savings from the source.

Postprocess compression of existing data results in physical-level changes to the data. This result means that SnapVault software recognizes the changes as changed blocks and includes them in its data transfers to the destination volume. As a result, SnapVault transfers are likely to be much larger than normal. If you can do so, NetApp recommends that you compress existing data on the source before you run baseline transfers for SnapVault software. For pre-existing SnapVault relationships, consider the big surge of data involved in the transfer and plan accordingly.

As a best practice, have the same compression type on the SnapVault source and destination to retain savings over the network.

Difference Between Adaptive Compression and Secondary Compression

Adaptive Compression

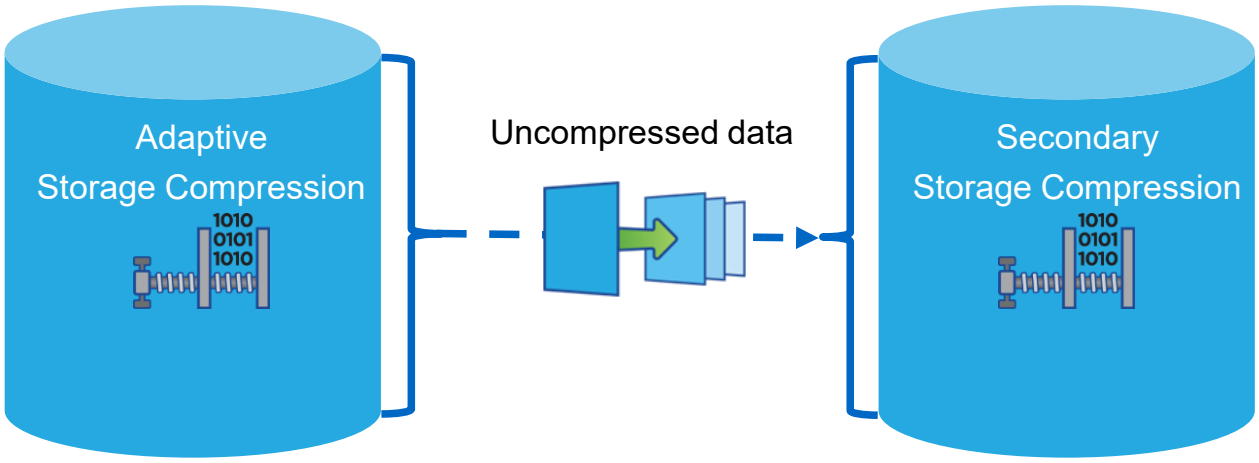
Adaptive compression combines fewer blocks of data into a compression group (8K). The compression group is then compressed and stored as a single block. When a user requests data from this compression group, less time is taken to decompress and provide that data to the user. This time saving improves the read performance. In general, adaptive compression is better suited for random workloads. Adaptive compression provides relatively less savings than secondary compression, but adaptive compression provides better performance.

Secondary Compression

Secondary compression combines large groups of data blocks into a compression group (32K). The compression group is then compressed and stored as fewer blocks. This compression reduces the size of the data and increases the free space in the storage system. In general, secondary compression is better suited for sequential workloads.

Both secondary compression and adaptive compression are supported on all types of disk media (hard disk drive, All Flash FAS, and Flash Pool).

SnapVault and Storage Compression



If compression is enabled on the SnapVault destination, the savings from the source are not retained over the network transfer, but they can be regained.

If the source and destination volumes have different compression types (for example, the source volume has adaptive compression and the destination volume has secondary compression), the savings from the source are not retained over the network transfer. Depending on whether the destination has inline or postprocess compression, the savings are regained.

As a best practice, enable compression on the SnapVault destination only if you cannot run compression on the source.

For more information regarding data compression and deduplication, see NetApp TR-4476.

SnapVault Relationships and ONTAP Versions

The following SnapVault relationships are possible using type `XDP` and policy `vault`.

Primary volume ONTAP version	Secondary volume can reside on a system running one of the following releases.			
	8.1.x	8.2.x	8.3.x	9.0
8.1.x	No	No	No	No
8.2.x	No	Yes	Yes	Yes
8.3.x	No	Yes	Yes	Yes
9.0	No	Yes	Yes	Yes

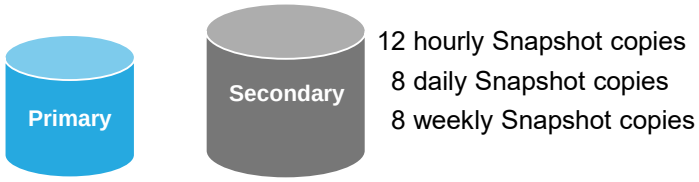
For SnapVault relationships, the version of ONTAP software running on the primary and secondary volumes must be ONTAP 8.2 or later software. The version of ONTAP software running on the secondary volume can be older or newer than the version running on the primary volume. When the primary and secondary volumes run different versions of ONTAP software, they should not be more than two major releases apart.

Planning Space Requirements

Estimate SnapVault primary data and secondary space requirements.

On the SnapVault secondary system, plan the space required for your backup plans:

- Size of the primary volume
- Rate of increase of the data on the primary volume
- Number of Snapshot copies to be retained on the secondary volume



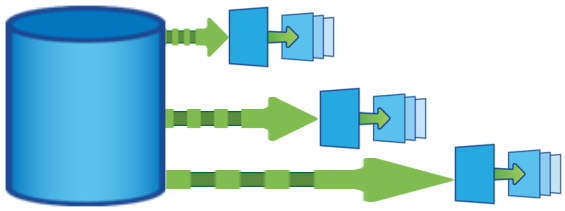
To avoid the inconvenience of running out of disk space, be sure to calculate the amount of disk space you need on the SnapVault secondary system. Consider the following factors as you plan the space required for your backups:

- Size of the primary volume
- Rate of increase of the data on the primary volume
- Number of Snapshot copies to be retained on the secondary volume

NetApp offers sizing guides for the major application servers that you can use to calculate disk space.

Creating a Tiered Backup Policy

In a tiered backup strategy, a SnapVault policy can have several rules. Each rule identifies a different set of Snapshot copies.



ONTAP software uses the `snapmirror-label` attribute to identify Snapshot copies between primary and secondary FlexVol volumes in a SnapVault relationship. When you configure rules in a SnapVault policy, you enter the `snapmirror-label` name that you want to use to identify the Snapshot copies to which the rule applies.

In a tiered backup strategy, a SnapVault policy might have several rules, and each rule identifies a different set of Snapshot copies. In this example, you have a volume to which you have assigned a Snapshot policy that specifies the following schedule:

- An hourly Snapshot copy: Every two hours, a Snapshot copy is created and is assigned the attribute `snapmirror-label hourly`.
- A daily Snapshot copy: Every day at 5 p.m., a Snapshot copy is created and is assigned the attribute `snapmirror-label daily`.
- A weekly Snapshot copy: Every Friday at 6 p.m., a Snapshot copy is created and is assigned the attribute `snapmirror-label weekly`.

Sample Snapshot Copy Schedules and Retention

For SnapVault backups

`Snapmirror-label` attribute value	Source volume: Snapshot copy schedule	Primary volume: Snapshot copies retained	SnapVault secondary volume: Snapshot copies retained
`weekly`	Every Sunday at 20:00	4	8
`nightly`	Every Monday through Friday at 22:00	10	60
`hourly`	Every hour from 07:00 through 18:00	11	120
Total	Not applicable	25	188

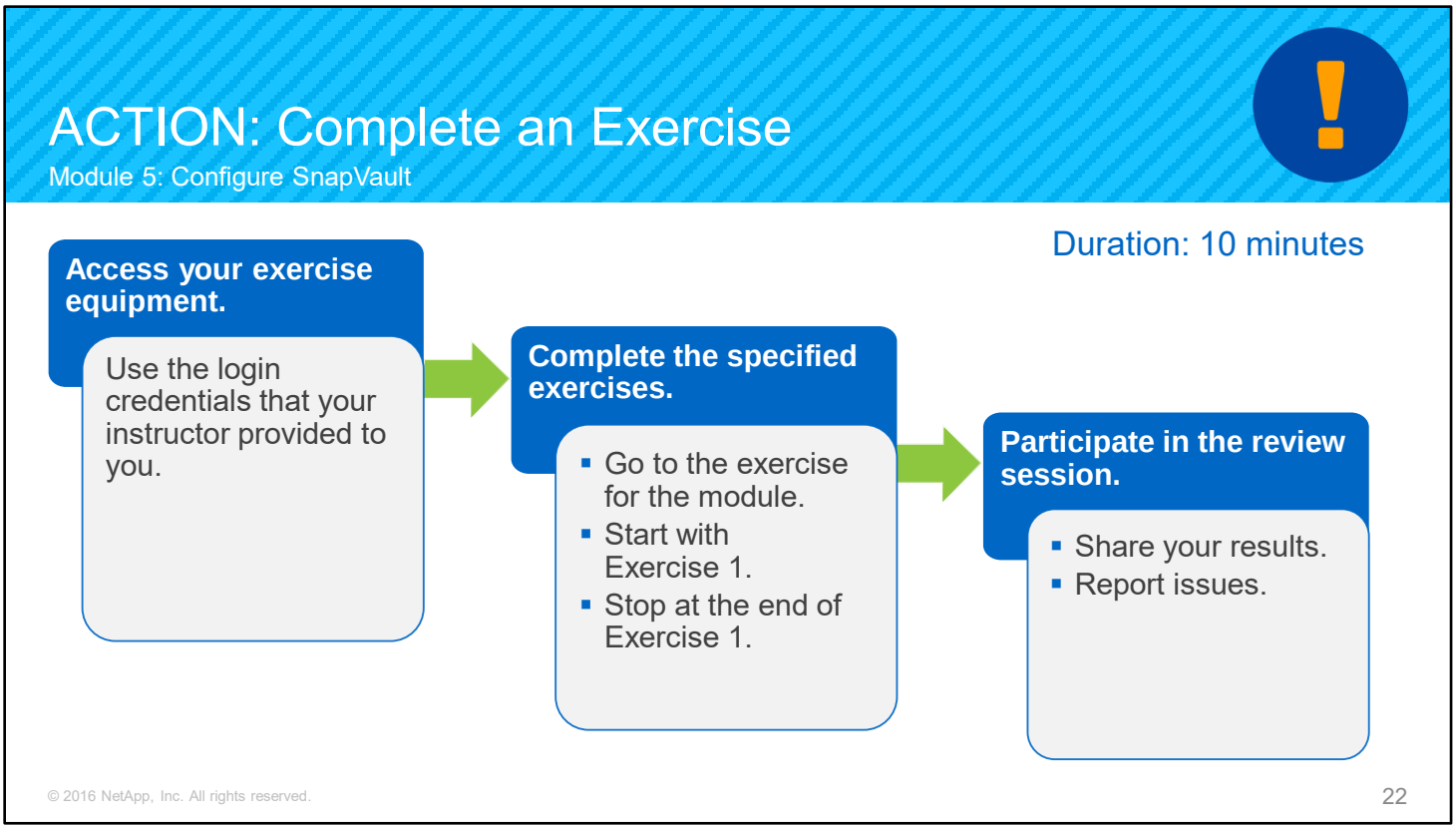
It is important to plan the Snapshot copy transfer schedule and retention for your SnapVault backups. When you plan SnapVault relationships, consider the following guidelines:

Before you create a SnapVault policy, create a table to plan which Snapshot copies you want replicated to the SnapVault secondary volume and how many of each you want to keep.

- Hourly (periodically throughout the day)
  Does the data change often enough throughout the day to make it worthwhile to replicate a Snapshot copy every hour, every two hours, or every four hours?
- Nightly
  Do you want to replicate a Snapshot copy every night or just workday nights?
- Weekly
  How many weekly Snapshot copies are useful to keep in the SnapVault secondary volume?

The primary volume should have an assigned Snapshot policy that creates Snapshot copies at the intervals that you need and labels each Snapshot copy with the appropriate `snapmirror-label` attribute name.

The SnapVault policy assigned to the SnapVault relationship should select the Snapshot copies that you want from the primary volume, identified by the `snapmirror-label` attribute name. The policy should also specify how many Snapshot copies of each name that you want to keep on the SnapVault secondary volume.



In this exercise you perform the following tasks:

1. Create a SnapVault relationship.
2. Create the SVM peer relationship.
3. Initialize the relationship.
4. Verify data transfer.

ACTION: Share Your Experiences

Roundtable questions for the exercise

- What did you have to do when you selected the destination SVM in Task 1, Step 8?
- How was the SnapMirror label selected for the SnapVault policy?

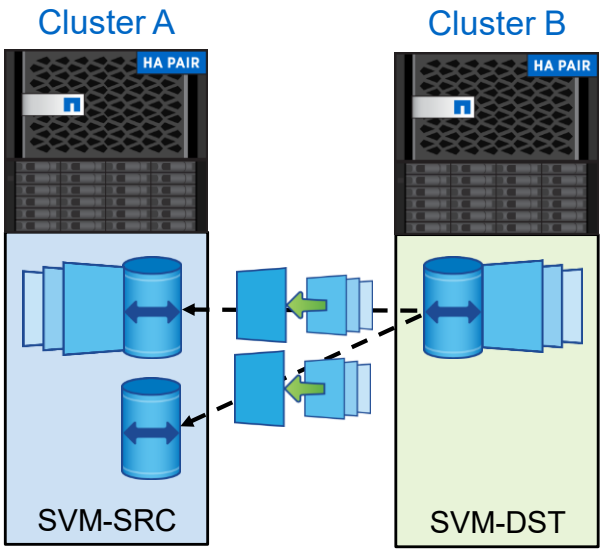
Lesson 2
Restoring Data Using SnapVault Software

Restoring Data with SnapVault Software

Guidelines

- You can restore data from the vault destination to the following:
  - The source volume
  - A volume other than the source
- You can restore from the following:
  - The latest Snapshot copy
  - An earlier Snapshot copy

NOTE: The restore operation deletes new Snapshot copies that were not backed up.



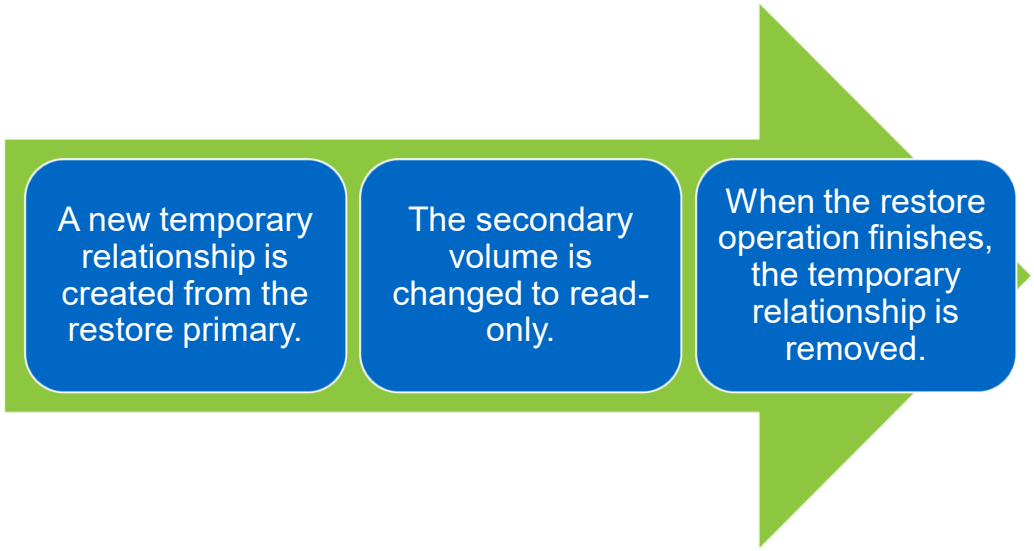
In the restore operation from a SnapVault backup, a single, specified Snapshot copy is copied from a SnapVault secondary volume to a specified volume. Restoring a volume from a SnapVault secondary volume changes the view of the active file system but preserves all earlier Snapshot copies in the SnapVault backup.

Before you restore a volume, you must shut down any application that accesses data in a volume to which a restore is writing data. Therefore, if you are using a logical volume manager (LVM), you must unmount the file system, shut down any database, and deactivate and quiesce the LVM. The restore operation is disruptive. When the restore operation finishes, the cluster administrator or SVM administrator must remount the volume and restart all applications that use the volume.

The restore secondary volume must not be the secondary of another mirror or the secondary of another SnapVault relationship. You can restore to the following volumes:

- Original primary volume: You can restore from a SnapVault secondary volume back to the original SnapVault primary volume.
- New, empty secondary volume: You can restore from a SnapVault secondary volume to a new, empty secondary volume. You must first create the volume as a data protection volume.
- New secondary volume that already contains data: You can restore from a SnapVault secondary volume to a volume that is populated with data. The volume must have a Snapshot copy shared with the restore primary volume and must not be a data protection volume.

Restore Data Workflow



A restore operation from a SnapVault backup consists of a series of actions that are performed on a temporary restore relationship and on the secondary volume. During a restore operation, the following actions occur:

- A new temporary relationship is created from the restore primary (which is the original SnapVault relationship secondary volume) to the restore secondary. The temporary relationship is a restore type (RST). The `snapmirror show` command displays the RST type while the restore operation is in progress.
  The restore secondary might be the original SnapVault primary volume or it might be a new SnapVault secondary volume.
- During the restore process, the restore secondary volume is changed to read-only.
- When the restore operation finishes, the temporary relationship is removed, and the restore secondary volume is changed to read/write.

Restoring a Volume

Restore a volume by using the snapmirror restore command:

```
svl-nau::> snapmirror restore -destination-path
rtp-nau://svm_blue/svm_red_red_share_CIFS_volume_vault
-source-path svl-nau://svm_red/red_share_CIFS_volume
-source-snapshot 5min.2016-07-12_2010
```

Select exactly which Snapshot copy to use in the restore operation.

If the data on a volume becomes unavailable, you can restore the volume to a specific time by copying a Snapshot copy in the SnapVault backup. You can restore data to the same primary volume or to a new location. This restore operation is a disruptive operation.

CIFS traffic must not be running on the SnapVault primary volume when a restore operation is running.

This task describes how to restore a whole volume from a SnapVault backup. To restore a single file or LUN, you can restore the whole volume to a different, nonprimary volume and then select the file or LUN. If you prefer, you can use the NetApp OnCommand management software online management tools.

If the volume to which you are restoring has compression enabled and the secondary volume from which you are restoring does not have compression enabled, disable compression. You disable compression to retain storage efficiency during the restore. (The `snapmirror restore` command warns you that all data newer than the Snapshot copy will be deleted.)

Restoring a Single File or LUN

- You can restore a single file or LUN or a set of files from a Snapshot copy in a SnapVault secondary volume to the active file system of a primary volume.
- You can restart a failed or aborted single file or LUN restore operation by reissuing the snapmirror restore command.
- Several SnapVault restore guidelines apply.

In ONTAP environments, you can restore a single file or single LUN from a SnapVault secondary volume by using the NetApp OnCommand management software online management tools. The following guidelines apply to SAN environments:

- When you restore a LUN by overwriting it, you do not need to configure new access controls.
- You must configure new access controls for the restored LUN only when you restore a LUN as a newly created LUN on the volume.
- If a LUN on the SnapVault secondary volume is online and mapped before the restore operation begins, it remains so during the restore operation and after the operation finishes.
- The host system can discover the LUN and issue a nonmedia access command for the LUN. Such inquiries or commands are to set persistent reservations while the restore operation is in progress.
- During a restore operation, you cannot use the `lun create` command to create a LUN in a volume.
- Restore operations from tape and from a SnapVault backup are identical.
- You cannot restore a single LUN from a SnapVault secondary volume on a system that is running in Data ONTAP operating in 7-Mode.

For more information about restoring LUNs, see the *ONTAP 9.0 SAN Administration Guide*.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

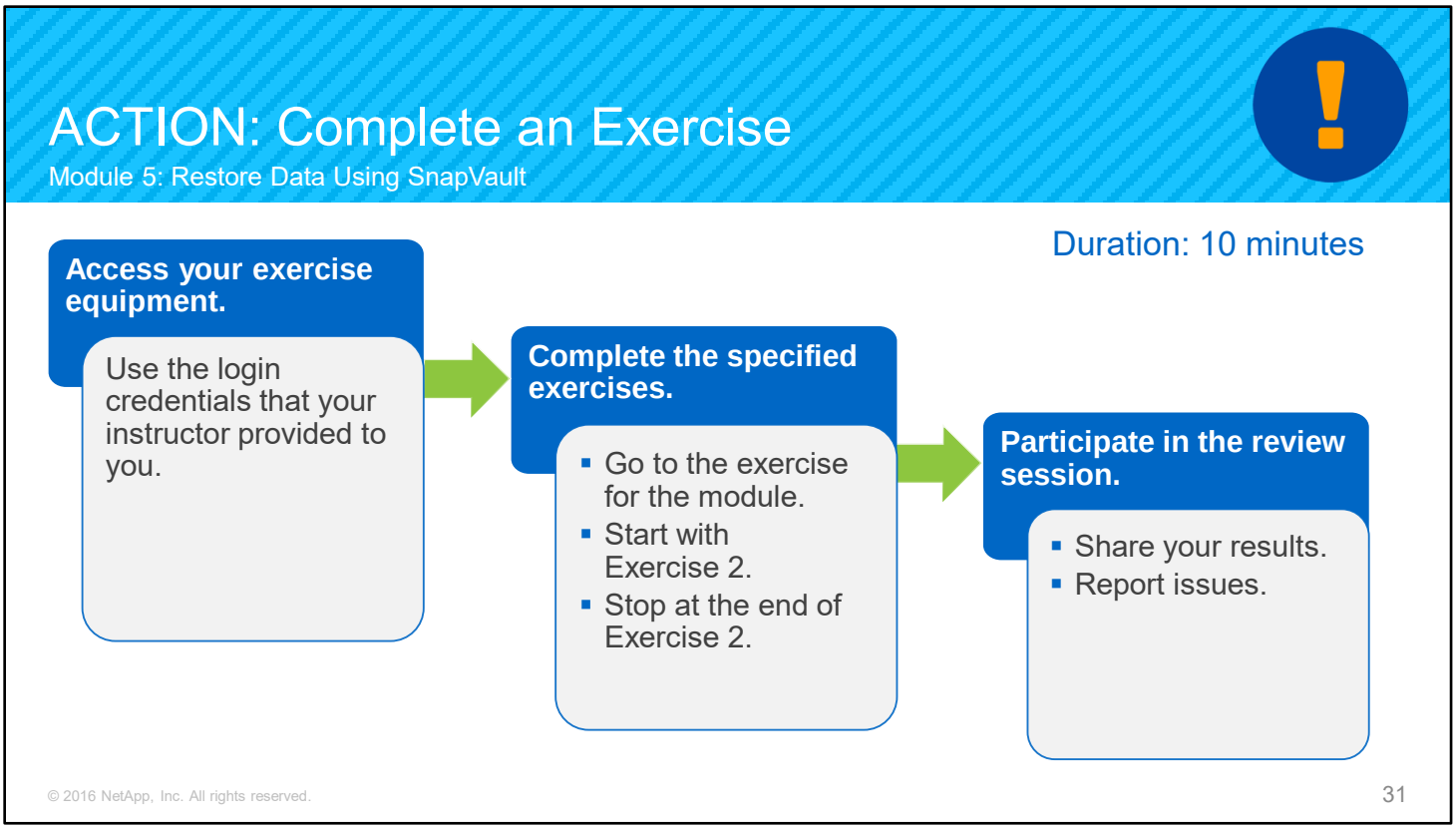
The source volume in a SnapVault relationship has developed inconsistency. The SnapVault updates occur nightly, but you suspect the inconsistency actually occurred two days ago. What would you do? (Select one.)

a. Use SnapVault software to restore from the Snapshot copy you know did not have the inconsistency.

b. Break the SnapVault relationship and direct the clients to use the SnapVault destination volume.

c. Break and release the SnapVault relationship and direct the clients to use the SnapVault destination volume.

d. Create a source volume and use SnapVault software to restore to that volume.



In this exercise you perform the following tasks:

1. Simulate data loss.
2. Use SnapVault software to recover an entire volume.

ACTION: Share Your Experiences

Roundtable questions for the exercise

- In Step 3, what were the options in the “Restore to” configuration?
- After the restore operation, what would have happened to the quotas that were configured on the volume?

References

- *ONTAP 9.0 Release Notes*
- *ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology*
- *ONTAP 9.0 Volume Backup Using SnapVault Express Guide*
- *ONTAP 9.0 Volume Restore Using SnapVault Express Guide*
- *NetApp Technical Report TR-4183: SnapVault Best Practices Guide Clustered Data ONTAP*
- *NetApp Technical Report TR-4476: NetApp Data Compression and Deduplication: Data ONTAP 8.3.1 and Later*

Module Review

This module focused on enabling you to do the following:

- Construct the required configuration to replicate data using SnapVault software
- Perform a SnapVault initial transfer
- Perform a manual SnapVault update
- Produce regularly scheduled SnapVault updates
- Restore data using SnapVault software

Module 6
SyncMirror and MetroCluster Software

About This Module

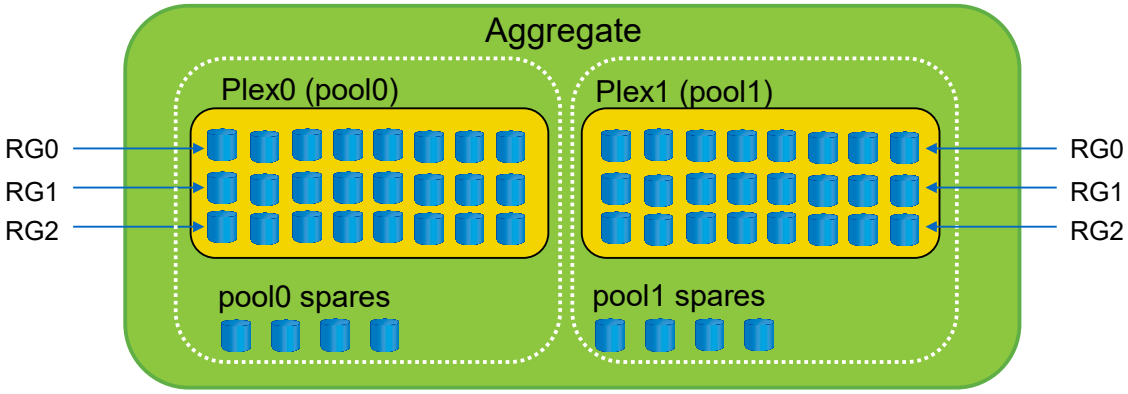
This module focuses on enabling you to do the following:

- Identify the components involved with SyncMirror software
- Explain the SyncMirror disk arrangement into pools and plexes
- Describe the basic operation of MetroCluster software
- Explain how MetroCluster software protects data in normal operation
- Describe how to perform the MetroCluster switchover, healing, and switchback processes

Lesson 1
SyncMirror Operation

Data Mirroring Using SyncMirror Software

- Provides real-time mirroring of data within a single aggregate at the RAID level
- Provides data resiliency and removes single points of failure in connecting to disks or array LUNs



The SyncMirror feature is an optional feature of ONTAP software that enables real-time mirroring of data within a single aggregate. The SyncMirror feature provides synchronous mirroring of data, implemented at the RAID level. You can use the SyncMirror feature to create aggregates that consist of two copies of the same WAFL (Write Anywhere File Layout) file system. The two copies, known as plexes, are simultaneously updated. Therefore, the copies are always identical. The two plexes are within a single aggregate.

Use the SyncMirror feature to provide increased data resiliency. The SyncMirror feature removes single points of failure in connecting to disks or array LUNs. Application servers that are stored on ONTAP software with the SyncMirror feature can prevent data loss due to disk, shelf, or controller failures.

With the SyncMirror feature, you can configure two physically separated sites, such as a Site A and a Site B. Data written to an aggregate in Site A is synchronously replicated in a set of disks that are on the remote Site B.

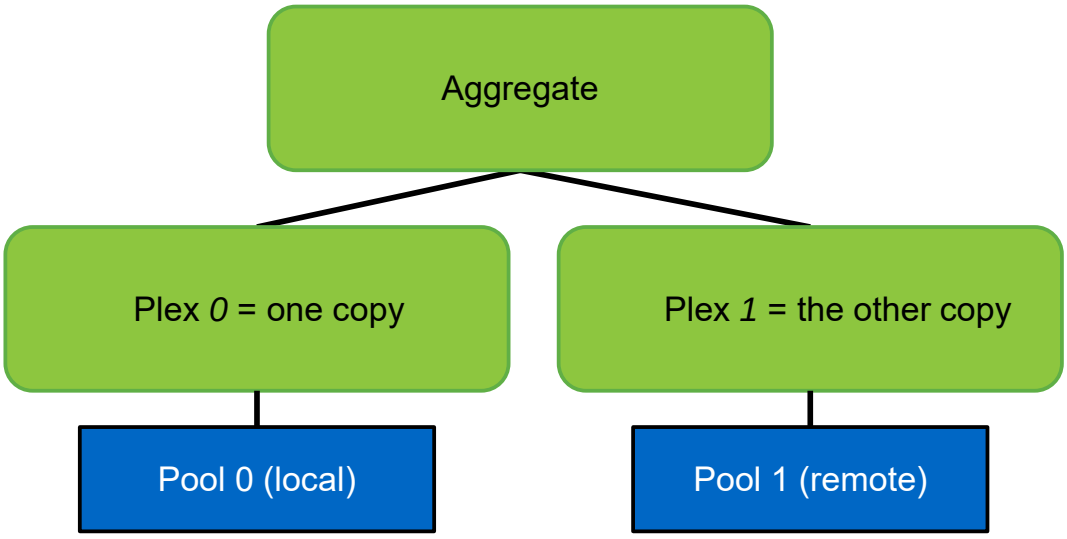
On the slide, a second plex has been created for the aggregate, plex1. The data in plex1 is a copy of the data in plex0, and the RAID groups are also identical. If 32 spare disks are allocated to pool0 or pool1, there would be 16 disks for each pool.

An aggregate that is mirrored using SyncMirror software requires twice as much storage as an unmirrored aggregate. Each of the two plexes requires an independent set of disks or array LUNs.

When SyncMirror software is used in a setup other than a MetroCluster configuration, each of the plexes can be on the same storage array or on different storage arrays.

Plexes can be considered local or remote in the context of the storage array that is connected to the ONTAP system on which the aggregate is configured. For example, in MetroCluster configurations, the plex at the local site is the local plex, and the one at the remote site is the remote plex.

Relationships of Plexes and Pools to an Aggregate



A SyncMirror aggregate has two plexes. This setup provides a high level of data availability because the two plexes are physically separated.

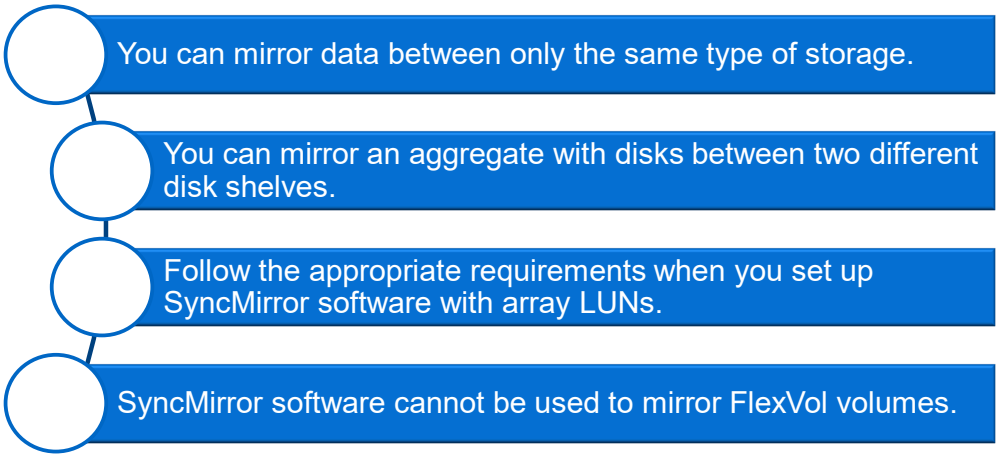
For a system that uses disks, the two plexes are on different shelves connected to the system with separate cables and adapters. Each plex has its own collection of spare disks. For a system that uses array LUNs, the plexes are on separate sets of array LUNs, either on one storage array or on separate storage arrays.

NOTE: You cannot set up SyncMirror software with disks in one plex and array LUNs in the other plex.

Physical separation of the plexes protects against data loss if one of the shelves or the storage array becomes unavailable. The unaffected plex continues to serve data while you fix the cause of the failure. After you fix the problem, the two plexes can be resynchronized.

SyncMirror Storage Type Considerations

Remember these guidelines about SyncMirror software.



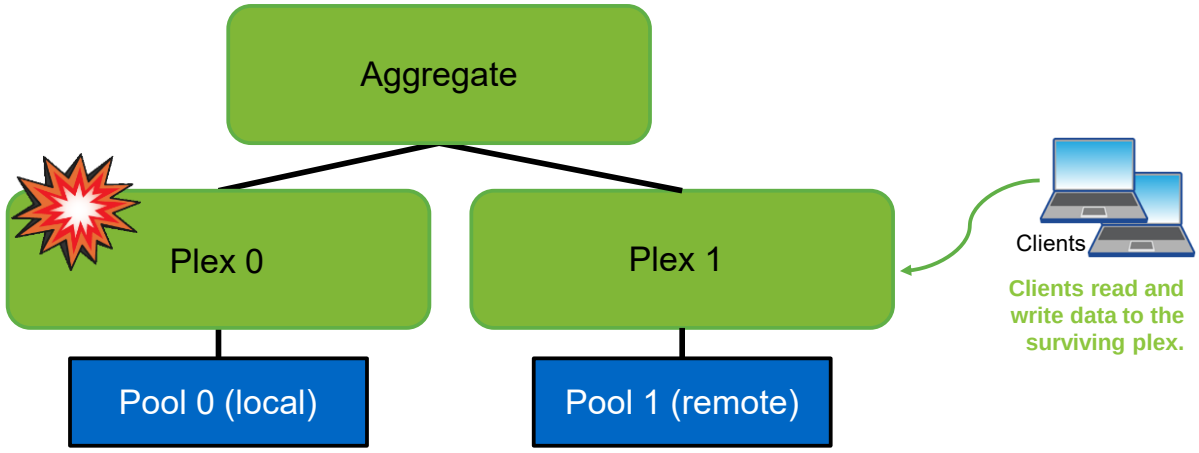
When you plan mirroring of aggregates for systems that can use both array LUNs and disks, consider the following:

- You can mirror data between only the same types of storage. You cannot mirror an aggregate between a native disk shelf on an ONTAP system and a storage array.
- If your ONTAP system has disk shelves, you can mirror an aggregate with disks between two different disk shelves. The rules for setting up mirroring with disks are the same for FAS systems and V-Series systems.
- When you set up SyncMirror software with array LUNs, you must follow the appropriate requirements because they are different from setting up SyncMirror software with disks.

Recovering from a SyncMirror Plex Failure

Part 1 of 4

If a plex fails, the surviving plex continues to serve data.

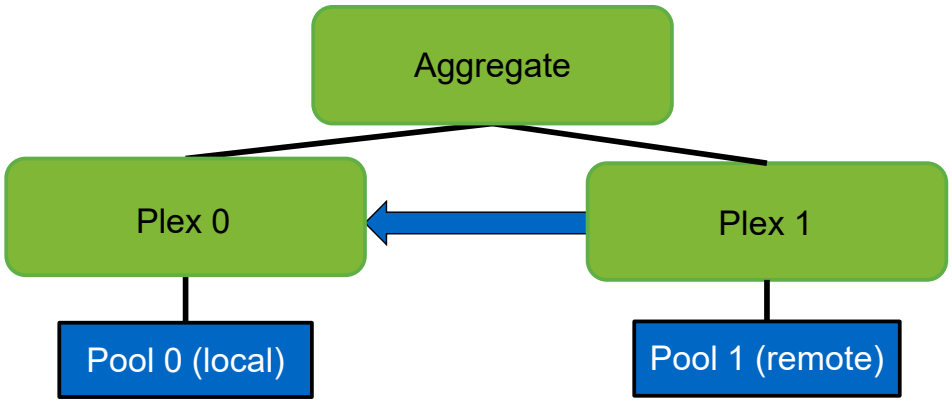


If the primary plex fails for any reason, the destination plex continues to serve data to the clients.

Recovering from a SyncMirror Plex Failure

Part 2 of 4

If the failed plex can be repaired, the two plexes resynchronize and reestablish the SyncMirror relationship.



If the failed plex can be repaired, when it is brought back online the system initiates resynchronization of the plex as part of online processing.

A mirrored aggregate can be configured with a resynchronization priority that is used to decide whether the aggregate can start a resynchronization operation or not.

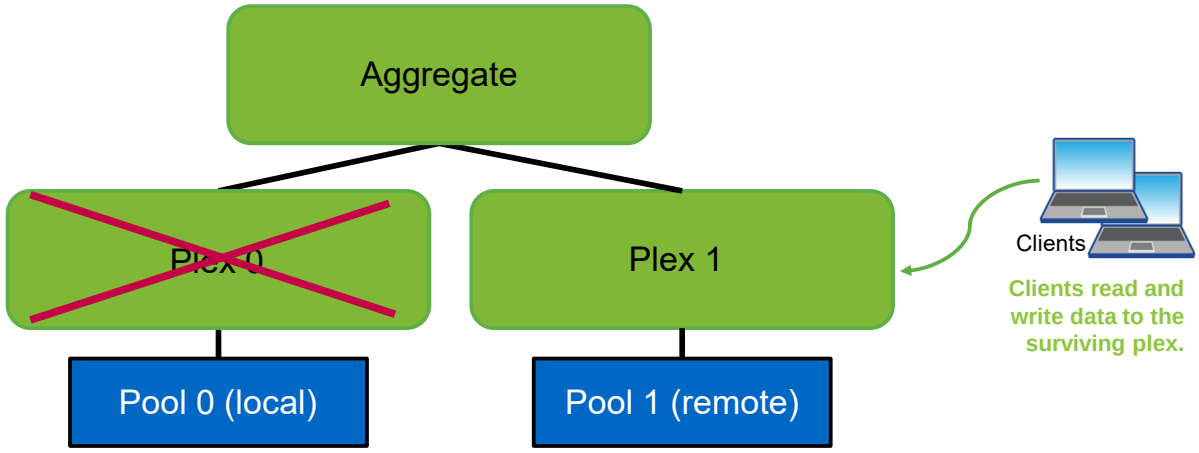
The valid values for this field are the following:

- High (fixed): ONTAP software aggregates always have this value set. These aggregates always start their resynchronization operation at the first available opportunity.
- High: This priority value starts to resynchronize the aggregates first.
- Medium: Resynchronization of these aggregates starts after all the system and data aggregates with “high” priority value have started.
- Low: These aggregates start resynchronization only after all the other aggregates have started.

Recovering from a SyncMirror Plex Failure

Part 3 of 4

If the failed plex cannot be repaired, destroy the failed plex by using the `storage aggregate plex delete` command.



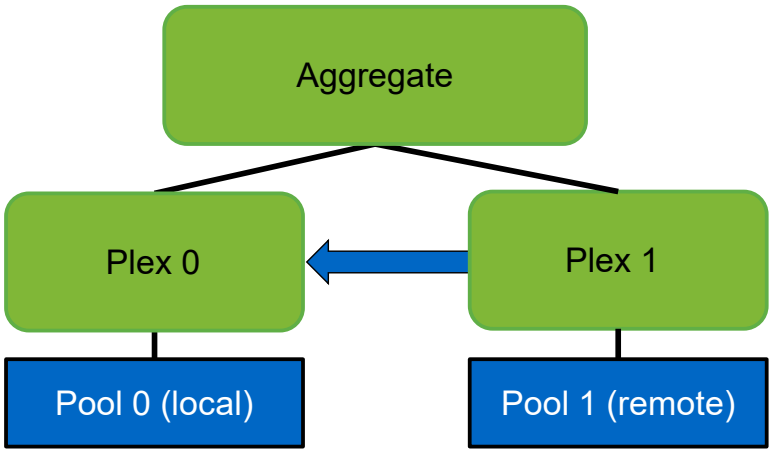
If the problem cannot be fixed, you can re-create the mirrored aggregate using a different set of disks or array LUNs.

The first step is to destroy the plex from the mirrored aggregate by using the `storage aggregate plex delete` command.

Recovering from a SyncMirror Plex Failure

Part 4 of 4

Re-create the mirrored aggregate using a different set of disks or array LUNs.



After the plex is destroyed, convert the aggregate to a mirrored aggregate by using the `storage aggregate mirror` command.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

Plex 0 in a mirrored aggregate has been damaged beyond repair. What would you do? (Select one.)

a. It is not possible to repair a mirrored aggregate when an entire plex is damaged.

b. Destroy plex 1, re-create the mirrored aggregate, and restore the data.

c. Replace all the failed disks and enable the plex to resynchronize.

d. Destroy the failed plex and re-create the mirrored aggregate using a new set of disks or LUNs.

ACTION: Try This Task

Using cluster svl-nau on your exercise kit, complete the following tasks:

- Enter the `storage aggregate mirror -aggregate svl01_data_001 -simulate` command.
- Enter the same command to simulate mirroring other aggregates in the cluster.

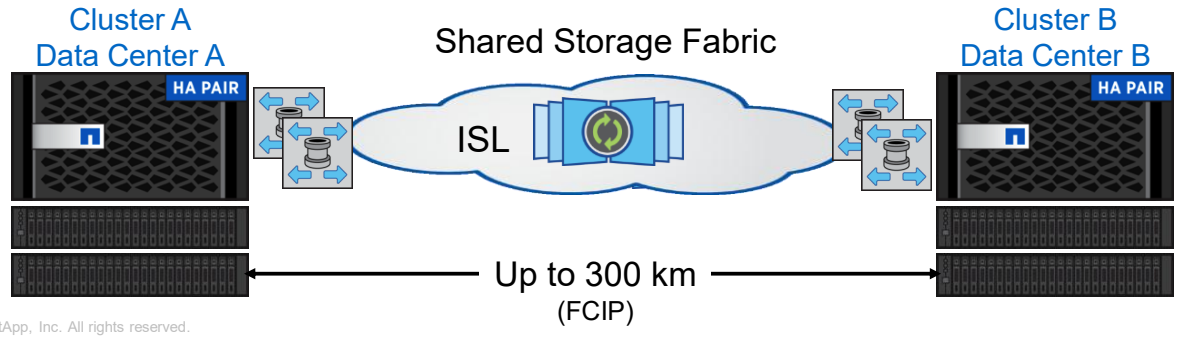
Answer these questions:

- Did the command output indicate a successful aggregate mirroring?
- Are any of the aggregates in svl-nau able to be mirrored?
- What would you do to enable successful mirroring of one of the svl-nau aggregates?

Lesson 2
MetroCluster Overview

MetroCluster Overview

- MetroCluster software has an independent cluster (one, two, or four nodes) at each site up to 200 km (FC) or 300 km (FCoIP) apart.
- FC and IP Inter-Switch Links (ISLs) and redundant fabrics connect the clusters and their storage.
- All storage is visible to all nodes.
- Switchover and switchback transfer the entire cluster workload between sites.
- High-availability (HA) failover manages nearly all planned and unplanned operations locally (four-node and eight-node configurations).



MetroCluster software protects data by using two separate clusters, one on each site, separated by up to 300 kilometers for FCoIP. The maximum distance between MetroCluster sites using FC is 200 kilometers.

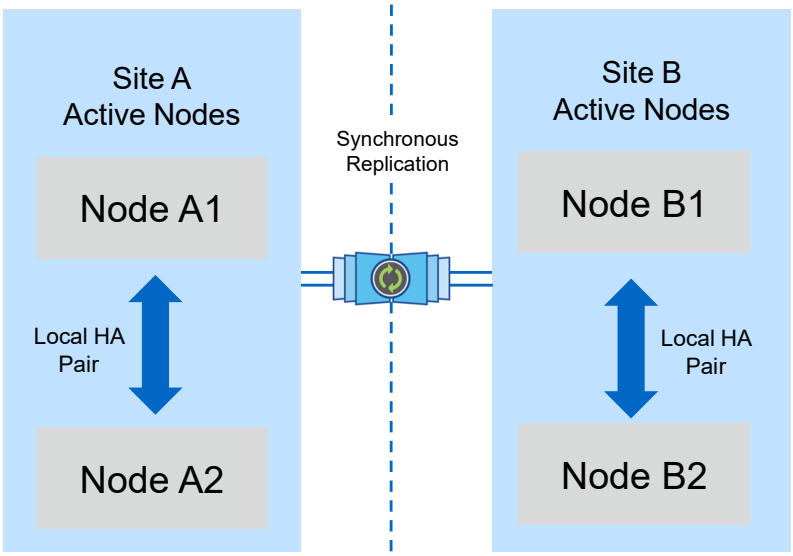
The clusters are connected through redundant fabrics. NVRAM is mirrored to the local high-availability (HA) partner and the disaster-recovery (DR) partner on the remote site. These partners share the ISL fabric as the storage replication.

Data is written to the primary copy and synchronously replicated to the secondary copy in the remote site.

MetroCluster configurations use SyncMirror software to provide data redundancy. Mirrored aggregates that use SyncMirror functionality provide data redundancy and contain volumes owned by the source and destination storage virtual machines (SVMs).

Writes are performed synchronously to both plexes and reads are performed from the local storage (by default), but reads can be configured to read from both local and remote storage. This flexibility can be useful when the two clusters are close enough that latency is not an issue, with the benefit that read performance can be increased.

Two Separate ONTAP Clusters



- Two ONTAP clusters synchronously replicate to each other.
- Best practice: Use a minimum of an HA pair at each site (four nodes total).
- Clients are served from all nodes in normal operation.
- Following are the available configurations:
  - Two-node (single node cluster at each site)
  - Four-node (an HA pair at each site)
  - Eight-node (two 4-node HA pairs at each site): NAS workloads only
- This arrangement supports All Flash FAS.

MetroCluster software consists of two ONTAP clusters that synchronously replicate to each other. They are two separate clusters, not a single cluster separated by some distance.

The minimum configuration for MetroCluster software is a disaster recovery group that consists of one HA pair at each site, for a total of four nodes (controllers).

Each cluster is an HA pair, so all nodes always serve clients.

MetroCluster Nondisruptive Operations

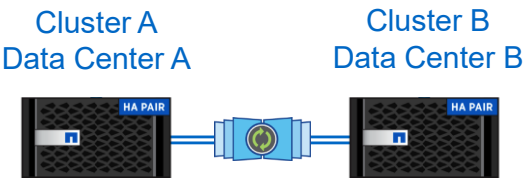
MetroCluster software extends nondisruptive operations beyond the data center.

ONTAP software provides nondisruptive operations (NDO) in the data center:

- Withstand component, node, or network failures
- Perform maintenance operations without disruption or downtime
- Perform technology refresh without disruption or downtime

ONTAP Software

MetroCluster software enables business continuity and continuous availability beyond the data center.

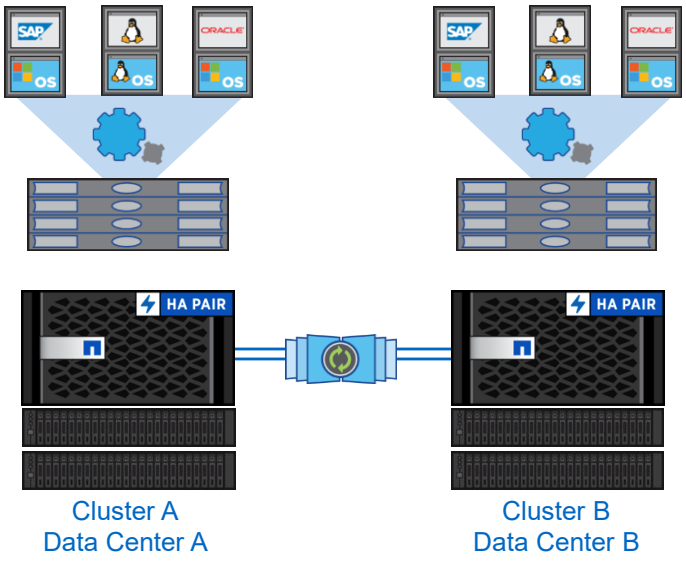


ONTAP Software
with MetroCluster Software

ONTAP software provides nondisruptive operations within a cluster and eliminates single points of failure. ONTAP software can withstand node, network, and disk failures, in addition to enabling administrators to perform maintenance without disruption or downtime.

MetroCluster software extends nondisruptive operations and continuous availability beyond the data center. MetroCluster software enables you to transparently fail over for planned maintenance and unplanned events without disruption of service.

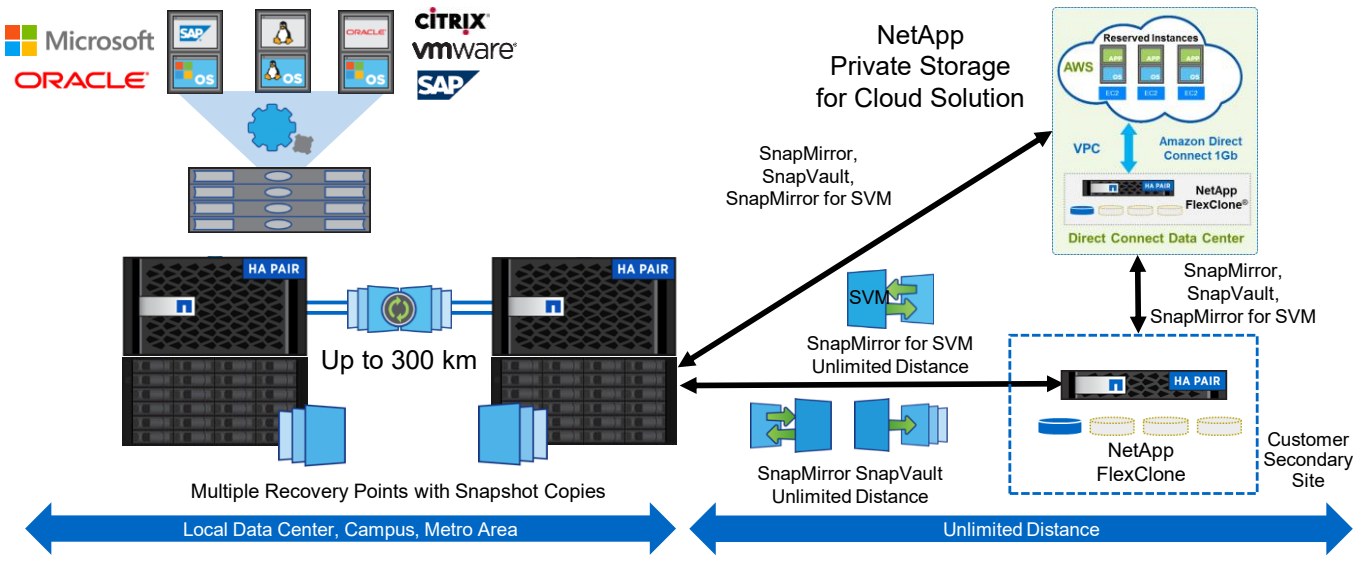
MetroCluster and Local HA Failover



- Operations are nondisruptive.
  - An ONTAP upgrade or platform refresh does not require an outage.
- Site switchover is required for only disasters and sitewide events.
  - All local component failures are managed locally.
  - Most workflows do not require site-level switchover.
- All nodes actively serve data to applications.

The two clusters in the peered network provide bidirectional disaster recovery. Each cluster can be the source and backup of the other cluster. Each cluster includes at least two nodes, which are configured as an HA pair. In the case of a failure or required maintenance within a single node's configuration, storage failover can transfer that node's operations to its local HA partner.

Protecting Data with MetroCluster Software



With MetroCluster software, customers can take data protection a step further.

Customers can achieve continuous availability and protection from local data center disasters with MetroCluster software. Customers can further enhance their disaster recovery protection with SnapMirror, which enables them to asynchronously replicate data over any distance. Data can be stored on disks for faster recovery or backed up to tape for archiving or near-line storage. This capability is sometimes referred to as three-way DR or zero data loss disaster recovery.

MetroCluster software can also be backed up remotely to disk and then tape using SnapVault. This option provides an even lower cost long-term archiving solution for data.

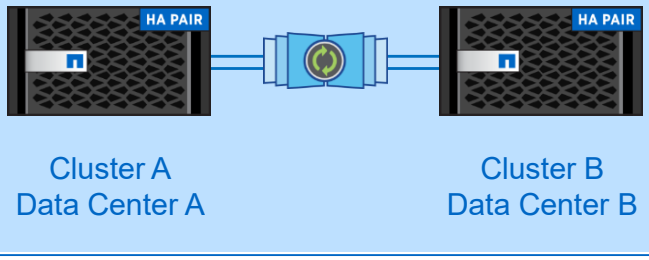
For a fully integrated business continuity solution with disaster recovery and backup, all three can be implemented. This flexibility provides the range of data storage and protection options needed to meet the most stringent enterprise demands.

MetroCluster Configurations

MetroCluster two-node and four-node configurations: unified storage

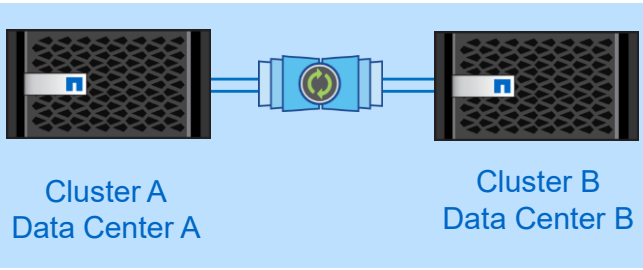
Four-node MetroCluster configuration: ONTAP 8.3.0 and later software

- Two-node (HA pair) cluster at each site
- Local high availability at each site
- Fabric configuration only
  Up to 200 km



Two-node MetroCluster configuration: ONTAP 8.3.1 and later software

- Single-node cluster at each site
- Stretch with optical SAS or bridge attached
  Up to 500 m
- Fabric configuration
  Up to 300 km



There are three basic MetroCluster configurations: two-node, four-node, and eight-node.

In the four-node configuration, a two-node HA pair cluster is at each data center. The HA pair provides redundancy and failover for localized failures in the cluster. The four-node configuration is supported in only a fabric configuration.

In the two-node configuration, a single node cluster is at each data center. In the case of local failure on the cluster, failover is given to the MetroCluster remote partner node. The two-node configuration can be either a fabric or stretch configuration.

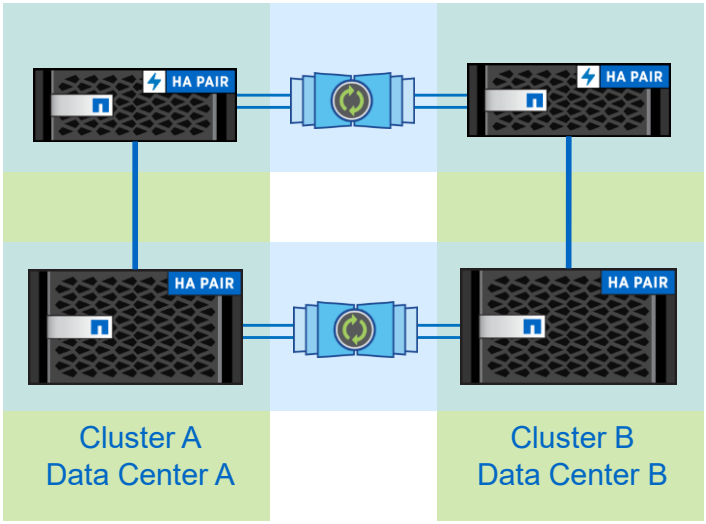
Eight-Node MetroCluster Configuration

Eight-node MetroCluster configuration (NAS only)

- Four-node (two HA pair) cluster at each site
- HA pairs replicated to respective pair at secondary site
- Fabric configuration only
  Up to 300 km (FCoIP); up to 200 km (FC)

Benefits

- Optimize cluster configuration.
- Mix All Flash FAS and FAS nodes and controller models.
- Nondisruptively move data between nodes in cluster to load-balance or service (changes are instantly replicated).



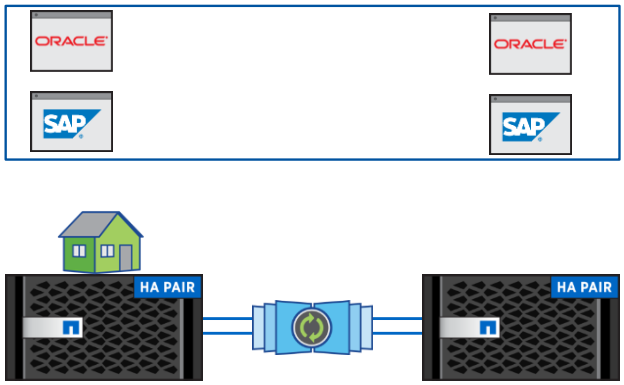
The eight-node configuration is deployed with two 4-node clusters at each site.

Controllers in the cluster do not have to be of the same model or the same media. However, each HA pair in a cluster is mirrored to the respective HA pair of the same configuration on the secondary site.

Benefits include data mobility, serviceability, and scale within the MetroCluster environment. Because you can mix controller types, you can incorporate both all solid-state drive (SSD) configurations with All Flash FAS and hybrid configurations with FAS in each cluster for flexibility and cost management.

Unmirrored Aggregates

- Mirroring is enabled or disabled at the aggregate granularity.
- Select aggregates to mirror or not mirror.
- Mix critical (RPO=0) and noncritical workloads in a single MetroCluster configuration.
- Supported on all two-node, four-node, and eight-node MetroCluster configurations

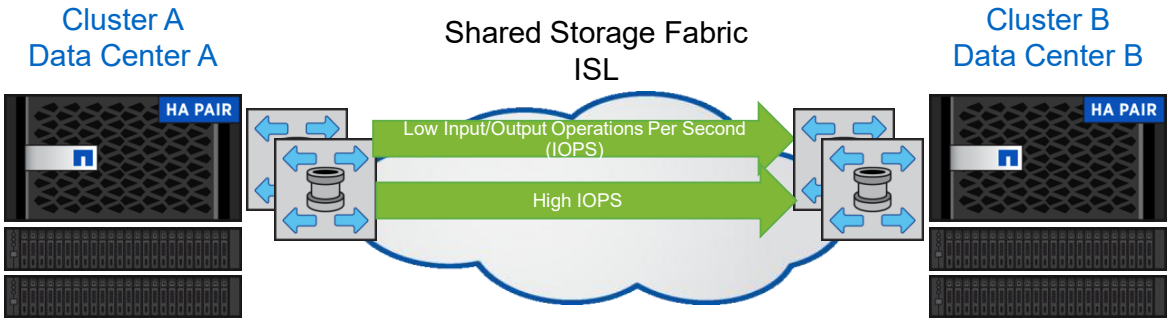


Example: Oracle and SAP data is synchronously replicated, and the home directory data is not replicated.

An extra feature with MetroCluster software in ONTAP 9 software includes the ability to select which aggregates you want to mirror and which ones you do not want to mirror. You can now share high priority and low priority workloads on the same MetroCluster configuration but protect (via synchronous replication) only the highest priority data.

Node-Level QoS

- Beginning with ONTAP 9.0 software, node-level Quality of Service (QoS) has been added to support MetroCluster operation.
- This functionality reduces node outage by prioritizing the I/O operations needed to complete a disaster-recovery operation, such as switchover or switchback.

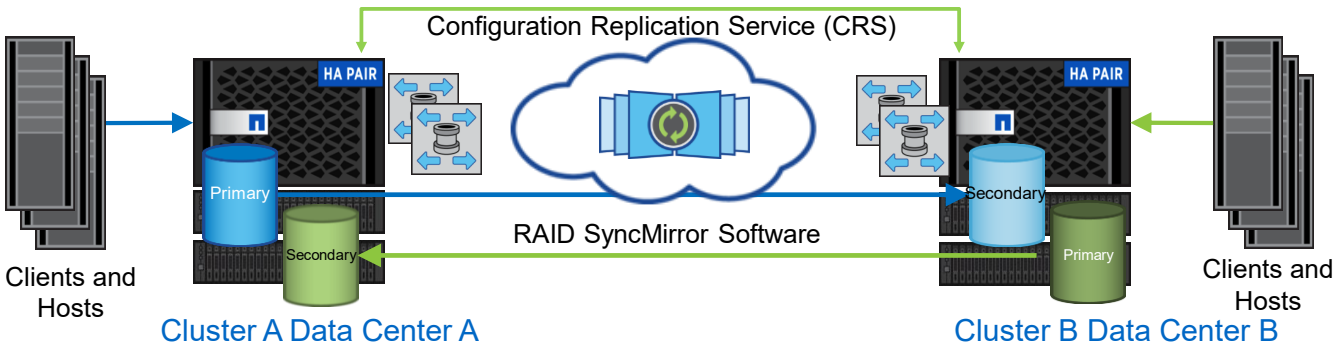


Quality of service (QoS) can be used in MetroCluster configurations to extend its typical use cases in an ONTAP cluster. QoS policies can be dynamically applied and modified as necessary.

Some examples for using QoS in MetroCluster environments are the following:

- In normal operation, when both clusters are active, QoS policies can be applied if periods of high traffic over the ISLs are observed. Limiting the application I/O necessarily lowers the ISL traffic for disk and NVRAM replication and prevents temporary overloading of the ISLs.
- When the configuration is running in switchover mode, fewer system resources are available because only half the nodes are active. Depending on the headroom applied to the system sizing, the reduction in available resources could affect client and application workloads.
- QoS policies can be configured to apply a ceiling (input/output operations per second [IOPS] or throughput) to noncritical workloads to provide more resource availability to critical workloads. The policies can be disabled after switchback when normal operation is resumed.

Active-Active Configuration



- Each site serves data to local clients and hosts and acts as secondary to the other site.
- Identity is preserved during switchover.
- The client and host network must span both sites.
- Writes are mirrored synchronously to both plexes.
- Root aggregates must be mirrored, whereas data aggregates can be mirrored or unmirrored.
- Cluster configuration is replicated through the cluster peering network using configuration replication service (CRS).

In an active-active configuration, both clusters serve data to local clients and hosts. Each cluster acts as the secondary to the other site.

When a switchover occurs for planned or unplanned operations, the identity is maintained. MetroCluster software preserves the identity of the storage access paths (IP address, LUN ID, worldwide port name [WWPN], TGID, and so on). Therefore, a spanned network for IP and SAN is required so they are accessible after switchover.

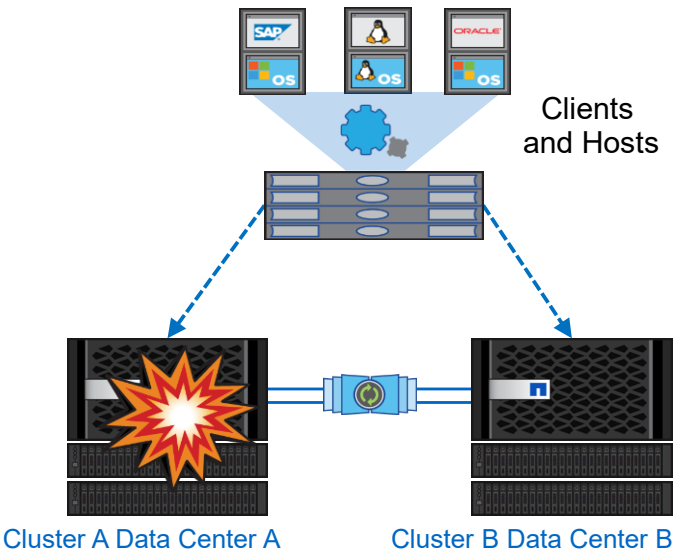
The network must span the clusters in both data centers. You could use a Layer-2 Ethernet spanned network or a SAN fabric spanning both sites. SCSI initiators are connected to both MetroCluster instances using a front-end SAN fabric that spans across both sites.

MetroCluster software also supports an active-passive configuration. In an active-passive configuration, the passive node does not have any primary plexes and serves as the secondary for the active node. The active node serves data to local clients and hosts. All other operations of MetroCluster software work the same. Because the configuration is in an active-passive configuration, you cannot place any workloads on the passive node.

MetroCluster software in ONTAP software cannot provide different IP addresses after switchover. Formerly, Data ONTAP operating in 7-Mode used the rc file to provide different IP addresses after switchover.

Planned Switchover

- Clients transparently fail over to the remote site, which enables the following:
  - Disaster-recovery testing
  - Tech refresh
  - Scheduled maintenance
  - Disaster avoidance
- Use one command to switch over from site A to site B.
  `metrocluster switchover`
- Verify the MetroCluster configuration before switchover.
  `metrocluster check, switchover -simulate`
- Use three commands to switch back.
  - `metrocluster heal –phase aggregates`
  - `metrocluster heal –phase root-aggregates`
  - `metrocluster switchback`



If you want to test the MetroCluster functionality or to perform planned maintenance, you can perform a negotiated switchover in which one cluster is cleanly switched over to the partner cluster. You can then heal and switch back the configuration.

Unplanned Switchover

Power Failure

Hardware or Software Error

Flood

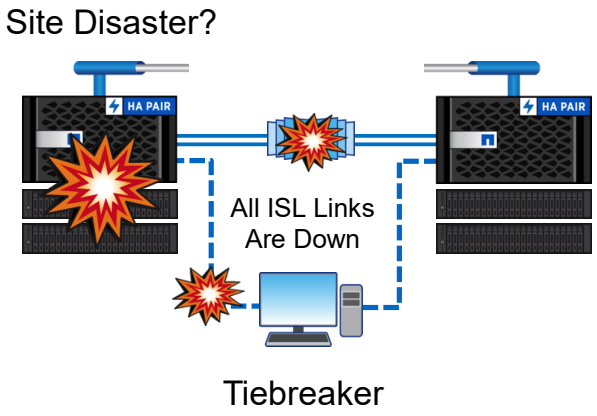
Earthquake

- Synchronous replication preserves your data.
- Clients transparently fail over to the remote site.
- Switchover is not automatic.
  Requires a `switchover` command: CLI or Tiebreaker.
- NetApp MetroCluster Tiebreaker
  Monitors, detects, and alerts if there is a disaster

In an unplanned outage or natural disaster (such as power failure, hardware or software malfunction, flood, or earthquake), synchronous replication assures zero data loss and transparent failover of clients to the remote data center.

MetroCluster Tiebreaker Software

- NetApp MetroCluster Tiebreaker
  - Observer mode (default)
  - Monitors, detects, and alerts if there is a disaster
  - Sends SNMP alerts if there is a disaster
  - Requires a policy-variance request (PVR) for automatic switchover
  - Switchover within client or host recovery time objective (RTO) <= 120 seconds
  - Packaged as a Red Hat Java application running on a third site with connectivity to both clusters
  - Available for download from the NetApp Support site
- Switchover not automatic
  - Site disaster or lost connectivity
  - Possible split-brain scenario
  - Requires switchover command

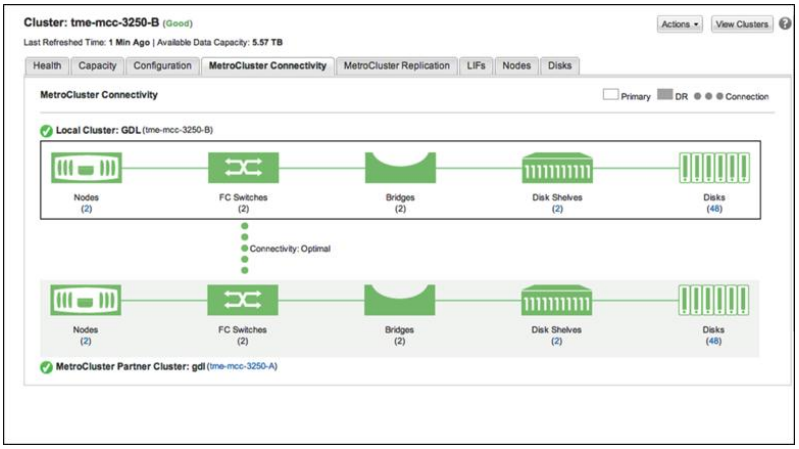


The MetroCluster Tiebreaker software provides detection, monitoring, and alerting in the event of an outage. The Tiebreaker does not provide automatic switchover by default. The Tiebreaker can be configured to perform automatic switchover, but it requires a policy-variance request (PVR) to make sure that you understand the caveats.

The Tiebreaker has built-in notifications if it cannot reach the clusters or cannot perform a switchover. In the case of temporary ISL downtime, clusters continue to serve data locally and resync when the links are restored.

Monitoring and Managing MetroCluster Software

- OnCommand Unified Manager 6.4 and later
  - Detailed monitoring and reporting
- OnCommand Performance Manager (OPM) 2.1 and later
  - Monitors cluster performance
- Configuration Advisor
  - Performs configuration verification checking
- Golden configuration files for Cisco and Brocade switches
  - Including planned Cisco MDS 9250i fibre switch (FCIP)



You can use ONTAP MetroCluster commands, OnCommand Unified Manager, and OnCommand Performance Manager to monitor the health of various software components and the state of MetroCluster operations.

Configuration Advisor is a configuration validation and health check tool. It can be deployed at both secure sites and nonsecure sites for data collection and system analysis. Configuration Advisor collects data, analyzes the data, and creates PDF, Word, and Excel reports on the system configuration summary and health check results. It also sends back a Configuration Advisor AutoSupport with all the collected data and metrics to NetApp over HTTP. After you run the Configuration Advisor, be sure to review the tool's output and follow the recommendations in the output to address any issue discovered.

Preconfigured files are available to quickly load Brocade and Cisco switches with the proper configuration.

ACTION: Topic for Discussion

You want to install the MetroCluster Tiebreaker software. Where would be the optimal location to install and configure the software?

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

You've installed the MetroCluster Tiebreaker software in observer mode. A disaster has taken site A down. What would you do? (Select one.)

a. Use the metrocluster switchover command to initiate the switchover of storage and client access to site B.

b. Nothing. The Tiebreaker software performs automatic switchover.

c. Turn off the SAN switches to prevent a split-brain scenario.

d. Use the metrocluster check command to verify that switchover is possible.

References

- *ONTAP 9.0 Release Notes*
- *ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology*
- *ONTAP 9.0 Commands: Manual Page Reference*
- *ONTAP 9.0 Fabric-attached MetroCluster Installation and Configuration Guide*
- *ONTAP 9.0 MetroCluster Management and Disaster Recovery Guide*
- *ONTAP 9.0 Stretch MetroCluster Installation and Configuration Guide*
- *NetApp Technical Report TR-4375: MetroCluster for Clustered Data ONTAP 8.3.2*
- *NetApp University course: ONTAP MetroCluster Installation*

Module Review

This module focused on enabling you to do the following:

- Identify the components involved with SyncMirror software
- Explain the SyncMirror disk arrangement into pools and plexes
- Describe the basic operation of MetroCluster software
- Explain how MetroCluster software protects data in normal operation
- Describe how to perform the MetroCluster switchover, healing, and switchback processes

Module 7
NDMP and Tape Backup

About This Module

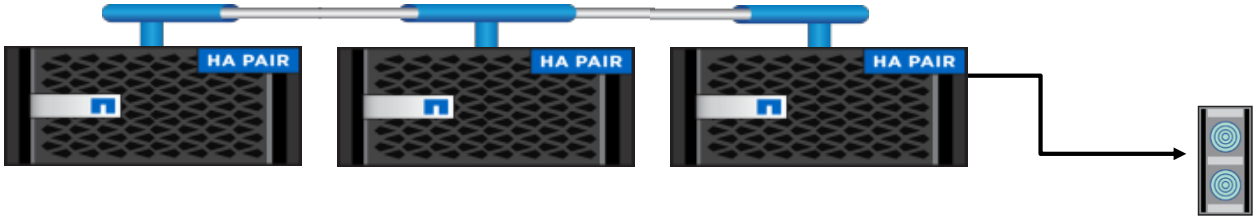
This module focuses on enabling you to do the following:

- Describe how ONTAP 9 software uses the NDMP and backup management software to move data from disk to tape
- Describe the three NDMP topologies
- Recognize the required NDMP configurations to prepare the cluster to communicate with backup management software
- Monitor NDMP-based operations from the ONTAP 9 CLI

Lesson 1
NDMP Fundamentals

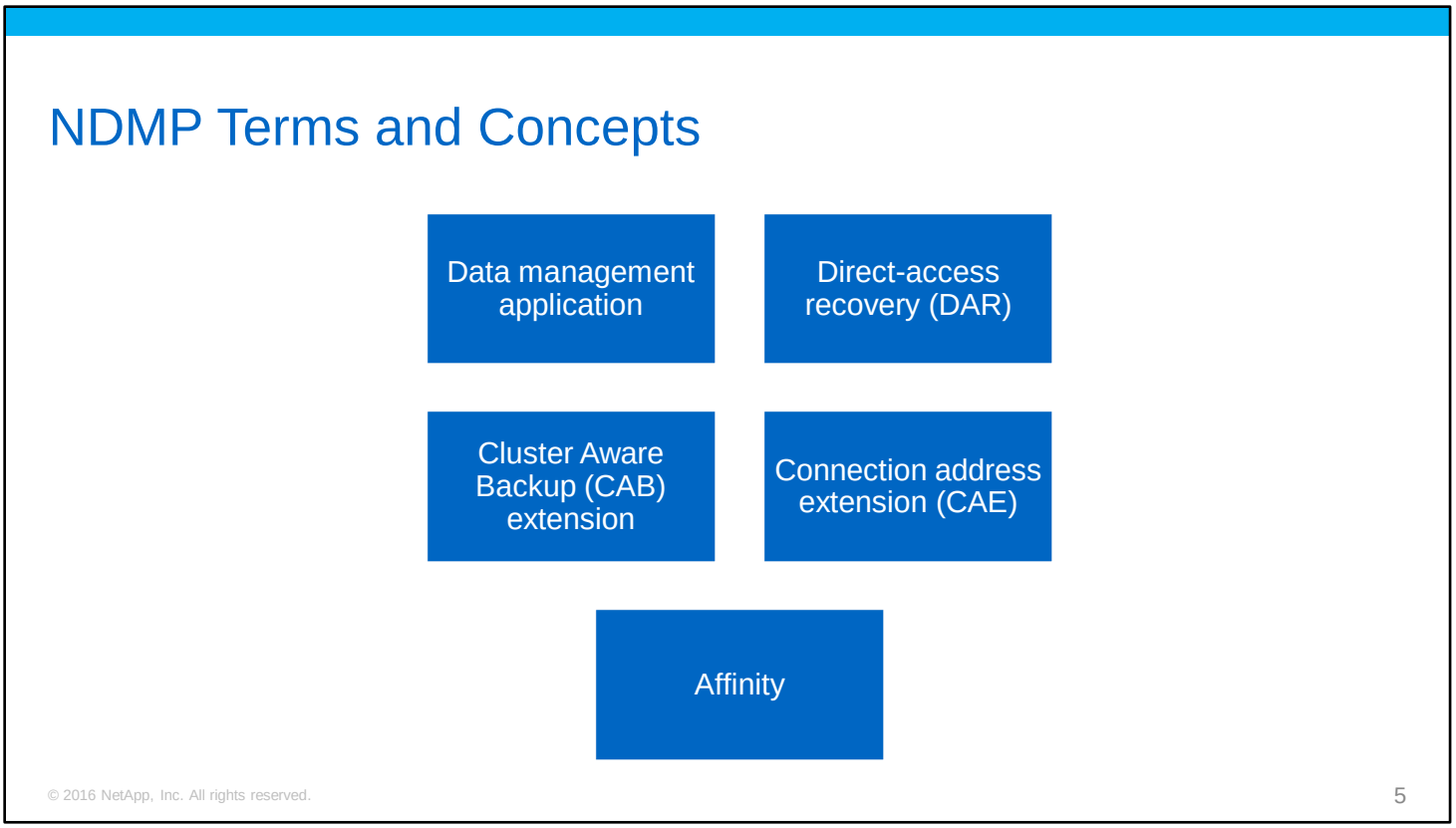
Introduction to NDMP Technology

- NDMP is an industry-standard protocol that can control backup, recovery, and data transfer between primary and secondary storage devices.
- All communications occur over TCP/IP or TCP/IP v6.
- NDMP provides low-level control of tape drives and media changers.



NDMP is an industry-standard protocol for controlling backup, recovery, and data transfer between primary and secondary storage devices, including storage systems and tape libraries.

Enabling the NDMP protocol on a NetApp storage system enables that storage system to communicate with NDMP-enabled backup applications.



Data Management Application

In the context of the NDMP, data management application refers to your backup application.

Direct-Access Recovery

DAR enables quick access to the secondary media during a recovery operation. In Data ONTAP 8.3 and later, enhanced DAR functionality is enabled by default. Enhanced DAR enables directory DAR and DAR of files with NT streams. You can enable or disable enhanced DAR in both node-scoped and storage virtual machine (SVM)-scoped NDMP modes.

CAB Extension

The CAB extension is an NDMP v4 protocol extension. This extension enables the NDMP server to establish a data connection on a node that owns a volume. This extension also enables the backup application to determine whether volumes and tape devices are on the same node in a cluster.

To enable the NDMP server to identify the node that owns a volume and to establish a data connection on such a node, the backup application must support the CAB extension. The CAB extension requires the backup application to inform the NDMP server about the volume to be backed up or restored before the application establishes the data connection. This requirement enables the NDMP server to determine which node hosts the volume and to appropriately establish the data connection.

When the backup application supports the CAB extension, the NDMP server provides affinity information about volumes and tape devices. Using this affinity information, if a volume and tape device are on the same node in a cluster, the backup application can perform a local backup instead of a three-way backup.

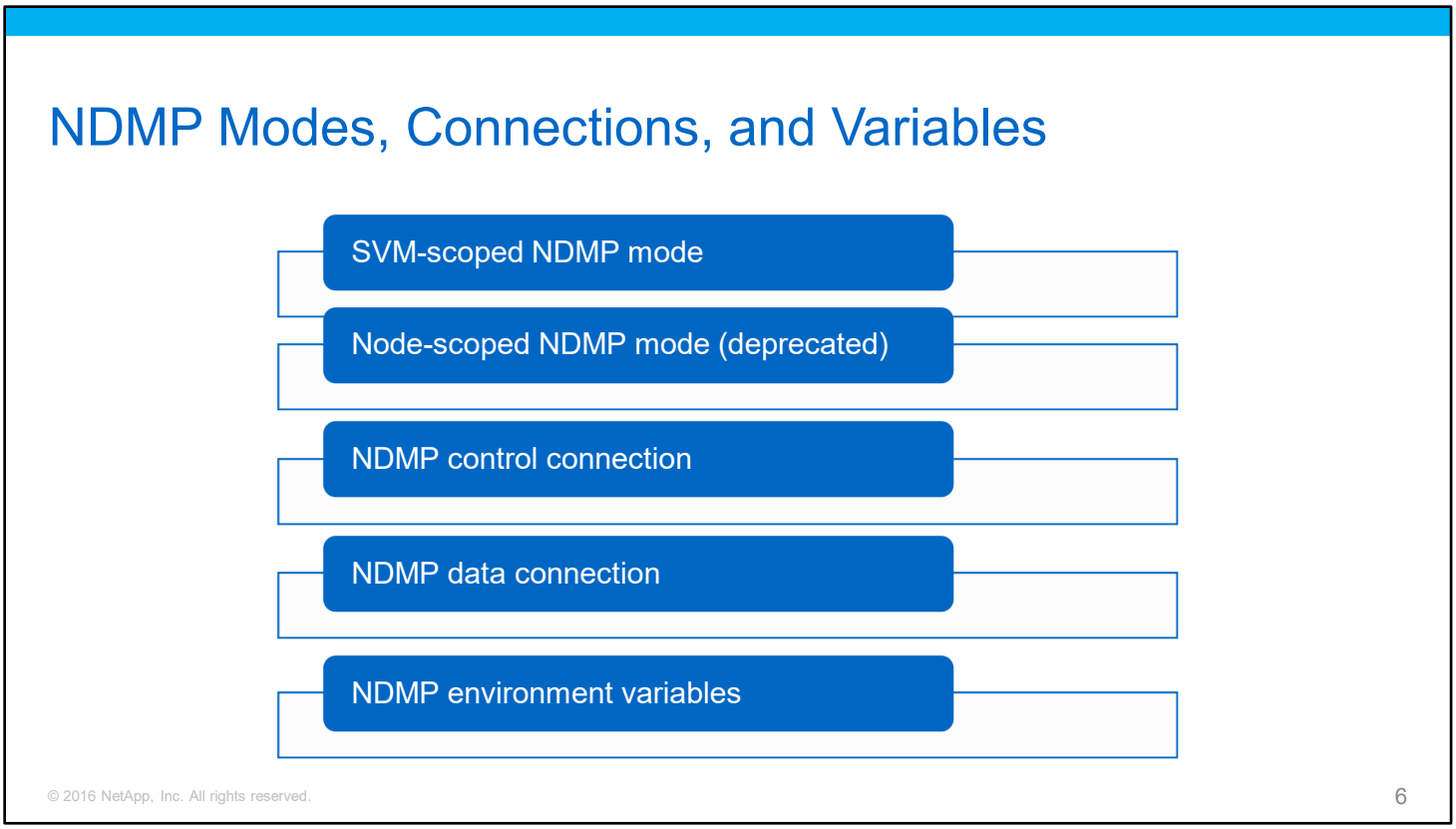
Connection Address Extension

The CAE is used for IPv6 support.

Affinity

When the backup application supports the CAB extension, the NDMP server provides unique location information about volumes and tape devices. Using this affinity information, if a volume and a tape device share an affinity, the backup application can perform a local backup instead of a three-way backup.

If the volume moves from Node 1 to Node 2, affinity information about the volume and tape device changes. Therefore, for a subsequent backup, the data management application performs a three-way NDMP backup operation. This backup ensures continuity of the backup policy for the volume, irrespective of the node to which the volume is moved.



SVM-Scoped NDMP Mode

SVM-scoped NDMP mode enables you to back up and restore all volumes that are hosted across different nodes in an SVM, as long as the backup application supports the CAB extension. Your backup application can perform a local backup or restore operation instead of a three-way restore operation if both these conditions are true:

- Your backup application supports the CAB extension.
- A volume and tape device share an affinity.

NOTE: The NDMP control connection can be established on a data or admin logical interface (LIF) only if the NDMP service is enabled on the SVM that owns the LIF.

Node-Scoped NDMP Mode

Node-scoped NDMP mode enables you to perform tape backup and restore operations at the node level. You must establish the NDMP control connection on a logical interface (LIF) that is hosted on the node that owns the volume or tape devices.

NOTE: Node-scoped NDMP mode is deprecated, and it will be removed in a future major release of ONTAP software.

SVM-Scoped NDMP Mode and ONTAP Upgrades or Installations

An upgrade of Data ONTAP software from 8.1 to 8.3 causes NDMP to follow the node-scoped behavior. You can explicitly disable node-scoped NDMP mode, so that tape backup and restore operations are performed in SVM-scoped NDMP mode.

A new installation of Data ONTAP 8.3 software causes NDMP to follow SVM-scoped mode by default. You can perform node-scoped NDMP operations if you explicitly enable node-scoped NDMP mode.

NDMP Control Connection

The NDMP control connection is used to manage NDMP backup and restore requests and replies.

NDMP Data Connection

The NDMP data connection is used only to transfer data.

NDMP Environment Variables

NDMP environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system.

Typically, the backup application sets the environment variables automatically. However, to support unique circumstances, the backup administrator can set some environment variables manually. A backup administrator rarely specifies environment variables. However, you might want to change the value of an environment variable to characterize or work around a functional or performance problem. Many backup applications provide a means to override or modify environment variables or to specify additional environment variables. For information, see your backup application documentation.

ONTAP software supports environment variables that have an associated default value. However, you can manually modify these default values.

For a complete list of environment variables that are supported for SMTape and dump operations, see the *Clustered Data ONTAP 8.3 Data Protection Tape Backup and Recovery Guide*.

Managing SVM-Scoped NDMP

The backup application supports CAB.

LIF Type	Volumes Available for Backup and Restore	Type Devices Available for Backup and Restore
Node-Management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	All volumes that belong to the SVM that hosts the data LIF	None
Cluster-Management LIF	All volumes in the cluster	All tape devices in the cluster
Intercluster LIF	All volumes in the cluster	All tape devices in the cluster

In SVM-scope, NDMP is “cluster-aware” and uses NDMP protocol extensions to establish efficient data connections throughout the entire cluster. When CAB is being used, an NDMP connection can be made to any node in the cluster and have all cluster resources (all volumes and all tape devices) available. Depending on the LIF type, there are still some limitations with NDMP and CAB. The CAB extension is available in only ONTAP 8.2 and later software and requires the backup application to support NDMP and the CAB extension. Not all third-party vendors support NDMP extensions.

Managing SVM-Scoped NDMP

The backup application does not support CAB.

LIF Type	Volumes Available for Backup and Restore	Type Devices Available for Backup and Restore
Node Management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	Only volumes that belong to the SVM hosted by a node that hosts the data LIF	None
Cluster Management LIF	All volumes hosted by a node that hosts the cluster-management LIF	None
Intercluster LIF	All volumes hosted by a node that hosts the intercluster LIF	Tape devices connected to the node hosting the intercluster LIF

The NDMP scope and LIF types also affect enabling and controlling NDMP debugging.

For more information about NDMP debugging in both node-scope and SVM-scope, see the following articles:

1014597: How to configure NDMP authentication in the ‘Vserver-scope’ mode

1013923: How to enable NDMP debug logging on a Data ONTAP 8.1.x Cluster-Mode storage system

1014439: How to enable NDMP debug logging on Vserver-scoped Vservers in clustered Data ONTAP 8.2

NDMP Backup Models

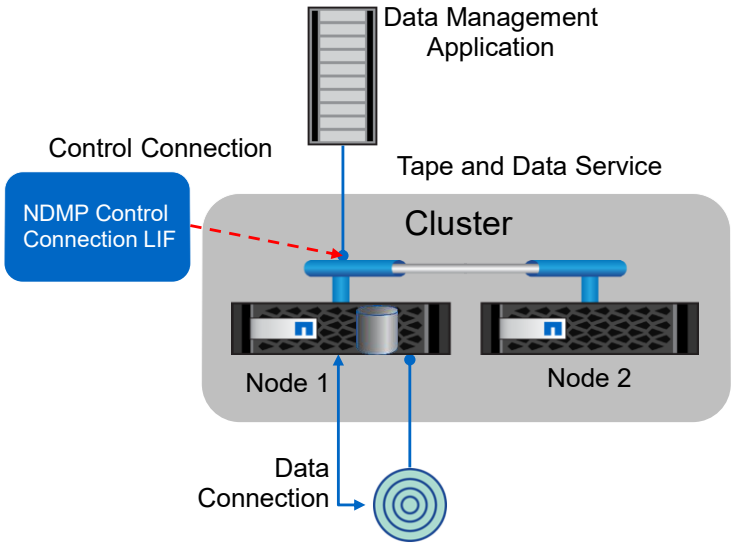
ONTAP software supports three models for NDMP backups:

- Direct (local)
- Indirect (remote)
- Three-way

The backup model is important because it defines “who is responsible for what.”

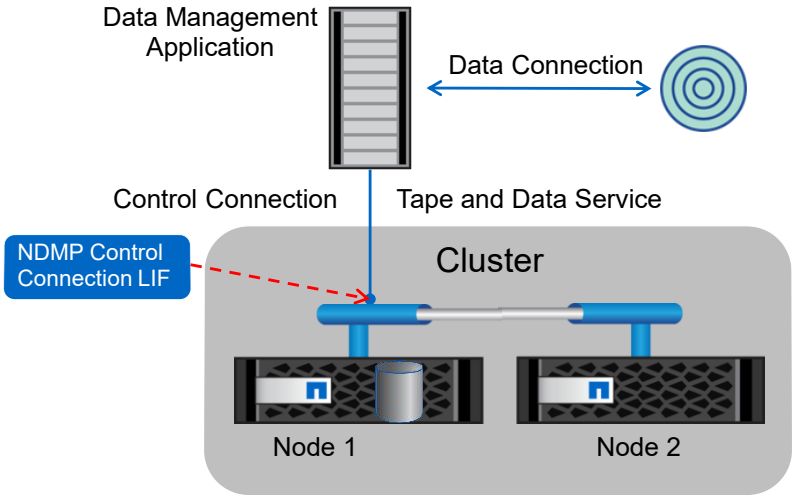
The following pages explore the three configuration models for NDMP backup of data.

Direct (Local) NDMP Backup



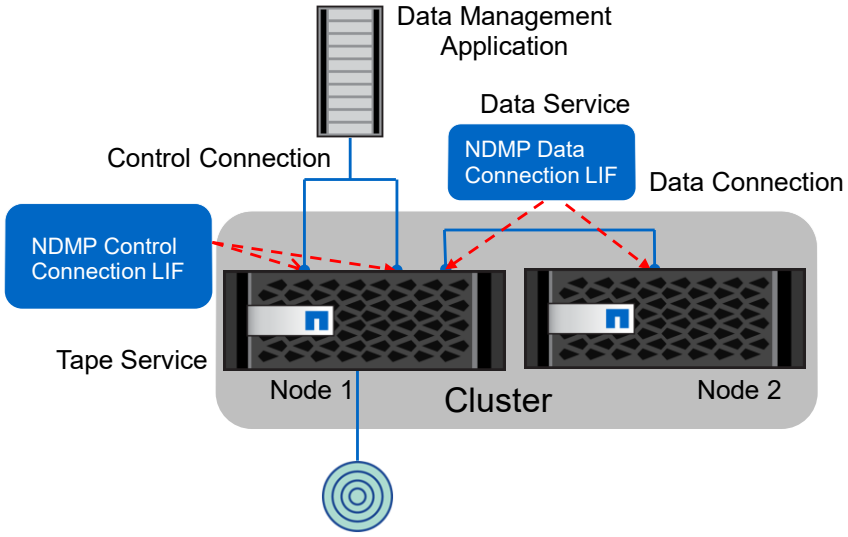
With a direct NDMP backup configuration, the tape drive is directly connected to the node where the data resides.

Indirect (Remote) NDMP Backup



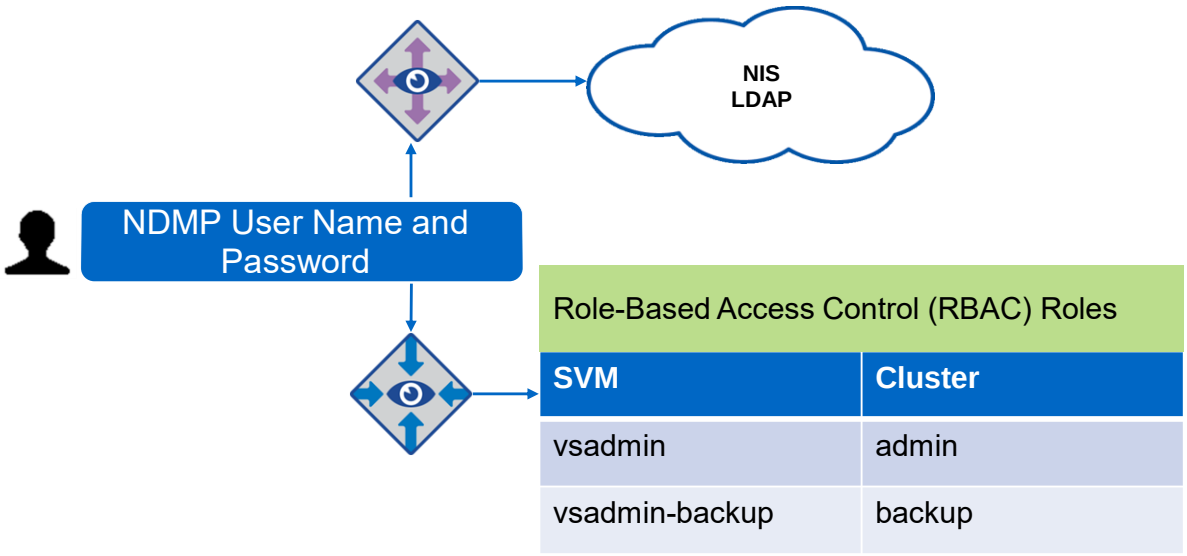
An indirect NDMP configuration uses the tape device connected to the device that runs the data management application.

Three-Way NDMP Backup



In a three-way NDMP configuration, the tape drive and the data management application have connections to one cluster node, but the data being backed up is on a different cluster node.

User Authentication



In node-scoped NDMP mode, both authentication methods are enabled by default: challenge and plaintext. You can disable plaintext, but you cannot disable challenge. In the plaintext authentication method, the login password is transmitted as clear text.

In SVM-scoped NDMP mode, the default authentication method is challenge. You can select to enable or disable plaintext or challenge. However, one authentication mode must be enabled.

ACTION: Take a Poll

What would you do?

Duration: 5 minutes

Your instructor begins a polling session.

- Questions appear in the polling panel.
- You answer the questions.
- After you answer the final question, you click the **Submit** button.

Your instructor ends the polling session.

- The correct answers are displayed.
- You compare your answers to the correct answers.

Your instructor discusses the answers.

Raise your hand to ask a question or make a comment.

Poll Question

What would you do?

You want to back up and restore all volumes across all nodes in an SVM. The data management application supports the NDMP protocol. What would you do? (Select two.)

a. Enable node-scoped NDMP mode.

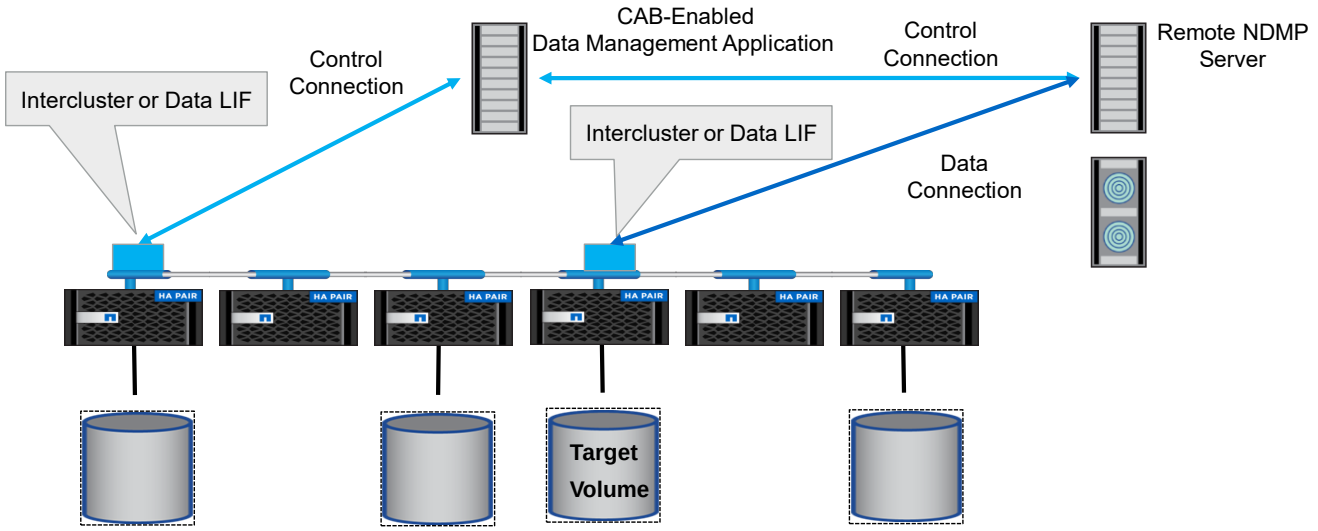
b. Configure a direct NDMP backup connection to every node in the cluster.

c. Enable SVM-scoped NDMP mode.

d. Make sure that the data management application supports the CAB extension.

Lesson 2
NDMP Management

SVM-Aware NDMP



With ONTAP 9.0 software, you can select to perform tape backup and restore operations at the SVM level.

For NDMP to be aware of an SVM, the NDMP data management application software must be enabled with CAB extensions, and the NDMP service must be enabled on the SVM.

After the feature is enabled, you can back up and restore all volumes that are hosted across all nodes in the SVM. An NDMP control connection can be established on different LIF types. You can establish an NDMP control connection on any data or intercluster LIF that is owned by an SVM that is enabled for NDMP and that owns the target volume. If a volume and tape device share an affinity and the data management application supports the CAB extensions, the backup application can perform a local backup or restore operation. Therefore, you do not need to perform a three-way backup or restore operation.

SVM-Scoped NDMP Management Commands

Use This Command	To Do This Action
`vserver services ndmp on`	Enable NDMP service
`vserver services ndmp off`	Disable NDMP service
`vserver services ndmp show`	Display an NDMP configuration
`vserver services ndmp modify`	Modify an NDMP configuration
`vserver services ndmp version`	Display the default NDMP version
`vserver services ndmp status`	Display all NDMP sessions
`vserver services ndmp probe`	Display detailed information about all NDMP sessions

This chart provides a basic list of ONTAP NDMP commands.

SVM-Scoped NDMP Management

```
svl-nau::> vserver add-protocols -vserver svm_yellow -protocols
ndmp
```

Add NDMP to the list of protocols enabled to run on the SVM.

```
svl-nau::> vserver services ndmp on -vserver svm_yellow
```

Enable the NDMP service for the SVM.

```
svl-nau::> vserver services ndmp show
VServer         Enabled   Authentication type
--------------- --------- -------------------
svl-nau         false     challenge
svm_yellow      true      challenge
```

Check that NDMP is enabled for the SVM.

The NDMP protocol is first added to the SVM; then it is enabled. The `vserver add-protocols` command specifically adds the protocols listed in the command. Any protocols not included in the command syntax are still available for the SVM.

Use the `vserver services ndmp show` command to verify that NDMP is enabled for the SVM.

Additional SVM-Scoped NDMP Management Commands

Use This Command	To Do This Action
`vserver services ndmp kill`	Terminate a specified NDMP session
`vserver services ndmp kill-all`	Terminate all NDMP sessions
`vserver services ndmp generate-password`	Generate the NDMP password
`vserver services ndmp extensions show (advanced)`	Display the NDMP extension status
`vserver services ndmp extensions modify (advanced)`	Modify (enable or disable) the NDMP extension status
`vserver services ndmp log start (advanced)`	Start logging for the specified NDMP session
`vserver services ndmp log stop (advanced)`	Stop logging for the specified NDMP session

This chart provides more advanced ONTAP NDMP commands.

ACTION: Try This Task

Using cluster svl-nau on your exercise kit, complete these tasks:

- Enter the `system services ndmp ?` command.
- Enter the `vserver services ndmp ?` command.

Answer these questions:

- How many commands are deprecated in the system services ndmp command syntax?
- How many commands are deprecated in the vserver services ndmp command syntax?

References

- *ONTAP 9.0 Release Notes*
- *ONTAP 9.0 Data Protection Using SnapMirror and SnapVault Technology*
- *ONTAP 9.0 Commands: Manual Page Reference*
- *ONTAP 9.0 Data Protection Tape Backup and Recovery Guide*
- *ONTAP 9.0 NDMP Configuration Express Guide*

Module Review

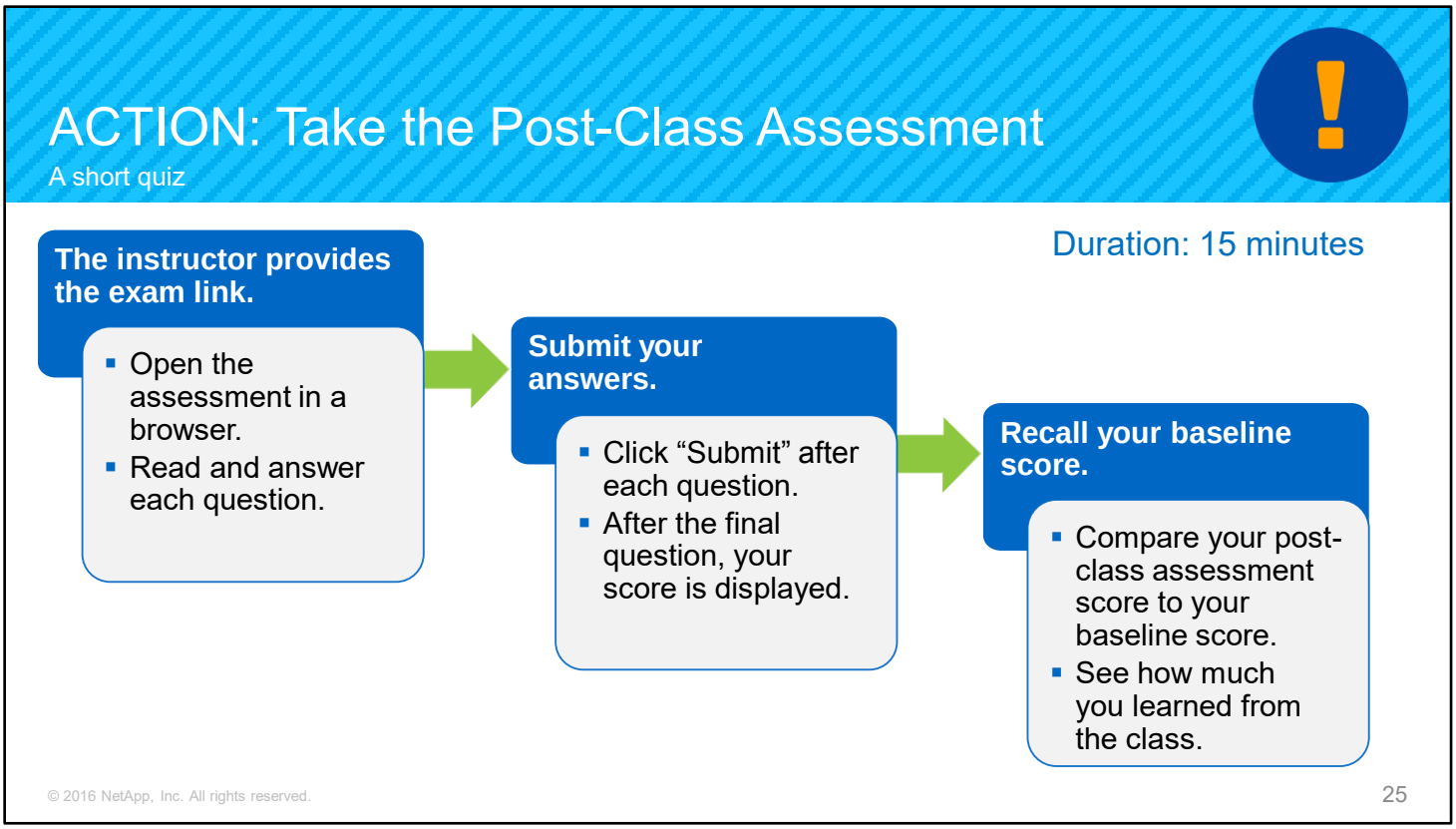
This module focused on enabling you to do the following:

- Describe how ONTAP 9 software uses the NDMP and backup management software to move data from disk to tape
- Describe the three NDMP topologies
- Recognize the required NDMP configurations to prepare the cluster to communicate with backup management software
- Monitor NDMP-based operations from the ONTAP 9 CLI

ACTION: Provide Feedback

Please take a few minutes to complete the survey for this course.

Your feedback is important for ensuring the quality of NetApp courses. Your instructor will give you instructions about how to find the survey for this class and about how to use the survey web site.



To measure your new knowledge of course topics, take the post-class assessment. You access the assessment via the link that is provided.

https://www.brainshark.com/netapp/DPA_posttest

You can compare your pre-assessment score with your post-assessment score to measure how much you have learned. All scores are private.

Thank You