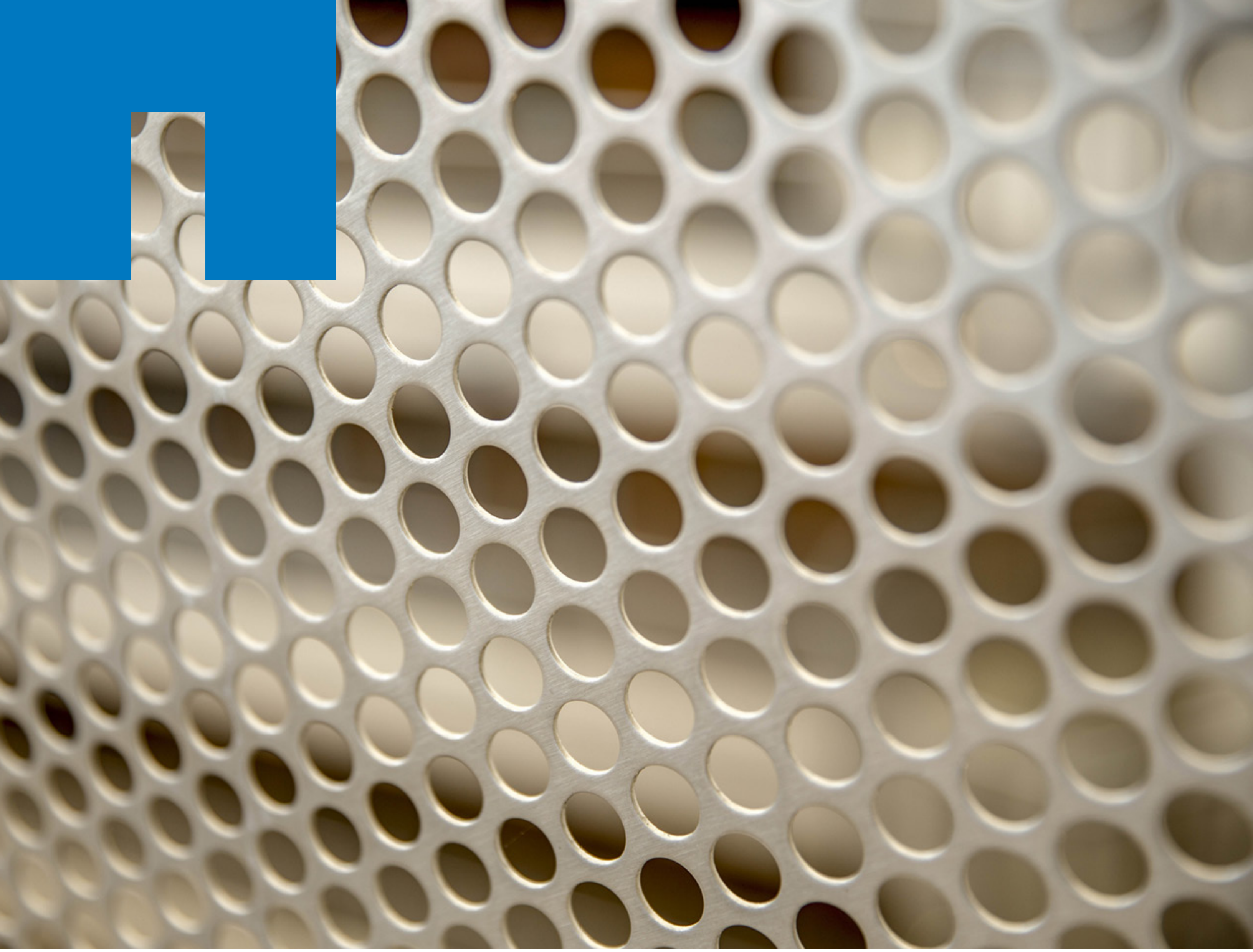


NETAPP UNIVERSITY

ONTAP Cluster Administration

Student Guide
Content Version 4

NetApp®

NETAPP UNIVERSITY

ONTAP Cluster Administration

Student Guide

Course ID: STRSW-ILT-ONTAPADM
Catalog Number: STRSW-ILT-ONTAPADM-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://mysupport.netapp.com/.

COPYRIGHT

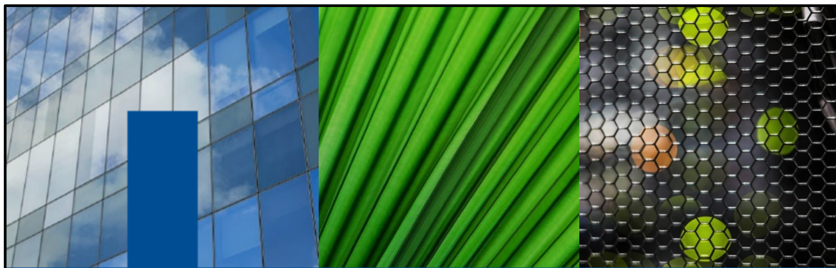
U.S. GOVERNMENT RIGHTS

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, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TABLE OF CONTENTS



Welcome!

ONTAP Cluster Administration

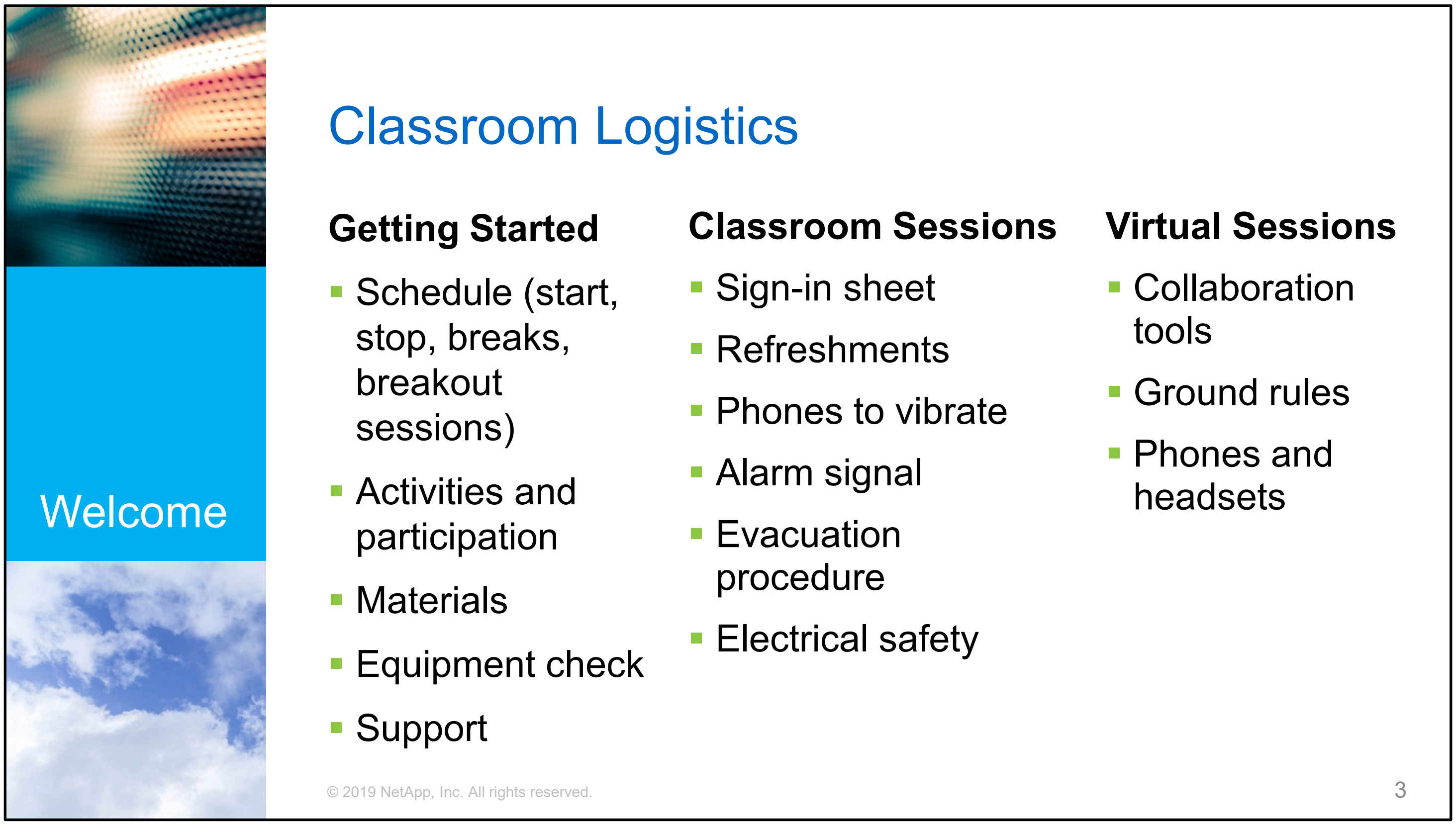
- Classroom only: Sign in.
- Be sure that you have downloaded your Student Guide and Exercise Guide.
- Virtual Session: Test your headset and microphone.
- Virtual Session: Provide yourself with two screens.

NetApp

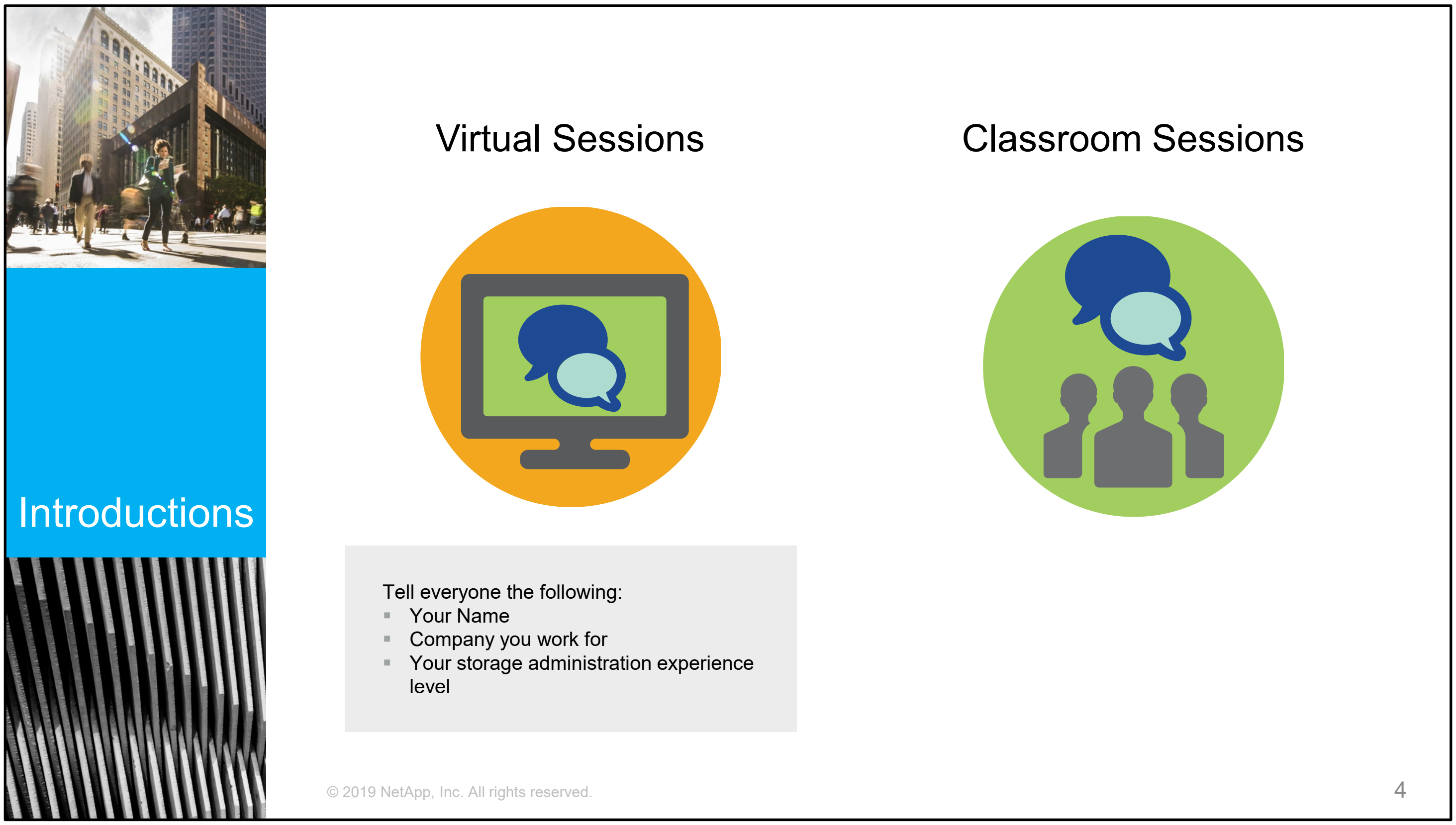
1

ONTAP Cluster Administration

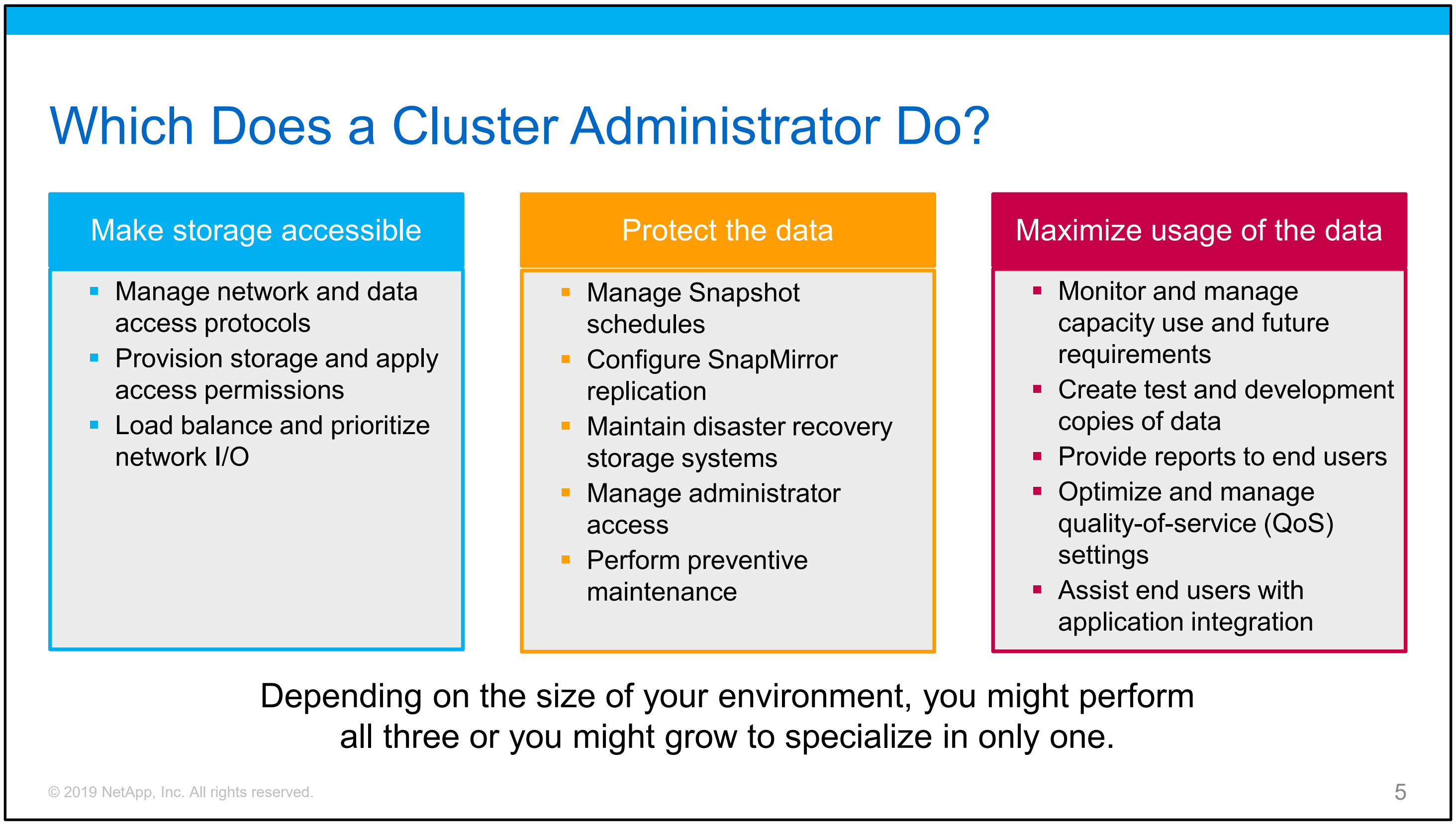
Course ID: STRSW-ILT-ONTAPADM



Set your phone to vibrate to prevent disturbing your fellow students. We realize that work does not always stop while in training. If you need to take call, feel free to step outside of the classroom.



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.



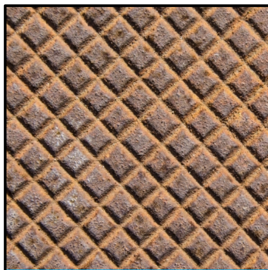
Before you see what this course is about, you should first understand the duties of a cluster administrator to put the modules of the course into context.

The first duty of a cluster administrator is to make the storage accessible. This duty is mostly associated with networking.

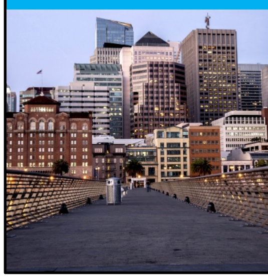
The second duty is to protect the data from loss or corruption.

The third duty is the help users and applications squeeze the most value from the data stored in the cluster.

In a small organization, you might be responsible for all of these duties. In a large organization, you might become a specialist in only one of these duties.



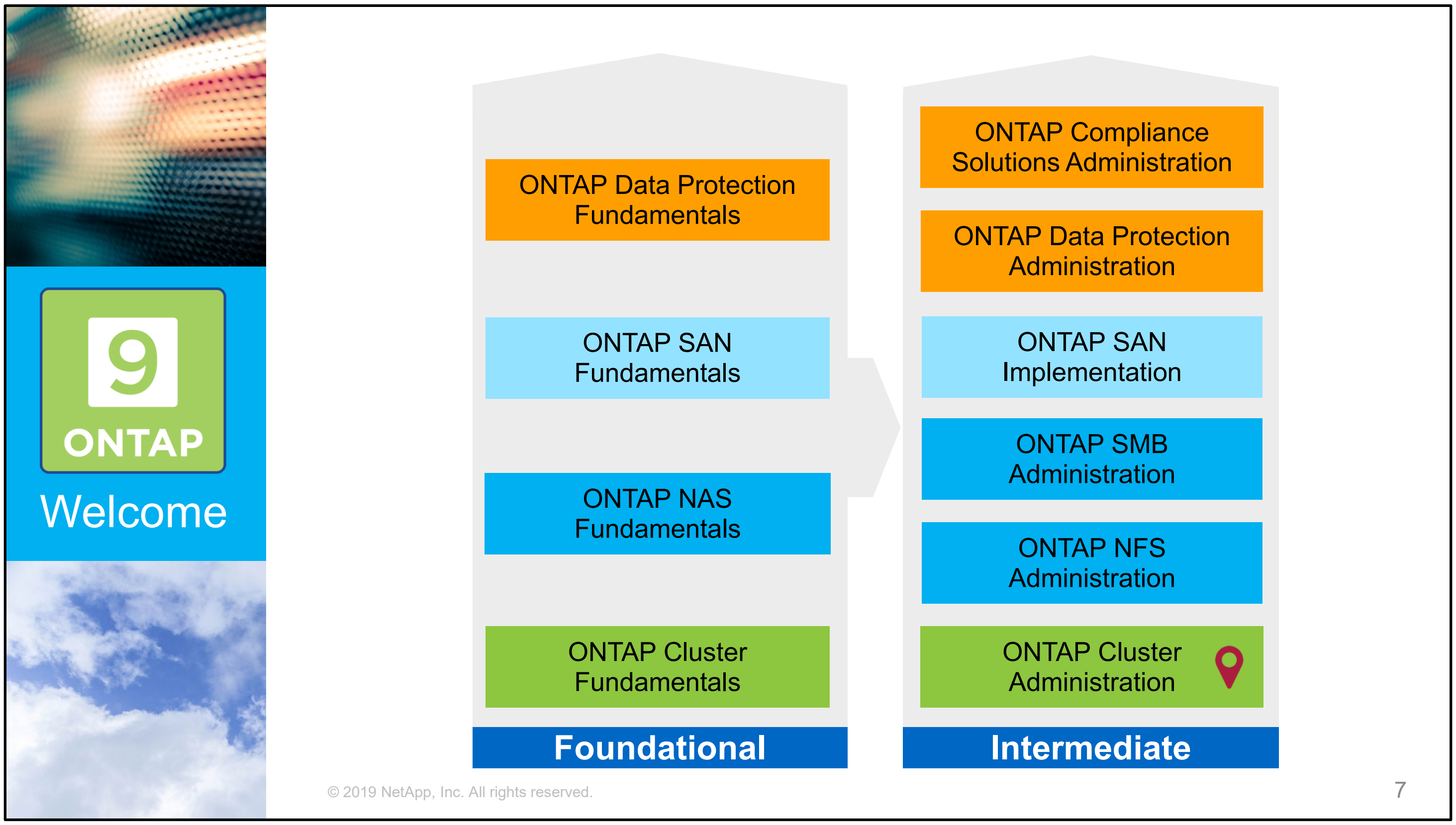
About This Course



This course focuses on enabling you to do the following:

- Define ONTAP cluster components
- Describe the role of a storage virtual machine (SVM) in the NetApp storage architecture
- Configure an ONTAP cluster
  - Configure and manage storage resources
  - Configure and manage networking resources
  - Create and configure an SVM
  - Create, manage, and protect FlexVol volumes
  - Implement storage efficiency features
- Manage ONTAP administrator access and user accounts
- Maintain your NetApp storage systems

During the next three days, you want to learn as much of the tasks and procedures for administrating an ONTAP cluster as possible. Unfortunately, this means that we cannot go as technically deep as you might want. This course is a launching platform for continued training to master your skills.



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 the 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 Cluster Fundamentals in preparation for this course.

What This Course Is Not

- An ONTAP 9 Fundamentals course
  You are expected to already be familiar with the core concepts and functionality of ONTAP 9.
- A certification test prep course
- A hardware installation and configuration course
- A data protection course
- A performance troubleshooting course
- A NAS or SAN administration course

This course assumes that although you might be new to ONTAP cluster administration, you have taken the prerequisite training to learn about ONTAP 9 software.

Although this course is recommended training for taking NetApp certification exams, it is not an exam preparation course.

Although you learn some hardware installation basics, if you want to learn how to physically install cluster hardware, you should take the online courses like NetApp Universal FAS Installation and the model-specific installation courses.

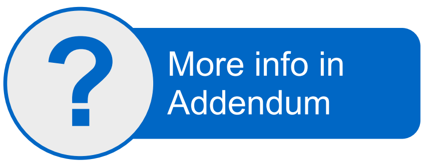
This course is often paired with the Data Protection course, so the course assumes that you will be taking that course at the end of the week.

Performance is a complicated topic with many variables, so this course covers only some recommended practices to keep cluster performance stable under general use.

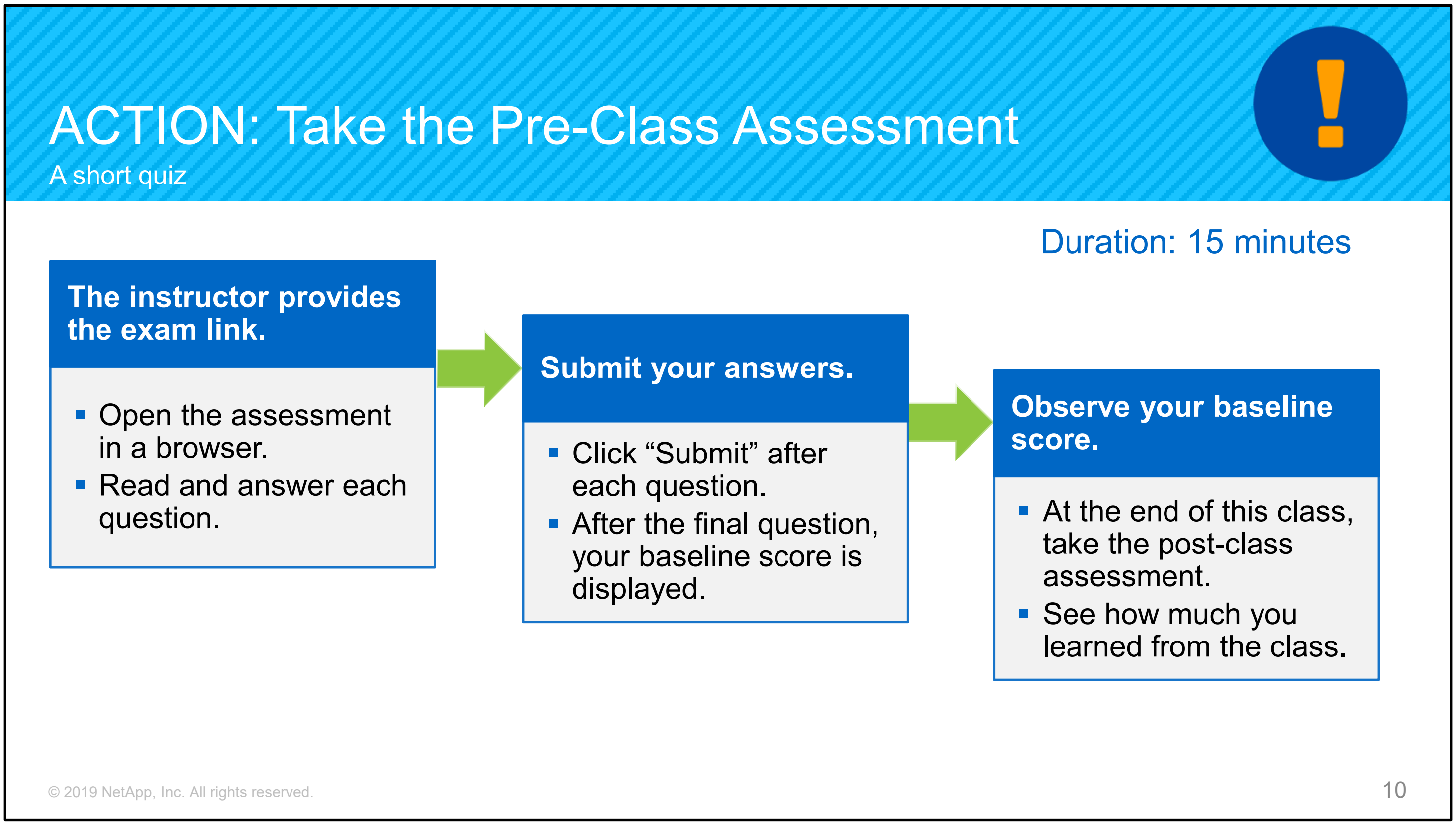
This course enables you to set up basic sharing of NAS and SAN data. For advanced uses, take the protocol-specific courses.

Student Guide Addendums

To maximize the time for exercises, not all the information to cover is included in the lecture portion. Whenever you see this graphic in the lower-left corner, you can find more information about the topic in the module addendum in your Student Guide.



Although it is necessary to cut some content while developing a course to fit the allotted training time, you should still find it useful. Content which did not make it into the lecture has been moved to addendums at the end of each module in your student guide. You can identify his content by this graphic on the final slide in the lecture that covers the topic.

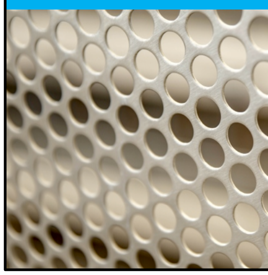


To measure your current knowledge of course topics, take the pre-class assessment by accessing the link that is provided. At the completion of the course, you can take the post-class assessment to measure how much you have learned.

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

Your score is private and is not retained or communicated.

Course Agenda



Day 1

Morning

- Introduction
- Module 1: NetApp ONTAP 9 Clusters
- Module 2: Cluster Setup

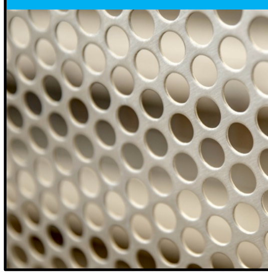
Afternoon

- Module 3: Cluster Management
- Module 4: Network Management

11

This schedule is based on average completion times for modules. Each class is composed of students with differing backgrounds and experience levels. This situation means that some modules might take more or less time to complete. Your instructor will adjust the schedule accordingly for breaks, meals, and start time of each module.

Course Agenda



Day 2

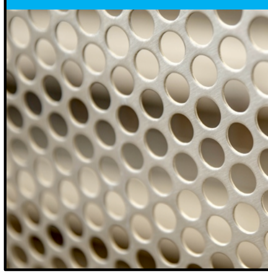
Morning

- Day 1 Review
- Module 5: Physical Storage Management
- Module 6: Logical Storage Management

Afternoon

- Module 7: Data Access

Course Agenda



Day 3

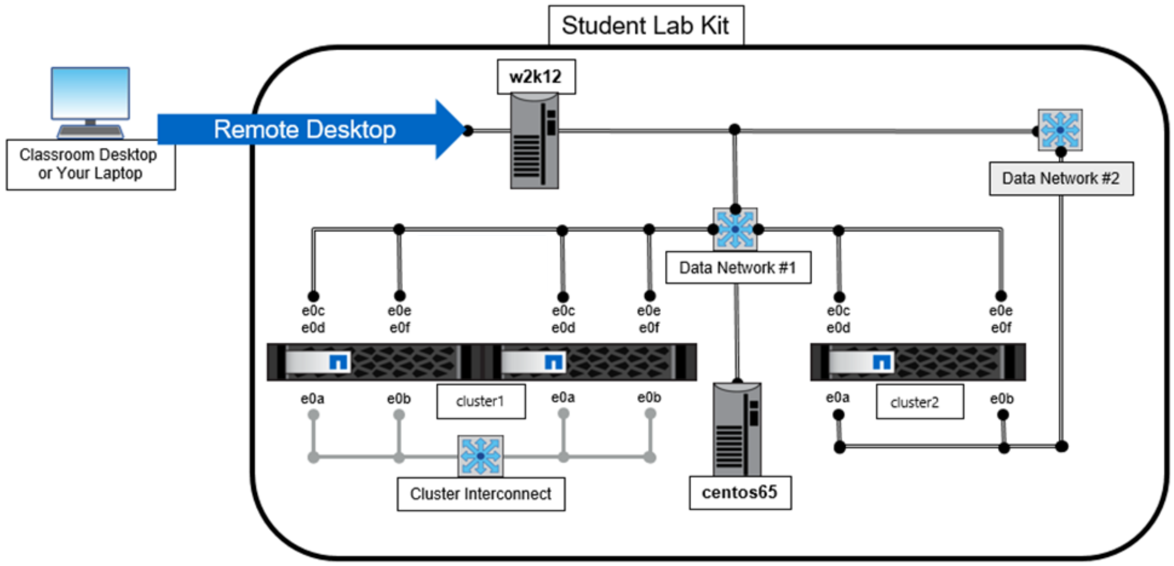
Morning

- Day 2 Review
- Module 8: Data Protection
- Module 9: Storage Efficiency

Afternoon

- Module 10: Cluster Maintenance
- Course Review and Post-Assessment

Class Equipment: Basic Architecture



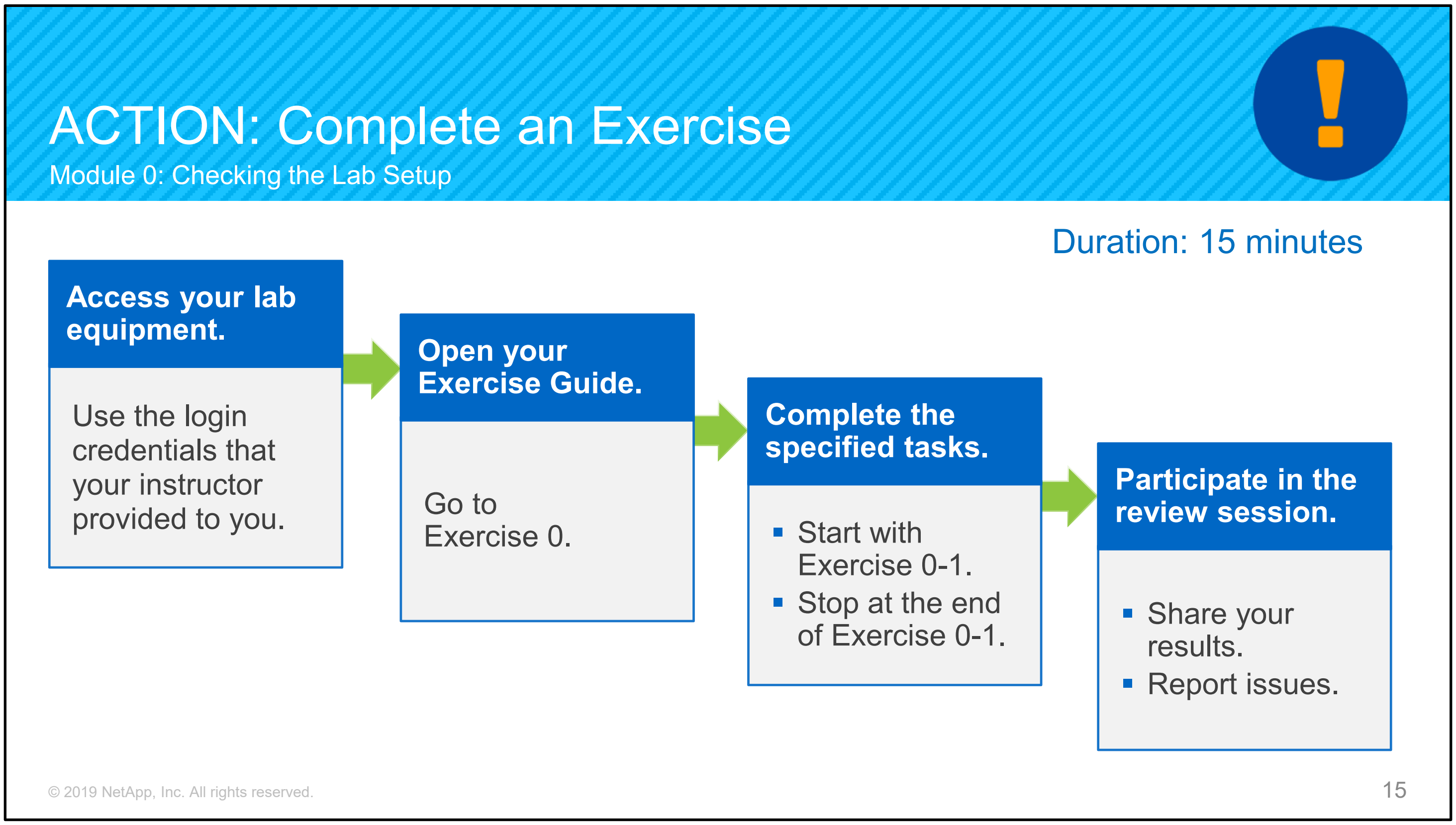
 14

Launch 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.

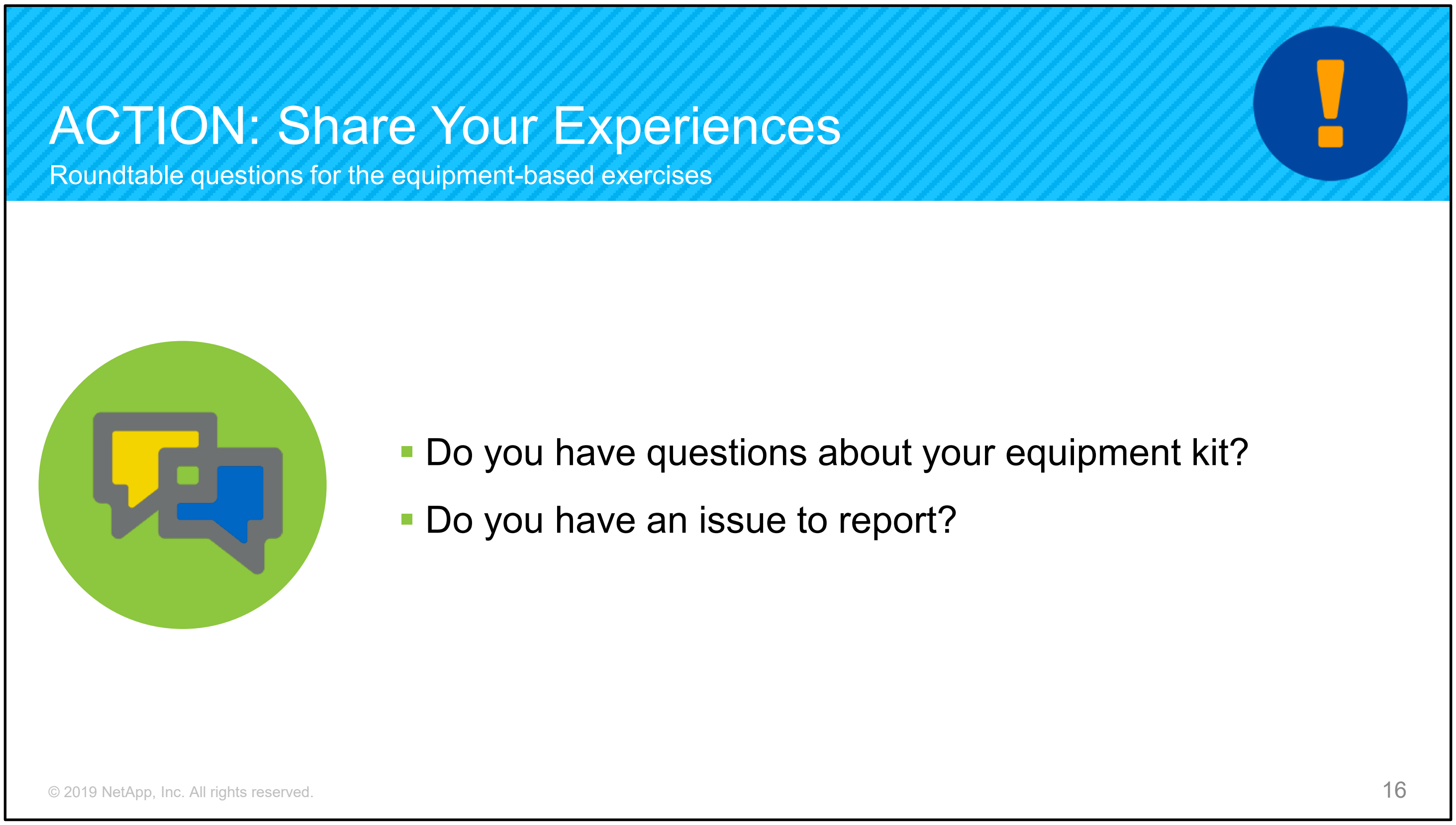
The Windows 2012 Server is your jumphost to access the lab environment.

Your exercise equipment consists of several servers:

- A 2-node ONTAP 9.5 cluster
- A one-node ONTAP 9.5 cluster
- A CentOS Linux server



See your exercise guide.



If you encounter an issue, notify your instructor immediately so that it can be resolved promptly.

Your Learning Journey

Bookmark these pages

NetApp University	NetApp
▪ 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	▪ New to NetApp Support Webcast Ensure a successful support experience ▪ NetApp Support Access downloads, tools, 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 facts and tips that can help you to 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 harness the accumulated knowledge of NetApp users and product experts. https://kb.netapp.com/support/index?page=home

Module 1
NetApp ONTAP 9 Clusters

About This Module

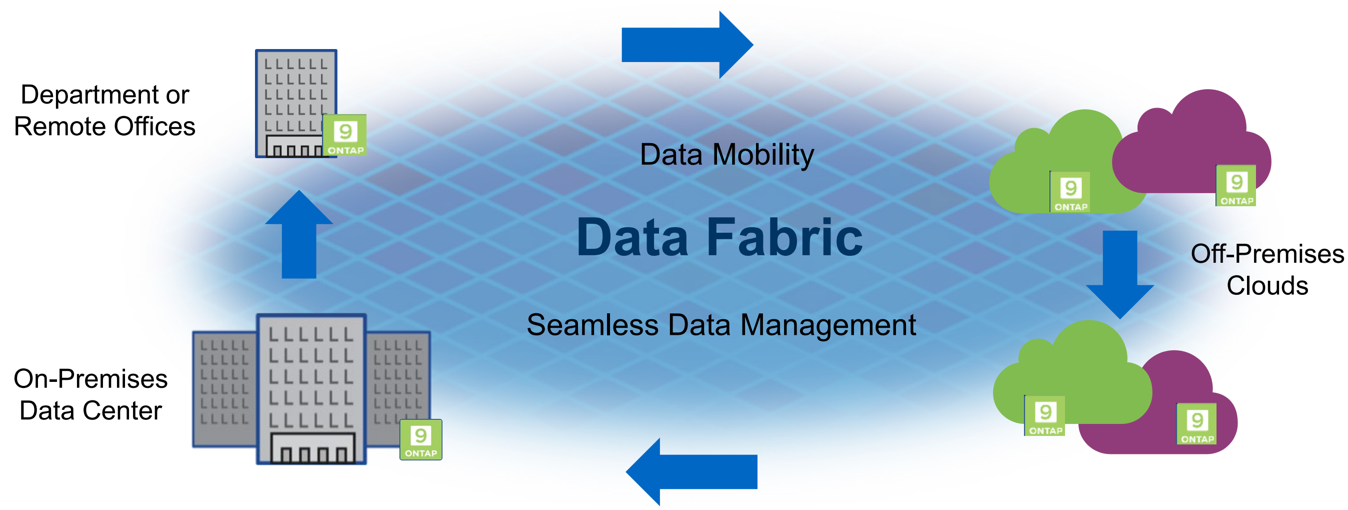
This module focuses on enabling you to do the following:

- Identify ONTAP deployment options
- Define ONTAP cluster components
- Describe the role of a storage virtual machine (SVM) in the NetApp storage architecture

This module covers ONTAP deployment options and cluster components for ONTAP 9.5 software as of February 2019.

Lesson 1
ONTAP Deployment Options

NetApp ONTAP Is the Foundation for Your Data Fabric



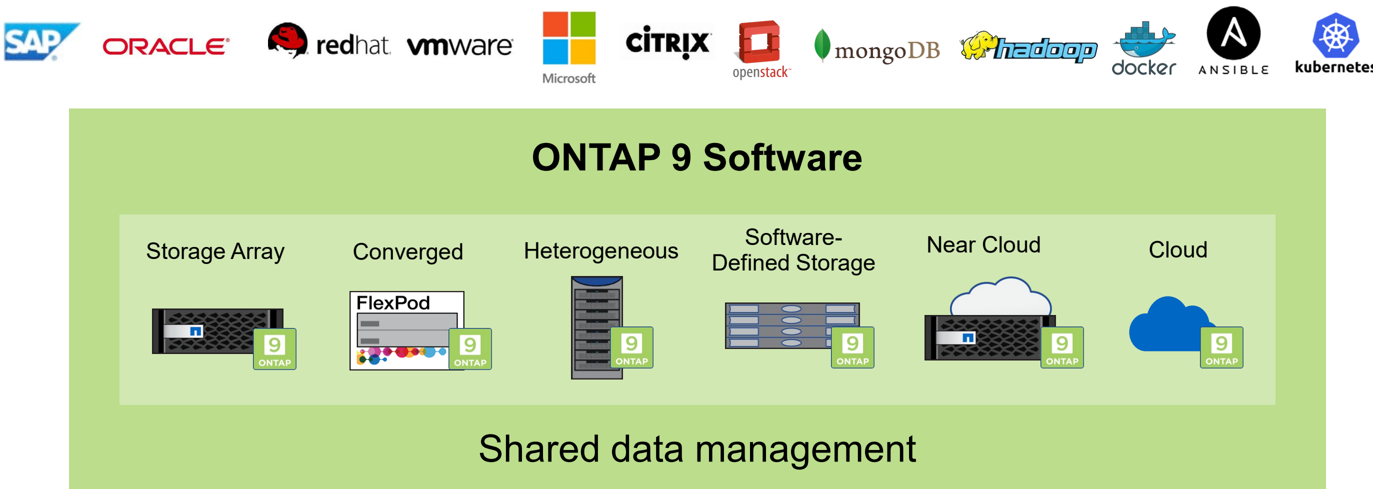
 4

The Data Fabric powered by NetApp weaves hybrid cloud mobility with uniform data management. NetApp works with new and existing partners to continually add to the fabric.

For more information about the Data Fabric, visit http://www.netapp.com/us/campaigns/data-fabric.

Standardize Data Management

ONTAP: For any application, anywhere



ONTAP 9 software has three major deployment options (ONTAP 9, ONTAP Select, and Cloud Volumes ONTAP), which you can use in various environments. Simply put, "it is just ONTAP!"

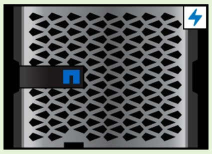
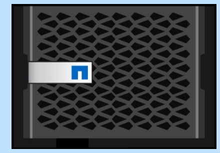
Standardize data management:

- Across architectures, blocks, or files, and on flash, disk, or cloud
- Across deployment models, from engineered storage arrays to commodity servers
- Across enterprise and emerging applications

Although this course focuses on physical ONTAP clusters, the knowledge also applies to Cloud Volumes ONTAP and ONTAP Select.

ONTAP 9.5 Supported Hardware Systems

January 2019

	AFF		FAS	
Enterprise Level		AFF A800 AFF A700 AFF A700s	FAS9000	
Mid Level		AFF A300	FAS8200	
Entry Level		AFF A220 AFF A200	FAS2700 FAS2600	

NOTE: See the Hardware Universe for technical details.

NetApp has a storage system to support the performance and budget needs of all customers. FAS storage systems generally have a corresponding AFF model that is built on the same hardware. The same is not true of AFF systems, which fill an expanding array of needs and price points as flash-based storage supplants disk-based storage.

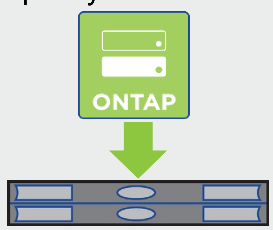
For more detailed information about the supported storages systems for ONTAP 9 software, see the Hardware Universe at http://hwu.netapp.com/.

Software-Defined Storage

NetApp ONTAP Select software

ONTAP Select Software

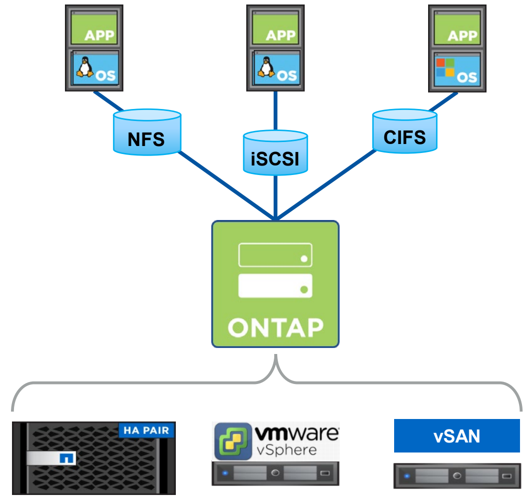
- Software-defined storage on third-party servers that is referred to as hybrid cloud infrastructure
- Suited for data center or remote office
- Flexible, capacity-based license



ONTAP Select Software

Overview

- ONTAP Select software features the following:
  - ONTAP software that runs on commodity hardware
    Note: ONTAP Select clusters cannot be mixed with AFF or FAS nodes in a cluster.
  - Enterprise data management services for server direct-attached storage (DAS), external array, and VMware vSAN
- ONTAP Select software provides a cloud-like experience on-premises:
  - Flexibility
  - Agility
  - Simplicity



More info in Addendum

ONTAP Select is ONTAP software that runs on commodity hardware (other vendor hardware).

ONTAP Select software has all of the benefits of ONTAP software: cluster-wide namespace, volume moves, workload rebalancing, nondisruptive upgrade (NDU), and nondisruptive operations (NDO).

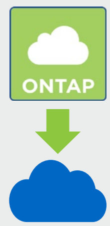
NOTE: ONTAP Select clusters cannot be mixed with FAS nodes or clusters.

Software-Defined Storage

NetApp Cloud Volumes ONTAP software

Cloud Volumes ONTAP

- Software-defined storage on public cloud services (like Amazon Web Services (AWS) or Microsoft Azure)
- Pricing system in which you pay for only what you use, when you use it
- New high availability and higher performance

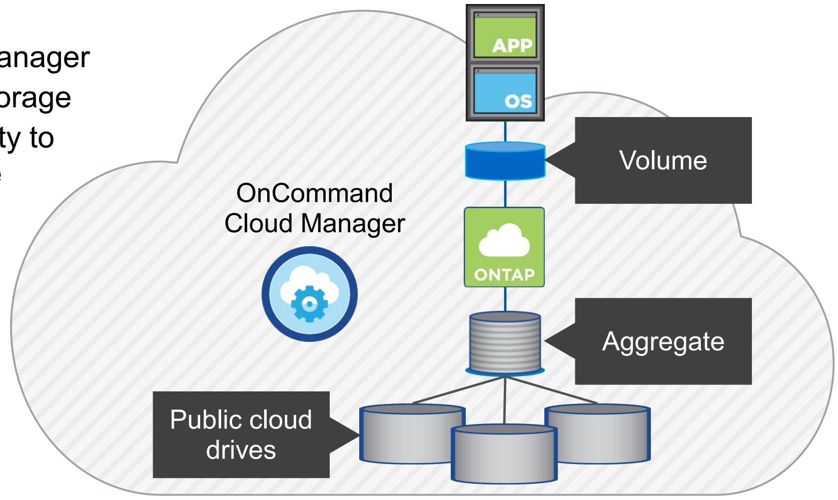


Cloud Volumes ONTAP was formerly marketed as ONTAP Cloud.

Cloud Volumes ONTAP

For AWS and Microsoft Azure

- AWS:
  - Deploys with OnCommand Cloud Manager
  - Uses Amazon Elastic Block Store storage
  - Uses a single node or high availability to protect against the failure of a single availability zone
- Microsoft Azure:
  - Deploys with OnCommand Cloud Manager
  - Uses Azure storage
  - Uses only a single node



? More info in Addendum

OnCommand Cloud Manager software deploys ONTAP 9 instances in the cloud. Cloud Volumes ONTAP enables a shared set of data services in the cloud. You can choose to own, lease, or rent on demand. You can explore and test the full power of ONTAP 9 software in the cloud with little risk. OnCommand Cloud Manager and OnCommand Insight simplify monitoring, provisioning, and data movement of all ONTAP 9 instances across clouds.

ONTAP Cloud High Availability for Amazon Web Services was introduced in ONTAP 9.0 software. ONTAP Cloud for Azure was introduced in ONTAP 9.1 software.

For more information about OnCommand Cloud Manager and Cloud Volumes ONTAP deployment options, see the following:

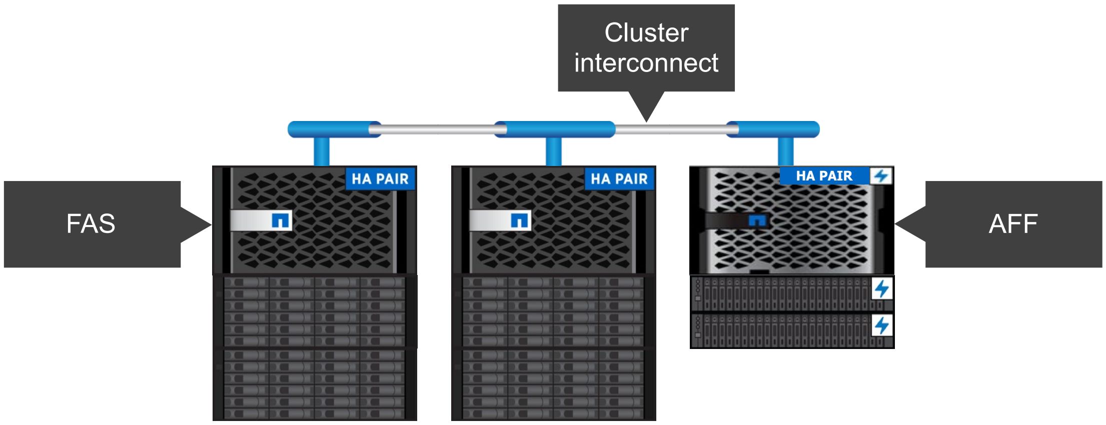
AWS Marketplace: https://aws.amazon.com/marketplace

Azure Marketplace: https://azure.microsoft.com/marketplace

Notice the graphic which indicates that there is more content on Cloud Volumes ONTAP in an addendum to this module.

Lesson 2
The Cluster

The Cluster



For product specifications, see the Hardware Universe:
hwu.netapp.com

You might wonder, “What *is* a cluster?” This course examines cluster components individually, but first, consider a high-level view.

A cluster is one or more FAS or AFF controllers that run the ONTAP software. In ONTAP terminology, a controller is called a node. In clusters with more than one node, a cluster interconnect is required so that the nodes appear as one cluster.

A cluster can be a mix of FAS and AFF models, depending on the workload requirements. Nodes can be added to or removed from a cluster as workload requirements change. For more information about the number and types of nodes, see the Hardware Universe at http://hwu.netapp.com/.

Node

Rear View

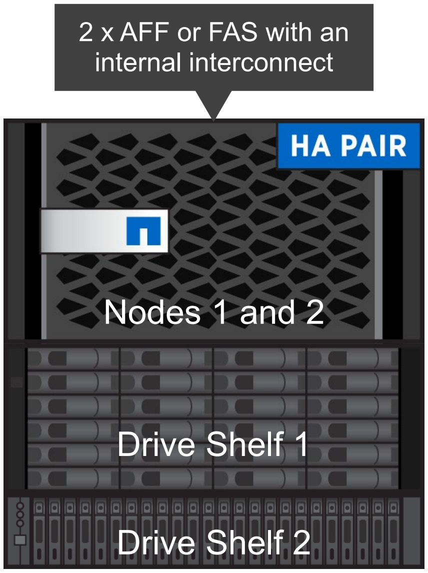
- A FAS or AFF storage controller that runs ONTAP software
- Storage and network ports
- Expansion slots
  Not all entry-level systems have expansion slots.
- NVRAM or NVMEM
- Drive shelves or internal drives or both

For product specifications, see the Hardware Universe:
hwu.netapp.com

 13

For information about specific controller models, see the product documentation on the NetApp Support site, or see the Hardware Universe at http://hwu.netapp.com/.

High-Availability Pair

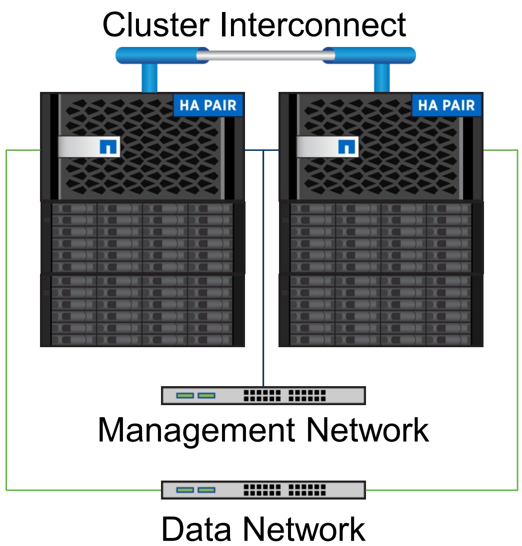


- Characteristics of a high-availability (HA) pair:
  - Two connected nodes in a partnership
  - Nodes that connect to the same drive shelves
  - Nodes that, by default, own the drives on their primary cabling path
  - A partnership in which, if a node fails, the surviving node takes control of the failed partner’s drives
- Components of HA pair connections:
  - HA interconnect
  - Multipath HA shelf connectivity

In multinode clusters, high-availability (HA) pairs are used.

The controllers in the nodes of an HA pair connect either through an HA interconnect, which consists of adapters and cables, or through an internal interconnect. In the example, the FAS8060 model uses an internal interconnect. The nodes must use redundant paths to connect to the same shelves.

Network



- Cluster interconnect:
  - Connection of nodes
  - Private network
- Management network:
  - Cluster administration
  - Ethernet network that can be shared with data

    Recommended practice: dedicated management network
- Data network:
  - One or more networks for data access from clients or hosts
  - Ethernet, FC, or converged network

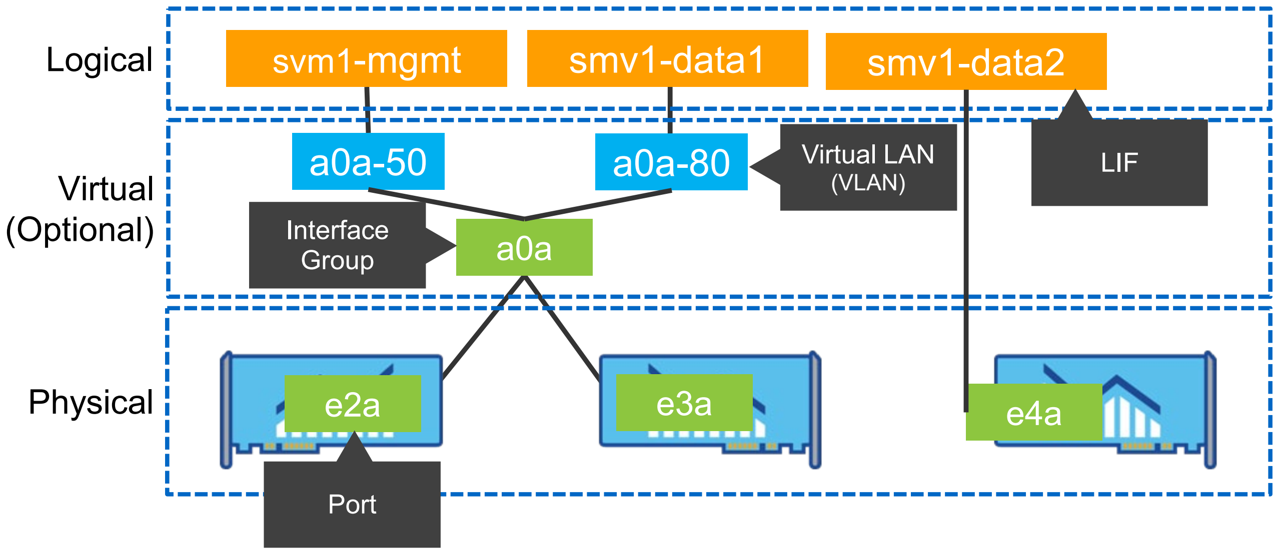
Clusters require one or more networks, depending on the environment.

The nodes communicate with each other over a cluster interconnect, even when the cluster is composed of only one HA pair. In a two-node cluster, the interconnect can be switchless. Clusters with more than two nodes require a private cluster interconnect that uses switches.

The management network is for cluster administration. Redundant connections to the management ports on each node and management ports on each cluster switch should be provided to the management network. In smaller environments, the management and data networks might be on a shared Ethernet network.

For clients and hosts to access data, a data network is also required. The data network includes one or more networks that are primarily used for data access by clients or hosts. Depending on the environment, there might be an Ethernet, FC, or converged network. Data networks can consist of one or more switches or even redundant networks.

Ports and LIFs

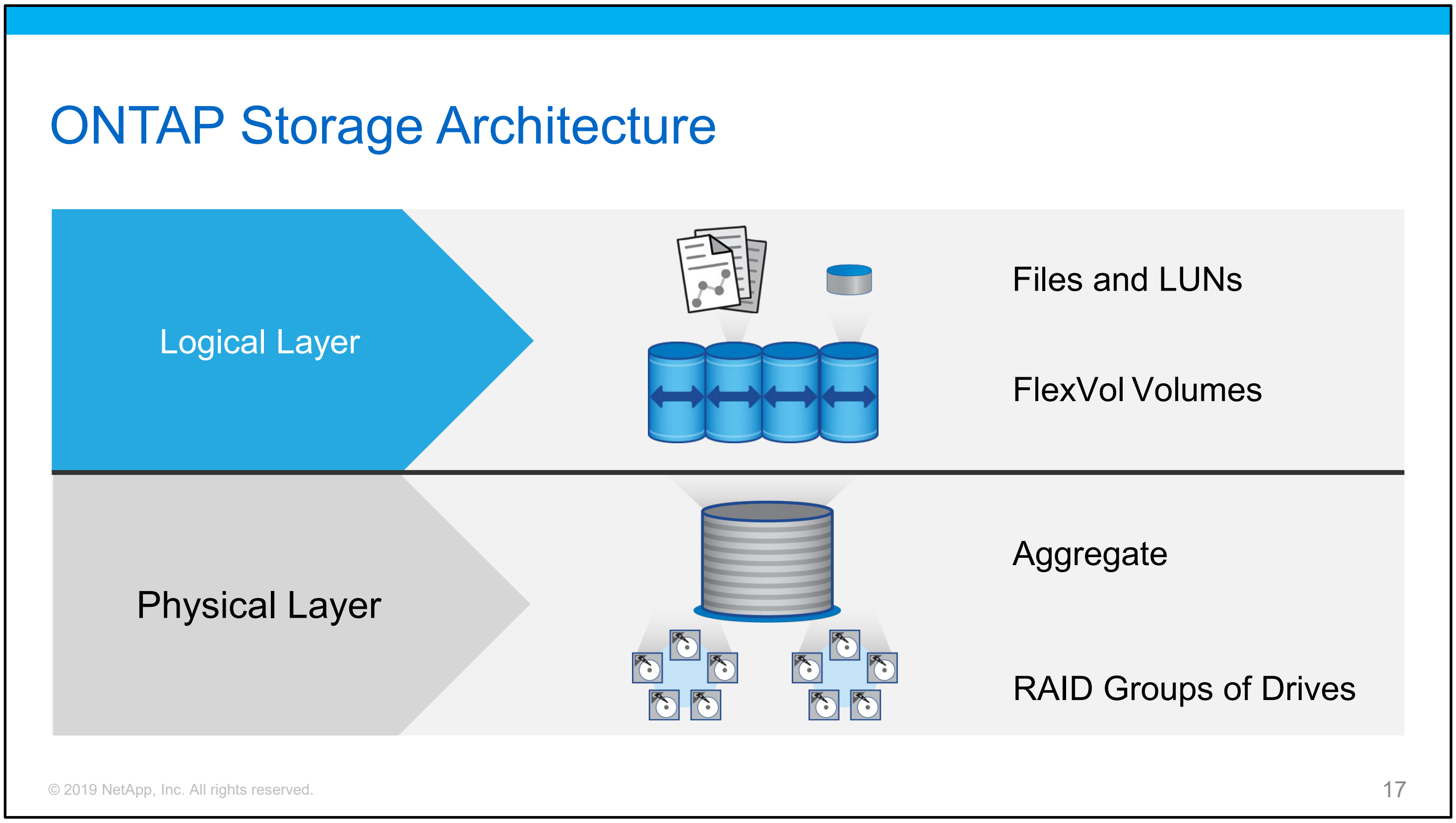


 16

Nodes have various physical ports that are available for cluster, management, and data traffic. The ports need to be configured appropriately for the environment.

Ethernet ports can be used directly or can be aggregated by using interface groups. Physical Ethernet ports and interface groups can be segmented by using virtual LANs (VLANs). Interface groups and VLANs are called *virtual ports*, which are treated like physical ports.

A LIF represents a network access point to a node in the cluster. A LIF can be associated with a physical port, an interface group, or a VLAN to interface with the management or data network.

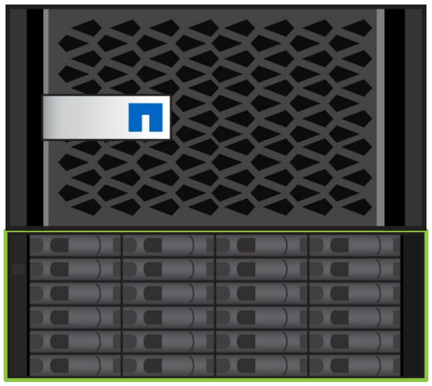


The ONTAP storage architecture dynamically maps physical storage resources to logical containers.

In ONTAP software, drives are grouped into RAID groups. An aggregate is a collection of physical drive space that contains one or more RAID groups. Each aggregate has a RAID configuration and a set of assigned drives. The drives, RAID groups, and aggregates make up the physical storage layer.

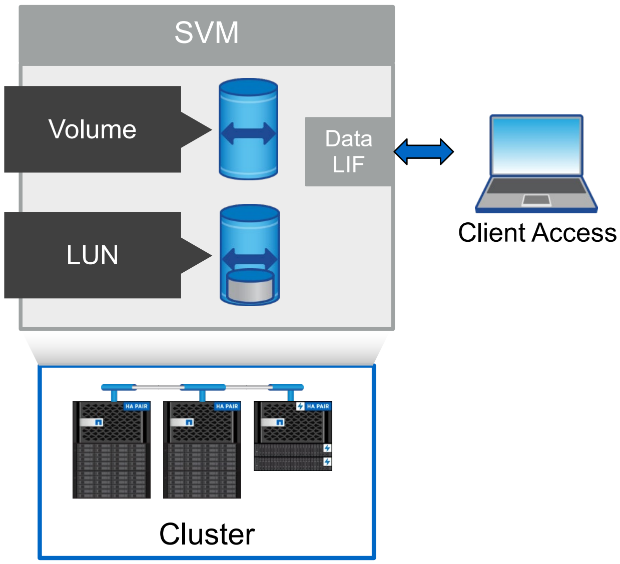
Within each aggregate, you can create one or more FlexVol volumes. A FlexVol volume is an allocation of drive space that is a portion of the available space in the aggregate. A FlexVol volume can contain files or LUNs. The FlexVol volumes, files, and LUNs make up the logical storage layer.

Physical Storage



- The physical internal and external drives to which the data is written and from which the data is read
- Covered in detail in Module 6

Logical Storage



- SVM:
  - Container for NAS data volumes and SAN LUNs
  - Access to client data through a LIF or LIFs
- Covered in detail in Module 7

 19

You use SVMs to serve data to clients and hosts. Like a virtual machine running on a hypervisor, an SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.

NOTE: SVMs were formerly called “vservers.” You still see that term in the ONTAP CLI.

An SVM serves data to clients and hosts from one or more volumes through one or more network LIFs. Volumes can be assigned to any data aggregate in the cluster. LIFs can be hosted by any physical or logical port. Both volumes and LIFs can be moved without disrupting data service, whether you are performing hardware upgrades, adding nodes, balancing performance, or optimizing capacity across aggregates.

The same SVM can have a LIF for NAS traffic and a LIF for SAN traffic. Clients and hosts need only the address of the LIF (IP address for NFS, SMB, or iSCSI; worldwide port name [WWPN] for FC) to access the SVM. LIFs keep their addresses as they move. Ports can host multiple LIFs. Each SVM has its own security, administration, and namespace.

Lesson 3
SVMs

SVM Types

Admin SVM:
- Is created during cluster setup
- Represents the cluster
- Exists once per cluster
- Owns cluster-scoped resources

Node SVM:
- Is created during cluster setup
- Represents an individual node
- Exists once per node in the cluster
- Owns node-scoped resources

Data SVM:
- Provides client access to user data
- Includes data volumes, LIFs, and protocols and access control
- Is for multiple use cases:
  - Secure multitenancy
  - Separation of resources and workloads
  - Delegation of management

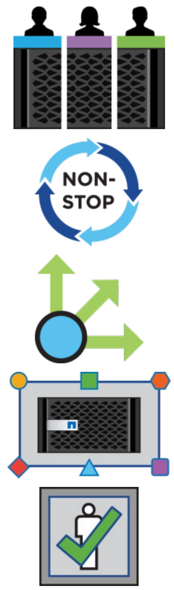
```
svl-nau::> vserver show
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume          Aggregate
----------- ------- ---------- ---------- ----------- ----------      ----------
svl-nau     admin   -          -          -           -               -
svl-nau-01  node    -          -          -           -               -
svl-nau-02  node    -          -          -           -               -
svm_green   data    default    running    running     svm_green_root  svl02_data_001
svm_red     data    default    running    running     svm_red_root    svl01_data_001
svm_yellow  data    default    running    running     svm_yellow_root svl01_data_002
6 entries were displayed.
```

 21

A data SVM contains data volumes and LIFs that serve data to clients. Unless otherwise specified, the term "SVM" refers to a data SVM. In the CLI, SVMs are displayed as "Vservers." SVMs might have one or more FlexVol volumes or scalable NetApp ONTAP FlexGroup volumes.

SVM Benefits

- Unified storage (with FlexVol volumes):
  - NAS protocols: CIFS and NFS
  - SAN protocols: iSCSI, FC (including FCoE), and NVMe over Fibre Channel (NVMe/FC)
- Nondisruptive operations (NDO) and nondisruptive upgrade (NDU):
  - Resource migration
  - Resource availability during hardware and software upgrades
- Scalability:
  - Addition and removal
  - Modification on demand to meet data-throughput and storage requirements



- Secure multitenancy:
  - Partitioning of a storage system
  - Isolation of data and management
  - No data flow among SVMs in the cluster
- Delegation of management:
  - User authentication and administrator authentication
  - Access assigned by the cluster administrator

SVMs provide many benefits.

The first benefit is unified storage. SVMs can serve data concurrently through multiple data access protocols. SVMs with FlexVol volumes provide file-level data access through NAS protocols, such as CIFS and NFS, and provide block-level data access through SAN protocols, such as iSCSI, FC, or FCoE. SVMs with FlexVol volumes can serve data to SAN and NAS clients independently at the same time.

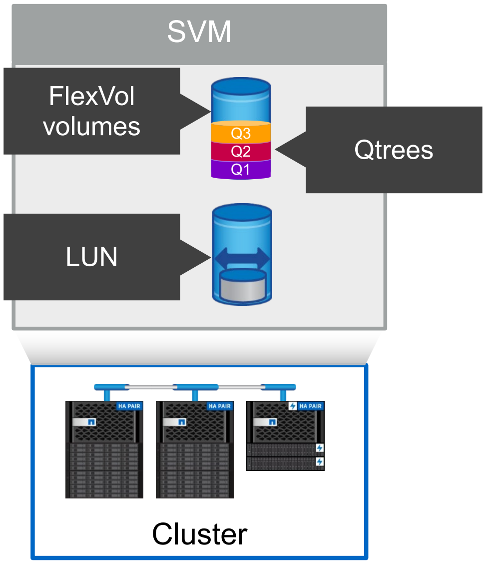
Another benefit is NDO. SVMs can operate continuously and nondisruptively. By enabling resources such as volumes and LIFs to move to other nodes, SVMs help clusters to operate continuously. Continuous operations are advantageous during software and hardware upgrades, the addition and removal of nodes, and all administrative operations.

A third benefit of SVMs is scalability. SVMs can be added, removed, or given more resources as the underlying physical storage grows. SVMs can be modified on demand to meet data-throughput requirements and other storage requirements.

SVMs are the fundamental unit of secure multitenancy. SVMs enable partitioning of the storage infrastructure so that the infrastructure appears as multiple independent storage systems. Partitions isolate data and management. Each SVM appears as a single independent server, which enables multiple SVMs to coexist in a cluster and prevents data from flowing among SVMs.

Finally, SVMs support delegation of management. Each SVM can have its own user authentication and administrator authentication. SVM administrators can manage the SVMs that they are authorized to access. Cluster administrators assign privileges to SVM administrators.

SVM with FlexVol Volumes



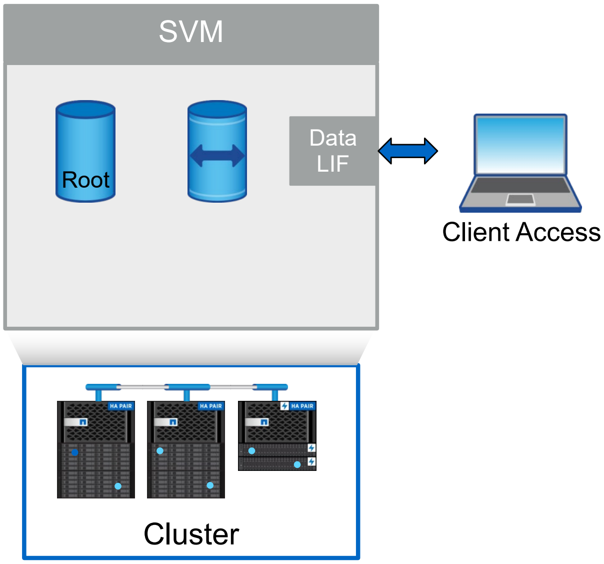
- FlexVol volume:
  - Representation of the file system in a NAS environment
  - Container for LUNs in a SAN environment
- LUN: Logical unit that represents a SCSI disk
- Quota tree (qtree):
  - Partitioning of FlexVol volumes into smaller segments
  - Management of quotas, security style, and CIFS opportunistic lock (oplock) settings

An SVM can contain one or more FlexVol volumes. In a NAS environment, volumes represent the file system where clients store data. In a SAN environment, a LUN is created in the volumes for a host to access.

In a SAN environment, the host operating system controls the reads and writes for the file system.

Qtrees can be created to partition a FlexVol volume into smaller segments, much like directories. Qtrees can also be used to manage quotas, security styles, and CIFS opportunistic lock (oplock) settings.

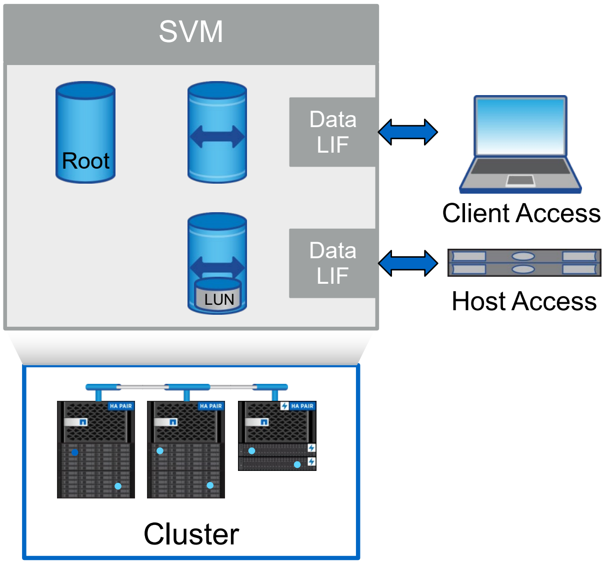
SVM Root Volume



- Is created when the SVM is created
- Serves as the NAS client entry point to the namespace that an SVM provides
  Therefore, it must be mirrored on all nodes to ensure that the namespace is always accessible.
- Should not be used to store user data
- Should not be confused with the node root volume (vol0)

When an SVM is created, a root volume is also created, which serves as the NAS client entry point to the namespace that the SVM provides. NAS client data access depends on the health of the root volume in the namespace. SAN client data access is independent of the root volume health in the namespace.

Data LIFs



- NAS data LIFs:
  - Multiprotocol (NFS, CIFS, or both)
  - Manually or automatically assigned IP addresses
  - Failover or migration to any node in the cluster
- SAN data LIFs:
  - Single protocol (FC or iSCSI):
    - An FC LIF is assigned a worldwide port name (WWPN) when it is created.
    - iSCSI LIF IP addresses can be assigned manually or automatically.
  - No failover
  - Restrictions on migration

25

Data LIFs that are assigned a NAS protocol follow slightly different rules than LIFs that are assigned a SAN protocol.

NAS LIFs are created so that clients can access data from a specific SVM. NAS LIFs are multiprotocol. A NAS LIF can be assigned NFS, CIFS, or both protocols. When the LIF is created, you can manually assign an IP address or specify a subnet so that the address is assigned automatically. NAS LIFs can fail over or migrate to any node in the cluster.

SAN LIFs are created so that a host can access LUNs from a specific SVM. SAN LIFs are single-protocol. A SAN LIF can be assigned either the FC or iSCSI protocol. When a LIF is assigned the FC protocol, a worldwide port name (WWPN) is automatically assigned. When a LIF is assigned the iSCSI protocol, you can either manually assign an IP address or specify a subnet so that the address is assigned automatically. Although SAN data LIFs do not fail over, SAN data LIFs can be migrated. However, restrictions exist on migration.

For more information about migrating SAN LIFs, see the *ONTAP 9 SAN Administration Guide*.

References

ONTAP 9 Documentation Center:
http://docs.netapp.com/ontap-9/index.jsp

- *ONTAP 9 Concepts*
- *High-Availability Configuration Guide*
- *System Administration Reference*

ONTAP 9 Documentation Center: - http://docs.netapp.com/ontap-9/index.jsp

What's New in ONTAP 9.5 - https://www.youtube.com/watch?v=zHJtjK6Ewvo

ONTAP Select: Introduction - https://www.youtube.com/watch?v=UyLGV07Q-0U

Cloud Volumes ONTAP - https://www.youtube.com/watch?v=KewTNwXiaIY

Knowledge Check: Question

1. Which two deployment options are software-defined? (Choose two.)

    a. ONTAP deployed on a FAS system

    b. ONTAP deployed on an AFF system

    c. ONTAP deployed on commodity hardware

    d. ONTAP deployed in the cloud

    e. ONTAP deployed by using a heterogeneous enterprise array

Knowledge Check: Question

2. Which set of networks is part of a cluster?

   a. data network, management network, and cluster interconnect

   b. data network, HA interconnect, and cluster interconnect

   c. HA interconnect, cluster interconnect, and backup network

   d. data network, cluster interconnect, and backup network

Knowledge Check: Question

3. Which pair of components is a major part of data SVMs?

   a. aggregates and network ports

   b. disks and nodes

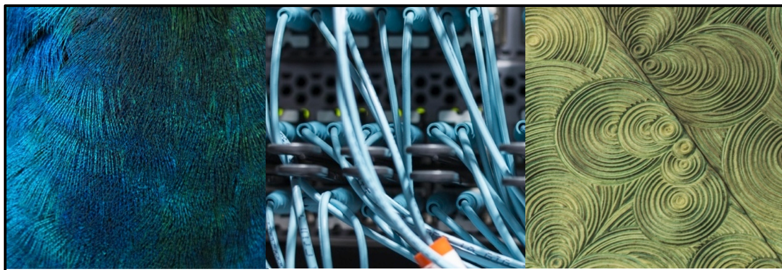
   c. data LIFs and aggregates

   d. volumes and data LIFs

Module Review

This module focused on enabling you to do the following:

- Identify ONTAP deployment options
- Define ONTAP cluster components
- Describe the role of an SVM in the ONTAP storage architecture



Addendum
ONTAP Select Learning Resources

Additional ONTAP Select Learning

Learn about advanced topics like supported configurations and deploying the software on VMware ESXi or Kernel-Based Virtual Machine (KVM) hosts:

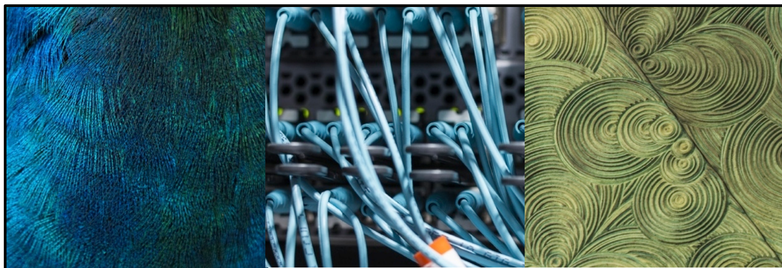
- ONTAP Select Installation and Deployment (web-based course)
- ONTAP Select Documentation Resources
- Technical Reports:
  - TR-4661: HCI File Services Powered by ONTAP Select
  - TR-4690: Oracle Databases on ONTAP Select
  - TR-4613: ONTAP Selection on KVM Product Architecture and Best Practices

ONTAP Select Documentation Resources

TR-4661: HCI File Services Powered by ONTAP Select

TR-4690: Oracle Databases on ONTAP Select

TR-4613: ONTAP Selection on KVM Product Architecture and Best Practices



Addendum
NetApp Cloud Volumes Learning Resources

Cloud Volumes Learning Resources

- Cloud Fundamentals (online course)
- Cloud Volumes ONTAP Fundamentals (online course)
- Cloud Volumes Documentation
- Technical Reports:
  - TR-4383: Performance Characterization of Cloud Volumes ONTAP for AWS
  - TR-4676: Performance Characters of Cloud Volumes ONTAP in Azure
- Video
  - ONTAP Cloud for AWS https://www.youtube.com/watch?v=sQKq9iJvD2o&t=7s
  - ONTAP Cloud for Azure https://www.youtube.com/watch?v=R2EWE3o6kxs

Cloud Fundamentals (online course)

Cloud Volumes ONTAP Fundamentals (online course)

Cloud Volumes Documentation

Technical Reports:

TR-4383: Performance Characterization of Cloud Volumes ONTAP for AWS

TR-4676: Performance Characters of Cloud Volumes ONTAP in Azure

Video:

ONTAP Cloud for AWS https://www.youtube.com/watch?v=sQKq9iJvD2o&t=7s

ONTAP Cloud for Azure https://www.youtube.com/watch?v=R2EWE3o6kxs

Module 2
Cluster Setup

About This Module

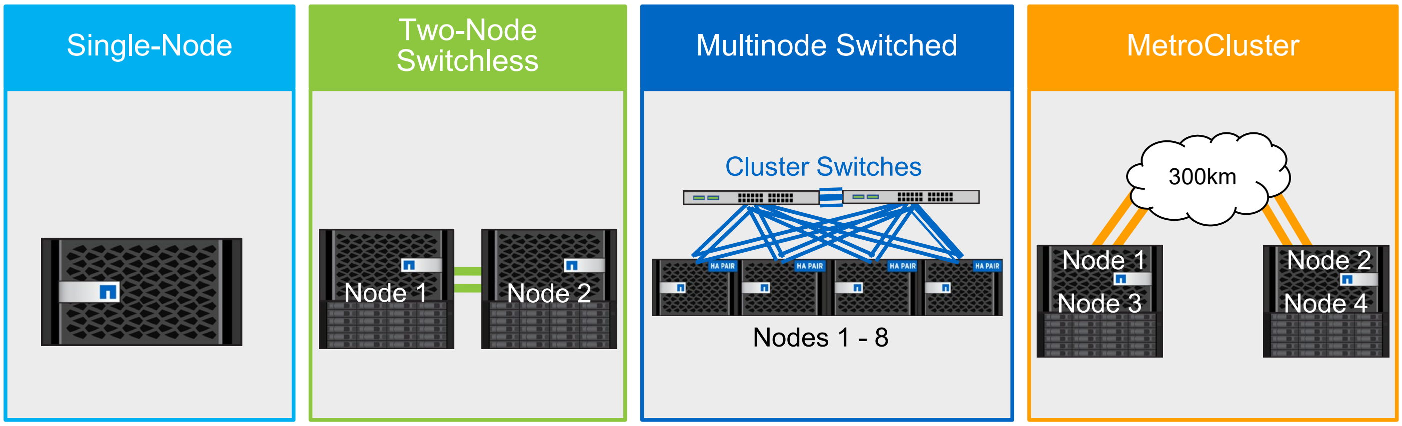
This module focuses on enabling you to do the following:

- Identify supported cluster configurations
- List the steps to set up a cluster
- Manage cluster nodes at the hardware level

In this module, you learn how to take newly installed cluster hardware and turn it into a functional ONTAP cluster.

Lesson 1
Supported FAS and AFF Configurations

Supported Cluster Configurations



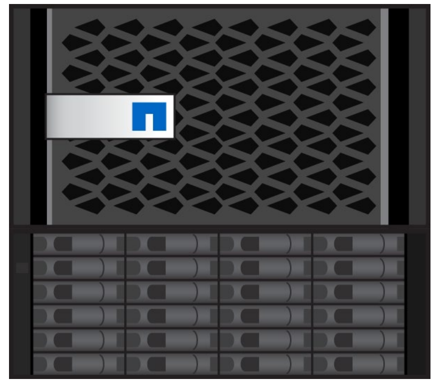
There are four types of NetApp ONTAP cluster configurations:

- Single-node
- Two-node cluster without network switches
- Multinode cluster that is made of high-availability (HA) pairs that are connected through network switches
- Geographically separated HA pairs that are connected in a MetroCluster cluster configuration

Single-Node Cluster

- Features of a single-node cluster:
  - Special implementation of a cluster that runs on a standalone node
  - An implementation for a workload that requires only one node and does not need nondisruptive operations (NDO)

  Use case: Data protection for a remote office or test and development
- Features and operations that a single-node cluster does not support:
  - Storage failover (SFO) and high availability
  - Operations that affect multiple nodes



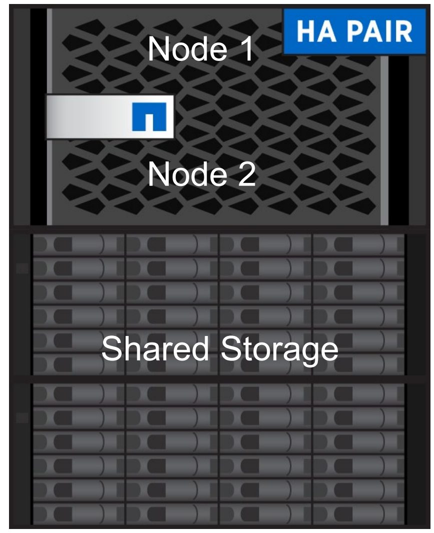
 5

Some features and operations are not supported for single-node clusters. Because single-node clusters operate in a standalone mode, storage failover (SFO) and cluster high availability are unavailable. If the node goes offline, clients cannot access data that is stored in the cluster. Also, any operation that requires more than one node cannot be performed. For example, you cannot move volumes, perform most copy operations, or back up cluster configurations to other nodes.

HA Pairs

High-availability (HA) pairs provide hardware redundancy that supports the following features:

- NDO and nondisruptive upgrade (NDU)
- Fault tolerance
- Takeover and giveback of partner storage
- Elimination of most hardware components and cables as single points of failure
- Improved data availability

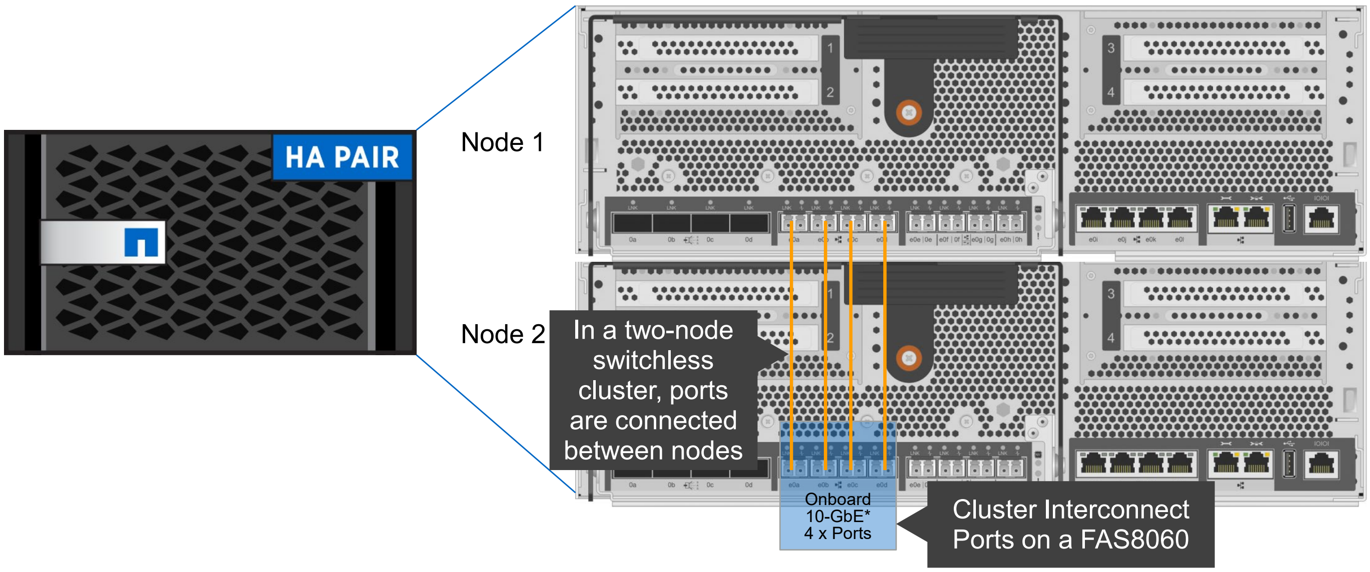


 6

Clusters of two or more nodes are built from HA pairs. HA pairs provide hardware redundancy that is required for NDO and fault tolerance. The hardware redundancy gives each node in the pair the software functionality to take over and return partner storage. Hardware redundancy also provides the fault tolerance that is required to perform NDO during hardware and software upgrades or maintenance.

A storage system has various single points of failure, such as certain cables or hardware components. An HA pair greatly reduces the number of single points of failure. If a failure occurs, the partner can take over and continue to serve data until the failure is fixed. The controller failover function provides continuous data availability and preserves data integrity for client applications and users.

Two-Node Switchless Cluster

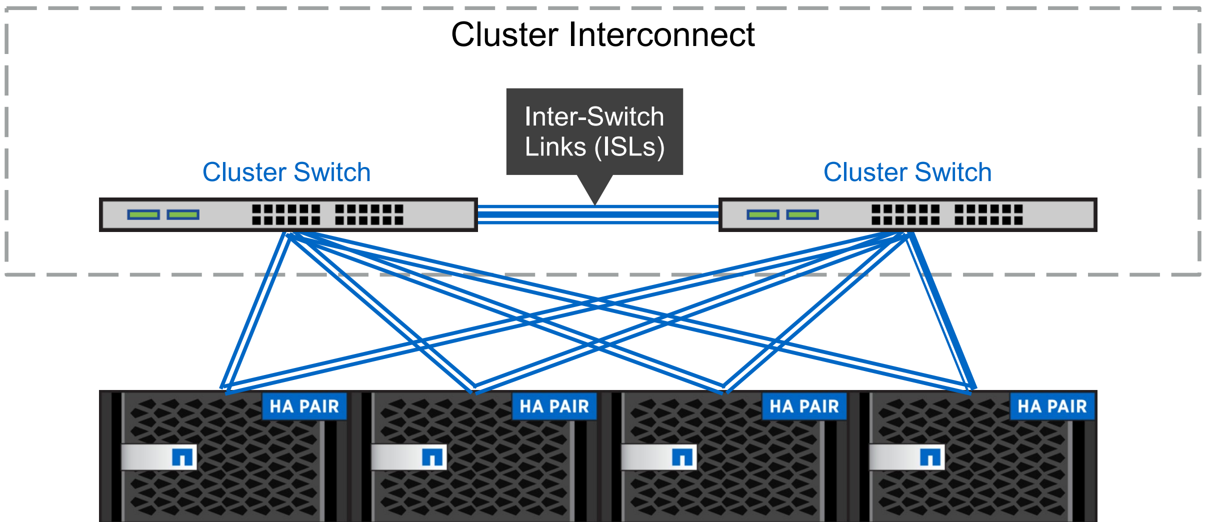


*GbE=Gigabit Ethernet

In clusters that have more than one node, a cluster interconnect is required for cluster communication and data sharing. The example here shows an enterprise class storage system with two controllers that are installed in the chassis. Each controller has a set of four onboard 10-Gigabit Ethernet (10-GbE) ports that are used to connect to the cluster interconnect.

In a two-node switchless cluster, a redundant pair of ports is cabled together as shown on the slide. To enable both HA and SFO functionality in two-node clusters in which both controllers share the chassis, the HA state must be set by the ha-config command in maintenance mode. In most shared chassis systems, the state is set automatically and requires no manual intervention.

Multinode Switched Clusters



More networking details are discussed in the Network Management module.

 8

If your workload requires more than two nodes, the cluster interconnect requires switches. The cluster interconnect requires two dedicated switches for redundancy and load balancing. Inter-Switch Links (ISLs) are required between the two switches. From each node, there should always be at least two cluster connections, one to each switch. The required connections vary, depending on the controller model and speed of the network ports. Larger systems might require as many as four connections per switch.

After the cluster interconnect is established, you can add more nodes, as your workload requires.

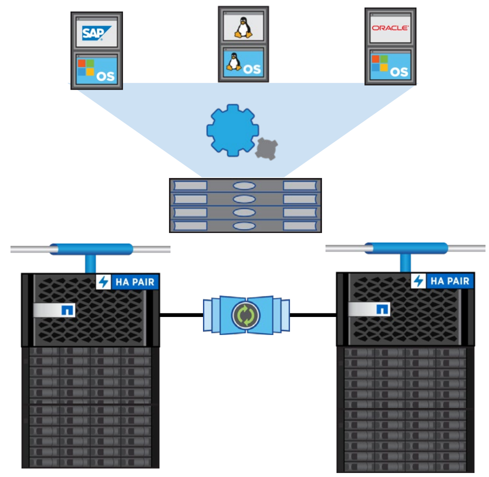
For more information about the maximum number and models of controllers that are supported, see the *ONTAP Storage Platform Mixing Rules* in the NetApp Library.

For more information about the cluster interconnect and connections, see the *ONTAP Network Management Guide*.

MetroCluster Software

Benefits of MetroCluster software:

- Geographic separation provides business continuity
- Continuous availability, leading to zero data loss
- Set-it-once simplicity
- Zero change management
- Unified solution (support for SAN and NAS)



Learn more about MetroCluster software in
ONTAP Data Protection Administration
– and –
ONTAP MetroCluster Installation.

MetroCluster high-availability and disaster recovery software uses geographic distance, up to 300km, and data mirroring to protect the data in a cluster.

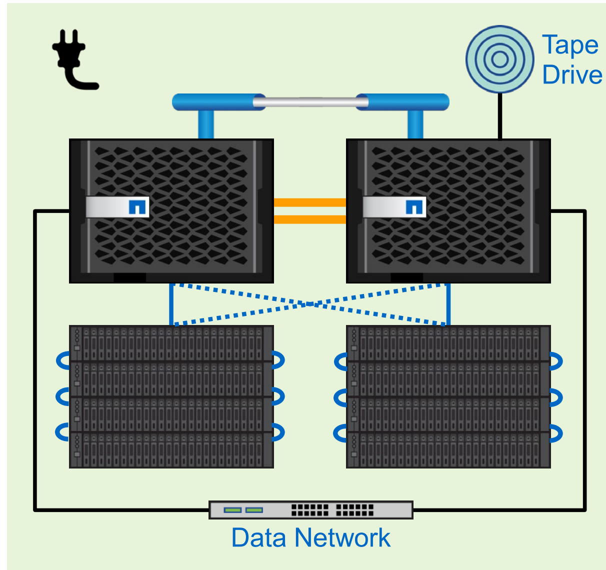
MetroCluster software provides disaster recovery through one MetroCluster command. The command activates the mirrored data on the surviving site.

Lesson 2
Setting Up a Cluster

Basic Hardware Setup Tasks

Connect the following hardware:

- HA interconnect
- Drive shelf to drive shelf cabling
- Controllers to drive shelves
- Controllers to cluster interconnect
- Controllers to networks
- Any tape devices
- Controllers and drive shelves to redundant power



If necessary, for your controller type, connect NVRAM HA cable between partners. The connections can be through the chassis, 10/40/100-GbE, or InfiniBand, depending on your storage controllers.

Create shelf stacks by cabling the drive shelves to each other.

Connect controllers to disk shelves. Verify that shelf IDs are set properly.

Connect controllers to networks. Connect any tape devices that you might have. (You can connect tape devices later.)

Connect controllers and disk shelves to power.

HA Interconnect Links

- Are used primarily to mirror NVRAM/NVMEM
- Provide a channel for certain types of communication traffic between the nodes in an HA pair:
  - Failover
  - Drive firmware
  - Heartbeat
  - Version information

Dual-Node Chassis
Uses an internal or node-to-node HA interconnect

Single-Node Chassis
Requires external HA interconnect cables

 12

HA interconnects connect the two nodes of each HA pair for all controllers. The connections are internally provided over the backplane in the chassis of a dual-controller configuration or through node-to-node cabling. For a chassis with a single controller, a dedicated HA interconnect cable is required. The dedicated interconnect cable is based on the model and enclosure. Visit the NetApp Support site to see the appropriate hardware configuration guide for your model of storage controller.

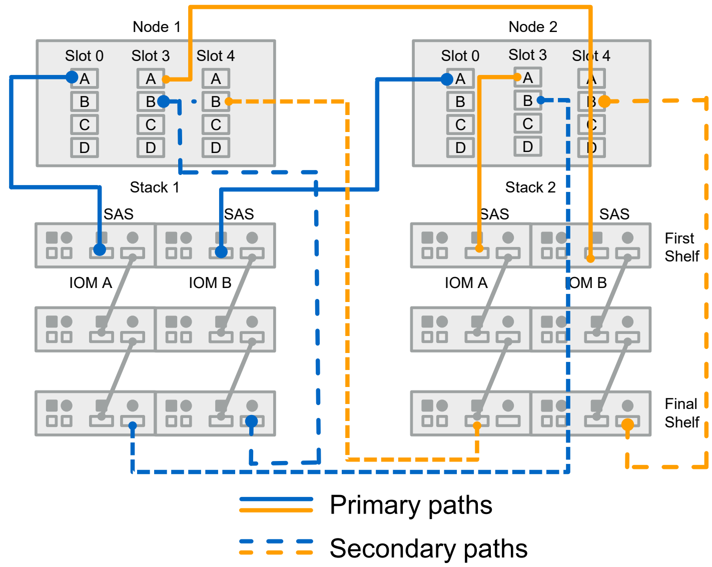
The following types of traffic flow over the HA interconnect links:

- **Failover:** The directives are related to performing SFO between the two nodes, regardless of which type of failure:
  - Negotiated (planned and in response to an administrator request)
  - Not negotiated (unplanned and in response to an improper system shutdown or booting)
- **Disk firmware:** Nodes in an HA pair coordinate the update of disk firmware. While one node updates the firmware, the other node must not perform any I/O to it.
- **Heartbeat:** Regular messages demonstrate availability.
- **Version information:** The two nodes in an HA pair must be kept at the same major and minor revision levels for all software components.

Drive Shelf Cabling

MPHA configuration

- Multipath high-availability (MPHA) cabling ensures that the storage controllers have redundant paths to all drives in the HA pair.
- MPHA cabling is required for HA pair configurations.
- Cabling is mirrored on both nodes to ensure that drive IDs are consistent within the HA pair.



 13

To provide fault tolerance, cluster nodes use two connections to every drive in the HA pair. In this example, both storage controllers own a stack of drive shelves.

Both storage controllers use their 0a ports to create the primary path to the first shelf in the shelf stack that is owned by node 1.

Both controllers use the 4b port to create the secondary path from the final shelf in the stack.

To connect to the shelf stack that is owned by node 2, both controllers connect to the first shelf in the stack with port 3a and to the final shelf with port 4b.

The cabling is mirrored so that both nodes generate the same drive ID for all the drives in the pair. If the nodes use different ports, a drive failure would be reported on both nodes but with different IDs. This situation causes confusion, and therefore accidents, when you try to replace a failed drive.

Powering on a System

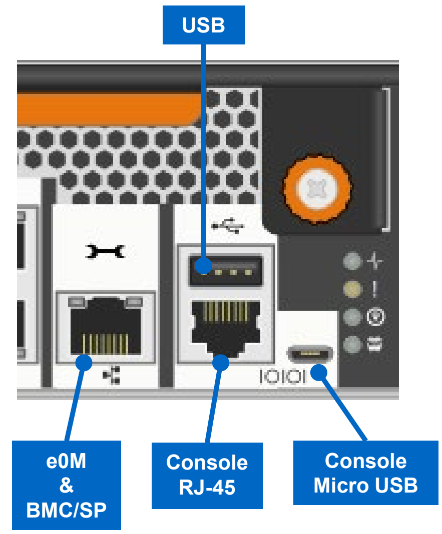
1. Power on network switches.
2. Power on drive shelves.
3. Power on tape devices (if present).
4. Power on storage controllers.

You should power on the hardware devices in a cluster in the order that is shown.

To power off the entire cluster, power off components in the reverse order.

Communication Connections

- Console connections:
  - RJ-45 that uses RS232C ANSI-115.2K-8-None-1
  - Micro-USB @ 115.2K baud rate
- Remote management device connection: Baseboard Management Controller (BMC) or Service Processor (SP)
- Management network connections (e0M)
- Cluster interconnect connections
- Data network connections

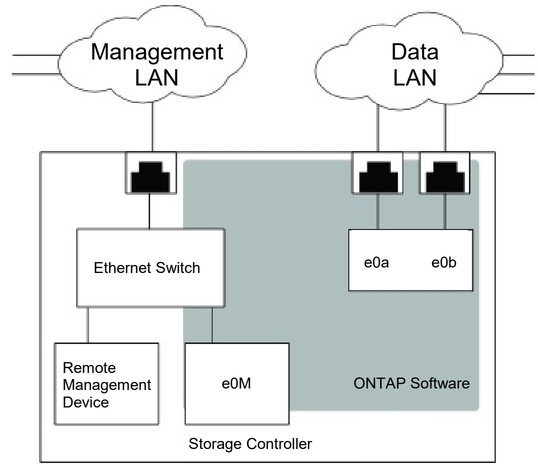


Each controller should have a console connection, which is required to get to the firmware and the boot menu. For example, you might use the console connection to the boot menu to access setup, installation, and initialization options. A remote management device connection, although not required, is helpful if you cannot get to the UI or console. Remote management enables remote booting, the forcing of core dumps, and other actions.

The full-sized USB interface is active during only boot device recovery and ONTAP software update or firmware update.

Management Interfaces

- e0M interface:
  - Is dedicated for management traffic
  - Is used for ONTAP system administration tasks
- BMC or SP interface:
  - Is used to manage and provide remote management capabilities for the storage system
  - Provides remote access to the console and provides monitoring, troubleshooting, logging, and alerting features
  - Remains operational
  - Uses the following setup command:
    `system service-processor`



Some storage system models include an e0M interface. The interface is dedicated to ONTAP management activities. An e0M interface enables you to separate management traffic from data traffic on your storage system for better security and throughput.

To set up a storage system that has the e0M interface, remember the following information:

- The Ethernet port that is indicated by a wrench icon on the rear of the chassis connects to an internal Ethernet switch.
- You should follow the ONTAP setup script.
- To manage LAN in environments in which dedicated LANs isolate management traffic from data traffic, use the e0M interface.
- Configure e0M separately from the BMC or SP configuration.
- Both configurations require unique IP and MAC addresses to enable the Ethernet switch to direct traffic to either the management interfaces or the BMC or SP.

For more information about configuring remote support, see the *ONTAP System Administration Guide* and *ONTAP Remote Support Agent Configuration Guide*.

Console on Boot

```
SP node2> system console
Type Ctrl-D to exit.

LOADER> boot_ontap
...
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
...
```


Typical boot sequence:

1. Loads the kernel into memory from the boot device
2. Mounts the “/” root image from rootfs.img on the boot device
3. Loads `Init` and runs start-up scripts
4. Loads NVRAM kernel modules
5. Creates /var partition on NVRAM (restored from the boot device if a backup copy exists)
6. Starts management processes
7. Loads the data and network modules
8. Mounts the vol0 root volume
9. Is ready for use

Boot Menu

```
^C
Boot Menu will be available.

Please choose one of the following:

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning
Selection (1-9)? 1
```


Generally, you allow a node to boot into ONTAP. The boot menu provides additional options that are useful for troubleshooting or maintenance. To access the boot menu, you must press `Ctrl+C when you are prompted during the boot sequence`.

Select one of the following options by entering the corresponding number:

1. Normal Boot: Continue to boot the node in normal mode.
2. Boot without /etc/rc: This option is obsolete: it does not affect the system.
3. Change password: Change the password of the node, which is also the "admin" account password.
4. Clean configuration and initialize all disks: Initialize the node disks and create a root volume for the node.

   NOTE: This menu option erases all data on the disks of the node and resets your node configuration to the factory default settings.

5. Maintenance mode boot: Perform aggregate and disk maintenance operations and obtain detailed aggregate and disk information. To exit Maintenance mode, use the halt command.
6. Update flash from backup config: Restore the configuration information from the node's root volume to the boot device.
7. Install new software first: Install new software on the node.

   NOTE: This menu option is for only installing a newer version of ONTAP software on a node that has no root volume installed. Do not use this menu option to upgrade ONTAP.

8. Reboot Node: Reboot the node.
9. Configure Advanced Drive Partitioning: For systems that support ADP, this option enables you to configure Advanced Drive Partitioning of the drives.

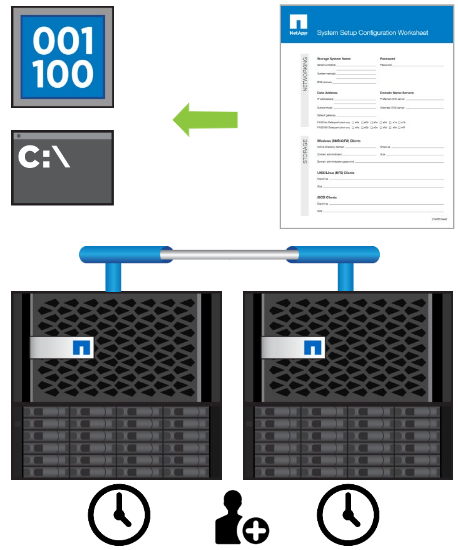
ACTION: Topic for Discussion

- Why might you need to access the boot menu?

Creating a Cluster

Cluster creation methods:

- CLI cluster setup wizard:
  - Use a wizard to create the cluster and join all nodes.
  - Configure the cluster time and AutoSupport functionality.
- Guided Cluster Setup with OnCommand System Manager:
  - Use the CLI to configure the node management interface.
  - Use a web browser to connect to the node management IP address.



? More info in Addendum

Note: NetApp recommends that you use the Guided Cluster Setup for consistency and simplicity.

After you install the hardware, you can set up the cluster by using the cluster setup wizard (through the CLI). In ONTAP 9.1 and later software, you can use the Guided Cluster Setup (through OnCommand System Manager).

Before you set up a cluster, you should use a cluster setup worksheet and record the values that you need during the setup process. Worksheets are available on the NetApp Support website. If you use the System Setup software, enter the information that you collected on the worksheet as the software prompts you.

Whichever method you select, you begin by using the CLI to enter the cluster setup wizard from a single node in the cluster. The cluster setup wizard prompts you to configure the node management interface. Next, the cluster setup wizard asks whether you want to complete the setup wizard by using the CLI.

If you press Enter, the wizard continues to use the CLI to guide you through the configuration. When you are prompted, enter the information that you collected on the worksheet. After you create the cluster, you use the node setup wizard to join nodes to the cluster one at a time. The node setup wizard helps you to configure each node's node-management interface.

After you use the CLI to add all nodes, you also need to manually configure a few items. Synchronizing the time ensures that every node in the cluster has the same time and prevents CIFS and Kerberos failures. You need to decide where to send event notifications: to an email address, a syslog server, or an SNMP traphost. NetApp also recommends that you configure the AutoSupport support tool.

To use Guided Cluster Setup instead of the CLI, use a web browser to connect to the node management IP that you configured on the first node. When you are prompted, enter the information that you collected on the worksheet. The Guided Cluster Setup discovers all of the nodes in the cluster and then configures the nodes simultaneously.

Additional Training

ONTAP Cluster Installation Workshop (instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000016609

Universal NetApp FAS Installation (web-based course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000027858

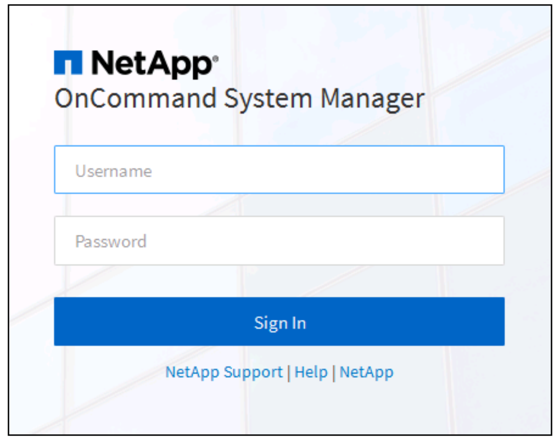
ONTAP Cluster Installation Workshop (instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000016609

Universal NetApp FAS Installation (web-based course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000027858

Lesson 3
Administration Interfaces

Cluster Administrators

- Manage the entire cluster:
  - All cluster resources
  - SVM creation and management
  - Access control and roles
  - Resource delegation
- Use login credentials:
  - User name (default): **admin**
  - Password: password that you created during cluster setup



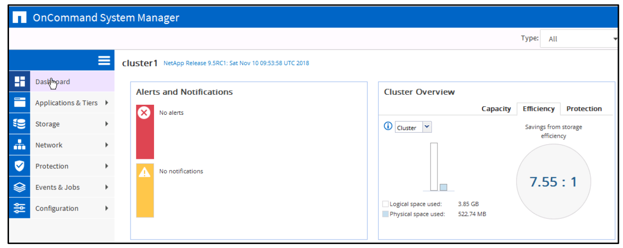
 23

After you use System Setup to create the cluster, a link is provided to launch OnCommand System Manager. Log in as the cluster administrator to manage the entire cluster. You manage all cluster resources, the creation and management of SVMs, access control and roles, and resource delegation.

To log in to the cluster, use the default user name “admin” and the password that you configured during cluster creation.

Managing Resources in a Cluster

- OnCommand System Manager:
  - Visual representation of the available resources
  - Wizard-based resource creation
  - Best practice configurations
  - Limited advanced operations
- The CLI:
  - Manual or scripted commands
  - Manual resource creation that might require many steps
  - Ability to focus and switch quickly among specific objects
- Automation Tools:
  - OnCommand Workflow Automation (WFA)
  - API/ZAPI
  - Ansible




```
login as: admin
Using keyboard-interactive authentication.
Password: *********
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01            true    true
cluster1-02            true    true
```


You can use many tools to create and manage cluster resources. Each tool has advantages and disadvantages.

OnCommand System Manager is a web-based UI that provides a visual representation of the available resources. Resource creation is wizard-based and adheres to best practices. However, not all operations are available. Some advanced operations might need to be performed by commands in the CLI.

You can use the CLI to create and configure resources. Enter commands manually or through scripts. Instead of the wizards that System Manager uses, the CLI might require many manual commands to create and configure a resource. Although manual commands give the administrator more control, manual commands are also more prone to mistakes that can cause issues. One advantage of using the CLI is that the administrator can quickly switch focus without needing to move through System Manager pages to find different objects.

You can also use automation tools like WFA or Ansible or script calls through APIs and ZAPIs to manage resources.

Clustershell

The default CLI, or shell, in ONTAP is called the clustershell and has the following features:

- Inline help
- Online manual pages
- Command history
- Ability to reissue a command
- Keyboard shortcuts
- Queries and UNIX-style patterns
- Wildcards

```
login as: admin
Using keyboard-interactive authentication.
Password: *********
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01            true    true
cluster1-02            true    true

cluster1::>
```

 25

The cluster has different CLIs or shells for different purposes. This course focuses on the clustershell, which starts automatically when you log in to the cluster.

Clustershell features include inline help, an online manual, `history` and `redo` commands, and keyboard shortcuts. The clustershell also supports queries and UNIX-style patterns. Wildcards enable you to match multiple values in command-parameter arguments.

Clustershell

Command scope

```
cluster1::> storage aggregate
```

```
cluster1::storage aggregate> modify
```


Typing the first two levels of the command directory puts you in the command directory. You can then type a command from that level or type a fully qualified command from a different command directory.

Clustershell

cluster1::>

Use of the question mark wildcard

```
cluster1::> storage aggregate
cluster1::storage aggregate> modify?
[-aggregate] <aggregate name>                Aggregate
[ -disktype|-T {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS  | SATA | SSD | VMDISK} ]
                                              Disk Type
[ -free-space-realloc {on|off|no_redirect} ]  Free Space Reallocation
[ -ha-policy {sfo|cfo} ]                      HA Policy
[ -percent-snapshot-space <percent> ]         Space Reserved for Snapshot Copies
[ -space-nearly-full-threshold-percent <percent> ]
                                              Aggregate Nearly Full Threshold Percent
[ -space-full-threshold-percent <percent> ]   Aggregate Full Threshold Percent
[ -hybrid-enabled {true|false} ]              Hybrid Enabled
[ -force-hybrid-enabled|-f [true] ]           Force Marking of Aggregate as Hybrid Enabled
[ -maxraidsize|-s <integer> ]                 Max RAID Size
 cluster1::storage aggregate> modify
```


At the command line, press the question mark (**?**) key to show the command directories and commands that are available at that command level.

Clustershell

Tab completion

```
cluster1::storage aggregate>   modify   [Tab]
    aggr0_n1 aggr0_n2 n1_data_001 n1_data_002
    n1_data_003 n2_data_001

cluster1::storage aggregate> modify -aggregate   [Tab] n2_data_001
-state online
Aggregate offline successful on aggregate: n2_data_001

cluster1::storage aggregate>
```


Press the Tab key to show available directories, commands, and parameters or to automatically complete a command (or a portion of a command). You can also use the Tab key to complete nonambiguous substrings of commands, parameters, and values.

Administrative Interfaces

Privilege levels

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous;
use them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
cluster1::*> set admin
cluster1::>
```

* In prompt indicates advanced privilege

The clustershell features privilege levels that force administrators to be mindful of commands that can harm the health of the storage system. The admin privilege level is used for most tasks. Advanced and diagnostic levels are reserved for more risky functions.

ONTAP software provides multiple sets of commands that are based on privilege levels. ONTAP offers administrative, advanced, and diagnostic levels. Use the `priv` command to set the privilege level.

The administrative level provides access to commands that are sufficient for managing your storage system. The advanced and diag levels provide access to the same administrative commands, plus additional troubleshooting and diagnostic commands.

Advanced level and diag level commands should be used only with the guidance of NetApp technical support.

Clustershell

Scope return

```
cluster1::storage disk option>..
cluster1::storage disk>top
cluster1::>
```


Use the `..` command to move up one level in the command hierarchy. Use the `top` command to move to the top level of the command hierarchy.

Clustershell

Additional features

The search path enables you to run commands out of context:

```
cluster1::system node> disk show = storage disk show
```

Abbreviation is permitted (shortest unambiguous sequences of characters):

```
cluster1::> aggr show = storage aggregate show
cluster1::> net int show = network interface show
```

You can run queries with patterns and wildcards:

```
cluster1::> storage disk show –physical-size >500gb
```

Use the up arrow key to review command history.

 31

You can abbreviate commands and parameters in the clustershell if the abbreviation is unambiguous in the current context. You can also run commands out of context if the command is not available in any other context.

References

- NetApp Hardware Universe: http://hwu.netapp.com
- ONTAP 9 Documentation Center: http://docs.netapp.com/ontap-9/index.jsp
  - *Software Setup Guide*
  - *Cluster Management Using OnCommand System Manager*
  - *System Administration Reference*

NetApp Hardware Universe: http://hwu.netapp.com

ONTAP 9 Documentation Center: http://docs.netapp.com/ontap-9/index.jsp

Module Review

This module focused on enabling you to do the following:

- Identify supported cluster configurations
- List the steps to set up a cluster
- Manage cluster nodes at the hardware level

ACTION: Try This Task

1. In your exercise kit, log in to cluster1.
2. Enter: **?**

   Is a `show` command available?
3. Enter: **`cluster show`**
   - How many nodes does the cluster have?
   - What is the status of the nodes?
4. Enter: **`cluster`**

   Which command scope are you in?
5. Enter: **?**
   - Is a show command available?
   - How do you exit to the root command scope?

Answers:

2. There is no show command at this level.

3a. The cluster has two nodes.

3b. Both nodes should be healthy and eligible.

4. You are in the cluster command scope.

5a. A show command is available.

5b. `top` or `..` returns you to the root of the command directory.

ACTION: Complete an Exercise

Module 2: Exploring ONTAP Management UIs

Duration: 30 minutes

Access your lab equipment.

Use the login credentials that your instructor provided to you.

Open your Exercise Guide.

Go to the exercise for the module.

Complete the specified tasks.

- Start with Exercise 2-1.
- Stop at the end of Exercise 2-1.

Participate in the review session.

- Share your results.
- Report issues.

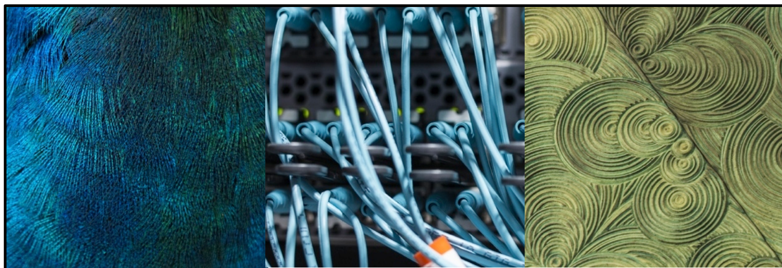
ACTION: Share Your Experiences

Roundtable questions for the equipment-based exercises

OnCommand System Manager versus clustershell:

- Which method do you prefer to use for configuring volumes?
- Which method do you prefer to use for configuring LUNs?

If you encounter an issue, notify your instructor immediately so that it can be resolved promptly.



Addendum
OnCommand System Manager: Guided Cluster Setup

Guided Cluster Setup

Set up the node management interface

- Boot a node that is part of the cluster.
- From the node management IP interface for the node, launch the cluster setup wizard.
- From the following URL, continue the cluster setup:
  https://<*node-management-IP-address*>

```
Welcome to the cluster setup wizard.

...

Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address: 192.168.0.51
Enter the node management interface netmask: 255.255.255.0
Enter the node management interface default gateway: <Enter>
A node management interface on port e0M with IP address
192.168.0.51 has been created.

Use your web browser to complete cluster setup by accessing
https://192.168.0.51

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

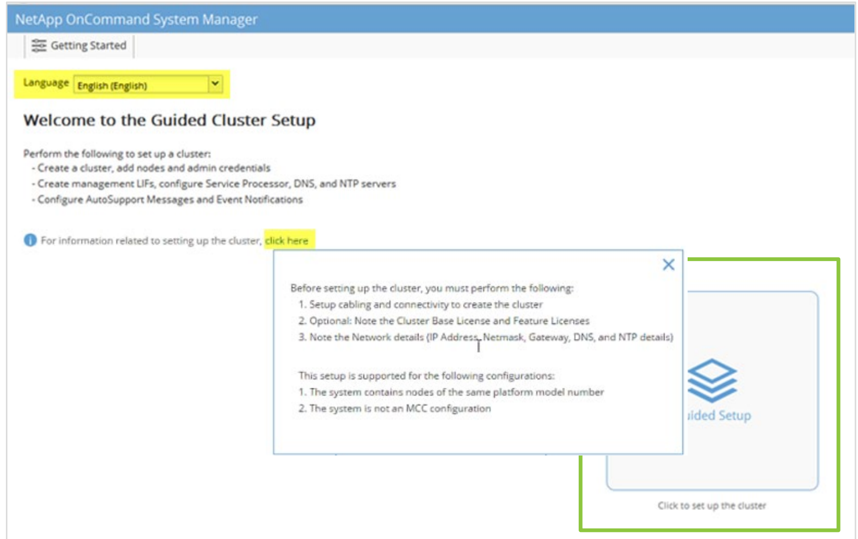
Help and AutoSupport messages are not shown.

Continue cluster setup with the Guided Cluster Setup wizard in OnCommand System Manager through a web browser.

Guided Cluster Setup

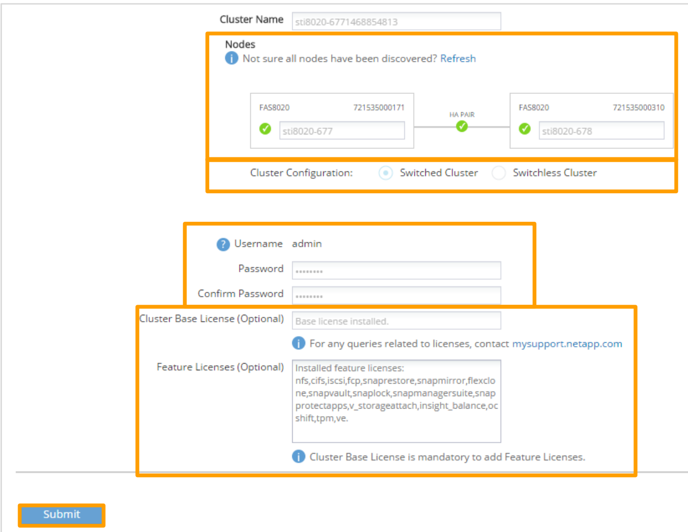
Welcome page

- If a node has a default password, the login page is not displayed. A language menu is available.
- For information about the prerequisites for cluster setup, click “**click here**.”
- After you review the prerequisites, click **Guided Setup**.



Guided Cluster Setup

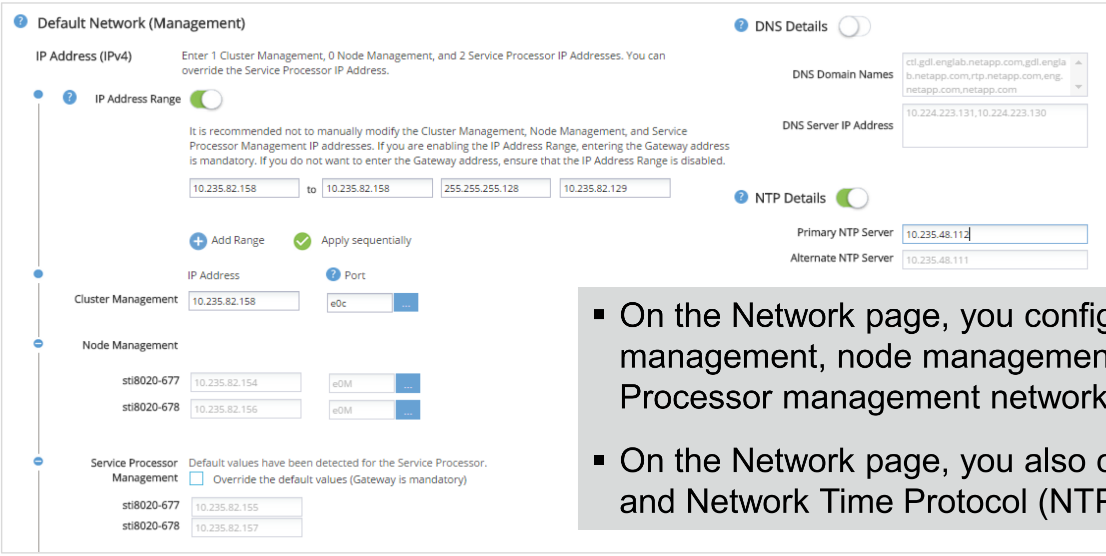
Cluster page



- Information about nodes is discovered and displayed.
- Depending on the network configuration, a single-node cluster, a two-node switchless cluster, or a switched cluster is created.
- Set an administrator password.
- Provide a base license and (optional) feature licenses.
- When you click Submit, the cluster creation process starts on the first node. Other nodes are then joined sequentially.

Guided Cluster Setup

Network page

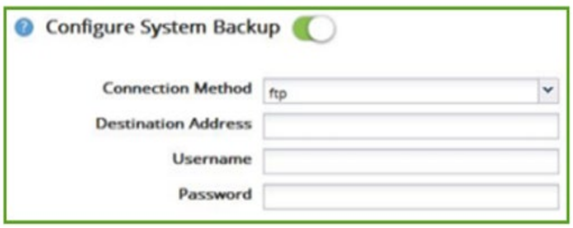


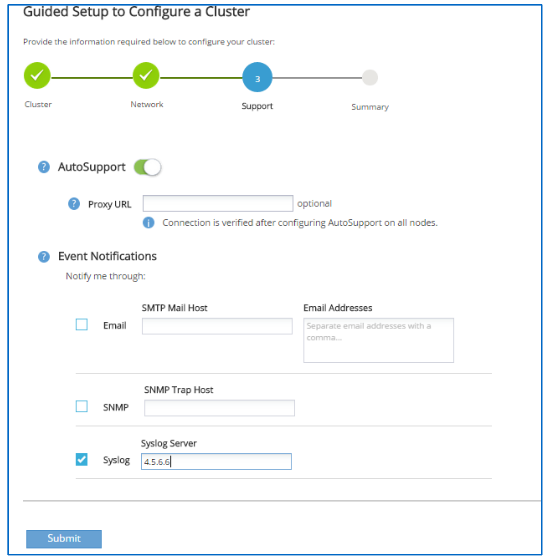
- On the Network page, you configure the cluster management, node management, and Service Processor management network interfaces.
- On the Network page, you also configure DNS and Network Time Protocol (NTP).

Guided Cluster Setup

Support page

- On the Support page, you configure AutoSupport and event notification.
- For single-node clusters, on the Support page, you configure system backup.

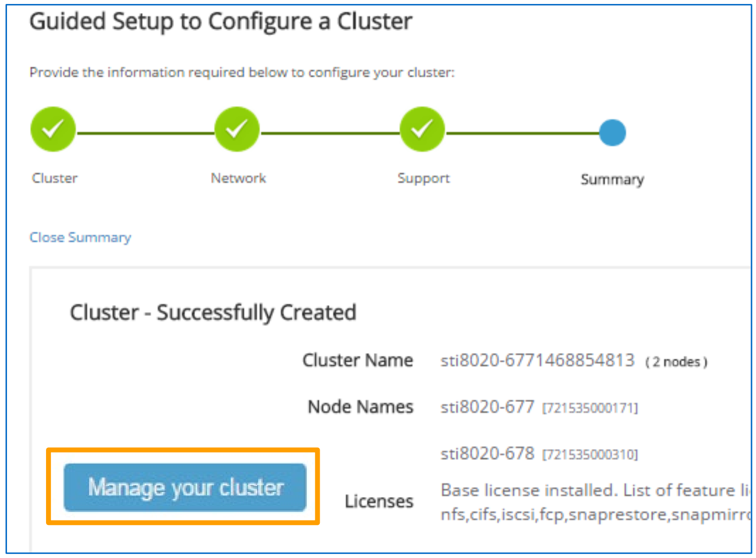




Guided Cluster Setup

Summary page

- The Summary page lists all of the configuration information from previous pages.
- If there is an error in the configuration, the Summary page shows the error.
- When you click "Manage your cluster," OnCommand System Manager is launched from the cluster management LIF that you created.



Module 3
Cluster Management

In this module, you learn how to configure key features of NetApp ONTAP software, such as role-based access control (RBAC), feature licensing, Network Time Protocol (NTP), and the AutoSupport tool. You also learn about policies and job schedules, which are used throughout this course.

About This Module

This module focuses on enabling you to do the following:

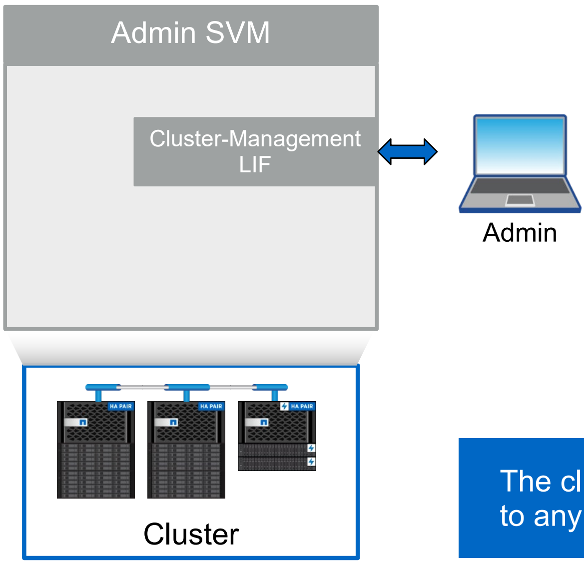
- Manage access control
- Set the date and time on cluster nodes
- Manage ONTAP software licenses
- Manage jobs and schedules

The cluster might require initial configuration, depending on the environment. This module discusses access control, date and time, licenses, jobs, and schedules. If you used System Setup software to create the cluster, some of the items might already be configured.

This module focuses on cluster administration. Two types of administrators can manage a cluster.

What a storage virtual machine (SVM) administrator can configure is based on how the cluster administrator has configured the SVM administrator's user account.

Admin SVM



Admin SVM:
- Automatic creation during the cluster creation process
- Representation of the cluster
- Primary access point for administration of nodes, resources, and data SVMs

An admin SVM does *not* serve data.
- A cluster must have at least one data SVM to serve data to clients.

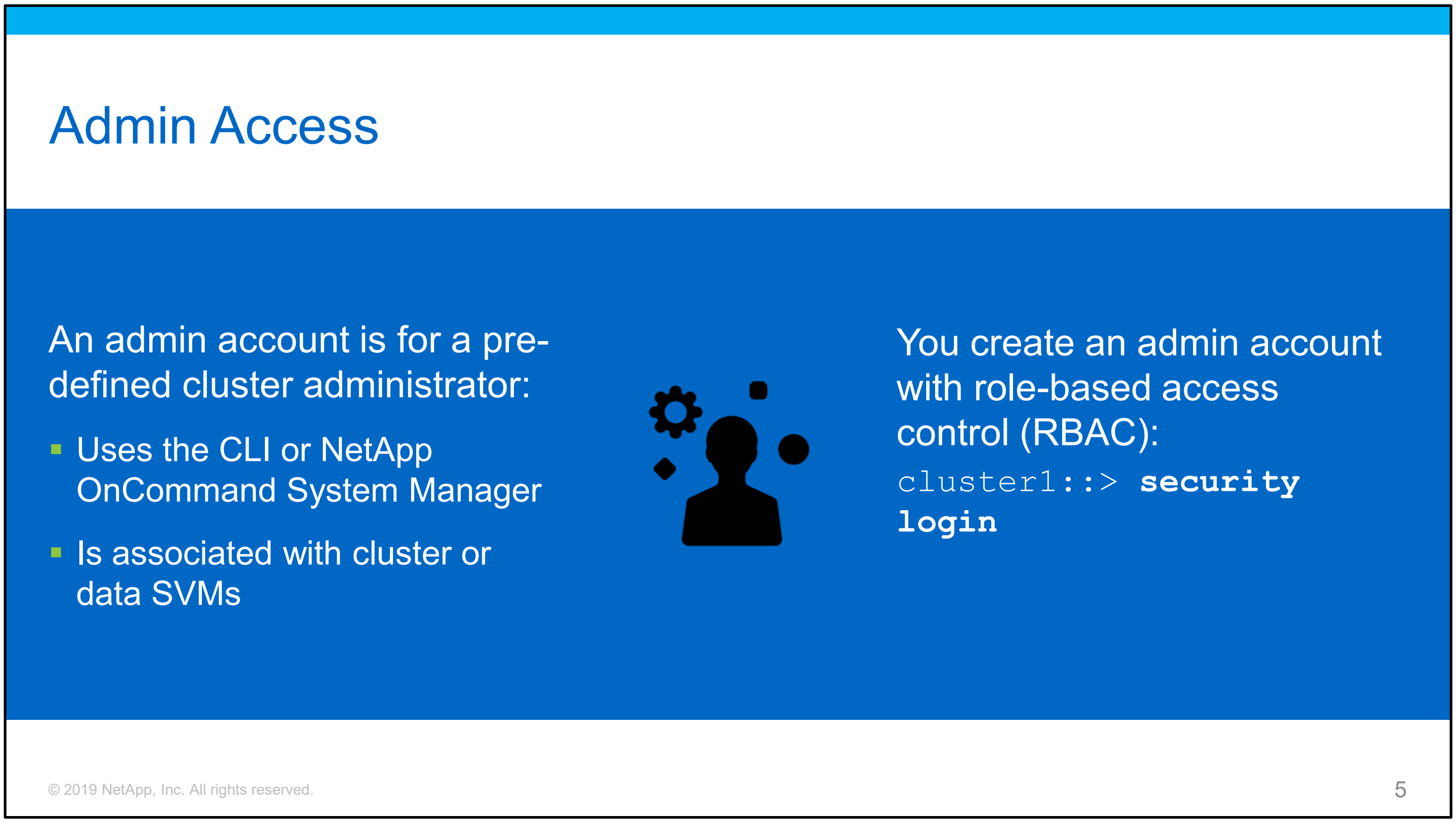
The cluster management LIF is configured to fail over to any node in the cluster.

 4

The admin SVM is used to manage the cluster.

There is only one admin SVM, which represents the cluster. Through the cluster management LIF, you can manage any node, resource, or data SVM.

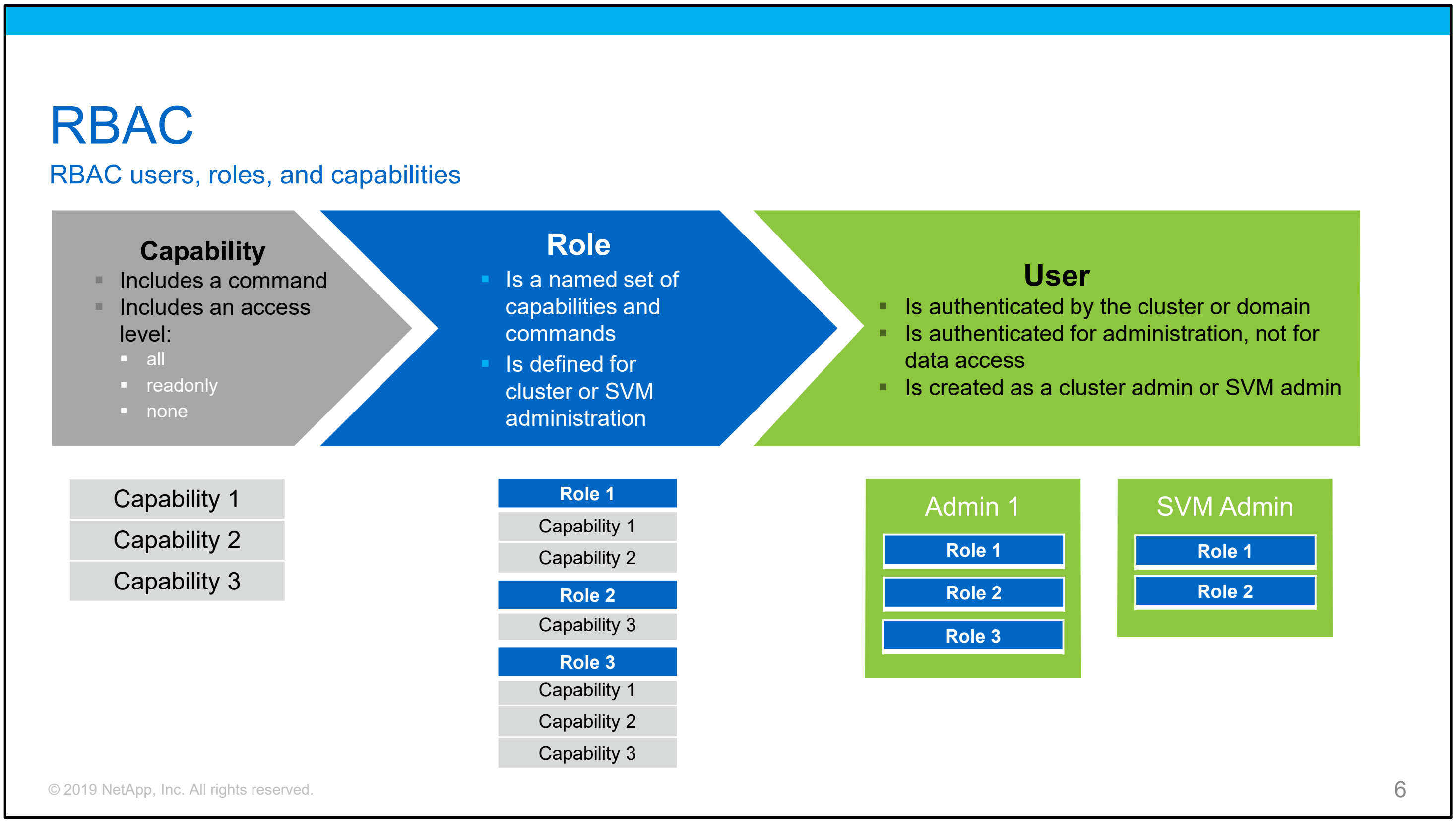
Unless otherwise specified, the term SVM typically refers to a data-serving SVM. Also, in the CLI, SVMs are displayed as “Vservers and many commands use a –vserver parameter to specify SVMs. The term vserver is a holdover from early versions of ONTAP (formerly Clustered ONTAP) and maintained for backward-compatibility.



You can use the default system administration account to manage a storage system, or you can create additional administrator user accounts to manage administrative access to the storage system.

You might want to create an administrator account for the following reasons:

- You can specify administrators and groups of administrators with differing degrees of administrative access to your storage systems.
- You can limit an administrator’s access to specific storage systems by providing an administrative account on only those systems.
- Creating different administrative users enables you to display information about who is performing which commands on the storage system.



You assign users to roles based on their responsibilities.

Each role is granted a set of rules that enables a set of capabilities. A role is defined as cluster-scoped or SVM-scoped. You can use built-in roles and create custom roles. The capabilities of the predefined roles cannot be changed.

Capabilities are a combination of a command and an access level. A command is a specific instruction or an entire command tree. The three access levels are all, read-only, and none.

Admins are assigned roles, and roles are assigned capabilities.

RBAC

Predefined roles in ONTAP software

Cluster-scoped roles:

- admin
- readonly
- none
- backup
- autosupport

```
::> security login role show -vserver svl-nau
```

Data SVM-scoped roles:

- vsadmin
- vsadmin-volume
- vsadmin-protocol
- vsadmin-backup
- vsadmin-snaplock
- vsadmin-readonly

```
::> security login role show -vserver svm_red
```


ONTAP software includes administrative access-control roles that can be used to subdivide administration duties for SVM administration tasks.

The vsadmin role is the superuser role for an SVM. The admin role is the superuser for a cluster.

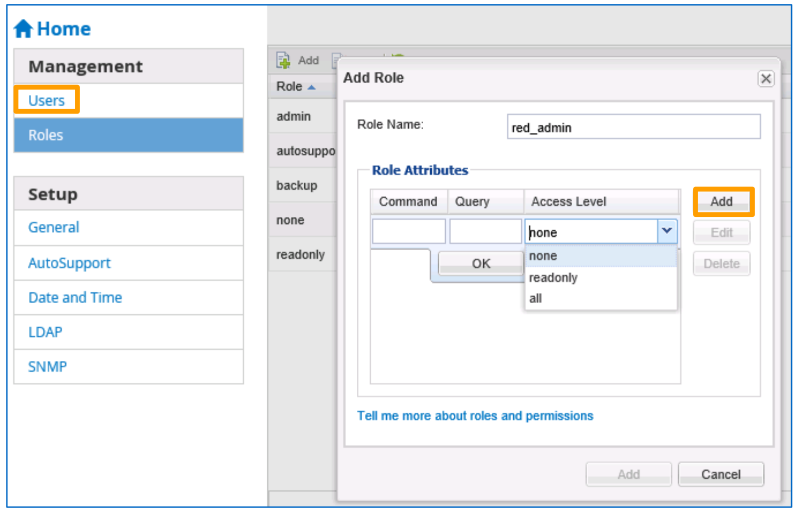
The vsadmin role grants the data SVM admin full administrative privileges for the SVM. Additional roles include the vsadmin-protocol role, the vsadmin-readonly role, and the vsadmin-volume role. Each role provides a unique SVM administration privilege.

A cluster admin with the “readonly” role can grant read-only capabilities. A cluster admin with the “none” role cannot grant capabilities.

RBAC

Custom roles

- Role name
- Command directory
- Query
- Access level




```
::> security login role create…
::> security login modify –vserver svm_red –user ken –role redvols
```

 8

Cluster admins can create access-control roles to apply to cluster or SVM admins. The roles can grant or limit authority to perform certain system administration tasks. An access-control role consists of a role name and a command or a command directory to which the role has access. The role can include an access level (none, readonly, or all) and a query that applies to the specified command or command directory. The example on the slide creates a role that is named svm1vols and that grants access to the volume commands but limits access to aggregates that start with the “aggr7” string. The role is assigned to a user who is named Ken.

After the role is created, you can apply the role to individual administrators:

```
c1::> security login role create -vserver svm1 -role svm1vols -cmddirname volume -query "-aggr aggr7*" -access all

c1::> security login modify -vserver svm1 -user ken -role svm1vols
```

Active Directory Authentication for Admins

- Active Directory authentication functionality is fully supported.
- No CIFS license is required.

```
::> security login create -vserver cluster1
-username learn\Administrator -application ssh
-authmethod domain
```


Active Directory authentication for cluster and SVM admins provides a dedicated, CIFS-licensed SVM that serves as a communication tunnel to the administration server. The enhancement satisfies customers who want to use Active Directory to authenticate their storage and SVM admins but do not need CIFS data access.

You must also create cluster user accounts for the domain users.

Administrative Security

- Use the `security` login command to configure role-based administrative access to the cluster.
- Configure by application: console, HTTP, SNMP, Secure Shell (SSH), and the ONTAPI interface library.
- To enable and disable security audit logging, use the following command:

```
::> security audit modify -cliget on -ontapiget on
```

- Audited commands go to the management log.
- Nodes track local SSH and console commands in the command history log.

NOTE: System log access is covered later in the course.

`-cliget`: This term specifies whether get requests for the CLI are audited. The default setting is off.

`-ontapiget`: This term specifies whether get requests for the ONTAP API (ONTAPI) interface library are audited. The default setting is `off`.

Security Login Banner and Message of the Day

For legal purposes, computer systems must display a warning to unauthorized users who are connecting to the system.

- This legal warning is configured in ONTAP software using the `security login banner` command.
- The message of the day (MOTD) subcommand enables you to show a message to all cluster and SVM administrators when they open a console session:

```
::> security login motd modify
```

 11

When you connect to any government or corporate system, one of the first things that you see is a warning about the legal consequences of unauthorized access. You can use the security login banner command to configure this legal warning on your cluster.

Another feature of the security login command is the MOTD (mote-D), or message of the day, subcommand. This command enables you to display a short message to anyone logging in through the CLI console. You might want to provide a reminder about a meeting, system maintenance, or planned downtime, or you might wish someone a happy birthday or work anniversary.

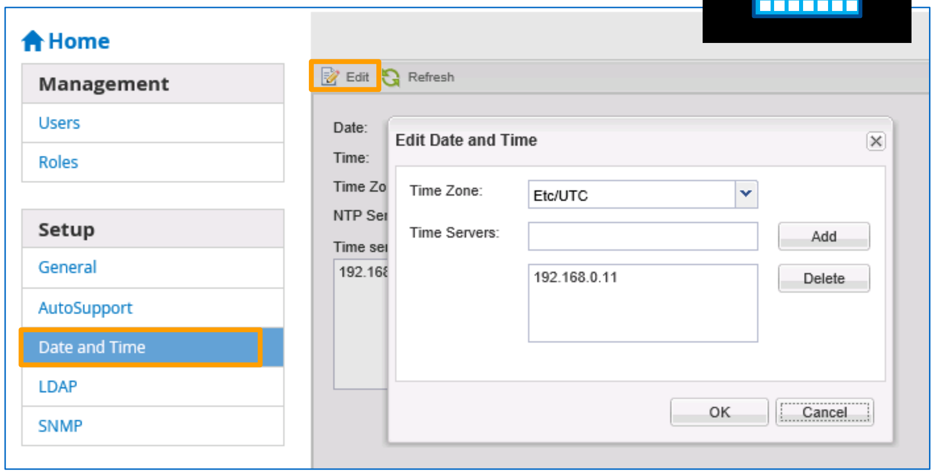
Date and Time

Date and Time

Ways to configure date and time:

- Manually: with CLI
- Automatically: with Network Time Protocol (NTP) servers

After you add an NTP server, the nodes require time to synchronize.




```
::> cluster time-service ntp server create -server xx.xx.xx.xx
::> date
```

 12

Problems can occur when the cluster time is inaccurate. ONTAP software enables you to manually set the time zone, date, and time on the cluster. However, you should configure the NTP servers to synchronize the cluster time.

To configure the date and time, in OnCommand System Manager, on the cluster system tools Configurations tab, click **Date and Time**. Click **Edit**. From the Time Zone list, select the time zone. In the Time Servers field, enter the NTP address. Click **Add**.

Adding the NTP server automatically configures all of the nodes in the cluster, but each node needs to synchronize individually. The synchronization for all of the nodes in the cluster might require a few minutes.

License Types

- Standard license
- Enterprise license
- Evaluation license
- Capacity license

A license is a record of one or more software entitlements. License keys, also known as license codes, enable you to use certain features or services on your cluster. Each cluster requires a cluster base license key, which you can install either during or after the cluster setup. Some features require additional licenses. ONTAP feature licenses are issued as packages, each of which contains one or more features. A package requires a license key, and installing the key enables you to access all of the features in the package. ONTAP software prevents you from installing a feature license before a cluster base license key is installed.

Standard and Enterprise Licenses

- Proof of sale is recorded as a license entitlement record.
- License keys are 28 characters long.
- Standard licenses are linked to the controller serial number (node locked).
  Features are licensed on every node and continue to function as long as one licensed node is running.
- Enterprise licenses enable the feature on the entire cluster.
  An enterprise license is not carried with nodes that are removed from the cluster.

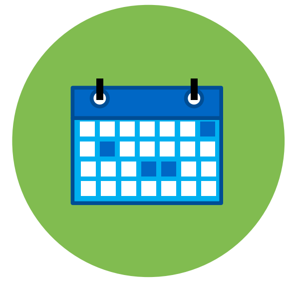
 14

Standard license: A standard license is issued for a node with a specific system serial number and is valid only for the node that has the matching serial number. Installing a standard, node-locked license entitles a node, but not the entire cluster, to the licensed functionality. For the cluster to be enabled, though not *entitled*, to use the licensed functionality, at least one node must be licensed for the functionality. However, if only one node in a cluster is licensed for a feature and that node fails, the feature no longer functions on the rest of the cluster until the licensed node is restarted.

Enterprise license: An Enterprise license is not tied to a specific system serial number. When you install an Enterprise license, all nodes in the cluster are entitled to the licensed functionality. The `system license show` command displays site licenses under the cluster serial number. If your cluster has an Enterprise license and you remove a node from the cluster, the node does not carry the Enterprise license with it. The node is no longer entitled to the licensed functionality. If you add a node to a cluster that has a Enterprise license, the node is automatically entitled to the functionality that the license grants.

Evaluation License

- Enables testing of software functionality before purchasing the license.
- Is a time-limited license.
- Can be renewed, but only a limited number of times before requiring a purchase.



An evaluation license enables you to try certain software functionality without purchasing an entitlement. If your cluster has an evaluation license for a package and you remove a node from the cluster, the node does not carry the evaluation license. Evaluation licenses are best used for proof of concept testing on test and development clusters rather than on a production cluster.

Capacity Licenses

- Capacity licenses are sold individually for increments of storage capacity (500TB, 100TB, 50TB, and so on).
- These licenses are used with ONTAP Select, Cloud Volumes, and FlexPool functionality.
- Additional capacity can be added to a capacity pool license at any time.
- Enforcement is performed at the aggregate level and relies on an aggregate lease.
- An expired lease prevents users from bringing aggregates back online after a manual reboot.
- License codes are shorter than 28 characters.

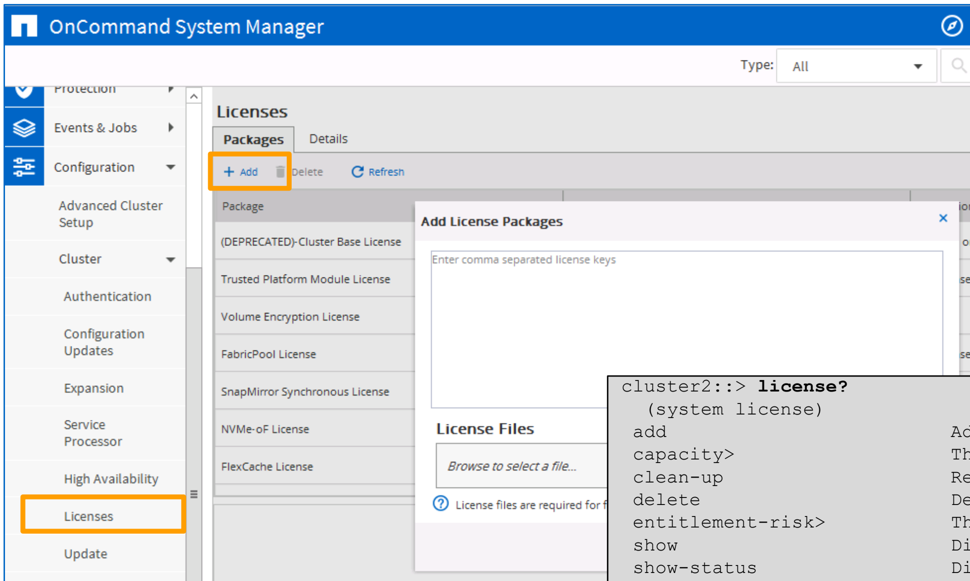
Capacity licenses are additional license requirements on a cluster on which storage capacity is sold in increments. ONTAP Select, Cloud Volumes, and FlexPools all require capacity licenses.

To increase the amount of storage capacity in the cluster, you must purchase a license for the increment or increments of capacity that you need.

If the lease on an aggregate expires, rebooting the system makes the aggregate inaccessible.

Unlike standard, enterprise, and evaluation licenses, the capacity licenses are not 28 characters long.

License Commands




```
cluster2::> license?
  (system license)
  add                         Add one or more licenses
  capacity>                   The capacity directory
  clean-up                    Remove unnecessary licenses
  delete                      Delete a license
  entitlement-risk>           The entitlement-risk directory
  show                        Display licenses
  show-status                 Display license status
  status>                     Display license status
```

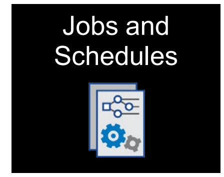
 17

ONTAP software enables you to manage feature licenses in the following ways:

- Add one or more license keys.
- Display information about installed licenses.
- Display the packages that require licenses and the current license status of the packages on the cluster.
- Delete a license from a cluster or from the node with the serial number that you specify.

NOTE: The cluster base license is required for the cluster to operate. ONTAP software does not enable you to delete the license.

- Display or remove expired or unused licenses.



Policy-Based Storage Services

Policy:

- A collection of rules that the cluster or SVM administrator creates and manages
- Predefined or created for managing data access

Policy examples:

- Firewall and security
- Export, quota, file, and data
- Snapshot and SnapMirror
- Quality of service (QoS)

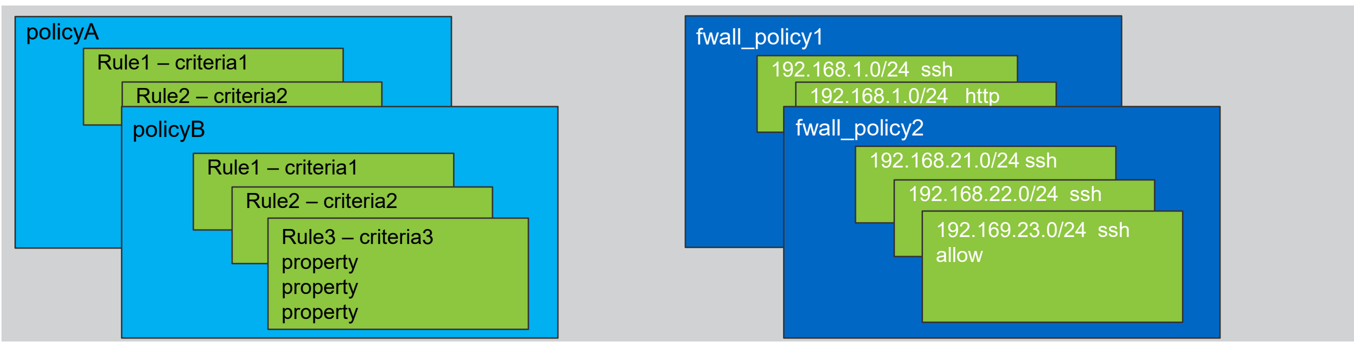
18

The following services are policy-based:

- Firewall
- System health
- SnapMirror
- Volume efficiency
- Volume FlexCache
- Volume quota
- Volume Snapshot
- SVM CIFS group
- SVM data
- SVM export
- SVM FPolicy
- SVM security file directory
- Quality of service (QoS) policy group
- Failover

Policy-Based Management

- You assign a policy to a service or resource.
- A rule criterion in the policy matches the service or resource.
- The matching rule properties apply to the service or resource.
- The example is a firewall that permits or denies access to a protocol for specific IP address ranges.



SVMs use policy-based management for many resources. A policy is a collection of rules or properties that the cluster administrator or SVM administrator creates and manages. Policies are predefined as defaults or created to manage various resources. By default, a policy applies to the current resources and to newly created resources, unless otherwise specified.

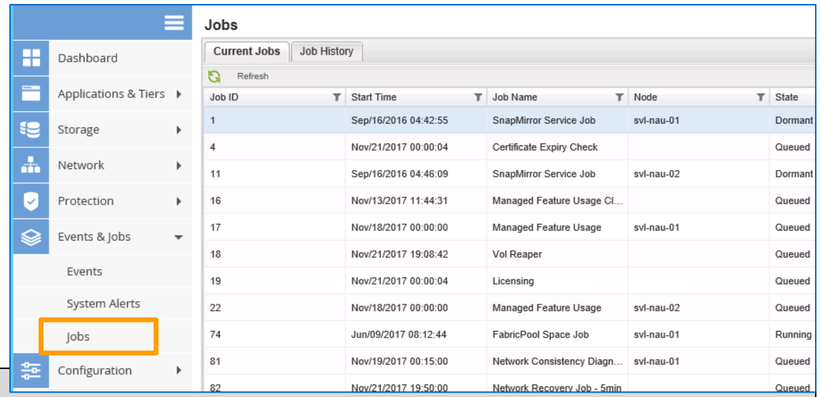
For example, Snapshot policies can be used to schedule automatic controller-based Snapshot copies. The policy includes such things as the schedule or schedules to use and how many copies to retain. When a volume is created for the SVM, the policy is applied automatically but can be modified later.

The efficiency policy is used to schedule postprocess deduplication operations. The policy might include when and how long deduplication runs.

The examples are only two of the policies that you encounter in ONTAP software. The advantage of policy-based management is that when you create a policy, you can apply the policy to any appropriate resource, either automatically or manually. Without policy-based management, you would need to enter the settings separately for each individual resource.

Jobs

- Asynchronous tasks
- Managed by the Job Manager
- Long-running operations
- In a job queue




```
::> job show
                                   Owning
Job ID Name                        Vserver    Node           State
------ --------------------- ---------- -------------- ----------
2      Vol Reaper                  rtp-nau    -              Queued
       Description: Vol Reaper Job
6      SnapMirror Service Job rtp-nau    rtp-nau-01     Dormant
       Description: SnapMirror Service Job
```

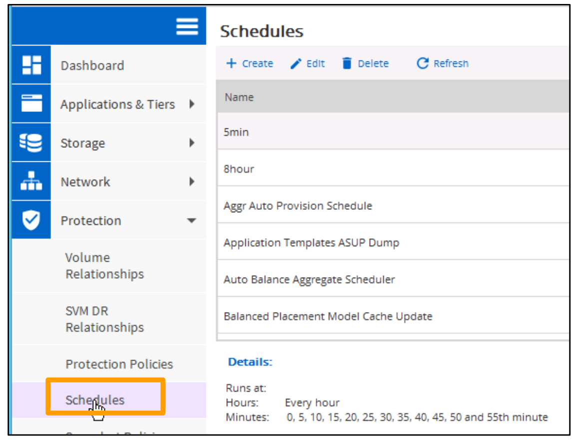

A job is any asynchronous task that Job Manager manages. Jobs are typically long-running volume operations such as copy, move, and mirror. Jobs are placed in a job queue. Jobs run in the background when resources are available. If a job consumes too many cluster resources, you can stop or pause the job until there is less demand on the cluster. You can also monitor jobs, view job history, and restart jobs.

Schedules

Schedules for tasks:

- Time-based schedules, which run at specific times (similar to UNIX cron schedules)
- Interval-based schedules, which run at intervals

```
::> job schedule show
Name          Type      Description
----------- --------- --------------------------------
5min          cron      @:00,:05,:10,:15,:20,:25,:30,:35
8hour         cron      @2:15,10:15,18:15
Auto Balance Aggregate Scheduler
              interval  Every 1h
RepositoryBalanceMonitorJobSchedule
              interval  Every 10m
daily         cron      @0:10
hourly        cron      @:05
monthly       cron      1@0:20
weekly        cron      Sun@0:15
```



 21

Many tasks, such as volume Snapshot copies, can be configured to run on specified schedules. Schedules that run at specific times are called cron schedules. The schedules are similar to UNIX cron schedules. Schedules that run at intervals are called interval schedules.

To manage schedules in System Manager, on the cluster Configuration tab, you click the Schedules link. You can create, edit, and delete schedules.

Knowledge Check: Question

The admin SVM manages the cluster and serves data.

a. true
b. false

References

- NetApp Hardware Universe
  http://hwu.netapp.com
- ONTAP 9 Documentation Center
  http://docs.netapp.com/ontap-9/index.jsp
  - *Administrator Authentication and RBAC Power Guide*
  - *System Administration Reference*
  - *ONTAP 9 Concepts*
- TR-4569: Security Hardening Guide for NetApp ONTAP 9
  https://www.netapp.com/us/media/tr-4569.pdf

NetApp Hardware Universe - http://hwu.netapp.com

ONTAP 9 Documentation Center - http://docs.netapp.com/ontap-9/index.jsp

Administrator Authentication and RBAC Power Guide

System Administration Reference

ONTAP 9 Concepts

TR-4569: Security Hardening Guide for NetApp ONTAP 9

https://www.netapp.com/us/media/tr-4569.pdf

Module Review

This module focused on enabling you to do the following:

- Manage access control
- Configure cluster settings
- Manage cluster-level features of ONTAP software

ACTION: Complete an Exercise

Module 3: Managing ONTAP Clusters and Administrators

Duration: 40 minutes

Access your lab equipment.

Use the login credentials that your instructor provided to you.

Open your Exercise Guide.

Go to the exercise for the module.

Complete the specified tasks.

- Start with Exercise 3-1.
- Stop at the end of Exercise 3-1.

Participate in the review session.

- Share your results.
- Report issues.

ACTION: Share Your Experiences

Roundtable questions for the equipment-based exercises

- How did the cluster behave after you specified the NTP server?
- Did the time synchronize immediately?

 26

Have a roundtable discussion with the class to answer these questions. You should also add any comments about experiences or “lessons learned” during the exercises that others might find helpful.

If you encounter an issue, notify your instructor immediately so that it can be resolved promptly.

Module 4
Network Management

About This Module

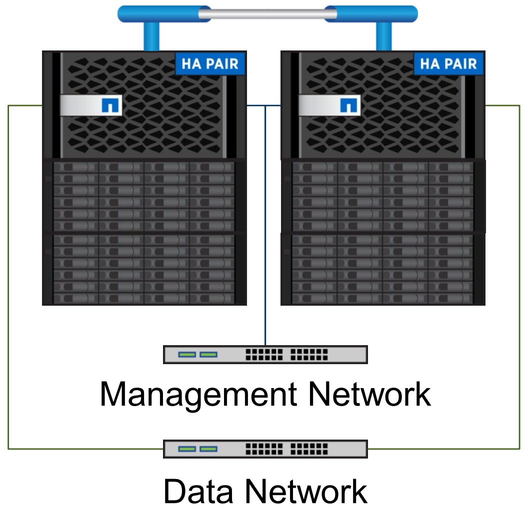
This module focuses on enabling you to do the following:

- Describe the interaction between physical and virtual network resources in a cluster
- Configure and manage physical and virtual networking resources

2

Lesson 1
NetApp ONTAP Network Review

ONTAP Network Types



- Cluster interconnect:
  - Connection of nodes
  - Private network
- Management network:
  - Cluster administration network
  - Possibly a shared Ethernet network with data
- Data network:
  - One or more networks that are used for data access from clients or hosts
  - Ethernet, FC, or converged network

HA: high-availability

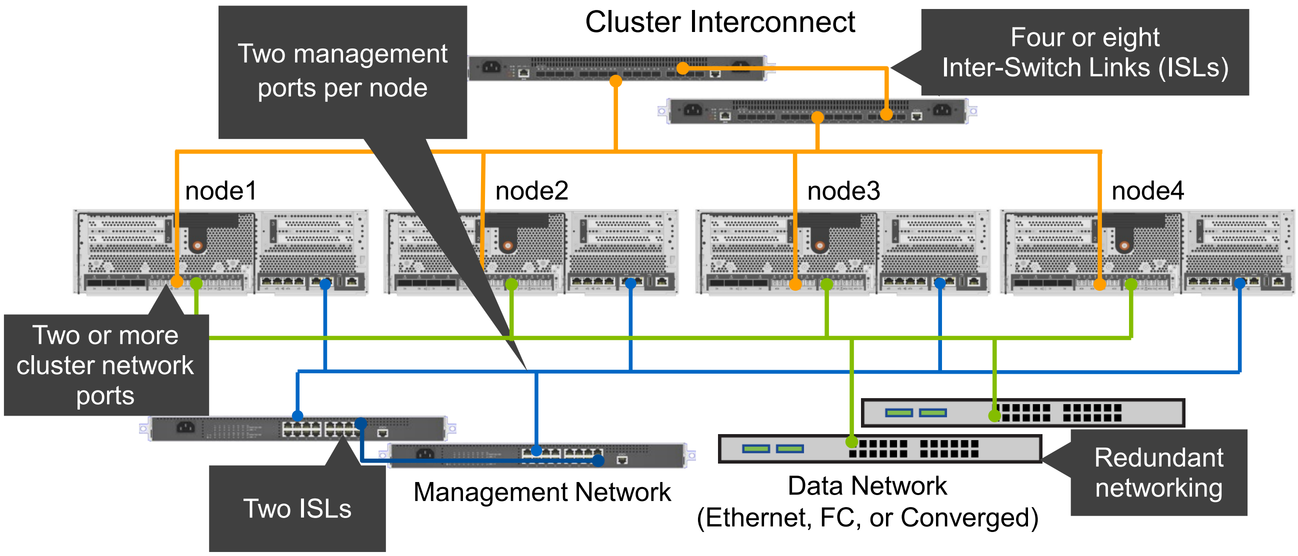
In multinode clusters, nodes need to communicate with each other over a cluster interconnect. In a 2-node cluster, the interconnect can be switchless. When you add more than two nodes to a cluster, a private cluster interconnect that uses switches is required.

The management network is used for cluster administration. Redundant connections to the management ports on each node and management ports on each cluster switch should be provided to the management network. In smaller environments, the management and data networks might be on a shared Ethernet network.

For clients and hosts to access data, a data network is required. The data network can be made up of one or more networks. Depending on the environment, the network might be an Ethernet, FC, or converged network. Data networks can consist of one or more switches or redundant networks.

Networks

NetApp recommends redundant data and management networks.



 5

An ONTAP software cluster is essentially a cluster of high-availability (HA) pairs. Therefore, you need a cluster network, or cluster interconnect, for all of the nodes to communicate with one another. If a node cannot see the cluster interconnect, the node is not part of the cluster. Therefore, the cluster interconnect requires adequate bandwidth *and* resiliency.

The figure shows a 4-node cluster and three distinct networks. ONTAP software requires both data and management connectivity, which can coexist on the same data network.

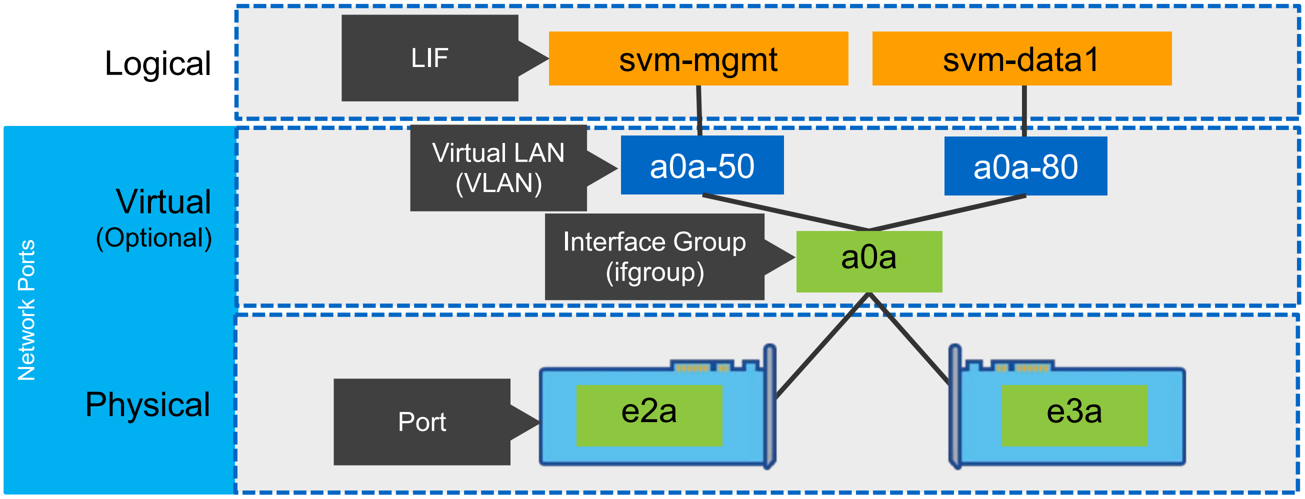
In multinode configurations, ONTAP software also requires a cluster interconnect for cluster traffic. In a 2-node configuration, the cluster interconnect can be as simple as to cable the two nodes or to use switches if expansion is desired. In clusters of more than two nodes, switches are required. For redundancy, you should always have at least one cluster port per switch on each node of the cluster. The number of cluster ports per node depends on the controller model and port speed.

Single-node clusters do not require a cluster interconnect if the environment does not require high availability and nondisruptive operations (NDO).

For site requirements, switch information, port cabling information, and controller onboard port cabling, see the Hardware Universe at hwu.netapp.com.

Lesson 2
Network Ports

ONTAP Networking



 7

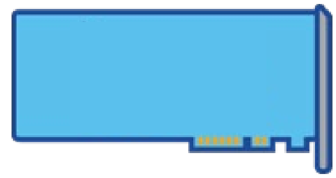
Nodes have physical ports that are available for cluster traffic, management traffic, and data traffic. The ports need to be configured appropriately for the environment. The example shows Ethernet ports. Physical ports also include FC ports and unified target adapter (UTA) ports.

Physical Ethernet ports can be used directly or combined by using interface groups (ifgroups). Also, physical Ethernet ports and ifgroups can be segmented by using virtual LANs (VLANs). VLANs and ifgroups are considered virtual ports but are treated like physical ports.

Unless specified, the term *network port* includes physical ports, ifgroups, and VLANs.

Physical Port Identification

- Ethernet ports are named e<*location*><*letter*>:
  - e0a is the first port on the controller motherboard.
  - e3a is a port on a card in slot 3.
- FC ports are named <*location*><*letter*>:
  - 0a is the first port on the controller motherboard.
  - 3a is a port on a card in slot 3.
- UTA ports have both an Ethernet name and an FC name, e<*location*><*letter*>/<*location*><*letter*>:
  - e0a/0a is the first port on the controller motherboard.
  - e3a/3a is a port on a card in slot 3.
  - Use of show commands returns only FC label names (even in Ethernet mode).



Port names consist of two or three characters that describe the port type and location. You should remember port-naming conventions on the network interfaces.

Ethernet ports: The first character describes the port type and is always e to represent Ethernet. The second character is a numeral that identifies the slot in which the port adapter is located. The numeral 0 (zero) indicates that the port is on the node motherboard. The third character indicates the port position on a multiport adapter. For example, the port name e0b indicates the second Ethernet port on the motherboard, and the port name e3a indicates the first Ethernet port on an adapter in slot 3.

FC ports: The name consists of two characters (dropping the e) but otherwise follows the same naming convention as Ethernet ports. For example, the port name 0b indicates the second FC port on the motherboard. The port name 3a indicates the first FC port on an adapter in slot 3.

UTA ports: A UTA port is physically one port but can pass either Ethernet traffic or FC traffic. Therefore, UTA ports are labeled with both the Ethernet name and the FC name. For example, the port name e0b/0b indicates the second UTA port on the motherboard. The port name e3a/3a indicates the first UTA port on an adapter in slot 3.

NOTE: UTA adapter ports are listed by only the FC label name when you use the ucadmin command, even when the personality is configured as 10-GbE.

Physical Ports Example

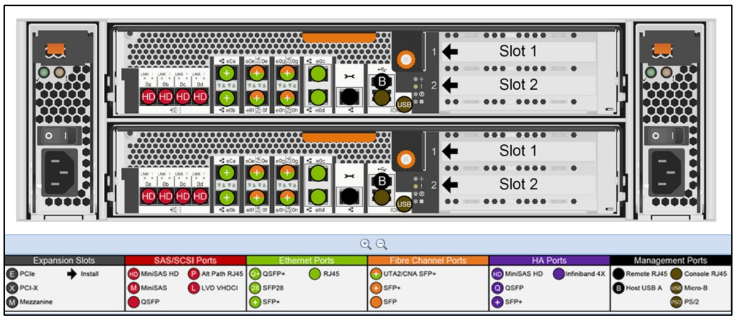
FAS8200

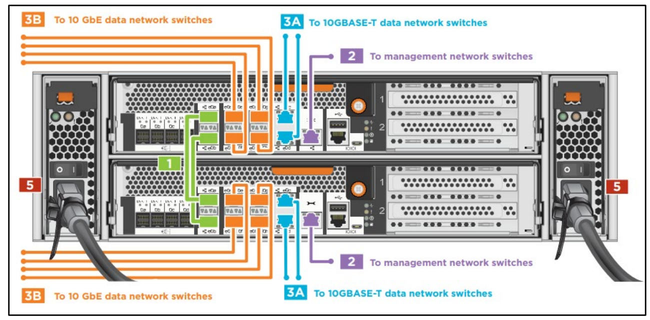
Hardware Universe

- Focused on port identification
- Downloadable Visio-template based picture

Installation & Setup Instructions (ISI)

- Focused on cabling
- PDF on MySupport website



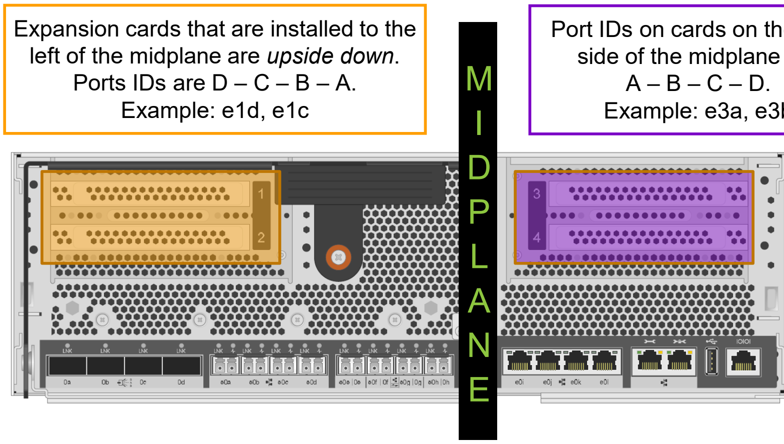


The numbers and types of ports varies by system model, but most systems have dedicated ports for connecting to external drive shelves, Ethernet networks, FC networks, and management networks. There are two primary sources for identifying ports and their use on an AFF or FAS system. In addition to all of the technical details, the Hardware Universe includes Visio-template based diagrams of the front and back of the storage controller. To see how the ports are to be cabled, the Installation and Setup Instructions (ISI) is the best source.

Port Identification on Expansion Cards

Expansion cards that are installed to the left of the midplane are *upside down*.
Ports IDs are D – C – B – A.
Example: e1d, e1c

Port IDs on cards on the right side of the midplane run
A – B – C – D.
Example: e3a, e3b



Pro tip: The A port is always the port closest to the midplane

 10

Systems with expansion ports have an internal circuit board called the midplane that connects expansion cards to the motherboard. Expansion cards that are installed on the left side of the midplane have to be mounted upside down. This configuration makes their port IDs backward. Because many expansion cards do not have labels on their ports, remember that the port closest to the midplane is port A.

NOTE: The AFF A800 and AFF A700s use Peripheral Component Interconnect Express (PCIe) subassemblies rather than a midplane. On these systems, the expansion cards are always oriented correctly.

Modifying Network Port Attributes

Set the UTA2 port personality

Insert the proper optical module before changing modes.

First remove any LIFs and take the port offline.

```
cluster2::> system node hardware unified-connect modify
            -node cluster2-01 -adapter 0e
            -mode fc|cna
cluster2::> system node reboot -node cluster2-01
```


UTA ports are managed in a similar way and require a reboot to take effect. The adapter must also be offline before you can make any changes.

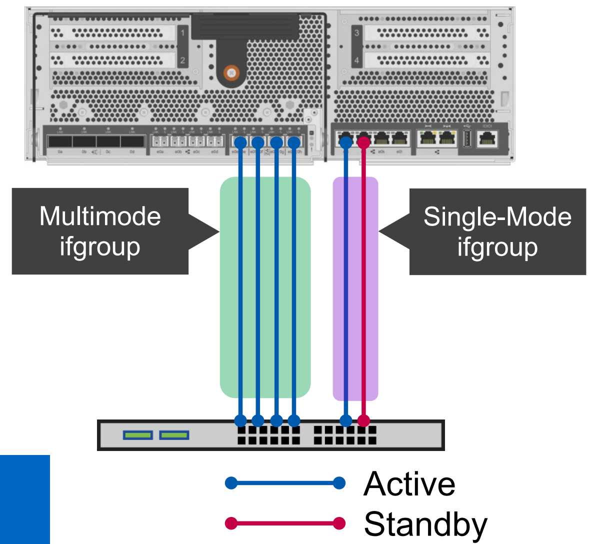
- When the adapter type is initiator, use the `run local storage disable adapter` command to take the adapter offline.
- When the adapter type is target, use the `network fcp adapter modify` command to take the adapter offline.

For more information about configuring FC ports, see the *ONTAP SAN Administration Guide* for your release, or attend the NetApp University SAN Implementation course.

ifgroups

- Combination of one or more Ethernet interfaces
- Three ifgroup modes:
  - Single mode (active-standby)
  - Static multimode (active-active)
  - Dynamic multimode with Link Aggregation Control Protocol (LACP)
- Naming syntax: a<*number*><*letter*> (for example, a0a)

NOTE: Vendors might use other terms for combining Ethernet interfaces (for example, Cisco EtherChannel).



An ifgroup combines one or more Ethernet interfaces, which can be implemented in one of three ways.

In single mode, one interface is active, and the other interfaces are inactive until the active link goes down. The standby paths are used only during a link failover.

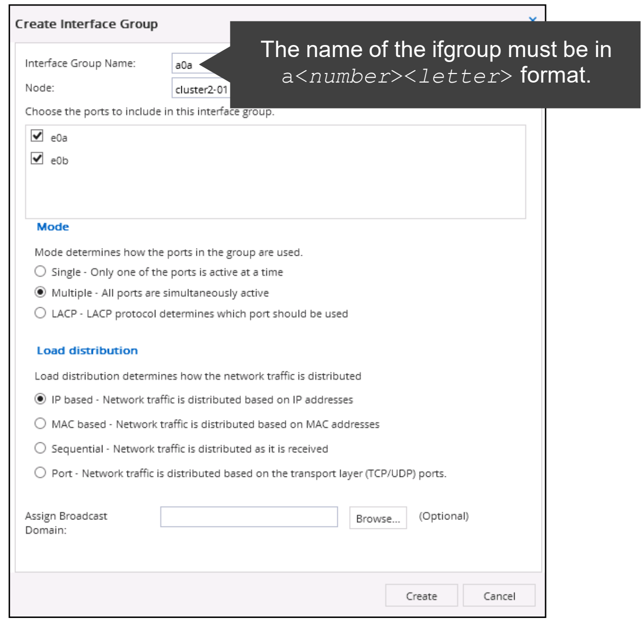
In static multimode, all links are active. Therefore, static multimode provides link failover and load-balancing features. Static multimode complies with the IEEE 802.3ad (static) standard and works with any switch that supports the combination of Ethernet interfaces. However, static multimode does not have control packet exchange.

Dynamic multimode is similar to static multimode but complies with the IEEE 802.3ad (dynamic) standard. When switches that support Link Aggregation Control Protocol (LACP) are used, the switch can detect a loss of link status and dynamically route data. NetApp recommends that when you configure ifgroups, you use dynamic multimode with LACP and compliant switches.

All modes support the same number of interfaces per ifgroup, but the interfaces in the group should always be the same speed and type. The naming syntax for interface groups is the letter “a”, followed by a number, followed by a letter (for example, a0a).

Vendors might use terms such as link aggregation, port aggregation, trunking, bundling, bonding, teaming, or EtherChannel.

Creating ifgroups




```
cluster2::> network port ifgrp create -node cluster2-01 -ifgrp a0a
-distr-func ip -mode multimode
```

 13

You can create ifgroups for higher throughput, fault tolerance, and elimination of single points of failure (SPOFs).

Manage ifgroups in a similar way, except for the following:

- You must name ifgroups by using the syntax a*<number><letter>*.
- You cannot add a port that is already a member of one ifgroup to another ifgroup.
- Multimode load-balancing methods include the following:
  - MAC: Network traffic is distributed by MAC addresses.
  - IP**:** Network traffic is distributed by IP addresses.
  - Sequential**:** Network traffic is distributed as it is received.
  - Port**:** Network traffic is distributed by the transport layer (TCP/UDP) ports.

For more information about load balancing, see TR-4182: *Ethernet Storage Best Practices for ONTAP Configurations*.

ifgroup Considerations

- Because of the limited capabilities of single mode, you should not use a single-mode ifgroup in ONTAP software.
- Use dynamic multimode (LACP) when you use ifgroups, to take advantage of performance and resiliency functionality:
  - An LACP-enabled switch is required.
  - All of the interfaces in the group are active, share a MAC address, and use load-balancing for outbound (not inbound) traffic.
  - A single host does not achieve larger bandwidth than any of the constituent connections.
    Two 10-Gigabit Ethernet (10-GbE) ports that are bound together do not equal one 20-GbE port.

You can configure ifgroups to add a layer of redundancy and functionality to an ONTAP software environment. You can also use ifgroups with a failover group to help to protect against Layer 2 and Layer 3 Ethernet failures.

A **single-mode ifgroup** is an active-passive configuration (one port sits idle, waiting for the active port to fail) and cannot aggregate bandwidth. NetApp advises against the use of the single-mode type of ifgroup. To achieve as much redundancy, you can use failover groups or one of the two multimode methods.

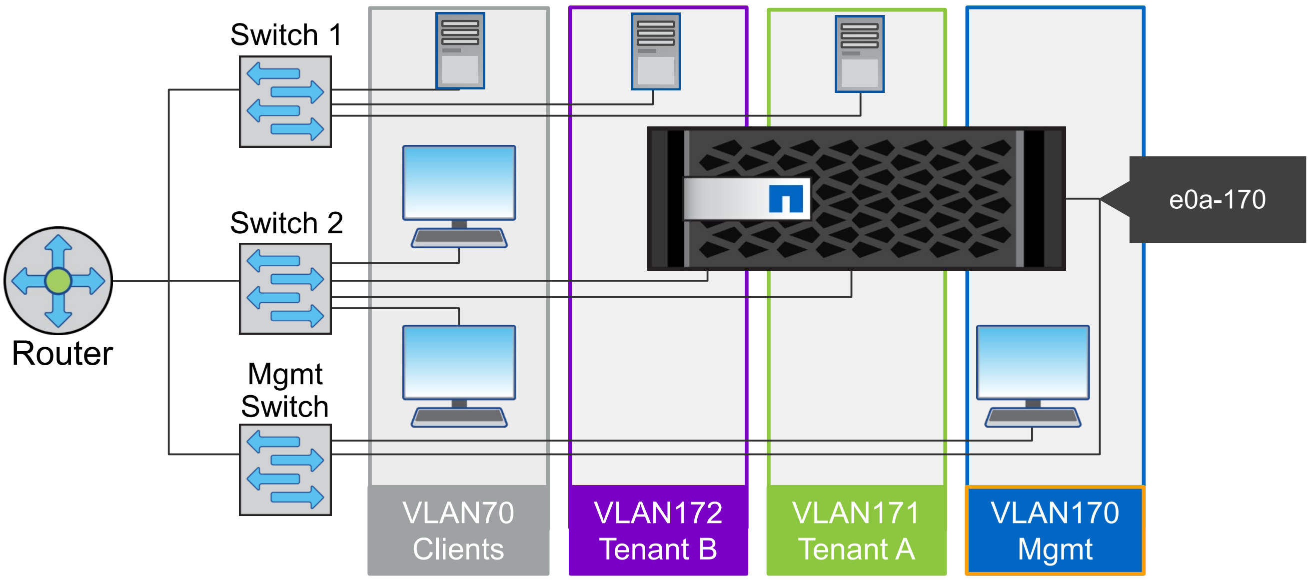
You might use a **static multimode ifgroup** if you want to use all the ports in the group to simultaneously service connections. Static multimode does differ from the type of aggregation that happens in a dynamic multimode ifgroup. No negotiation or automatic detection happens within the group concerning the ports. A port sends data when the node detects a link, regardless of the state of the connecting port on the switch side.

You might use a **dynamic multimode ifgroup** to aggregate bandwidth of more than one port. LACP monitors the ports on an ongoing basis to determine the aggregation capability of the ports. LACP also continuously provides the maximum level of aggregation capability that is achievable between a given pair of devices. However, all the interfaces in the group are active, share MAC address, and load-balance outbound traffic. A single host does not necessarily achieve larger bandwidth, exceeding the capabilities of any constituent connections. For example, adding four 10-GbE ports to a dynamic multimode ifgroup does not result in one 40-GbE link for one host. The situation is because of the way that both the switch and the node manage the aggregation of the ports in the ifgroup. A recommended best practice is to use the dynamic multimode type of ifgroup so that you can take advantage of all the performance and resiliency functionality that the ifgroup algorithm offers.

You can use two methods to achieve path redundancy when you use iSCSI in ONTAP software. You can use ifgroups or you can combine hosts to use multipath I/O over multiple distinct physical links. Because multipath I/O is required, ifgroups might have little value.

For more information, see TR-4182: *Ethernet Storage Best Practices for ONTAP Configurations*.

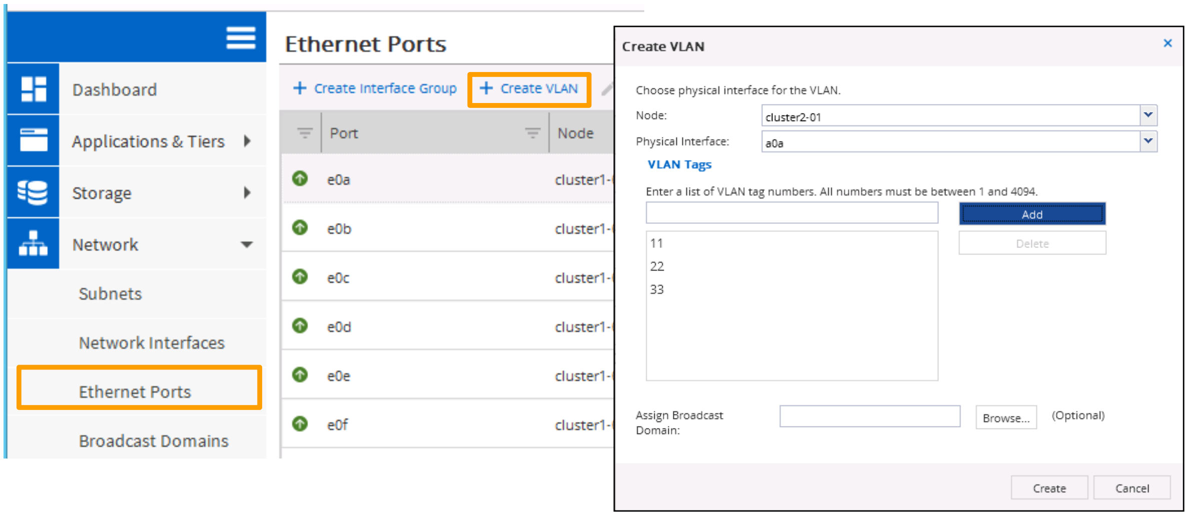
VLANs



 15

A port or ifgroup can be subdivided into multiple VLANs. Each VLAN has a unique tag that is communicated in the header of every packet. The switch must be configured to support VLANs and the tags that are in use. In ONTAP software, a VLAN ID is configured into the name. For example, VLAN e0a-70 is a VLAN with tag 70 that is configured on physical port e0a. VLANs that share a base port can belong to the same or different IPspaces. The base port can be in a different IPspace than the VLANs that share the base port. IPspaces are covered later in this module.

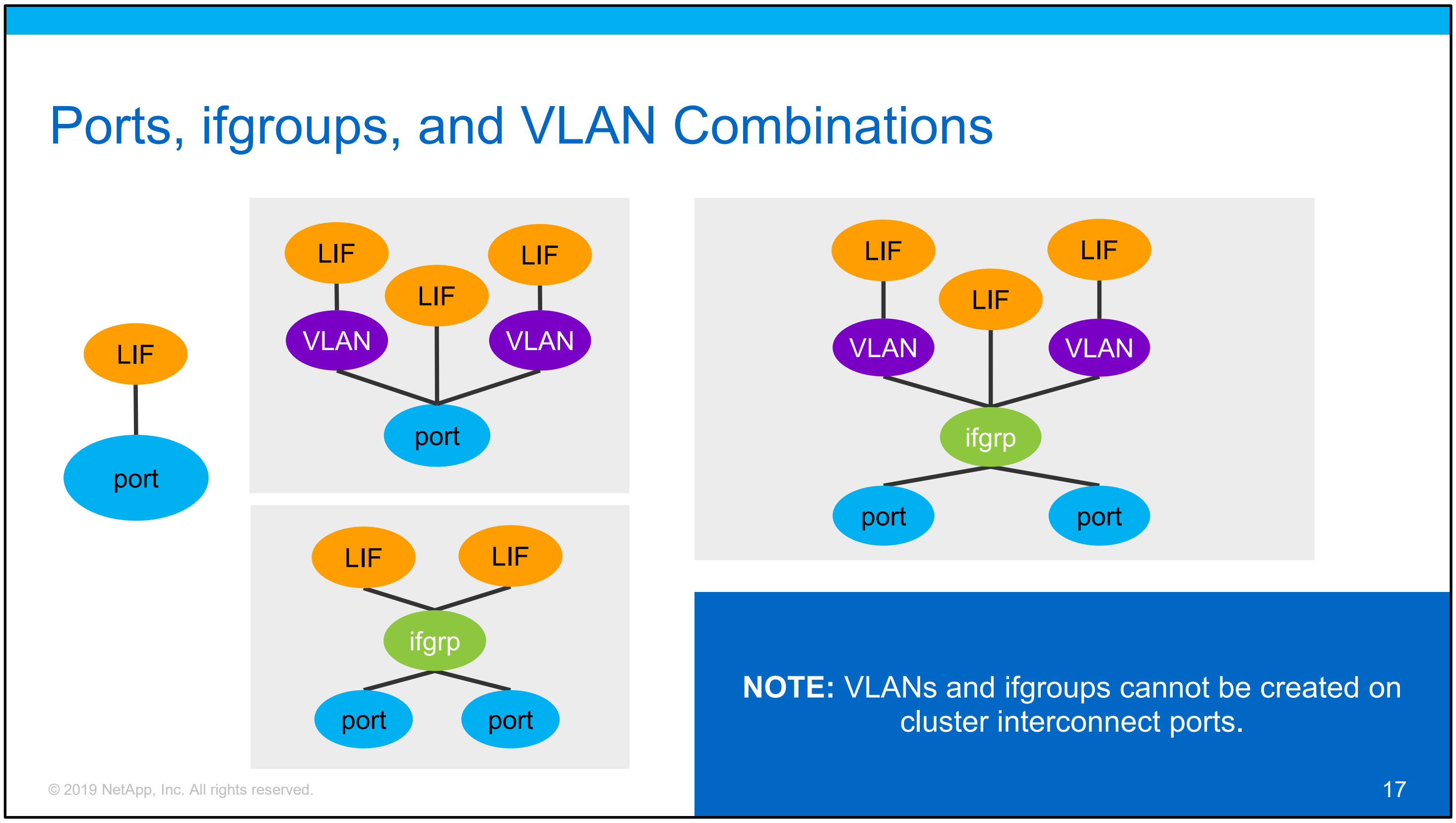
Creating VLANs




```
cluster2::> network port vlan create -node cluster2-01 -vlan-name a0a-11
```


16

You can create a VLAN for ease of administration, confinement of broadcast domains, reduced network traffic, and enforcement of security policies.



Most small to medium environments and FC environments use physical ports.

Ethernet environments in which multiple physical networks are impossible often use VLANs to separate management traffic from data traffic. VLANs are also often used to separate differing workloads. For example, you might separate NAS traffic from iSCSI traffic for performance and security reasons.

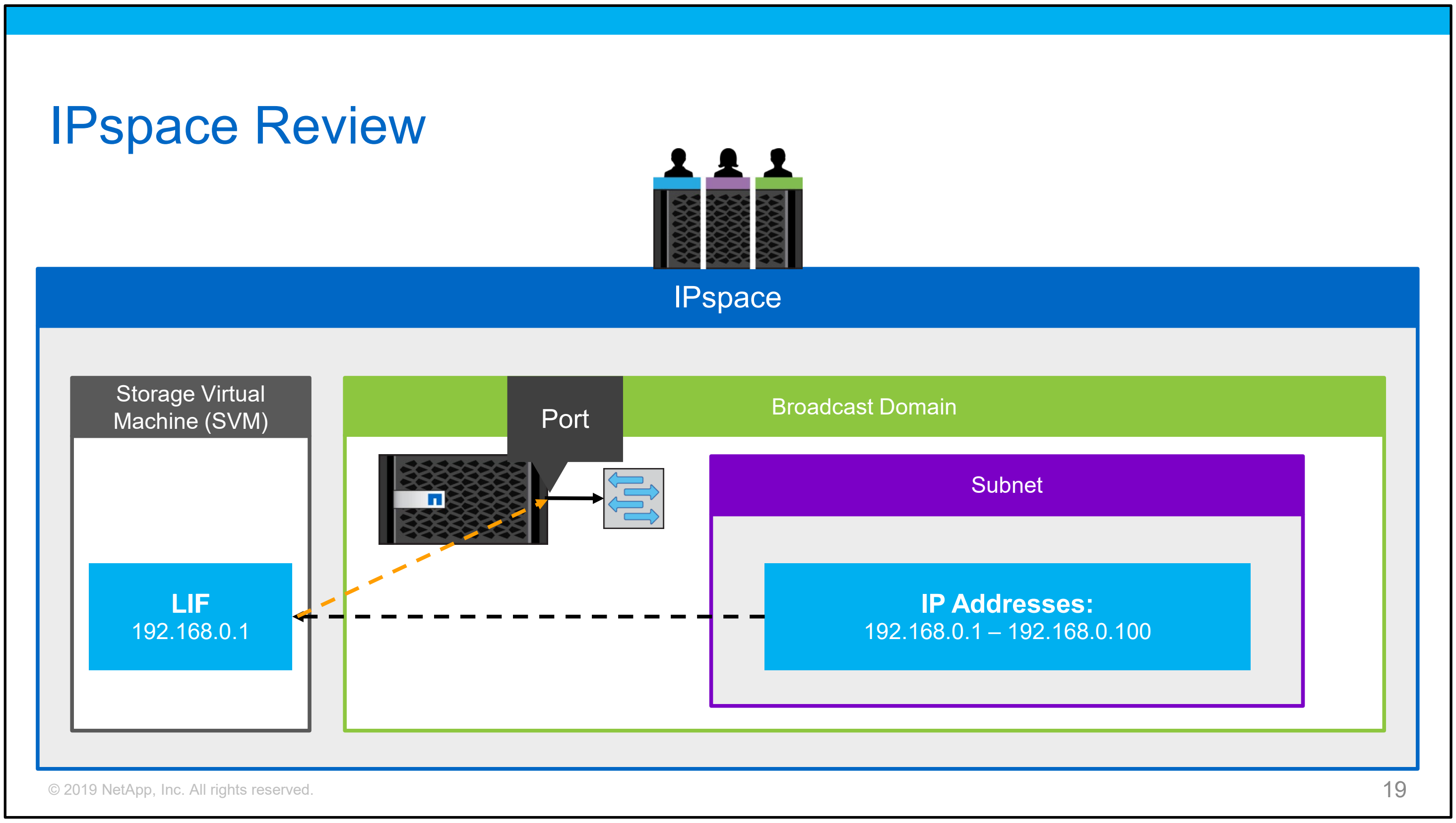
In Ethernet environments in which many application servers or hosts share switches and ports, dynamic multimode ifgroups of four Ethernet ports per node are frequently used for load balancing.

Environments that use ifgroups typically also use VLANs to segment the network. Segmentation is typical for service providers with multiple clients that require the bandwidth that ifgroups provide and the security that VLANs provide.

Finally, it is not unusual for different types of ports to be used in mixed environments that have various workloads. For example, an environment might use ifgroups with VLANs that are dedicated to NAS protocols, a VLAN that is dedicated to management traffic, and physical ports for FC traffic.

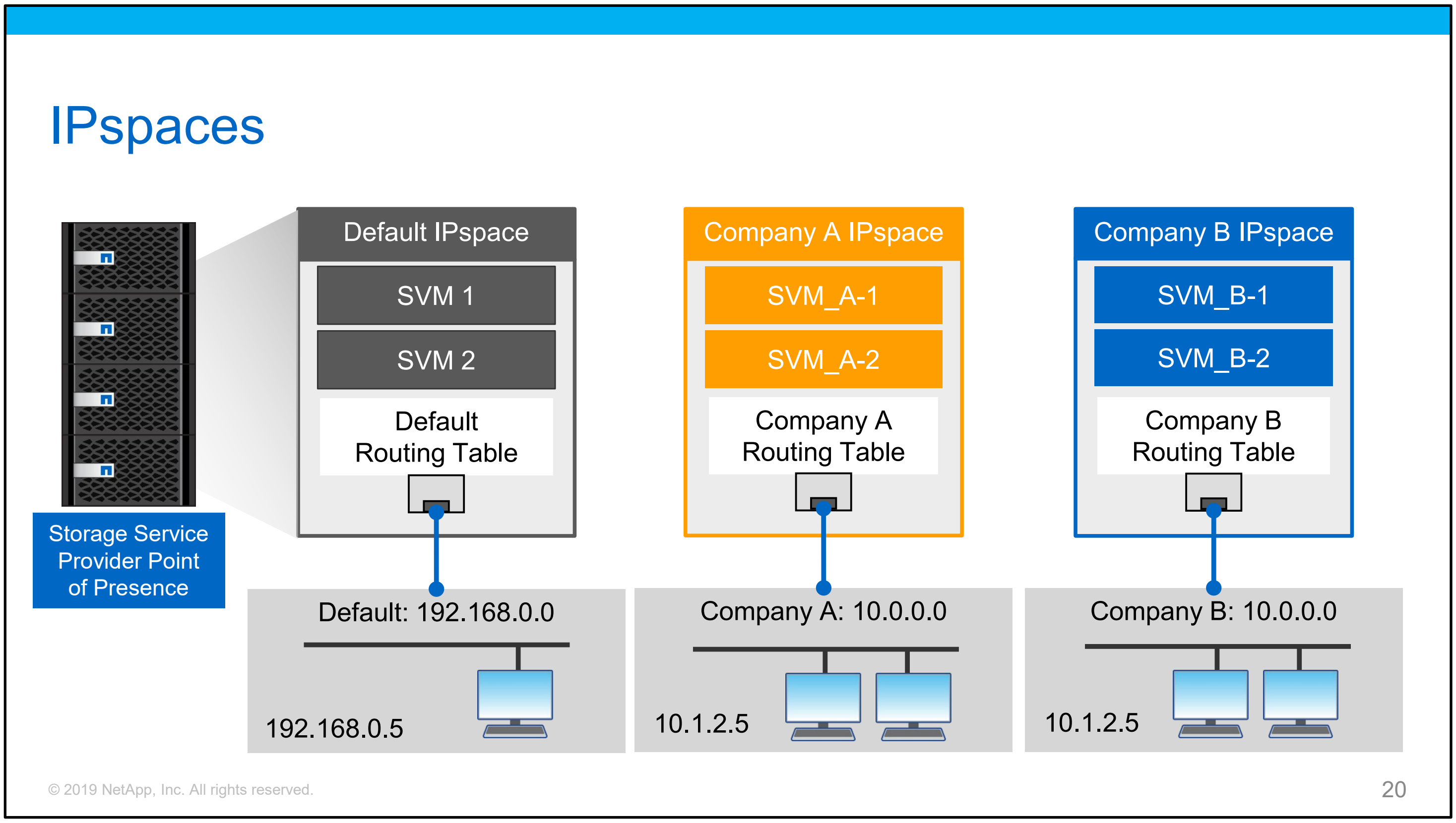
ifgroups and VLANs cannot be created on cluster interconnect ports.

Lesson 3
Network Traffic Segregation



ONTAP software has a set of features that work together to enable multitenancy. An IPspace is a logical container that is used to create administratively separate network domains. An IPspace defines a distinct IP address space that contains storage virtual machines (SVMs). The IPspace contains a broadcast domain, which enables you to group network ports that belong to the same Layer 2 network. The broadcast domain contains a subnet, which enables you to allocate a pool of IP addresses for your ONTAP network configuration.

When you create a LIF on the SVM, the LIF represents a network access point to the node. You can manually assign the IP address for the LIF. If a subnet is specified, the IP address is automatically assigned from the pool of addresses in the subnet, much like how a Dynamic Host Configuration Protocol (DHCP) server assigns IP addresses.



The IPspace feature enables clients from more than one disconnected network to access a storage system or cluster, even if the clients use the same IP address.

An IPspace defines a distinct IP address space in which virtual storage systems can participate. IP addresses that are defined for an IPspace are applicable only within the IPspace. A distinct routing table is maintained for each IPspace. No cross-IPspace traffic routing occurs. Each IPspace has a unique assigned loopback interface. The loopback traffic on each IPspace is isolated from the loopback traffic on other IPspaces.

Example

A storage service provider needs to connect customers of companies A and B to a storage system on the storage service provider premises. The storage service provider creates SVMs on the cluster, one per customer. The storage service provider then provides one dedicated network path from one SVM to the A network and another dedicated network path from the other SVM to the B network.

The deployment should work if both companies use nonprivate IP address ranges. However, because the companies use the same private addresses, the SVMs on the cluster at the storage service provider location have conflicting IP addresses.

To overcome the problem, two IPspaces are defined on the cluster, one per company. Because a distinct routing table is maintained for each IPspace and no cross-IPspace traffic is routed, the data for each company is securely routed to the respective network. Data is securely routed even if the two SVMs are configured in the 10.0.0.0 address space.

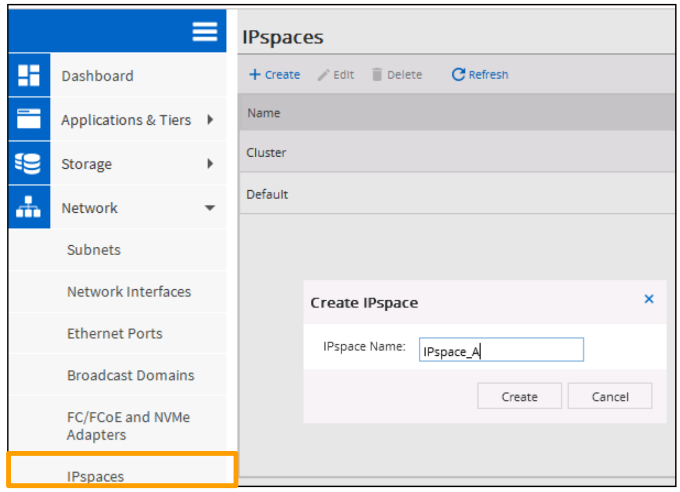
Also, the IP addresses that are referred to by various configuration files (the /etc/hosts file, the /etc/hosts.equiv file, the /etc/rc file, and so on) are relative to the IPspace. Therefore, the IPspaces enable the storage service provider to use the same IP address for the configuration and authentication data for both SVMs, without conflict.

Managing IPspaces

Create

You can create IPspaces when you need your SVMs to have distinct and secure storage, administration, and routing:

```
cluster1::> network ipspace create –
ipspace IPspace_A
```



 21

IPspaces are distinct IP address spaces in which SVMs reside. All IPspace names must be unique within a cluster.

- If necessary, you can change the name of an existing IPspace (except for the two system-created IPspaces) by using the `network ipspace rename` command.
- If you no longer need an IPspace, you can delete the IPspace by using the `network ipspace delete` command.

NOTE: No broadcast domains, network interfaces, or SVMs can be associated with an IPspace that you want to delete. You cannot delete the system-defined Default and Cluster IPspaces.

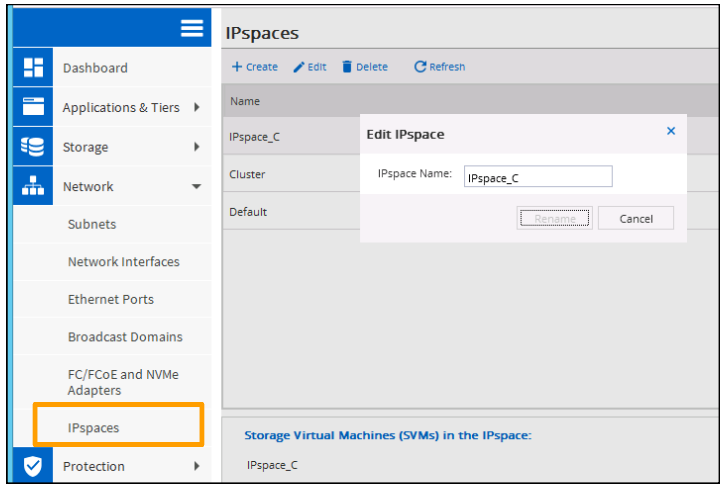
You can display the list of IPspaces that exist in a cluster. You can also view the SVMs, broadcast domains, and ports that are assigned to each IPspace.

After you create an IPspace but before you create the SVMs in the IPspace, you might need to create a broadcast domain that defines the ports of the IPspace.

Managing IPspaces

IPspaces can be renamed or deleted:

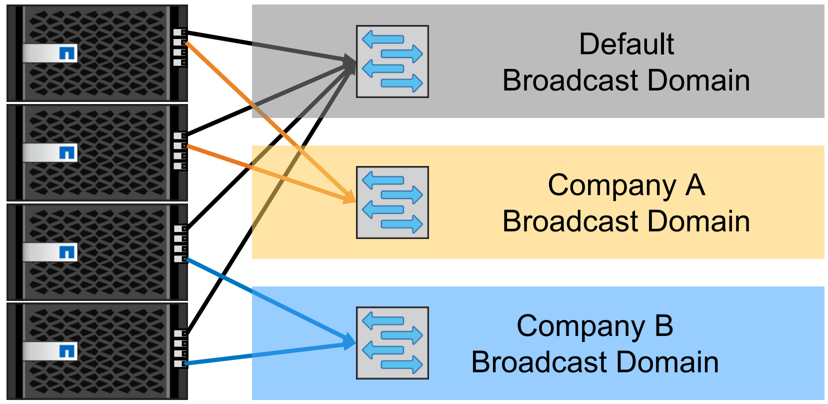
```
::> network ipspace rename -ipspace
IPspace_A -new-name IPspace_C
    or
::> network ipspace delete -ipspace
IPspace_A
```



Broadcast Domains

Overview

- Broadcast domains enable you to group network ports that belong to the same Layer 2 network.
- An SVM can then use the ports in the group for data or management traffic.



Broadcast domains can contain physical ports, ifgroups, and VLANs.

Broadcast domains are often used when a system administrator wants to reserve specific ports for use by a certain client or group of clients. A broadcast domain should include ports from many nodes in the cluster to provide high availability for the connections to SVMs.

The figure shows the ports that are assigned to three broadcast domains in a 4-node cluster:

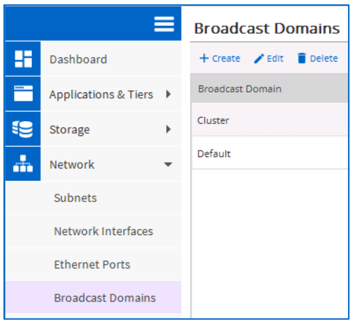
- The Default broadcast domain, which was created automatically during cluster initialization, is configured to contain a port from each node in the cluster.
- The Company A broadcast domain was created manually and contains one port each from the nodes in the first HA pair.
- The Company B broadcast domain was created manually and contains one port each from the nodes in the second HA pair.
- The Cluster broadcast domain was created automatically during cluster initialization, but it is not shown in the figure.

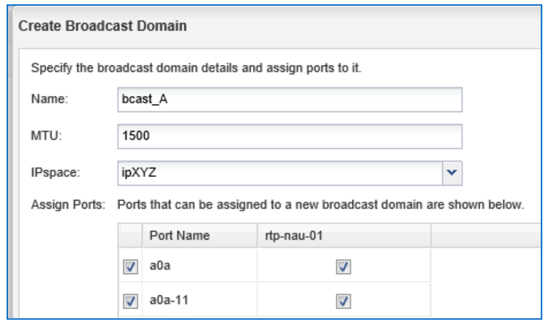
The system administrator created the two broadcast domains specifically to support the customer IPspaces.

Broadcast Domains

Managing broadcast domains

You create broadcast domains to group ports for an IPspace.






```
cluster1::> network port broadcast-domain create -broadcast-domain bcast_A -mtu
1500 -ipspace ipXYZ -ports cluster1-01:a0a,cluster1-01:a0a-11…
cluster1::> network port broadcast-domain add-ports…
cluster1::> network port broadcast-domain remove-ports…
```

 24

You create a broadcast domain to group network ports in a cluster that belongs to the same Layer 2 network. SVMs can then use the ports.

NOTE: The ports that you plan to add to the broadcast domain must not belong to another broadcast domain.

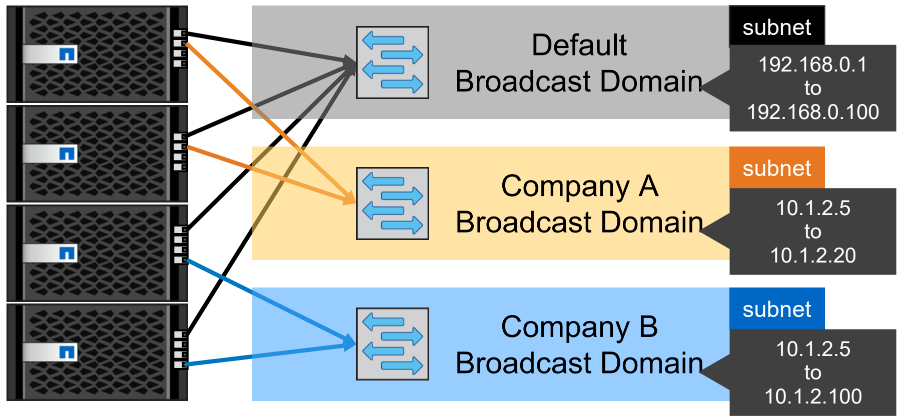
- All broadcast domain names must be unique within an IPspace.
- The ports that you add to a broadcast domain can be network ports, VLANs, or ifgroups.
- You add ports by using the `network port broadcast-domain add-ports` command.
- If the ports that you want to use belong to another broadcast domain but are unused, use the `network port broadcast-domain remove-ports` command to remove the ports from the existing broadcast domain.
- The maximum transmission unit (MTU) value of the ports that you add to a broadcast domain are updated to the MTU value that is set in the broadcast domain.
- The MTU value must match all the devices that are connected to the Layer 2 network.
- If you do not specify an IPspace name, the broadcast domain is created in the Default IPspace.

You can rename or delete broadcast domains that you create but not the system-created Cluster and Default broadcast domains.

To make system configuration easier, a failover group of the same name is created automatically and contains the same ports. All failover groups that relate to the broadcast domain are removed when you delete the broadcast domain.

Subnets

- Subnets enable the allocation of specific blocks, or pools, of IP addresses for easier LIF creation.
- A subnet is created within a broadcast domain and contains a pool of IP addresses that belong to the same Layer 3 subnet.



Subnets are recommended for easier LIF creation.

 25

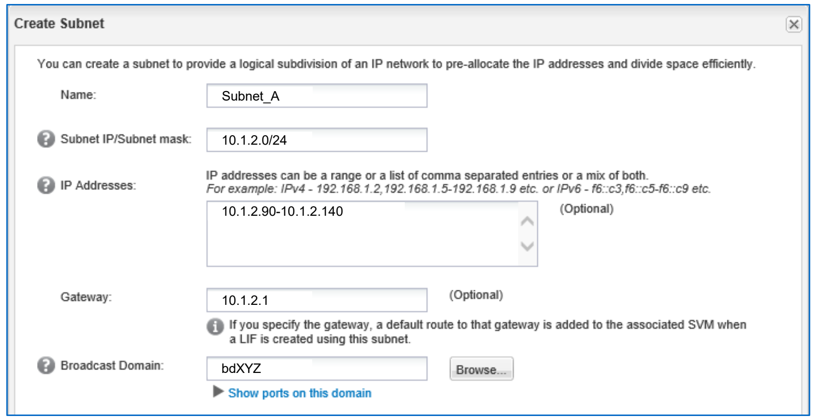
Subnets enable you to allocate specific blocks, or pools, of IP addresses for your ONTAP network configuration. The allocation enables you to create LIFs more easily when you use the `network interface create` command, by specifying a subnet name instead of specifying IP address and network mask values.

IP addresses in a subnet are allocated to ports in the broadcast domain when LIFs are created. When LIFs are removed, the IP addresses are returned to the subnet pool and are available for future LIFs.

You should use subnets because subnets simplify the management of IP addresses and the creation of LIFs. Also, if you specify a gateway when you define a subnet, a default route to that gateway is added automatically to the SVM when a LIF is created with that subnet.

Creating Subnets

- The broadcast domain and IPspace where you plan to add the subnet must exist.
- Subnet names must be unique within an IPspace.
- IP addresses in the specified range must not be in use by a LIF.




```
cluster1::> network subnet create –subnet-name subnet_A –broadcast-domain bdXYZ –
ipspace ipXYZ –subnet 10.1.2.0/24 –gateway 10.1.2.1              -ip-ranges
10.1.2.90-10.1.2.140 -force-updatelif-associations true
```


You create a subnet to allocate, or reserve, specific blocks of IPv4 or IPv6 addresses for ONTAP network configuration.

When you create subnets, consider the following limitations:

- When you add IP address ranges to a subnet, no IP addresses in the network can overlap (so that different subnets, or hosts, do not attempt to use the same IP address).
- If you do not use subnets or do not specify a gateway when you define a subnet, you must use the `route create` command to manually add a route to the SVM.
- The value `true` can be set for the `-force-update-lif-associations` option. The command fails if any SP or network interfaces currently use the IP addresses in the specified range. Setting the value to `true` associates any manually addressed interfaces with the current subnet and enables the command to succeed.

Subnets

Subnets and gateways

- When you create subnets, considering the following information:
  - If a gateway is specified, when a LIF is created with the subnet, a default route is added automatically to the SVM.
  - If you do not use subnets, or if you do not specify a gateway when defining a subnet, you must use the `route create` command to add a route to the SVM manually.
- If you add or change the gateway IP address, the following changes occur:
  - The modified gateway is applied to new SVMs when a LIF is created in an SVM that uses the subnet.
  - A default route to the gateway is created for the SVM (if the route does not exist).

NOTE: When you change the gateway IP address, you might need to manually add a new route to the SVM.

Subnets

Verifying subnets

To view broadcast domains:

```
::> network subnet show
Subnet                         Broadcast              Avail/
Name          Subnet           Domain     Gateway      Total  Ranges
-----------   ---------------  ---------  ------------ ------ ------
subnet_def    192.168.0.0/24   Default    192.168.0.1  10/50  192.168.0.101-192.168.0.150
subnet_A      10.1.2.0/24      bd_A       10.1.2.1     4/51   10.1.2.90-10.1.2.140
subnet_B      10.1.2.0/24      bd_B       10.1.2.1     4/51   10.1.2.90-10.1.2.140
```

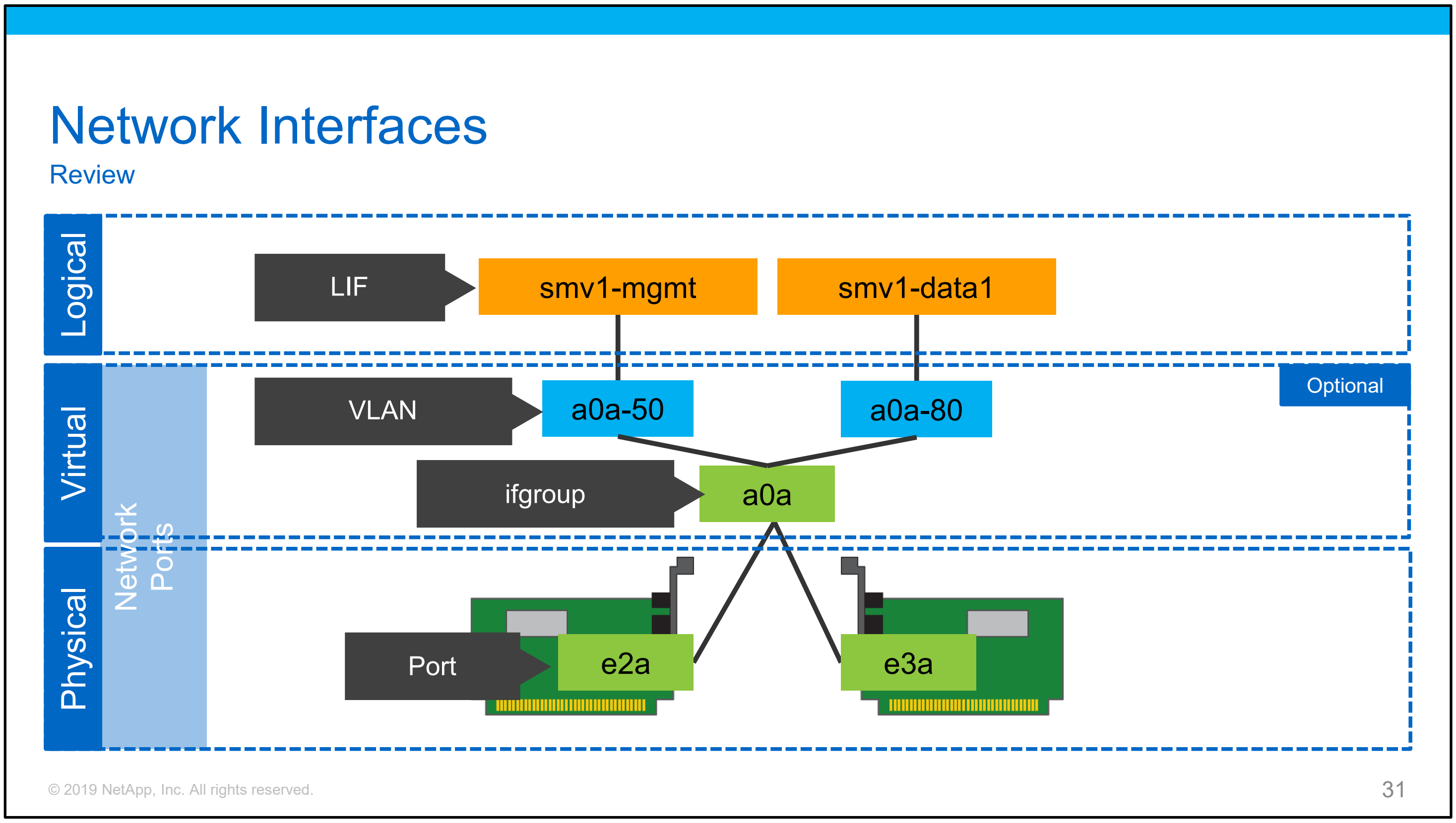
Subnets A and B have the same subnet and gateway but different domains

Notice how subnets A and B use overlapping IP ranges.

ACTION: Topics for Discussion

- When do you need to create IPspaces, broadcast domains, or subnets?

Lesson 4
LIFs



A LIF is associated with a physical port, an ifgroup, or a VLAN. Virtual storage systems (VLANs and SVMs) own the LIFs. Multiple LIFs that belong to multiple SVMs can reside on a single port.

LIFs

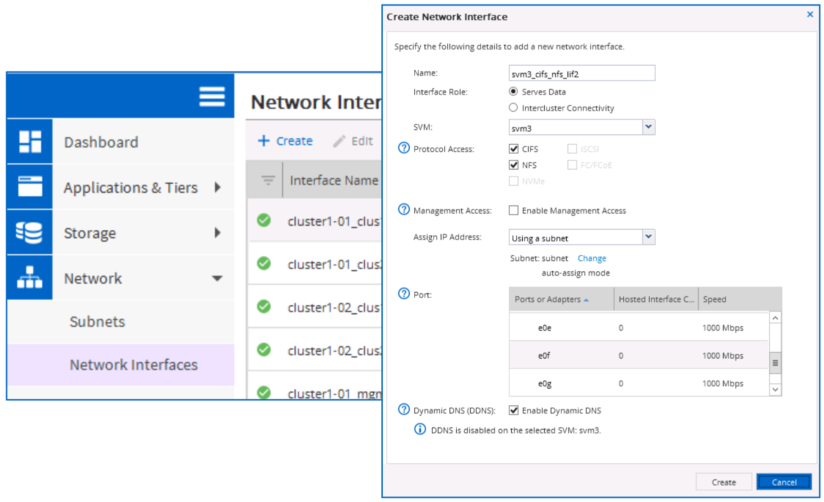
- An IP address or worldwide port name (WWPN) is associated with a LIF:
  - If subnets are configured (recommended), an IP address is automatically assigned when a LIF is created. Otherwise, IP addresses must be manually assigned.
  - When an FC LIF is created, WWPNs are automatically assigned.
- One node-management LIF exists per node.
- One cluster-management LIF exists per cluster.
- Cluster LIFs depend on the cluster configuration.
- Multiple data LIFs are enabled per port (client-facing for NFS, CIFS, iSCSI, and FC access).
- For intercluster peering, intercluster LIFs must be created on each node.

Data LIFs can have a many-to-one relationship with network ports. Many data IP addresses can be assigned to a single network port. If the port becomes overburdened, NAS data LIFs can be transparently migrated to different ports or nodes. Clients know the data LIF IP address but do not know which node or port hosts the LIF. If a NAS data LIF is migrated, the client might unknowingly be contacting a different node. The NFS mount point or CIFS share is unchanged.

Creating Data LIFs

Specify the subnet name to automatically assign an IP address.

You must specify the IP address when subnets are not configured.




```
cluster1::> network interface create -vserver svm3 -lif svm3_nfs_lif2 -role data –
data-protocol nfs -home-node cluster1-01 -home-port e0f          -subnet-name
snDefault
```

 33

A LIF is an IP address or WWPN that is associated with a physical port. If a component fails, most LIF types (excluding SAN) can fail over to or be migrated to a different physical port. Failover and migration ensure that communication with the cluster continues.

- The underlying physical network port must be configured to the administrative `up` status.
- If you plan to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must exist.
- You can create IPv4 and IPv6 LIFs on the same network port.
- You cannot assign NAS and SAN protocols to a LIF.
- The supported protocols are CIFS, NFS, FlexCache, iSCSI, and FC.
- The `data-protocol` parameter must be specified when the LIF is created and cannot be modified later.
- If you specify none as the value for the `data-protocol` parameter, the LIF does not support any data protocol.
- The `home-node parameter` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.
- The `home-port parameter` is the port or ifgroup to which the LIF returns when the `network interface revert` command is run on the LIF.
- All of the name mapping and host-name resolution services must be reachable from the data, cluster-management, and node-management LIFs of the cluster.

These services include the following and others:

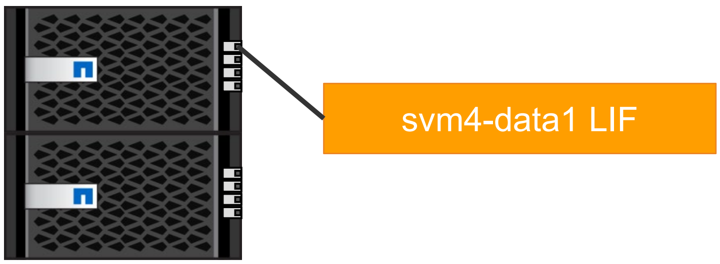
- DNS
- Network Information Service (NIS)
- Lightweight Directory Access Protocol (LDAP)
- Active Directory

- A cluster LIF should not be on the same subnet as a management LIF or a data LIF.
- When you use a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created with that subnet.

Lesson 5
Nondisruptive LIF Configuration

Nondisruptive LIF Features

Part 1 of 4



- **LIF failover:** Automatic migration that occurs because of a link failure or reboot

Why migrate a LIF? Migration might be necessary for troubleshooting a faulty port or to offload a node for which data network ports are saturated with other traffic. The LIF fails over if its current node is rebooted.

Unlike storage failover (SFO), LIF failover and migration do not cause a reboot of the node from which the LIF is migrating. After a LIF is migrated, the LIF can remain on the new node for as long as the administrator wants.

Failover groups for LIFs can be based on the broadcast domain or user defined. You create a failover group of network ports so that a LIF can automatically migrate to a different port if a link failure occurs on the LIF's current port. The failover group enables the system to reroute network traffic to other available ports in the cluster.

- The ports that are added to a failover group can be network ports, VLANs, or ifgroups.
- All of the ports that are added to the failover group must belong to the same broadcast domain.
- A single port can reside in multiple failover groups.
- If you have LIFs in different VLANs or broadcast domains, you must configure failover groups for each VLAN or broadcast domain.
- Failover groups do not apply in SAN iSCSI or FC environments.

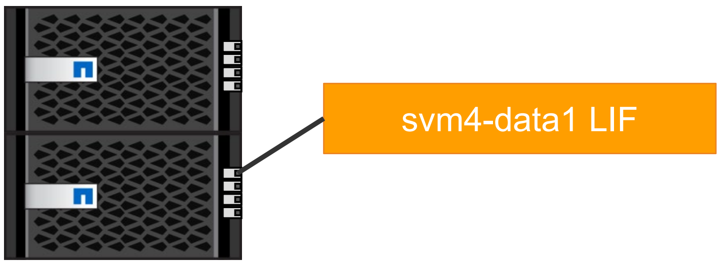
You can configure a LIF to fail over to a specific group of network ports by applying a failover policy and a failover group to the LIF. You can also disable a LIF from failing over to another port. You can choose from many failover policies:

- `Broadcast-domain-wide`: All ports on all nodes in the failover group
- `System-defined`: Only the ports on the LIF's home node and a non-SFO partner
- `Local-only`: Only the ports on the LIF's home node
- `SFO-partner-only`: Only the ports on the LIF's home node and SFO partner
- `Disabled`: No ports fail over

NOTE: LIFs for SAN protocols do not support failover and so are always set to *disabled*.

Nondisruptive LIF Features

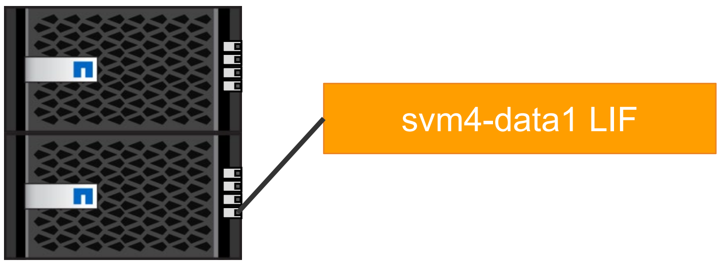
Part 2 of 4



- **LIF failover:** Automatic migration that occurs because of a link failure or reboot
- **LIF migrate:** Manual movement of a LIF to another port

Nondisruptive LIF Features

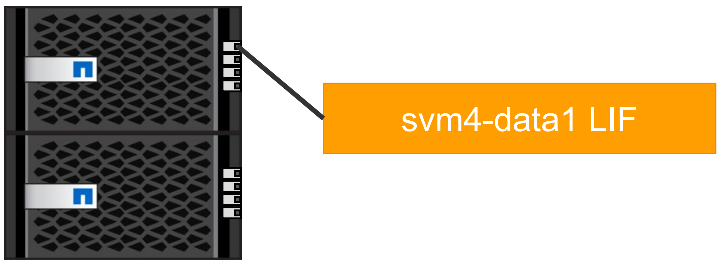
Part 3 of 4



- **LIF failover:** Automatic migration that occurs because of a link failure or reboot
- **LIF migrate:** Manual movement of a LIF to another port
- **LIF revert:** Manual or automatic sending of a LIF back to the home (node and) port

Nondisruptive LIF Features

Part 4 of 4

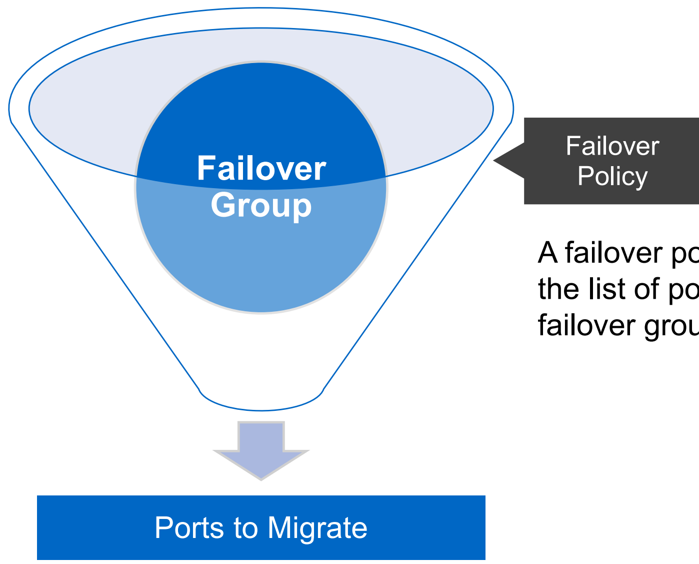


- **LIF failover:** Automatic migration that occurs because of a link failure or reboot
- **LIF migrate:** Manual movement of a LIF to another port
- **LIF revert:** Manual or automatic sending of a LIF back to the home (node and) port

 38

Failover Groups Versus Failover Policies

A failover group is a list of ports (physical or virtual):
- Defines the targets for the LIF
- Is automatically created when you create a broadcast domain
- Does not apply to iSCSI or FC SAN LIFs



A failover policy restricts the list of ports within a failover group.

Failover Groups

Based on the broadcast domain

Failover groups that are based on the broadcast domain are created automatically, based on the network ports in the broadcast domain:

- A Cluster failover group contains the ports in the Cluster broadcast domain.
- A Default failover group contains the ports in the Default broadcast domain.
- Additional failover groups are created for each broadcast domain that you create.

There are two types of failover groups. These groups are groups that the system creates automatically when a broadcast domain is created and groups that a system administrator defines.

The ports in the Cluster broadcast domain are used for cluster communication and include all cluster ports from all nodes in the cluster.

The ports in the Default broadcast domain are used primarily to serve data but also for cluster and node management.

Failover groups have the same name as the broadcast domain and contain the same ports as the groups in the broadcast domain.

Failover Groups

User-defined

You create custom failover groups for specific LIF failover functionality in one or more of the following circumstances:

- The automatic failover groups do not meet your requirements.
- You require only a subset of the ports that are available in the broadcast domain.
- You require consistent performance:
  For example, you have configured SnapMirror replication to use high-bandwidth ports. You might create a failover group that consists of only 10-GbE ports to ensure that the LIFs fail over to only high-bandwidth ports.

? More info in Addendum

You can create user-defined failover groups for special failover situations in which the groups that are based on the broadcast domain do not meet your needs.

Failover Policies

Failover Policy	Available Target Ports	Details
Broadcast-domain-wide	The LIF fails over to a port in the same broadcast domain as the home port (including any port from any node in the failover group).	Default for cluster-management LIF
System-defined	The LIF fails over to only a port on the home node or a non-SFO partner.	Default for data LIFs **Recommended for nondisruptive software updates**
Local-only	The LIF fails over to only a port on the home node of the LIF.	Default for cluster LIFs, node management LIFs, and intercluster LIFs
SFO-partner-only	The LIF fails over to only a port on the home node or SFO partner.	
Disabled	Failover is disabled for the LIF.	LIF that is not configured for failover

The table shows the default policies. Usually, you should use the default policies.

Failover Policies and Groups

LIF Name	LIF Role	Default Failover Group	Default Failover Policy
Clus1	Cluster	Cluster	Local-only
cluster1-01_mgmt1	Node management	Default	Local-only
cluster_mgmt	Cluster management	Default	Broadcast-domain-wide
svm1_nas_lif01	Data	Default	System-defined

The table shows how failover policies and groups work together. Groups include all possible failover targets, whereas policies limit targets within the group.

ACTION: Topics for Discussion

- What are the benefits of each type of failover group and failover policy type?
- When should you use ifgroups or failover groups? Do you need both?

Lesson 6
Routing Management

Routing Management

Overview

You control the outbound traffic of LIFs by configuring route tables and static routes.

The following is true of route tables:

- Route tables are routes that are automatically created in an SVM when a service or application is configured for the SVM.
- Routes are configured for each SVM, identifying the SVM, subnet, and destination.
- Route tables are per-SVM, so routing changes to one SVM do not pose a risk of corrupting another SVM route table.
- The system SVM of each IPspace has its own route table.

Route tables: System SVMs can own LIFs, and the system SVMs might need route configurations that differ from the configurations on data SVMs.

Routing Management

Static routes

Static routes:

- A static route is a defined route between a LIF and a specific destination IP address.
- The route can use a gateway IP address.

? More info in Addendum

NOTE: If a default gateway is defined when you create a subnet, a default route to the gateway is added automatically to the SVM that uses a LIF from the subnet.

Host-Name Resolution

Overview

Two methods support host-name resolution: DNS and hosts tables.

- You configure DNS and the hosts table in the admin SVM.
  - When you set up the cluster, you should configure DNS.
  - As nodes join the cluster, configurations are propagated to each node.
  - By default, the order of lookup is hosts table and then DNS.
- Cluster and SVM administrators can configure DNS in a data SVM.
- Each SVM has its own DNS configuration.

? More info in Addendum

Host-name resolution for the admin SVM

Only cluster administrators can configure DNS and the hosts table for host-name lookup in the admin SVM. All applications except CIFS discovery use the host-name configuration of the admin SVM. You cannot use NIS configuration for the admin SVM.

Host-name resolution for the admin SVM is configured when the cluster is created.

- Hosts table configuration for the admin SVM: You can use the `vserver services dns hosts` command to configure the hosts table that resides in the root volume of the admin SVM.
- DNS configuration for the admin SVM: If you want to configure DNS after you set up the cluster, use the `vserver services dns create` command.

Host-name resolution for a data SVM

A cluster or SVM administrator can configure DNS for host-name lookup in a data SVM. DNS configuration is mandatory when CIFS is used for data access.

DNS services can also be configured on an SVM for FlexVol volumes by using the Vserver Setup wizard. If you want to configure DNS later, you must use the `vserver services dns create` command.

Managing the hosts table (cluster administrators only)

A cluster administrator can add, modify, delete, and view the host-name entries in the hosts table of the admin SVM. An SVM administrator can configure the host-name entries for only the assigned SVM.

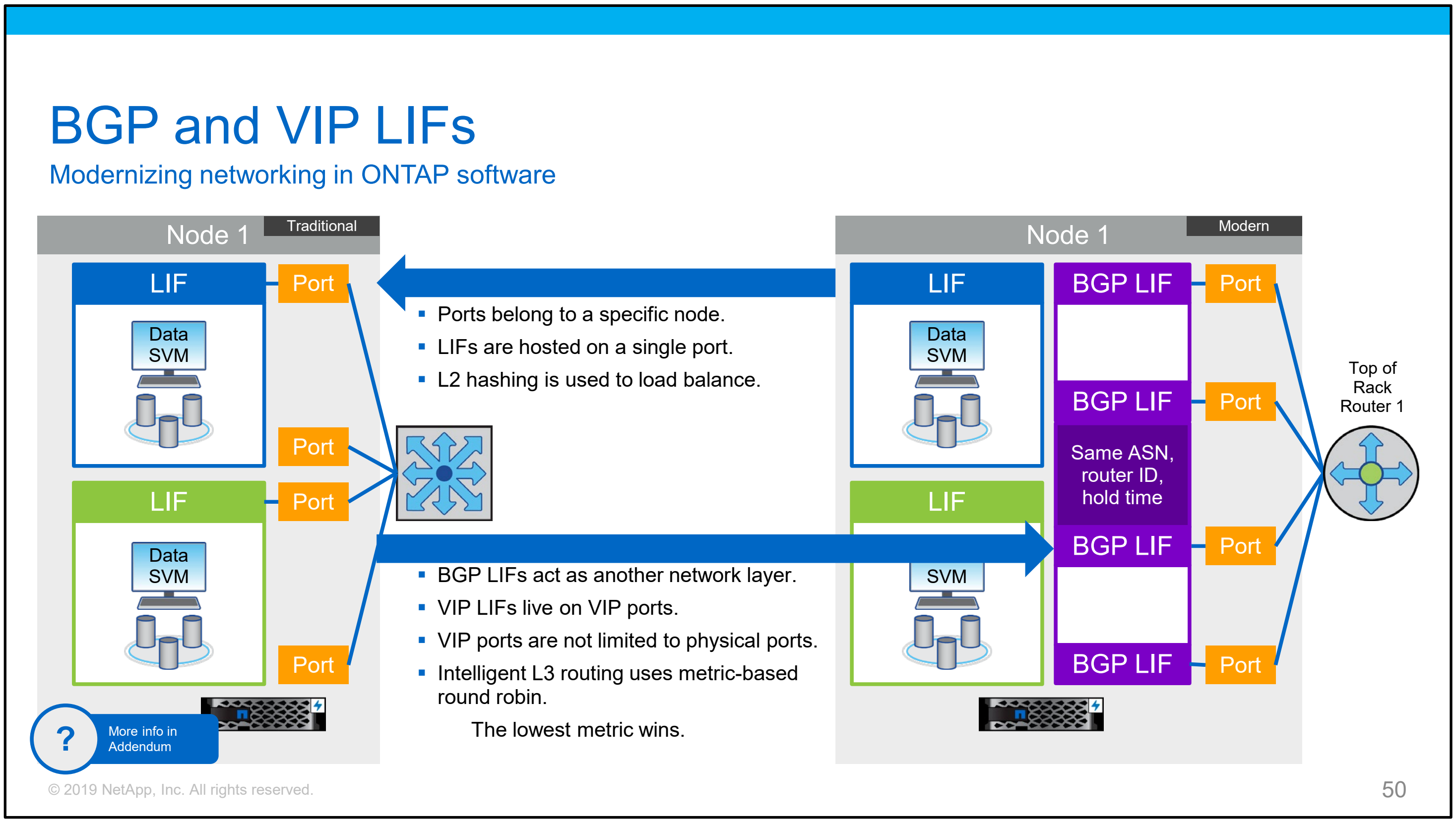
Border Gateway Protocol Routing

- ONTAP 9.5 software supports Layer 3 (L3) routing through Border Gateway Protocol (BGP).
- Previous ONTAP versions used Layer 2 (L2) routing, which creates hash tables of routes based on “distance.” The fewer the hops between two points is assumed to be the optimal route.
- Layer 3 routing with BGP uses metrics to pick routes based on metrics like latency and bandwidth availability.
- Support for BGP also enables the separation of LIFs from the physical hardware and makes them entities of the network that is called virtual IPs (VIPs).
- L3 routing might also reduce expenses by reducing the number of routers needed in the network.

Support for the Border Gateway Protocol (BGP) brings Layer 3 (L3) routing to ONTAP software. L3 routing is considered more effective at finding the best route between two network locations. Previous versions of ONTAP software supported only Layer 2 (L2) routing, which assumes that the fewer hops between locations means that the route is shorter and therefore more efficient. BGP instead relies on metrics to determine which route or routes are operating more efficiently. One of the ways that BGP works is by creating more flexibility in route choices by moving LIFs into the network that is called virtual IPs. A standard LIF is tied to physical hardware, which means that its routing options are restricted to physical cabling connections. VIPs provide better redundancy for IP failover events and avoid inactive links.

An analogy for L2 and L3 routing would be the road system for vehicle traffic. In L2 routing, a trip from San Francisco to Los Angeles would only consider the major highways that connect the two cities (for example, Interstate 5) regardless of traffic congestion or construction. L3 routing considers all roads and would route over state highways and surface streets if the metrics indicate that they are faster in some areas.

Maintaining an L2 network requires numerous L2 routers and switches that must be supported by many L3 switches. By supporting L3 routing, a data center might be able to operate with fewer L3 switches, which would reduce expenses.



BGP LIFs overcome the limits of traditional LIFs, which are bound to a single port on a specific node. A BGP LIF can be bound to multiple ports on multiple nodes.

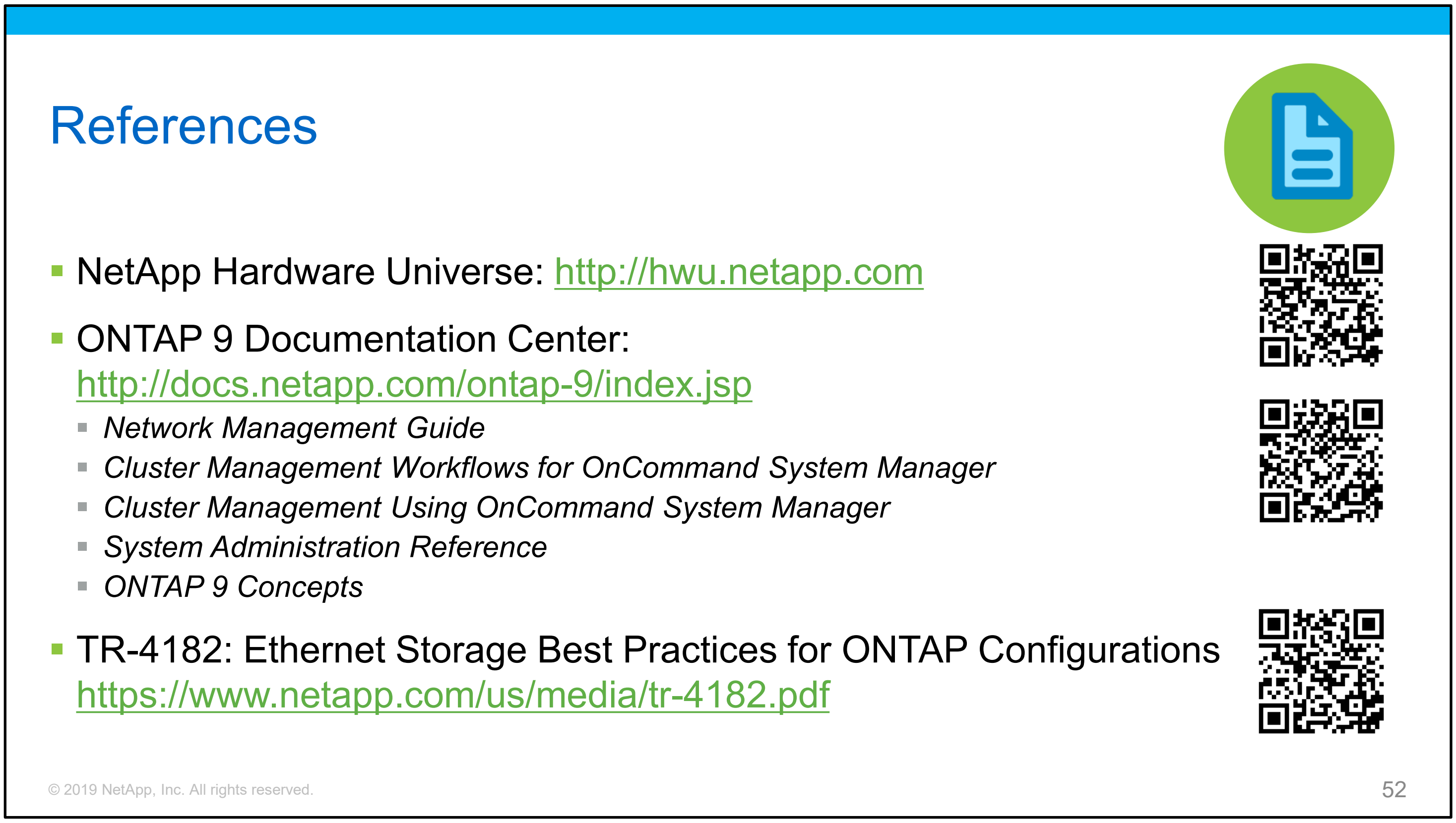
VIP LIFs that are bound to virtual ports work with BGP LIFs to enable clients to use the most optimal port that is available in the cluster to access a data SVM.

Work with your network administrators to determine how to best implement BGP and VIPs into your environment.

Knowledge Check: Question

Which statement about LIFs is true?

a. One cluster-management LIF exists per node.
b. One port can host multiple data LIFs.
c. Cluster LIFs and data LIFs can share a port.
d. A data LIF can be associated with multiple SVMs.



NetApp Hardware Universe: http://hwu.netapp.com

ONTAP 9 Documentation Center: http://docs.netapp.com/ontap-9/index.jsp

- *Network Management Guide*
- *Cluster Management Workflows for OnCommand System Manager*
- *Cluster Management Using OnCommand System Manager*
- *System Administration Reference*
- *ONTAP 9 Concepts*

TR-4182: Ethernet Storage Best Practices for ONTAP Configurations https://www.netapp.com/us/media/tr-4182.pdf

Module Review

This module focused on enabling you to do the following:

- Describe the interaction between physical and virtual network resources in a cluster
- Configure and manage physical and virtual networking resources

ACTION: Complete an Exercise

Module 4: Managing Physical and Logical Network Resources

Duration: 40 minutes

Access your lab equipment.

Use the login credentials that your instructor provided to you.

Open your Exercise Guide.

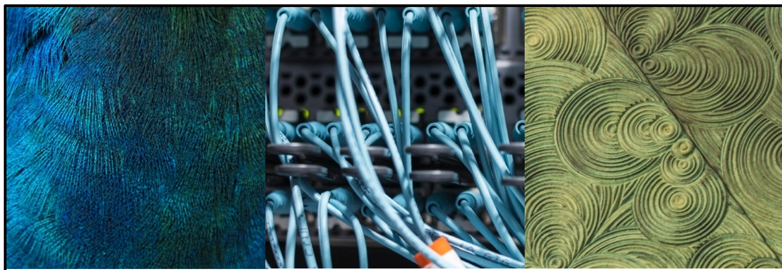
Go to the exercise for the module.

Complete the specified tasks.

- Start with Exercise 4-1.
- Stop at the end of Exercise 4-2.

Participate in the review session.

- Share your results.
- Report issues.



Addendum
Failover Group Commands

Failover

Managing failover groups and LIFs

Create a failover group:

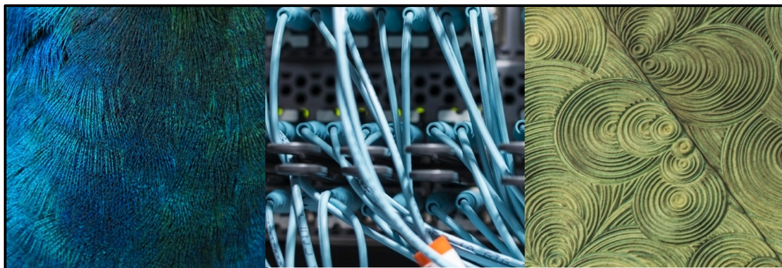
```
::> net int failover-groups create -vserver svm4 -failover-group fg_svm4 -
targets cluster1-01:e0f,cluster1-02:e0f
```

Add or remove targets from a failover group:

```
::> network interface failover-groups add-targets
::> network interface failover-groups remove-targets
```

Configure failover for an existing LIF:

```
::> net int modify -vserver svm4 -lif svm4_nfs_lif1 -failover-policy
broadcast-wide-domain -failover-group fg_svm4
```



Addendum
Routing Management Commands

Routing Management

Managing routes

Create a static route:

```
::> network route create -vserver svm4 -destination 0.0.0.0/0 -gateway
192.168.0.1
```

Delete a static route:

```
::> network route delete -vserver svm4 -destination 0.0.0.0/0 -gateway
192.168.1.1
```

Display static routes:

```
::> network route show
Vserver  Destination   Gateway      Metric
-------- ------------  -----------  -------
Svm4     0.0.0.0/0     192.168.0.1  20 ...
```


You can use the optional `-metric` parameter with the `network route create` command to specify a hop count for the route. The default settings for the parameter are 10 for management interfaces, 20 for data interfaces, and 30 for cluster interfaces. The parameter is used for source-IP address selection of user-space applications such as Network Time Protocol (NTP).

Host-Name Resolution

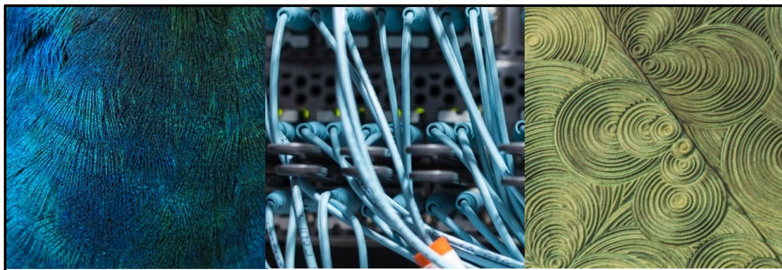
Table entries

Create a hosts table entry:

```
::> vserver services name-service dns hosts create -vserver svm4 -address
192.168.0.11 -hostname test.example.com -alias test
```

Create a DNS table entry:

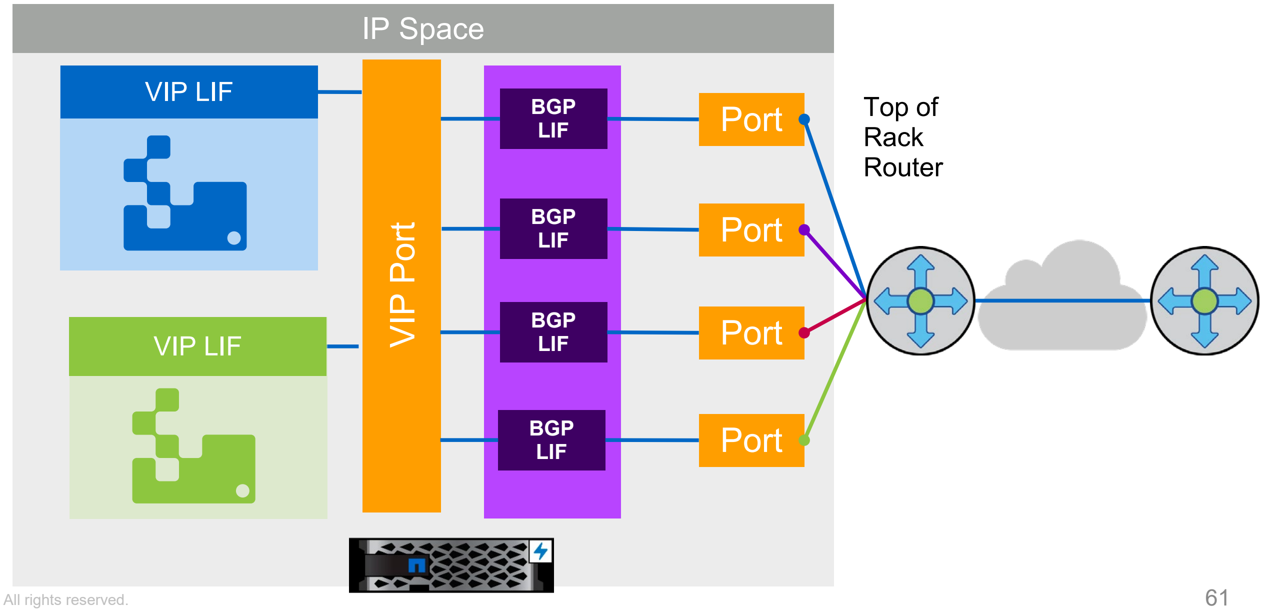
```
::> vserver services name-service dns create -vserver svm4 -domains
example.com -name-servers 192.168.0.11
```



Addendum
BGP and VIP LIFs

Modernizing the Data Center Network with Routing and Virtual IP

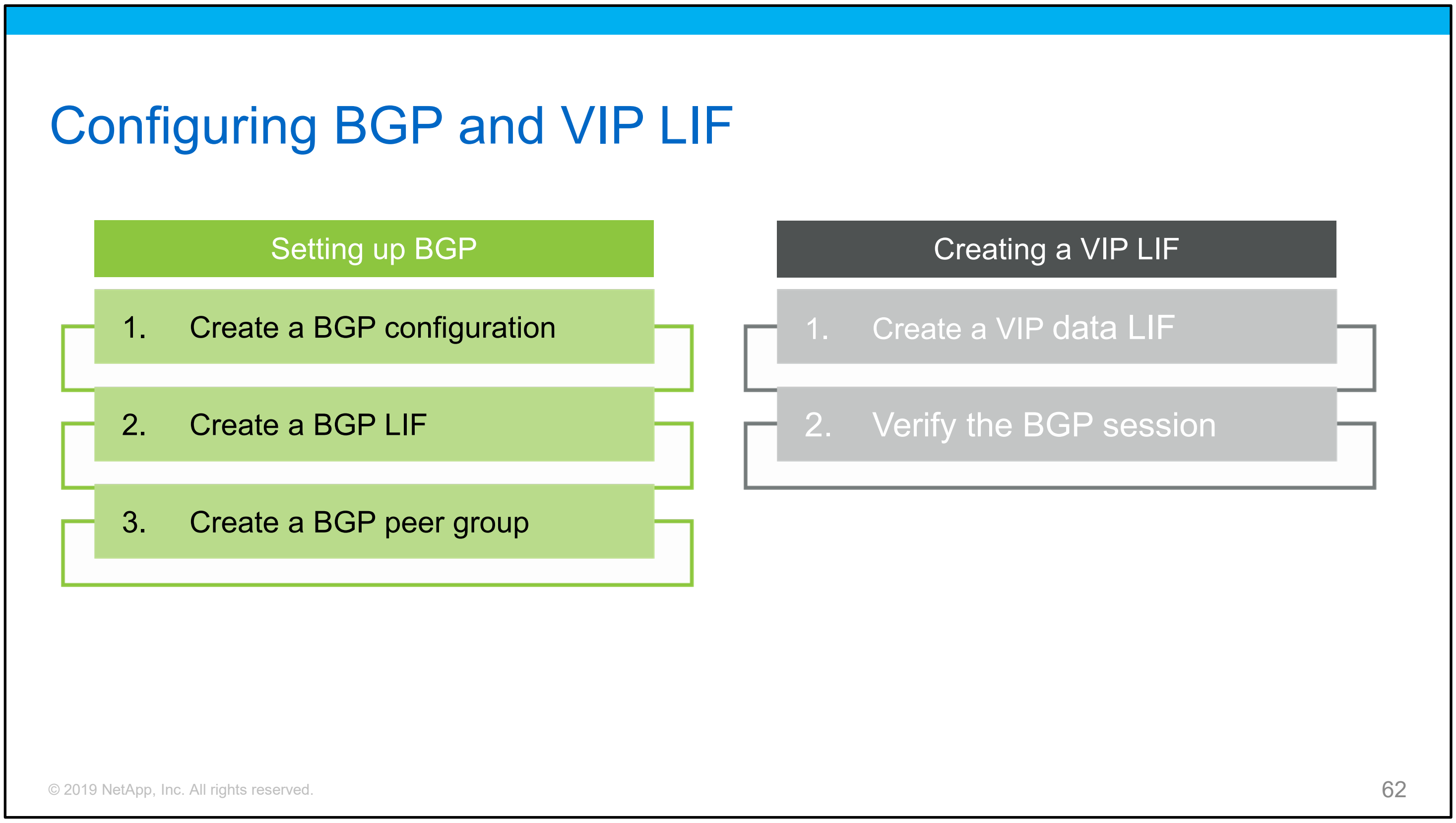
Full link use, direct cross data center traffic, and failure resiliency with a routed topology including BGP support



The next-generation data centers rely on network Layer 3 and require LIFs to be failed-over across subnets. Most of the Massively Scalable Data Center (MSDC) deployments use BGP or Open Shortest Path First (OSPF) as routing protocols to exchange the routes. BGP is most widely used by customers that require virtual IP (VIP) functionality. BGP is used by routers to exchange routing information so that the routers can dynamically update their routing tables with the best available routes to a destination. BGP is a connection-based protocol that runs over TCP. For BGP to work, there has to be a connection setup between the two BGP endpoints (generally routers).

VIP enables users to create a data LIF that is not part of any subnet and is reachable from all physical ports of an IPspace on the local node. A VIP LIF is not hosted on any physical interface. It is hosted on a system-created pseudo interface (VIP port).

For ONTAP 9.5 software, BGP is the routing protocol that is supported for advertising VIP.



Setting up BGP involves optionally creating a BGP configuration, creating a BGP LIF, and creating a BGP peer group. Before you begin, a peer router must be configured to accept BGP connection from the BGP LIF for the configured autonomous system number (ASN). ONTAP software automatically creates a default BGP configuration with default values when the first BGP peer group is created on a given node. A BGP LIF is used to establish BGP TCP sessions with peer routers. For a peer router, a BGP LIF is the next hop to reach a VIP LIF. Failover is disabled for the BGP LIF. A BGP peer group advertises the VIP routes for all of the SVMs in the peer group's IPspace.

When you create a VIP LIF, VIP port is automatically selected if you do not specify the home port with the network interface create command. By default, the VIP data LIF belongs to the system-created broadcast domain named “Vip” for each IPspace. You cannot modify the VIP broadcast domain.

A VIP data LIF is reachable simultaneously on all ports that host a BGP LIF of an IPspace. If there is no active BGP session for the VIP's SVM on the local node, the VIP data LIF fails over to the next VIP port on the node that has a BGP session that is established for that SVM.

For more information about BGP and VIP LIFs, see the *Network Management Guide*.

Setting Up BGP

Example workflow

Create a BGP configuration (advanced command):

```
cluster1::*> network bgp config create -node node1 -asn 65502 -holdtime
180 -routerid 1.1.1.1
```

Create a BGP LIF:

```
cluster1::> network interface create -vserver cluster1 -lif bgp1 -service-
policy net-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

Create a BGP peer group (advanced command):

```
cluster1::*> network bgp peer-group create -peer-group group1 -ipspace
Default -local-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65502 -route-
preference 100
```


For more information about syntax and usage, see the Network Management Guide > Configuring virtual IP (VIP) LIFs section and the Command man pages for the “network bgp” commands.

Create VIPs

Example workflow

Enable multipath routing (advanced command):

```
::*> network options multipath-routing modify -is-enabled true
```

Create a VIP data LIF:

```
::> network interface create -vserver vs34 -lif vip1 -role data        -
data-protocol cifs,nfs,fcache -home-node gw-node1 -address 3.3.3.3    -is-
vip true
```

Verify that the BGP session is in `up` status:

```
::> network bgp vserver-status show

           Node        Vserver  bgp status
           ----------  -------- ---------
           node1       vs1      up
```


For more information on syntax and usage, see the Network Management Guide > Configuring virtual IP (VIP) LIFs section and the Command man pages for the “network bgp” commands.

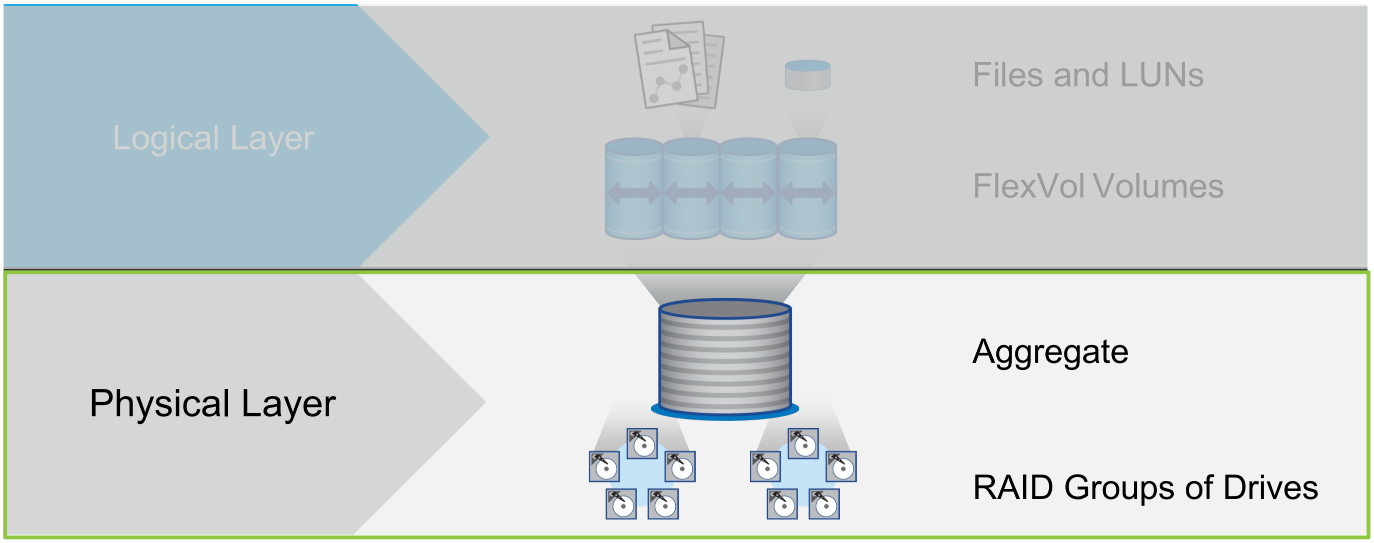
Module 5
Physical Storage Management

About This Module

This module focuses on enabling you to do the following:

- Describe NetApp ONTAP storage architecture concepts
- Manage physical storage resources, including drives, RAID groups, and aggregates
- Create data aggregates
- Create Flash Pool aggregates
- Describe FabricPool aggregates

ONTAP Storage Architecture



 3

The ONTAP software storage architecture uses a dynamic virtualization engine in which data volumes are dynamically mapped to physical space.

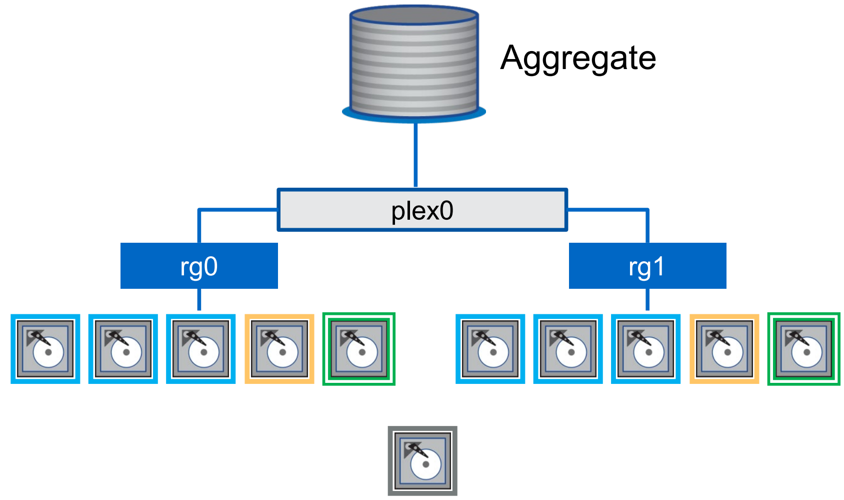
In ONTAP software, disks are grouped into RAID groups. An aggregate is a collection of physical disk space that contains one or more RAID groups. Each aggregate has a RAID configuration and a set of assigned disks. The disks, RAID groups, and aggregates make up the physical storage layer.

Within each aggregate, you can create one or more FlexVol volumes. A FlexVol volume is an allocation of disk space that is a portion of the available space in the aggregate. A FlexVol volume can contain files or LUNs. The FlexVol volumes, files, and LUNs make up the logical storage layer.

Lesson 1
Drives, RAID, and Aggregates

Physical Storage Hierarchy

- **Drive:**
  Hard disk drive (HDD) or
  solid-state drive (SSD or NVMe)
- **RAID group:**
  Drive-level protection
- **Plex:**
  Logical container for RAID groups
  Used by mirrored aggregates
- **Aggregate:**
  Logical pool of storage



5

The ONTAP storage architecture hierarchy contains the following elements:

- **Drives:** Drives play different roles at different times, depending on the state of the drive. Potential drives states include the following:
  - Data
  - Parity
  - Double-parity
  - Triple-parity
  - Spare
  - Broken
  - Unowned
  - Uninitialized (not zeroed)
- **RAID groups:** Each RAID group contains physical disks and is associated with a plex. A RAID group has either a RAID 4, NetApp RAID-DP, or NetApp RAID-TEC configuration.
- **Plexes:** Each plex is associated with an aggregate and contains RAID groups. Typically, an aggregate has only one plex. Aggregates that use SyncMirror technology have two plexes (plex0 and plex1), Plex1 contains a mirror of the plex0 data.
- **Aggregates:** Each aggregate contains a plex or plexes, a RAID configuration, and a set of assigned physical disks to provide storage to the volumes that the aggregate contains.

Drive Types

SATA	SAS	SSD	NVMe
Same technology that is used in consumer disk drives: ▪ Single I/O path ▪ High capacity but moderate IOPS ▪ Low signal voltages: cable length limit of 1 meter ▪ SAS-to-SATA adapters that enable use in SAS shelves	Serial attached SCSI: ▪ Point-to-point serial protocol ▪ Multipath I/O ▪ Moderate capacity by high IOPS ▪ Higher signal voltage: cable lengths up to 10 meters	Based on flash memory chip technology that is similar to USB flash drives: ▪ No spinning platter ▪ Quick reads and writes ▪ Use similar to that of a SAS hard disk drive Can also be used as an aggregate-specific cache	Nonvolatile memory enhanced: ▪ Storage-class memory (SCM) product that passes I/O directly over the Peripheral Component Interconnect Express (PCIe) bus. ▪ A flash module to accelerate spinning disks ▪ A drive to complement or substitute for SSDs

AFF systems use only SSD drives. FAS systems use a mix of drive types.

SATA is the disk technology that is used in most consumer-grade PCs. These drives have high capacities but moderate IOPS. SATA-to-SAS adapters enable the use of these drives in SAS shelves.

SAS is a point-to-point serial protocol that replaced parallel SCSI to resolve contention issues from multiple devices sharing a system bus. SAS disks can use multiple I/O paths.

SSDs are fast and reliable and use long-lasting technology that is based on the same flash technology that is used for USB flash drives. SSDs can be configured as data storage or as aggregate-specific cache similar to Flash Cache modules.

NVMe (nonvolatile memory enhanced) is a new class of drive and a memory product. These drive and storage class memory (SCM) products pass I/O directly to the PCIe bus rather than through a SATA or SAS interface with the PCIe bus. This arrangement enables NVMe products to operate hundreds of times faster than traditional SSDs. NetApp uses NVMe as both a memory product for the acceleration of spinning disks through flash modules and a drive.

Drive Ownership

- A drive is unusable until the drive is assigned ownership to a storage controller.
  - By default, ownership is automatically assigned.
  - Ownership can be manually assigned or changed.
  - Software disk ownership is made persistent by writing the ownership information onto the drive.
- Spare drives can be reassigned or unassigned.

```
::> storage disk show -container-type unassigned
                Usable           Container
Disk            Size   Shelf Bay   Type       Position  Aggregate Owner
--------------- ------ ----- ----- ---------- --------- --------- -----
9.11.18              -    11    18 unassigned present   -         -
```


ONTAP software automatically assigns drives to a storage controller during the initial hardware setup and checks occasionally to determine whether new drives have been added. When the drive is assigned, the disk ownership information is written to the drive so that the assignment remains persistent.

Ownership can be modified or removed. The data contents of a drive are not destroyed when the drive is marked as unowned. Only the disk-ownership information is erased.

Automatic ownership assignment is enabled by default. If your system is not configured to assign ownership automatically or if your system contains array LUNs, you must assign ownership manually.

NOTE: The NetApp best practice is to unassign only spare drives.

Drive Capacity

Market and physical capacity

Drive capacity is a confusing and contentious subject for many reasons. Consider a 2TB disk drive:

- **Market Capacity**. 2TB is the number that is used when you purchase the disk drive. It is formulated by using base-10 numbering (2000 GB) versus base-2 (2048 GiB) and is derived by rounding up actual physical capacity to an even number.
- **Physical or Raw Capacity**. The number of sectors on the drive is computed by using base-2 numbering. After subtracting blocks that are used to store checksum information, a 2TB drive is really a 1,864GiB drive.

Drive capacity is often confusing and contentious. Even on a new system with no data on it, the total capacity reported by the system is significantly smaller than the total of the capacity numbers that are physically shown on the drive carriers.

The root of this issue is how drives are marketed. When drives had very small capacities, it was easier to sell a drive if it was marketed as 100MB rather than 86MB. Vendors and resellers calculated the marketing capacity by using base-10 numbering rather than the base-2 numbering system that is used by computers. Unfortunately, this marketing practice still occurs today. The differences in capacities can be hundreds of gigabytes.

Physical or raw capacity is the actual base-2 computed capacity that the drive is capable of when it leaves the factory.

Disk Drive Capacity

Usable capacity

- **Usable Capacity**. The base-2 calculated disk space that is available for storing data:
  - Sector normalization. NetApp purchases disks from multiple vendors. Not all vendors’ physical capacity is the same. For ONTAP software to use all “2TB” drives equally, the available sectors are right-sized to the same number. This arrangement might result in 1,860GiB.
  - NetApp WAFL reserve. This reserve is 10% of capacity that is set aside to prevent the file system from completely filling up and becoming unable to function.

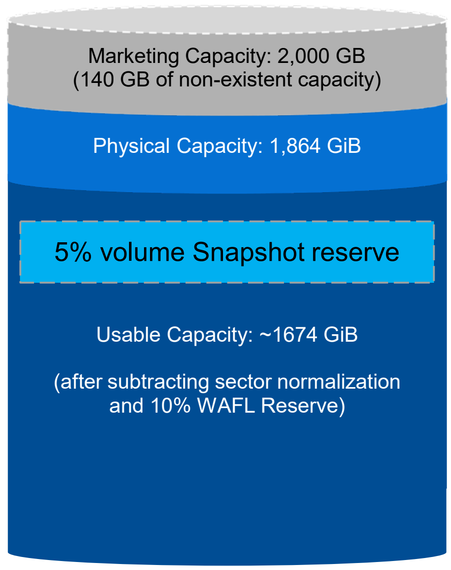
The space available for data is now ~ 1,674 GiB, which appears to an end-user as if 300GB has vanished.

Finally, FlexVol volumes for NAS protocols (CIFS and NFS) are created with a Snapshot reserve, which the customer might perceive as more lost space. However, Snapshot copies are data, so the reserve is still “usable” space.

Usable capacity is the disk blocks that are available to store data after the differences in calculation and overhead are considered. Because not all manufacturers create drives of the same capacity, NetApp normalizes all disks to the size of the smallest available disk capacity. WAFL then reserves the top 10% of capacity for its use.

Now that you know the difference between market capacity and usable capacity, you need to define what usable means. NetApp considers all blocks in the active file system and in Snapshot reserves as usable space because Snapshot copies hold older copies of data blocks for the purposes of recovering or restoring older versions of files. To offset this perception, ONTAP supports deduplication and compression to enable customers to pack more data into fewer disk blocks.

2TB Drive Capacity Visualization

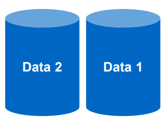


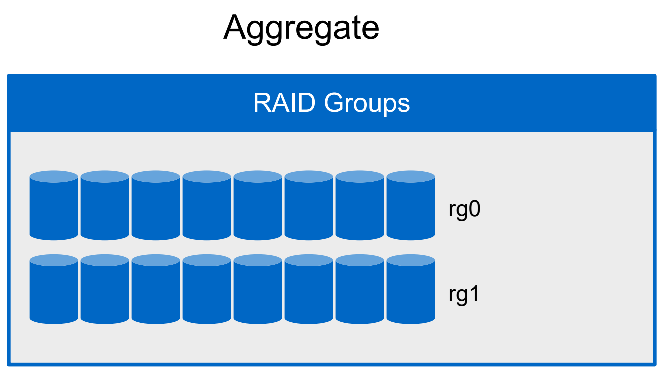
This diagram illustrates the differences in capacities and the gap between market capacity and usable capacity.

Drive Roles

Data drive

Data drive: Stores data inside RAID groups within data aggregates



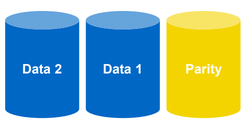


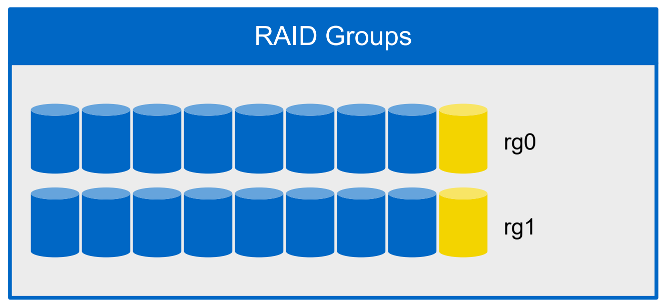
The primary role for a drive is to store data.

Drive Roles

Parity drive

Parity drive: Stores row parity information that is used for data reconstruction when a single drive fails within the RAID group





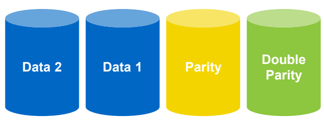
The key component of RAID group functionality is the parity drives. Parity stores the sum of all block values in a stripe. A parity drive can protect against the loss of a single drive within a RAID group.

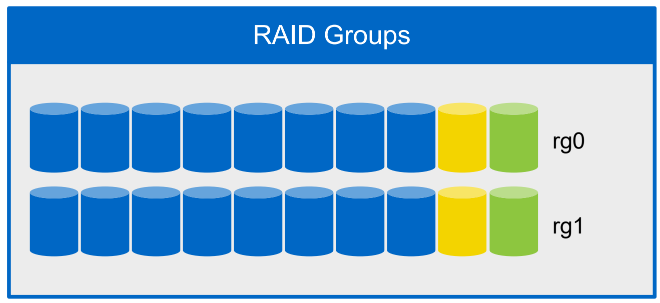
If you add a spare drive to an aggregate and the spare is larger than the other data drives, the spare becomes a parity drive. However, the spare does not use the excess capacity unless another drive of similar size is added. The second largest additional drive has full use of additional capacity.

Drive Roles

dParity drive

dParity drive: Stores diagonal parity information that is used for data reconstruction when two drives fail within the RAID group





13

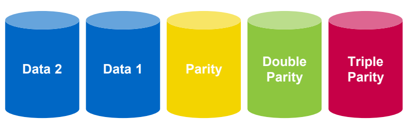
The dParity drive stores diagonal parity values in a RAID DP group. This capability provides protection against two drive failures in a RAID group. Most drive failures are not due to mechanical reasons but are failures in the drive medium. These failures are called soft failures. When drive capacities grew to 1TB, the industry saw an increase in soft failures. More blocks mean more probability of a soft failure. As capacities increased, so did the rebuild times. During the hours it takes to rebuild one failed drive, another drive in the same RAID group could experience a soft failure. This failure could cause the aggregate to go offline to protect against further failures, which could result in data loss. This condition is known as a double-disk failure.

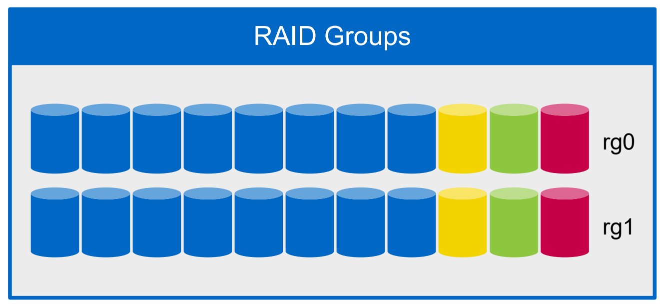
It is important to know that a NetApp storage system can safely experience multiple drive failures and remain operational. The distinction is that the failures must occur in the same RAID group to qualify as a double-disk failure.

Drive Roles

tParity drive

tParity drive: Stores anti-diagonal parity information that is used for data reconstruction when three drives fail within the RAID group





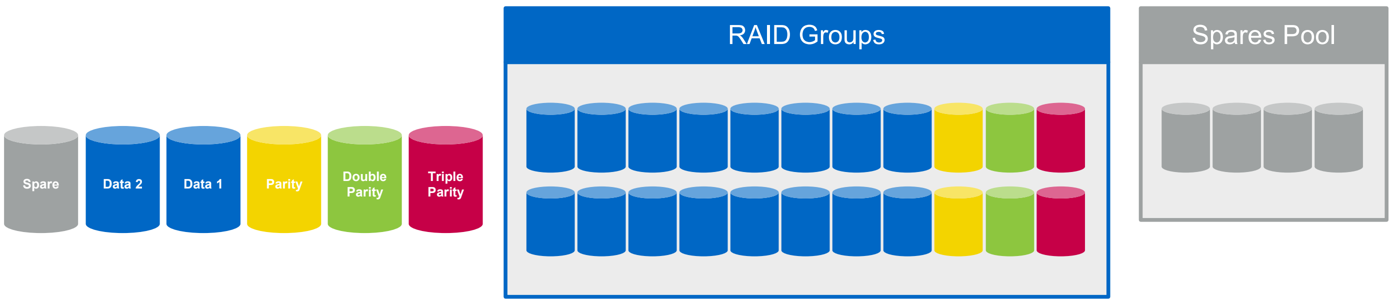
The tParity drive is the third parity drive that is used by RAID-TEC groups. The tParity drive protects against a third drive failure. RAID-TEC is required when you use drives with capacities of 6TB because of the increased probability of soft failures.

Drive Roles

Spare drive

Spare drive:

- Assigned to a storage system but not in use by a RAID group
- Used to create aggregates, add capacity to aggregates, and to replace failing drives.
  Spare drives must be “zeroed” before use.

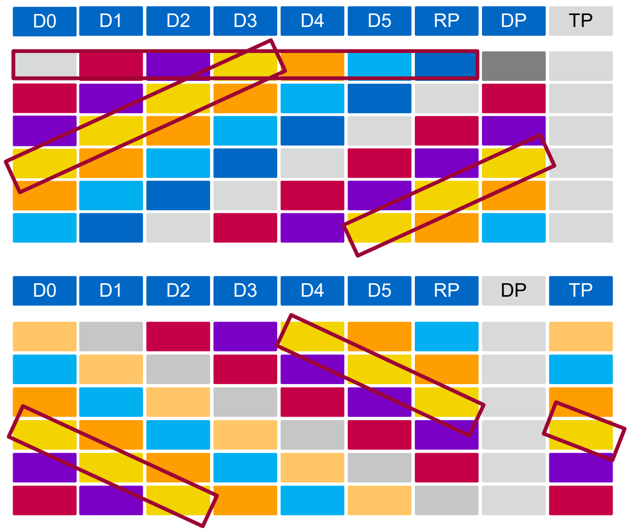


Not all drives are used to store data. To replace failed drives as quickly as possible, storage systems require that a small percentage of drives is set aside as spares. Storage administrators can also use them to grow an aggregate by adding them to a RAID group.

Before a spare drive can be used, all the data blocks must be set to a value of zero. This process is referred to as “zeroing.” New purchased drives and replacement drives that are sent by the NetApp Support team are already zeroed. If a drive is removed from a RAID group for any reason, it must be zeroed in OnCommand System Manager or the CLI before it is added to the spares pool. Verify that all spare and unused drives are zeroed regularly. An unused drive that is not zeroed is not counted as a spare and is not used to replace a failed drive.

ONTAP RAID Technologies

Description



- RAID 4 (row parity)
  - Adds a *row parity* drive
  - Protects against single-disk failure or media error
- RAID DP (double parity) technology
  - Adds a *diagonal parity* disk to a RAID 4 group
  - Protects against two concurrent drive failures within a RAID group
- RAID-TEC (triple erasure coding) technology
  - Adds a *triple-parity* disk to a RAID DP group
  - Protects against three concurrent drive failures

16

RAID 4

In a RAID 4 group, parity is calculated separately for each row. In the example, the RAID 4 group contains seven disks, with each row containing six data blocks and one parity block.

RAID DP Technology

In a RAID DP group, a diagonal parity set is created in addition to the row parity. Therefore, an extra double-parity drive must be added. In the example, the RAID DP group contains eight drives, with the double parity calculated diagonally by using seven parity blocks.

- The number in each block indicates the diagonal parity set to which the block belongs.
- Each row parity block contains even parity of data blocks in the row, not including the diagonal parity block.
- Each diagonal parity block contains even parity of data and row parity blocks in the same diagonal.

RAID-TEC Technology

In a RAID-TEC group, an anti-diagonal parity set is created in addition to both the row parity and diagonal parity sets. Therefore, an extra third-parity drive must be added. In the example, the RAID-TEC group contains nine drives, with the triple parity calculated anti-diagonally by using seven parity blocks.

- Seven diagonals (parity blocks) exist, but ONTAP software stores six diagonals (p-1).
- The missed diagonal selection is arbitrary. Here, diagonal 6 is missing and is not stored or calculated.

Regarding diagonal numbers, the following guidelines apply:

- The set of diagonals collectively spans all of the data drives and the row parity drive.
- Each diagonal misses only one drive, and each diagonal misses a different drive. Each drive misses a different diagonal.
- The diagonal sequencing within a given disk starts with the diagonal number that corresponds with the given drive number. So, the first diagonal on drive number 0 is diagonal 0, and the first diagonal on disk N is diagonal N. The diagonals on the disk wrap around when the end of the diagonal set is reached.

RAID Group Sizes

Default RAID group sizes:

- 21 drives for SATA or NL-SAS drives
- 24 drives for SAS, SSD, or NVMe drives

When you expand an aggregate, always add the equivalent of half the RAID group size (7 to 14 drives) to avoid a degradation in performance.

Disk Type	Group Type	Default	Maximum
SATA	RAID4	7	7
	RAID-DP	14	20
	RAID-TEC	***21***	***29***
NL-SAS	RAID4	7	7
	RAID-DP	14	20
	RAID-TEC	***21***	***29***
SAS	RAID4	8	14
	RAID-DP	16	28
	RAID-TEC	***24***	***29***
SSD or NVMe	RAID4	8	14
	RAID-DP	23	28
	RAID-TEC	***24***	***29***

 17

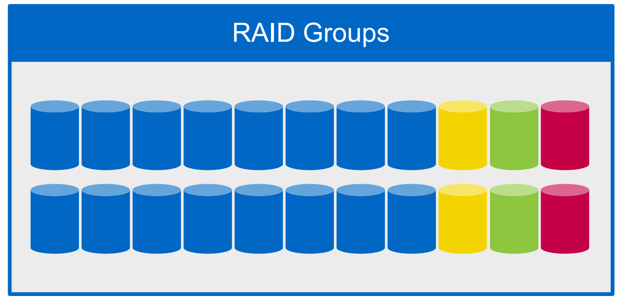
To create a RAID-TEC aggregate, you need a minimum of seven drives.

Ideally, you want to use fully populated RAID groups to create aggregates. At a minimum, RAID groups should be half their maximum size. Then when you grow the aggregates (through adding to the RAID groups), you can add half the RAID group size to make the RAID group fully populated. Adding fewer drives might result in a degradation in performance.

When drives are added to a RAID group, WAFL directs all writes to the new drives until they are as full as the other drives in the RAID group. If there are too few drives to process the I/O, latency increases and performance might decline.

RAID Group Recommendations

- Drives must be the same type:
  - SAS, SATA, or SSD and NVMe
  - Array LUNs
- Drives should be the same speed and size:
  - SAS 15K or 10K
  - SATA 7.2K
- You should provide sufficient hot spares.



 18

A RAID group consists of one or more data drives or array LUNs, across which client data is striped and stored. A RAID group includes as many as two parity drives, depending on the RAID level of the aggregate that contains the RAID group.

You change the size of RAID groups on a per-aggregate basis. You cannot change the size of an individual RAID group.

When sizing RAID groups of hard disk drives (HDDs) or solid-state drives (SSDs), observe the following guidelines:

- RAID groups are composed of the same disk type.
- All RAID groups in an aggregate should have the same number of drives.

If you cannot follow the guideline, any RAID group with fewer drives should have only one drive less than the largest RAID group.

NOTE: The SSD RAID group size can differ from the RAID group size for the HDD RAID groups in a flash pool aggregate. Usually, you should verify that you have only one SSD RAID group for a flash pool aggregate, to minimize the number of SSDs that are required for parity.

- The recommended range of RAID group sizes is as follows:
  - Between 12 and 20 for SATA HDDs
  - Between 20 and 28 for SAS HDDs and SSDs

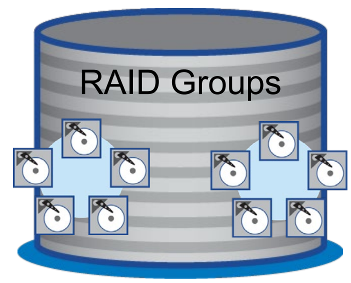
The reliability and smaller size (faster rebuild times) of performance HDDs can support a RAID group size of up to 28, if needed.

- You should not mix 10K-RPM and 15K-RPM hard disks in the same aggregate. Mixing 10K-RPM disks with 15K-RPM disks in the same aggregate effectively throttles all disks down to 10K RPM. Throttling results in longer times for corrective actions, such as RAID reconstructions.

Recommendations about spares vary by configuration and situation. For information about best practices for working with spares, see Technical Report 3437: *Storage Subsystem Resiliency Guide*.

Aggregates

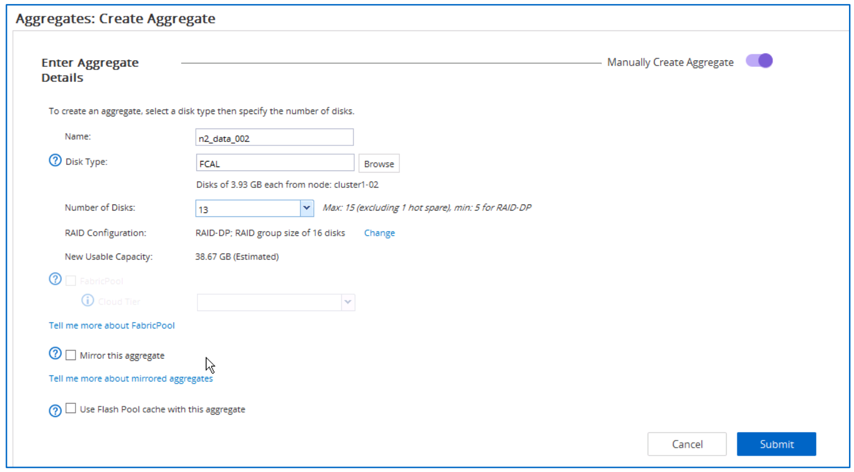
- Aggregates are logical containers for the drives that are managed by a node.
- Aggregates consist of one or more RAID groups.
- You can use aggregates to do the following:
  - Isolate workloads with different performance demands
  - Tier data with different access patterns
  - Segregate data for regulatory purposes
- A single node owns an aggregate, but ownership can be transferred to the partner in a high-availability (HA) pair.
  - During an HA failover, aggregate ownership is temporarily transferred to the surviving partner.



Create an Aggregate

Information to provide:

- Aggregate name
- Disk type
- Owning node
- Number of disks
- RAID type




```
cluster2::> aggr create -aggregate n2_data_02 -node cluster1-02
          -disktype fcal -diskcount 8
```


For most disk types, RAID DP is the default.

RAID-TEC is the only available RAID type if the following are true:

- The drive type of the aggregate drives is FSAS or mSATA.
- The drive size is equal to or larger than 10TB.

ACTION: Try This Task

Use cluster1 in your exercise kit to try the following tasks:

1. Open a PuTTY session and use the `aggr show` command.
   - Can you tell which node owns the aggregate?
   - What is the RAID status?
   - How can you determine how many disks are in each aggregate?
2. Different commands show similar things in different ways:
   - Enter **`aggr show -aggregate aggr0_cluster1-01`**.
   - Enter **`storage disk show -aggr aggr0_cluster1-01`**.

   How do the outputs of the commands differ?
3. How can you find a "broken" disk?

1a. The owning node is listed in the Nodes column.

1b. RAID status should be raid_dp, normal.

1c. Use the `-instance` switch and review the "number of disks" field or use the `aggr show -fields diskcount` command.

2. The `aggr show` command displays extensive information about the aggregate, including the list of disks. `storage disk show` displays a list of disks in the aggregate and information about the disks.

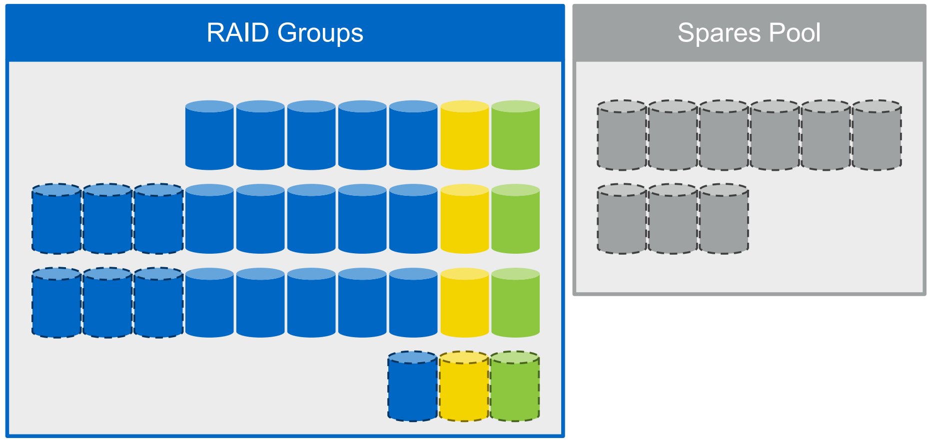
3. Type: `storage disk show -broken`.

Adding Drives to an Aggregate

To add capacity to an aggregate, you add more drives. Careful planning ensures that you use the fewest drives to add the maximum amount of capacity.

Example: Aggregate composed of 1TB drives.

- Three drives add 3TB of capacity and fill out the Raid group.
- To add 4TB, you need six drives.
  - You have no more spares.
  - The "runt" RAID group decreases performance because IOPS is serviced by a single drive.



 22

You can add drives from the spares pool to an aggregate to increase the aggregate's capacity. When you add drives, consider the size of RAID groups in the aggregate. Plan to fill complete RAID groups to maximize the amount of usable space that is gained in comparison to the number of drives that are used for parity. In the second example, six drives are added to the aggregate. However, only four of the six drives add capacity to the aggregate, because two drives are used for parity drives in a new RAID group.

By using all available spares, you have triggered an ONTAP protection feature that will trigger a shutdown in 24 hours unless enough spares are assigned to the storage controller.

The new RAID group that is created does not have enough data drives to stripe data across. This condition results in uneven I/O performance because the "runt" RAID group cannot provide the same number of IOPS as the other RAID group.

When you add drives, also consider the following:

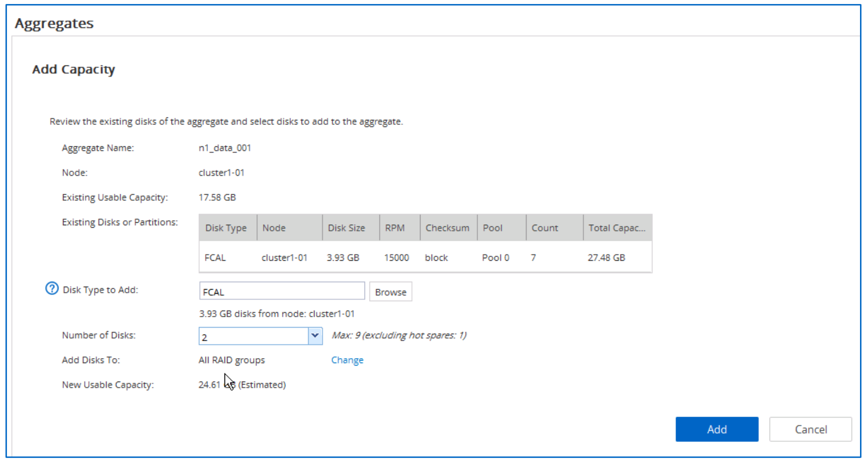
- Addition of drives that the same system owns
- Benefits of keeping your RAID groups homogeneous for drive size and speed
- Types of drives that can be used together
- Checksum rules when drives of more than one checksum type are in use
- Addition of the correct drives to the aggregate (the disk addition operation cannot be undone)
- Method of adding drives to aggregates from heterogeneous storage
- Minimum number of drives that you must add for best performance
- Number of hot spares to provide for protection against drive failures
- Requirements for adding drives from multidisk carrier drive shelves

Adding Capacity to Aggregates

Provide the following information:

- Aggregate name
- Disk type
- Number of disks

You cannot shrink aggregates.




```
::> storage disk show -spare -owner cluster1-01
::> storage aggregate add-disks –aggr n1_data_001 disks 2
```

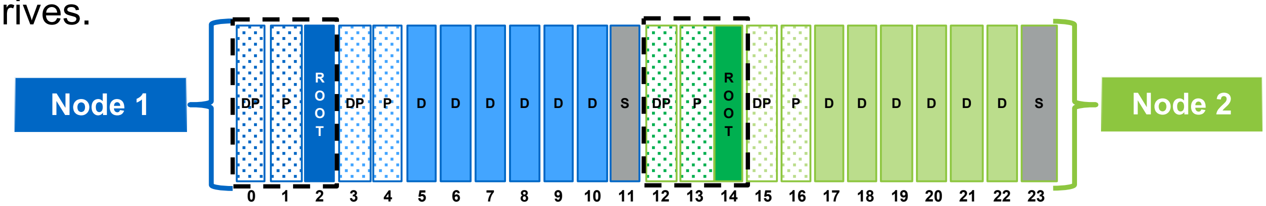
ACTION: Topic for Discussion

- What is one alternative to adding a few disks to an aggregate when all current RAID groups are full?

Lesson 2
Advanced Drive Partitioning

Why Slice Drives into Partitions?

Before ONTAP 8.3 software, the following is how entry-level HA pairs used their drives.



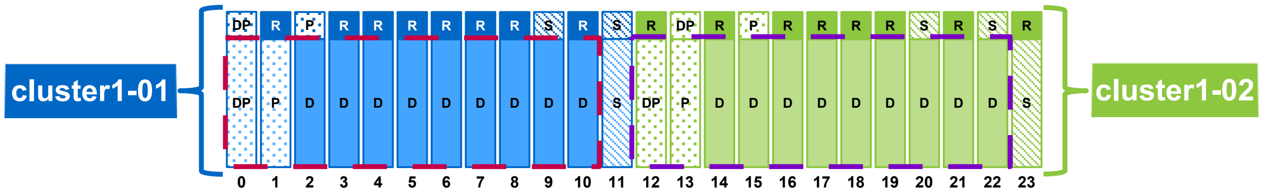
- Of the 24 drives in the chassis, each node can use only 6 drives to store data:
  - 4 x parity
  - 1 x spare
  - 1 x root aggregate (only usable by the root volume)
  - 6 x data
- Efficiency was limited to about 40%.

 26

Before the introduction of Advanced Drive Partitioning, entry-level systems with internal drives had to split ownership of the drives. Each system requires a root aggregate which consumes three drives to hold a root volume that is generally only 150GB in size. The data aggregate needs two drives for parity, and the system requires at least one spare drive.

Some customers would only assign four drives to node 2, making it an active-standby. Node 1 gained eight more drives but had to do all of the work.

Root-Data Advanced Disk Partitioning

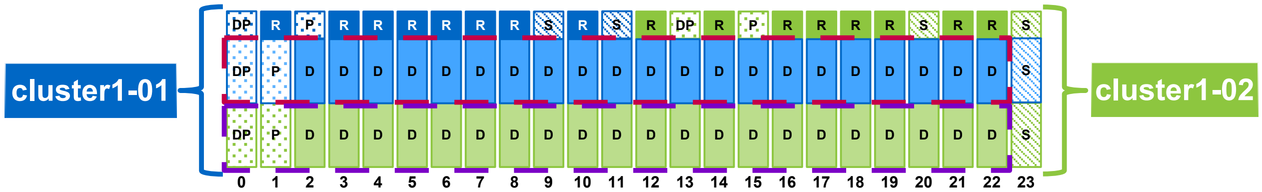


- SSDs are partitioned into one small root partition and one large data partition.
- Standard aggregate configuration per node is as follows:
  - A root aggregate RAID group of 8 data + 2 parity partitions and 2 spare root partitions
  - A data aggregate RAID group of 9 data + 2 parity partitions and 1 spare data partition
- Total usable capacity is 18 data partitions out of a total of 24, which achieves 75% efficiency.

The figure shows the default configuration for a single-shelf AFF system.

Root-Data-Data Advanced Disk Partitioning

ONTAP 9 and later software

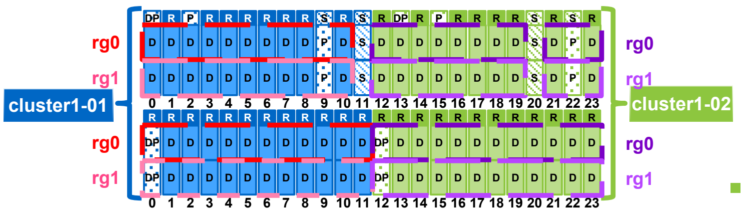


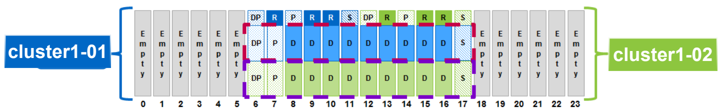
- SSDs are partitioned into one small root and two data partitions, each of which is half the size of a root-data partition.
- The standard aggregate configuration per node is as follows:
  - A root aggregate RAID group of 8 data + 2 parity partitions and 2 spare root partitions (no change from root-data partition)
  - A data aggregate RAID group of 21 data + 2 parity partitions and 1 spare data partition
- The total usable capacity is 42 data partitions out of a total of 48: 87.5% efficiency, or 16.7% more usable capacity (0.875 / 0.75).

The figure shows the default configuration for a single-shelf AFF system in ONTAP 9 software.

Root-Data-Data Advanced Disk Partitioning

Additional root-data-data partitioning information





- Root-data-data partitioning is supported on only AFF systems:
  - Default root aggregate provisioning method for AFF
  - Unsupported on entry-level FAS or AFF MetroCluster software
- Data partition assignments with two shelves are similar to root-data partitioning:
  - Data partitions on an SSD are assigned to the same node.
  - Twice as many RAID groups are used.
- Half-shelf AFF systems have 50% more usable capacity than with root-data partitioning.

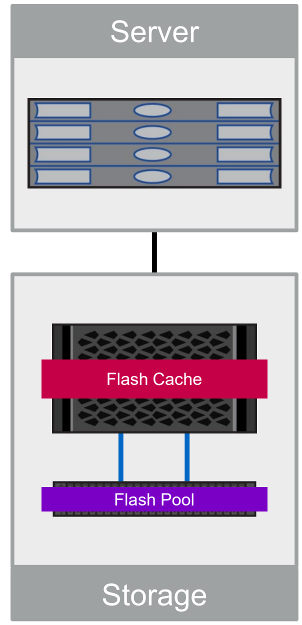
The figures show the default configuration for two-shelf and half-shelf AFF systems in ONTAP 9 software.

For root-data partitioning and root-data-data partitioning, RAID uses the partitions in the same way as physical disks. If a partitioned disk is moved to another node or used in another aggregate, the partitioning persists. You can use the disk in only RAID groups that are composed of partitioned disks. If you add an unpartitioned drive to a RAID group that consists of partitioned drives, the unpartitioned drive is partitioned to match the partition size of the drives in the RAID group. The rest of the disk is unused.

Lesson 3
Flash Cache and Flash Pool Features

NetApp Virtual Storage Tier

- Flash Cache intelligent caching:
  - Has highest performance for file services
  - Improves latency for random reads
  - Delivers predictable, high-speed data access for all protocols
  - Maintains deduplicated and compressed blocks in the cache
  - Is shared by all volumes on a node
- Flash Pool intelligent caching:
  - Has the highest performance for OLTP
  - Is best for SATA enablement across multiple workloads
  - Caches for reads *and* writes
  - Automates the use of SSD technology



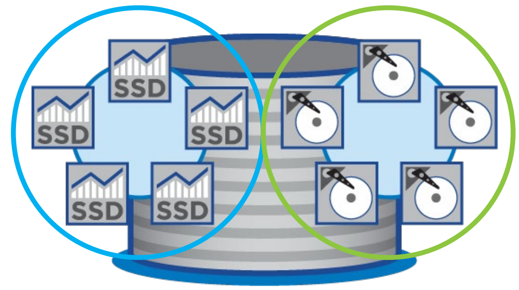
At the storage level, there are two ways to implement Virtual Storage Tier (VST):

- The controller-based Flash Cache feature accelerates random-read operations and generally provides the highest performance solution for file-services workloads. Flash Cache intelligent caching combines software and hardware within NetApp storage controllers to increase system performance without increasing the drive count. The Flash Cache controller-based solution is available to all volumes that are hosted on the controller. A frequently seen use case for Flash Cache is to manage VMware boot storms.
- The Flash Pool feature is implemented at the disk-shelf level, enabling SSDs and traditional HDDs to be combined in a single ONTAP aggregate. Flash Pool technology provides read caching and write caching and is well-suited for OLTP workloads, which typically have a higher percentage of write operations.

Both VST technologies improve overall storage performance and efficiency and are simple to deploy and operate.

Flash Pool Aggregates

- Contents of Flash Pool aggregates:
  - SAS or SATA drives for user data
  - SSDs for high-performance caching
- Ways that flash pools improve performance:
  - Offload read operations
  - Offload repetitive write operations
- Two types of flash pools:
  - Dedicated SSD
  - Shared storage pool
- Use case: OLTP workloads



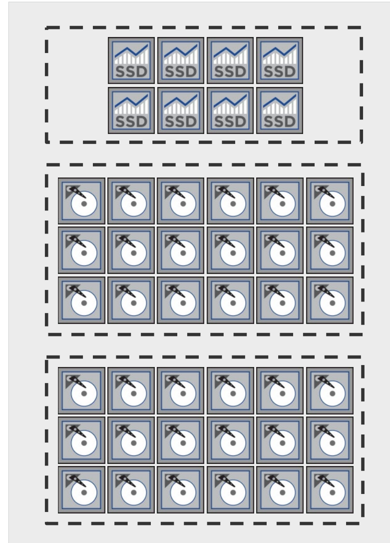
A flash pool aggregate is a special type of hybrid data aggregate.

A flash pool aggregate combines SAS or SATA drives and SSDs to provide high performance in a more economical way than an SSD aggregate. The SSDs provide a high-performance cache for the active dataset of the data volumes that are provisioned on the flash pool aggregate. The cache offloads read operations and repetitive write operations to improve response times and overall throughput for disk I/O-bound data-access operations.

Flash pools can improve workloads that use OLTP, such as database application data. Flash pools do not improve the performance of predominantly sequential workloads.

Blocks in the SSD Tier

- Flash pool metadata
- Read-cached blocks:
  - Cached copies of blocks from the HDD tier
  - Still exist on the HDD tier
- Write-cached blocks:
  - Written directly to the SSD tier
  - Not yet written to the HDD tier



The following blocks are stored in the SSD tier of the flash pool:

Flash pool metadata: All metadata that is associated with the flash pool is stored in the SSD tier of the aggregate.

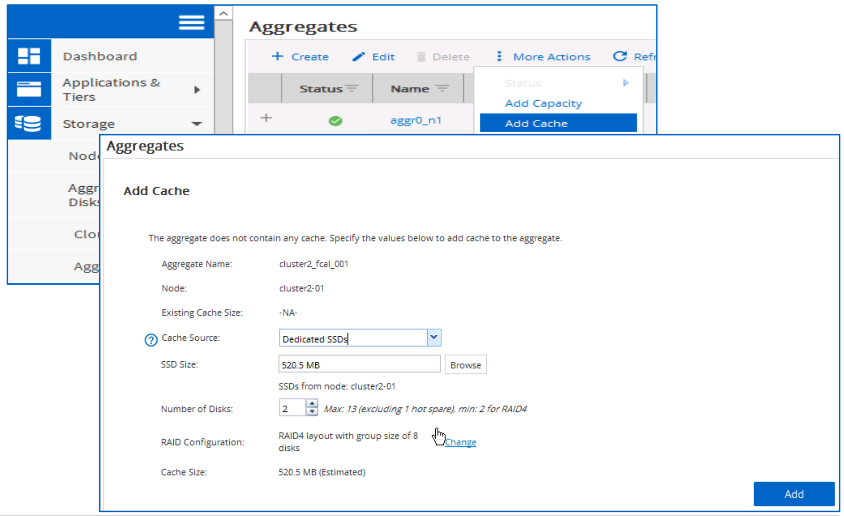
Read-cached blocks: Read-cached blocks are stored in the SSD tier. Almost all data from the active file system in a read/write volume is eligible to be read-cached in the SSD tier.

Write-cached blocks: Write-cached blocks are associated with a FlexVol volume that is written directly to the SSD tier of the aggregate. Only one copy of the block exists. A hard-disk block is reserved for write-cached blocks for an eventual move into the HDD tier after access to the block ceases.

Create a Flash Pool Aggregate

Provide the following information:

- Existing aggregate name
- Cache source or drive type
- Number of drives
- RAID type (RAID_4 by default)




```
::> aggr modify -aggregate cluster2_fcal_001 -hybrid-enabled true
::> aggr add-disks -aggr cluster2_fcal_001 -disktype SSD -diskcount 2
```

 34

In a Flash Pool aggregate, the SSD RAID group size can be different from the RAID group size for the HDD RAID groups. Usually, you should ensure that you have only one SSD RAID group for a Flash Pool aggregate to minimize the number of SSDs that are required for parity.

For information about best practices for working with aggregates, see Technical Report 3437: *Storage Subsystem Resiliency Guide.*

To see the physical and usable capacity for a specific drive, see the Hardware Universe at hwu.netapp.com.

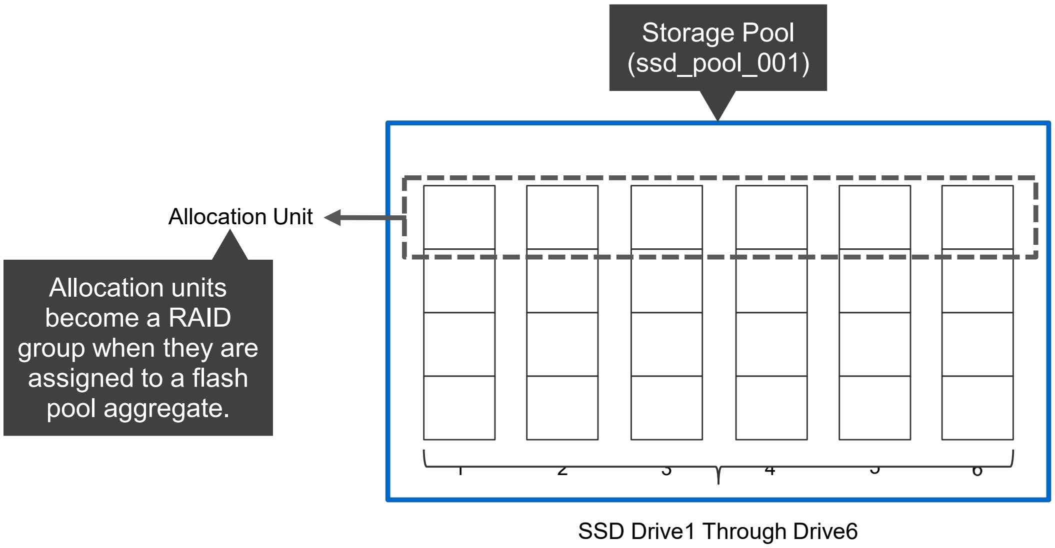
SSD Partitioning for Flash Pool Intelligent Caching

- Increased storage use for SSDs in flash pool aggregates
- Ability to share spares between HA partners
- Better use of SSD performance

SSD partitioning for Flash Pool intelligent caching enables customers to group SSDs into a shared resource, which is allocated to multiple flash pool aggregates. The feature spreads the cost of the parity SSDs over more aggregates, increases SSD allocation flexibility, and maximizes SSD performance.

SSD Partitioning for Flash Pool Cache

Creation



SSD storage pools provide SSD caching to two or more flash pool aggregates. Creating an SSD storage pool requires between 2 and 28 spare SSD drives.

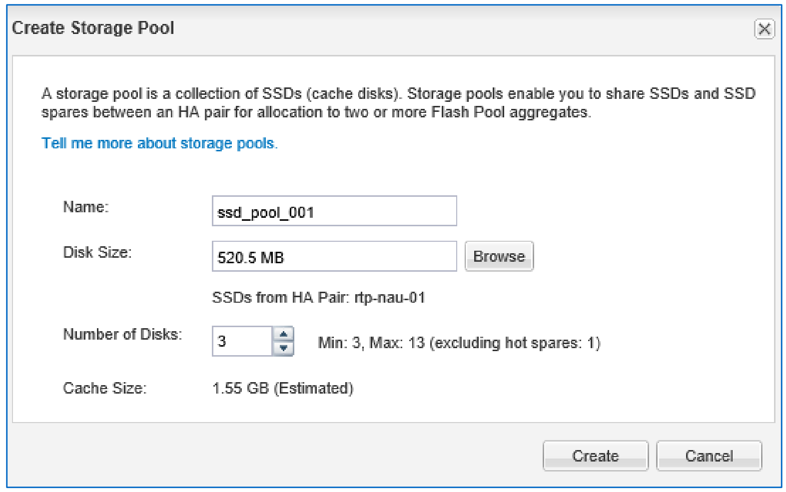
In the example, SSD Drive1 through Drive6 are available as spares. The ‘`storage pool create`’ command is used to create the storage pool. The unit of allocation for an SSD storage pool is equal to a single slice from each SSD drive in the storage pool. The ‘`storage pool create`’ command slices each SSD drive into four equal pieces, making an allocation unit that equals one fourth of all of the SSD disks in the storage pool.

An allocation unit becomes a RAID group when the allocation unit is assigned to a flash pool aggregate.

Create an SSD Storage Pool

Provide the following information:

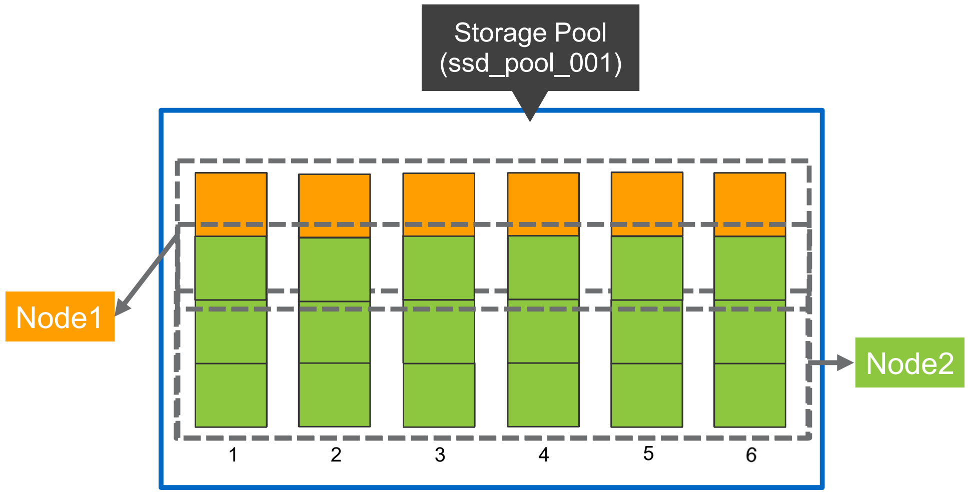
- Storage pool name
- Number of drives
- Size of SSDs from the HA pair (if multiple sizes are available)




```
::> storage pool create -storage-pool ssd_pool_001 -disk-count 3
```

SSD Partitioning for Flash Pool Cache

Ownership

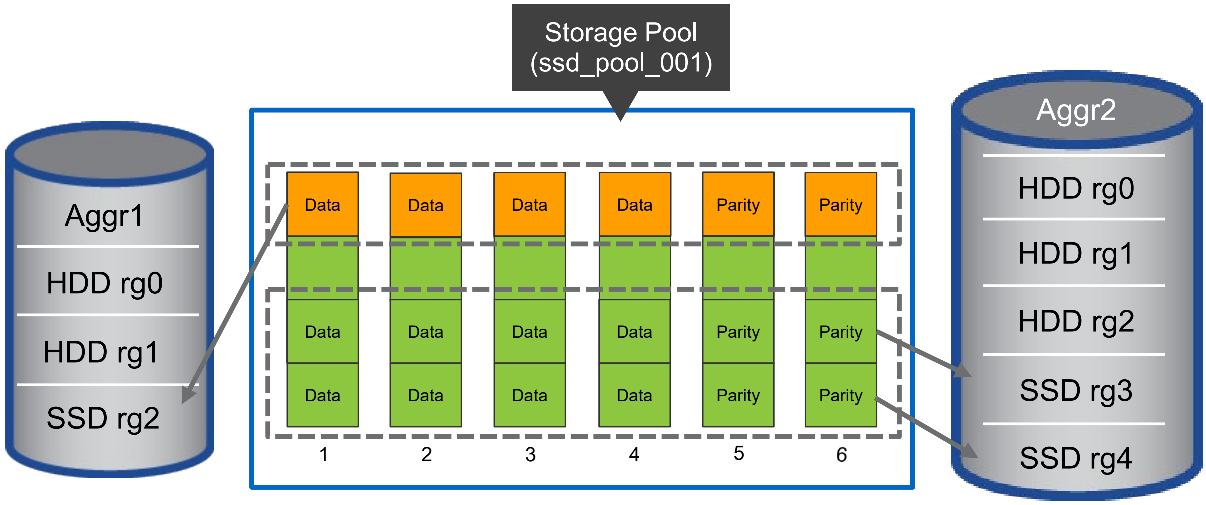



```
cluster1::> storage pool reassign -storage-pool ssd_pool_001
    -from-node cluster1-01 -to-node cluster1-02 -allocation-units 1
```


By default, two allocation units are assigned to each node in the HA pair. To change the ownership of one or more allocation units of a storage pool from one HA partner to the other, use the `storage pool reassign` command. In the example, one allocation unit is reassigned from Node1 to Node2.

SSD Partitioning for Flash Pool Cache

Ownership



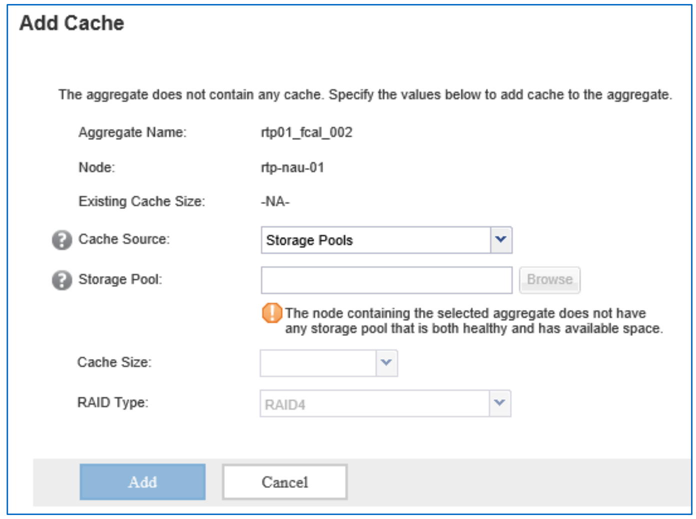
 39

By default, two allocation units are assigned to each node in the HA pair. To change the ownership of one or more allocation units of a storage pool from one HA partner to the other, use the `storage pool reassign` command. In the example, one allocation unit is reassigned from Node1 to Node2.

Create a Flash Pool that uses an SSD Storage Pool

Provide the following information:

- Existing aggregate name
- Storage pool name




```
::> storage aggregate add-disks -aggregate rtp01_fcal_002 -
allocation-units 1 -storage-pool ssd_pool_001
```

NetApp Virtual Storage Tier

Feature comparison

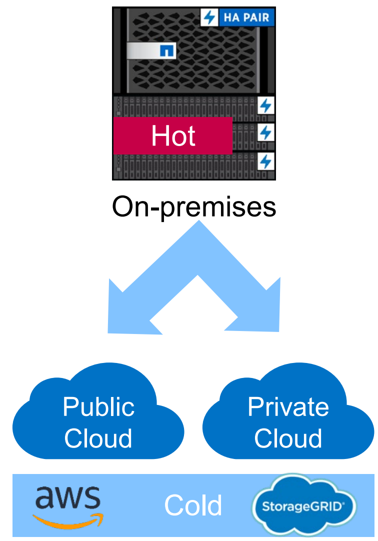
	Flash Cache	Flash Pool
What is the feature?	▪ A controller-based PCIe card ▪ A plug-and-play device	▪ Storage-level, RAID-protected cache (specific to aggregates)
What does the feature do?	▪ Provides per-controller cache ▪ Caches random reads	▪ Caches random reads and overwrites ▪ Provides cached data persistence through failovers
Where does the feature fit?	▪ With random-read workloads, such as file services ▪ With workloads that contain multiple volumes that are in various aggregates on a controller	▪ With random-overwrite-heavy workloads such as OLTP workloads ▪ Where consistent performance is required

The Flash Cache and Flash Pool features bring flash technology to ONTAP software. The table compares the primary uses and benefits of both features.

Lesson 4
FabricPool Aggregates

FabricPool Aggregates
Overview

- What FabricPool aggregates contain:
  - A performance tier for frequently accessed (“hot”) data, which is on an all-SSD aggregate
  - A capacity tier for infrequently accessed (“cold”) data, which is on an object store
- How FabricPool can enhance the efficiency of your storage system:
  - Automatically tier data based on frequency of use
  - Move inactive data to lower-cost cloud storage
  - Make more space available on primary storage for active workloads
  - View how much data in a volume is inactive by using inactive data reporting



 43

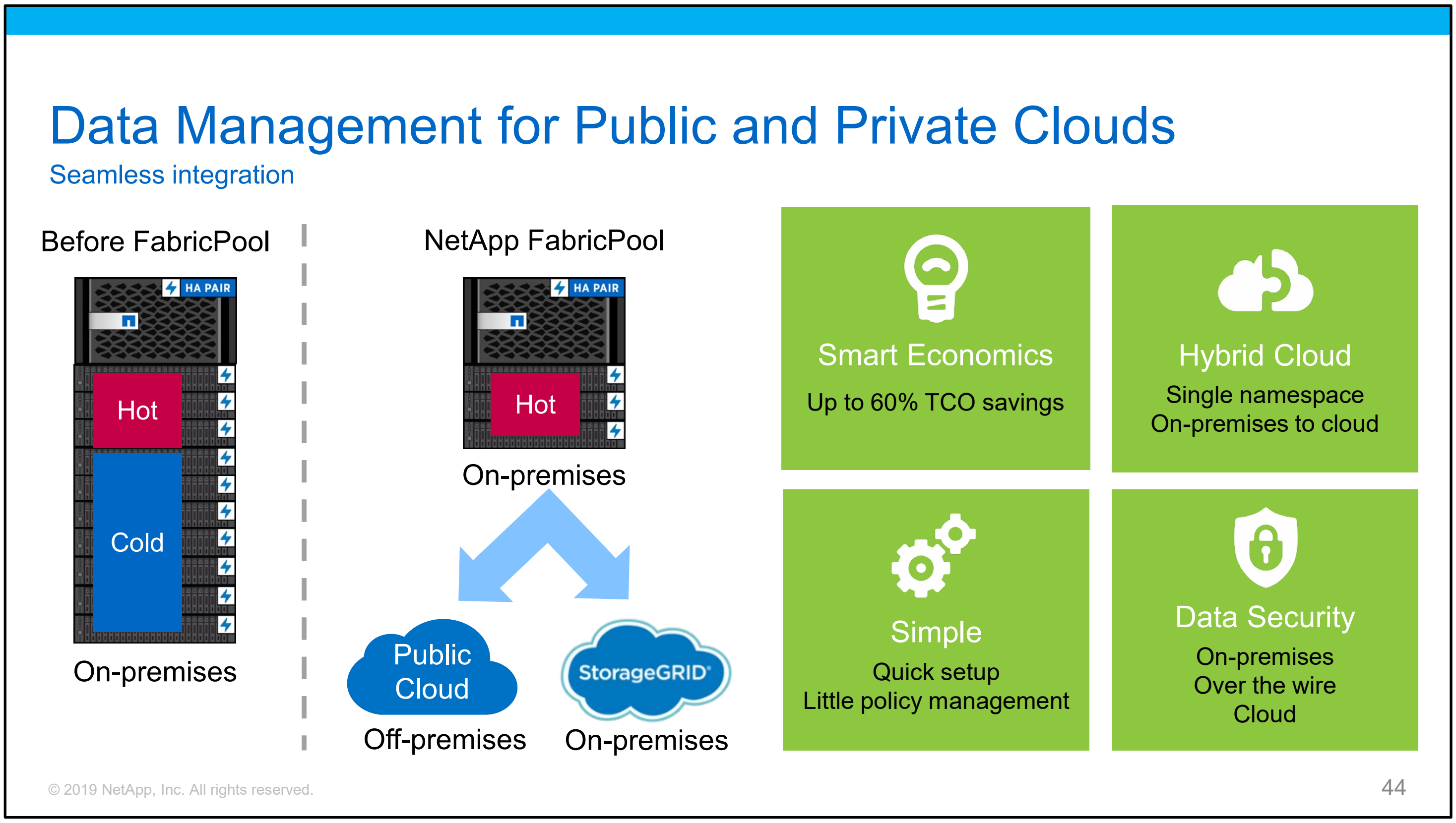
A FabricPool aggregate is new type of hybrid data aggregate that was introduced in ONTAP 9.2 software.

A FabricPool aggregate contains a performance tier for frequently accessed (“hot”) data, which is on an all-SSD aggregate. The FabricPool aggregate also has a capacity tier for infrequently accessed (“cold”) data, which is on an object store. FabricPool supports object store types that are in the public cloud using Amazon Web Services (AWS) Amazon Simple Storage Service (Amazon S3). FabricPool uses the NetApp StorageGRID solution to support object store types in private clouds.

Storing data in tiers can enhance the efficiency of your storage system. FabricPool stores data in a tier based on whether the data is frequently accessed. ONTAP software automatically moves inactive data to lower-cost cloud storage, which makes more space available on primary storage for active workloads.

Use the `-fields` parameter of the `volume show` and `aggregate show` commands to view the amount of data that is inactive.

For more information about FabricPool aggregates, see the *Disks and Aggregates Power Guide*.



Your FabricPool benefits are amazing.

Smart Economics:

You can decrease TCO because you can use flash efficiently (by using flash exclusively for hot data). You can also decrease dollars per terabyte (TB) by moving cold data to cheaper storage.

Hybrid Cloud:

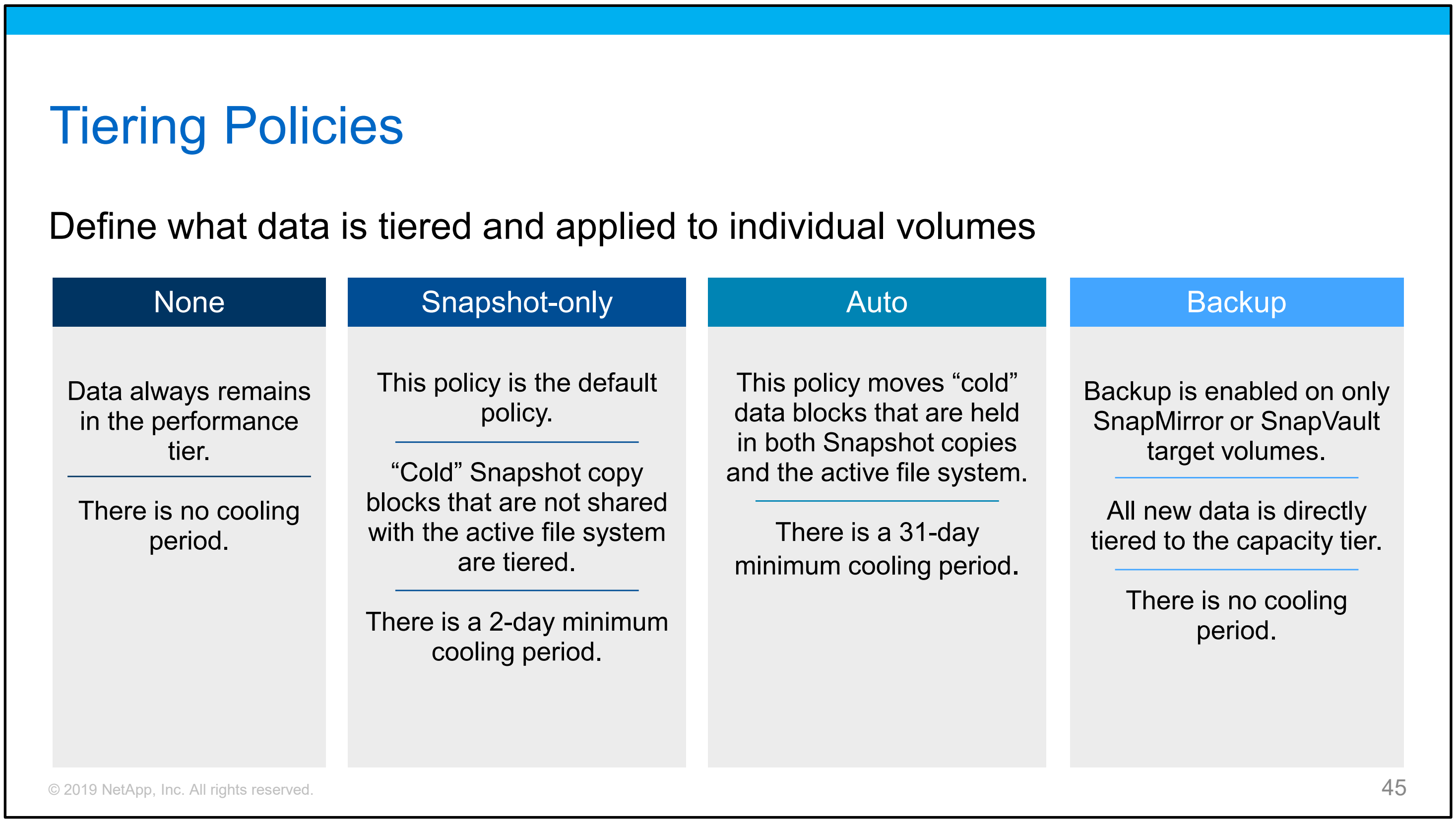
The FabricPool approach is a simpler way to organize data in the cloud because applications access data as if the data were on your premises in the primary data tier.

Simple:

You can complete one or two wizard-like setup windows, and your FabricPool is provisioned. Unlike other tiering solutions that you might have seen, FabricPool requires little to no policy management. FabricPool creates policies automatically that are based on best practices.

Security:

FabricPool can tier encrypted data. In addition, data is encrypted as it moves to and from the performance and cloud tiers.



Volumes with the None tiering policy never move their data out of the performance tier.

By default, a FabricPool moves data blocks inside Snapshot copies which are not shared by the active file system and have not been accessed for at least 2 days.

The Auto tiering policy maximizes space available in the performance storage tier. This policy moves all data blocks to the capacity storage tier when the blocks have not been accessed in the previous 31 days.

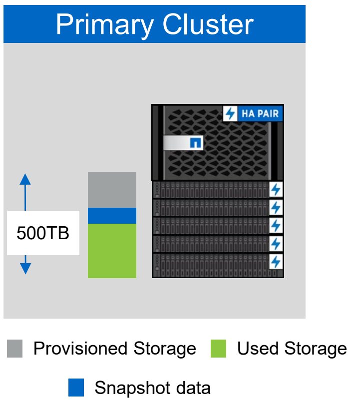
The Backup tier conserves space on secondary storage that is used for backup and disaster recovery. Newly transferred data is automatically directed to the cloud tier instead of the secondary storage.

NOTE: Moving a volume resets the cooling period for all blocks in the volume. This affects volumes with the Snapshot-only and Auto tiering policies because moved data goes into the performance tier until it cools off.

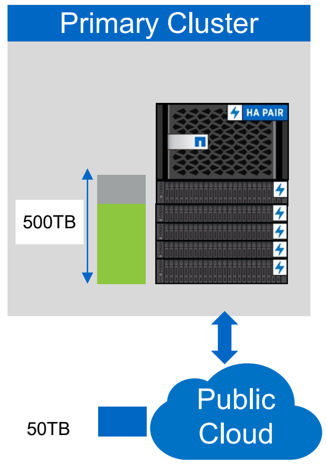
Make Room for Active Workloads on Primary Storage

Snapshot-only tiering to the cloud

Before FabricPool



After FabricPool

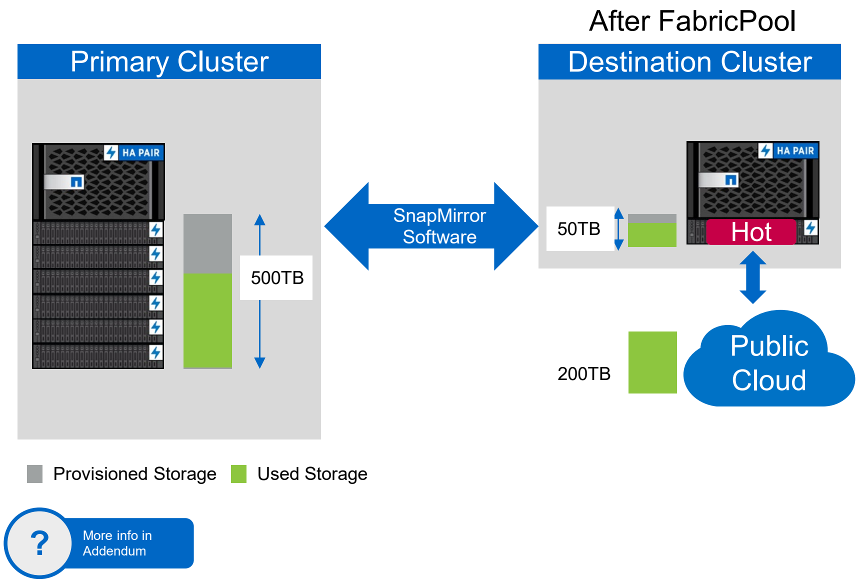


- In this example, Snapshot copies consume ~10% of used capacity.
- Moving Snapshot data enables active workloads to use the performance drives (SSDs) more effectively.

NOTE: Snapshot tiering is not the same as a backup.

Shrink Your Secondary Storage Footprint

Backup tiering secondary data to the cloud



- Expand the capacity of a destination cluster by automatically tiering data to the cloud.
- The secondary data center footprint reduces by up to 90%.
  Hot data (~10-20%) stays on-premises, and the remaining 80-90% goes to the cloud object store.
- This method requires no changes to existing data protection policies. It works seamlessly.

Learn more about FabricPool in the module addendum.

Knowledge Check: Question

1. Which statement is true of Advanced Disk Partitioning?
    a. Both nodes must have a root partition and a data partition assigned.
    b. Both nodes must have a root partition assigned.
    c. Data partitions can be assigned to any node in a cluster.
    d. Root partitions can be assigned to any node in a cluster.

Knowledge Check: Question

2. What does a Flash Pool aggregate contain?
   a. HDDs only
   b. SSDs only
   c. HDDs for data storage and SSDs for caching
   d. HDDs and SSDs that are all used for data caching

References

Documentation

- NetApp Hardware Universe: http://hwu.netapp.com
- ONTAP 9 Documentation Center: http://docs.netapp.com/ontap-9/index.jsp
  - *Disks and Aggregates Power Guide*
  - *Cluster Management Using OnCommand System Manager*
  - *ONTAP 9 Concepts*
- TR-4070: NetApp Flash Pool Design and Implementation Guide https://www.netapp.com/us/media/tr-4070.pdf
- TR-4598: FabricPool Best Practices https://www.netapp.com/us/media/tr-4598.pdf

50

NetApp Hardware Universe: http://hwu.netapp.com

ONTAP 9 Documentation Center: http://docs.netapp.com/ontap-9/index.jsp

Disks and Aggregates Power Guide

Cluster Management Using OnCommand System Manager

ONTAP 9 Concepts

TR-4070: NetApp Flash Pool Design and Implementation Guide https://www.netapp.com/us/media/tr-4070.pdf

TR-4598: FabricPool Best Practices
https://www.netapp.com/us/media/tr-4598.pdf

References

Videos

- ONTAP 9 Feature Overview: FabricPool
  https://www.youtube.com/watch?v=5WRe4wkku10
- FabricPool Using OnCommand System Manager 9.5
  https://www.youtube.com/watch?v=Fy30d36HxBU
- Cloud Tiering with FabricPool in ONTAP 9.4
  https://www.youtube.com/watch?v=RF_qh9LEjzo
- Archiving Volumes with FabricPool
  https://www.youtube.com/watch?v=5tDJAkqN2nA

 51

ONTAP 9 Feature Overview: FabricPool - https://www.youtube.com/watch?v=5WRe4wkku10

FabricPool Using OnCommand System Manager 9.5 https://www.youtube.com/watch?v=Fy30d36HxBU

Cloud Tiering with FabricPool in ONTAP 9.4 - https://www.youtube.com/watch?v=RF_qh9LEjzo

Archiving Volumes with FabricPool - https://www.youtube.com/watch?v=5tDJAkqN2nA

Module Review

This module focused on enabling you to do the following:

- Describe ONTAP storage architecture concepts
- Manage physical storage resources, including disks, RAID groups, and aggregates
- Create data aggregates
- Create Flash Pool aggregates
- Describe FabricPool aggregates

ACTION: Complete an Exercise

Module 5: Managing Physical Storage

Duration: 15 minutes

Access your lab equipment.

Use the login credentials that your instructor provided to you.

Open your Exercise Guide.

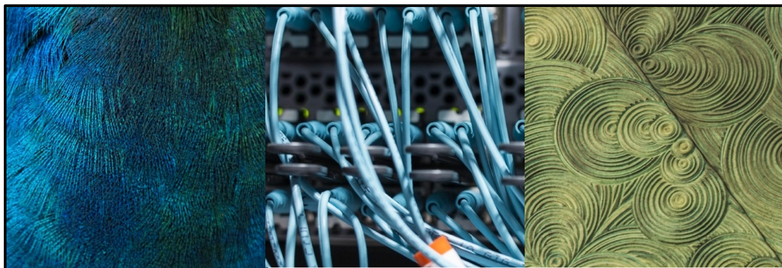
Go to the exercise for the module.

Complete the specified tasks.

- Start with Exercise 5-1.
- Stop at the end of Exercise 5-2.

Participate in the review session.

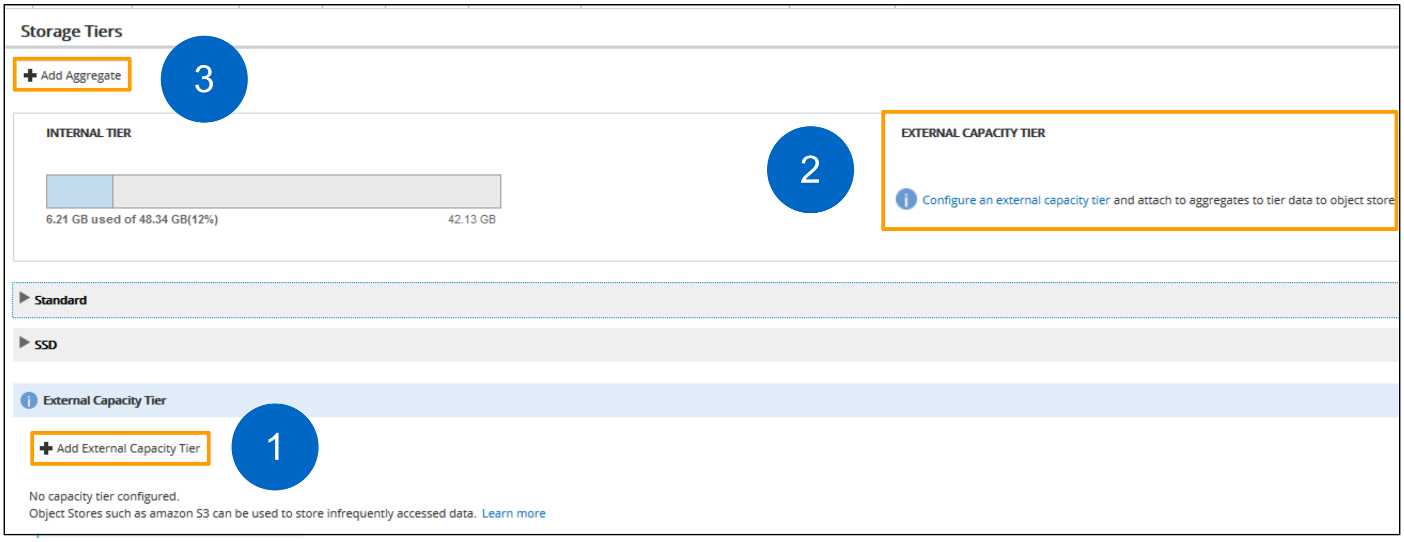
- Share your results.
- Report issues.



Addendum
FabricPool in OnCommand System Manager

FabricPool in OnCommand System Manager

Adding storage tiers



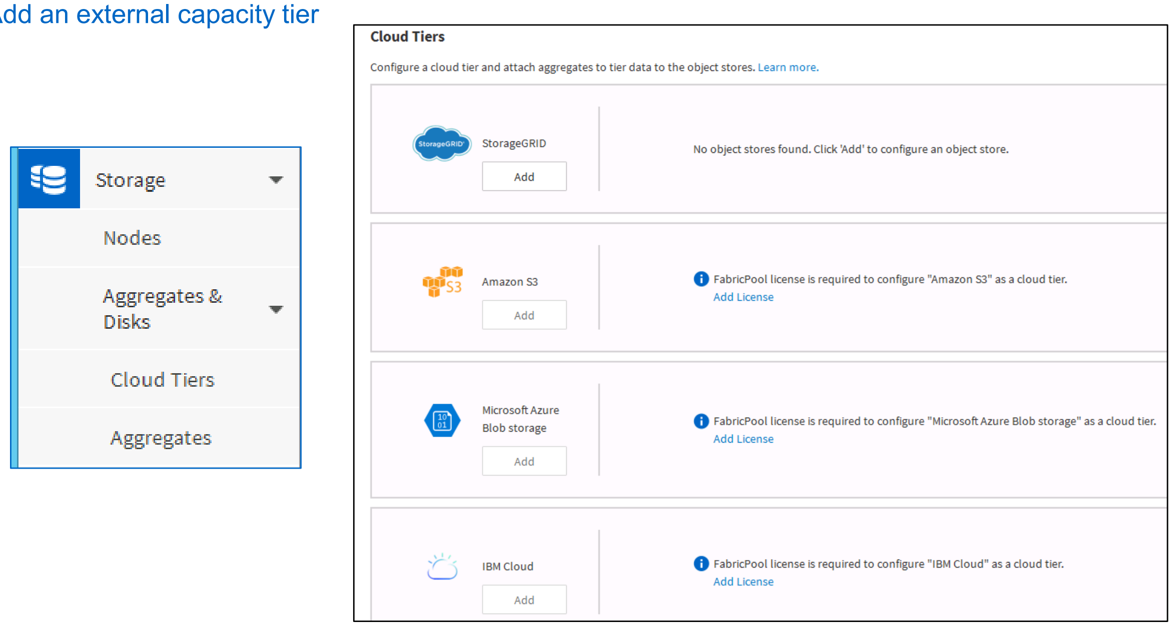
FabricPool aggregates are aggregates that have an object store attached. You set up an aggregate to use FabricPool by first specifying the configuration information of the object store that you plan to use as the capacity tier. Then you attach the object store to an all-flash (all-SSD) aggregate.

Using OnCommand System Manager enables you to create an aggregate and set it up to use FabricPool at the same time. (When you use the ONTAP CLI to set up an aggregate for FabricPool, the aggregate must exist.)

Under the Storage Tiers tab, use the Add External Capacity Tier button to add an object store.

FabricPool in OnCommand System Manager

Add an external capacity tier

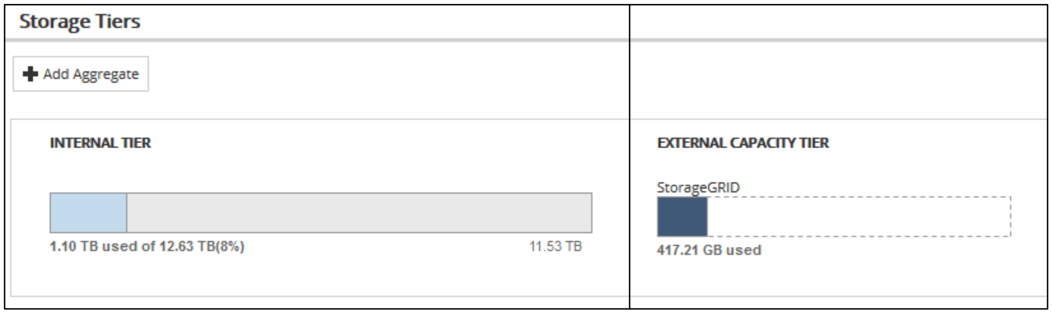


56

Selecting **Storage** > **Cloud Tiers** enables you to configure the object store to multiple object stores.

FabricPool in OnCommand System Manager

Storage tiers




```
cluster1::> storage aggregate object-store show
cluster1::> storage aggregate object-store show-space
```

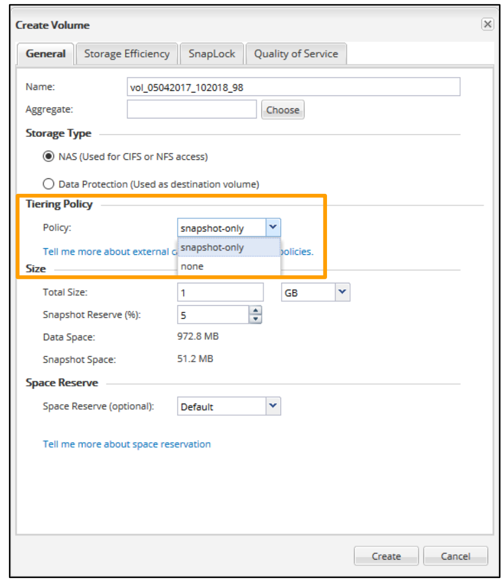

After you configure a capacity tier, the Storage Tiers section includes Internal Tier and External Capacity Tier information.

FabricPool in OnCommand System Manager

Volume snapshot-only tiering policy

When volumes are created on a FabricPool-enabled aggregate, be aware of the following:

- You should select a tiering policy. The default policy is snapshot-only.
- Changing the tiering policy of a volume after creation only changes the subsequent tiering behavior for the volume. (Changing the policy does not retroactively move data to the capacity tier.)



When you create a volume for FabricPool, you can specify a tiering policy. If no tiering policy is specified, the created volume uses the default snapshot-only tiering policy.

You need to know how much data is stored in the performance and capacity tiers for FabricPool. That information helps you to determine whether you need to change the tiering policy of a volume, increase the FabricPool licensed usage limit, or increase the storage space of the capacity tier.

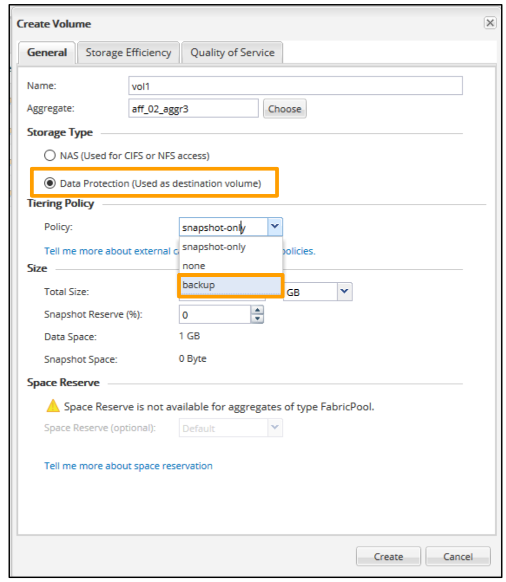
You can change the tiering policy to control whether the data of a volume is moved to the capacity tier when the data becomes inactive (cold). Changing the tiering policy of a volume changes only the subsequent tiering behavior for the volume. Changing the policy does not retroactively move data to the capacity tier.

FabricPool in OnCommand System Manager

Volume backup tiering policy

Create a backup volume on a FabricPool-enabled aggregate:

1. Select the **Data Protection** storage type.
2. Select the **backup** tiering policy.



When you create a backup volume for FabricPool, you select the Data Protection volume type and backup tiering policy.

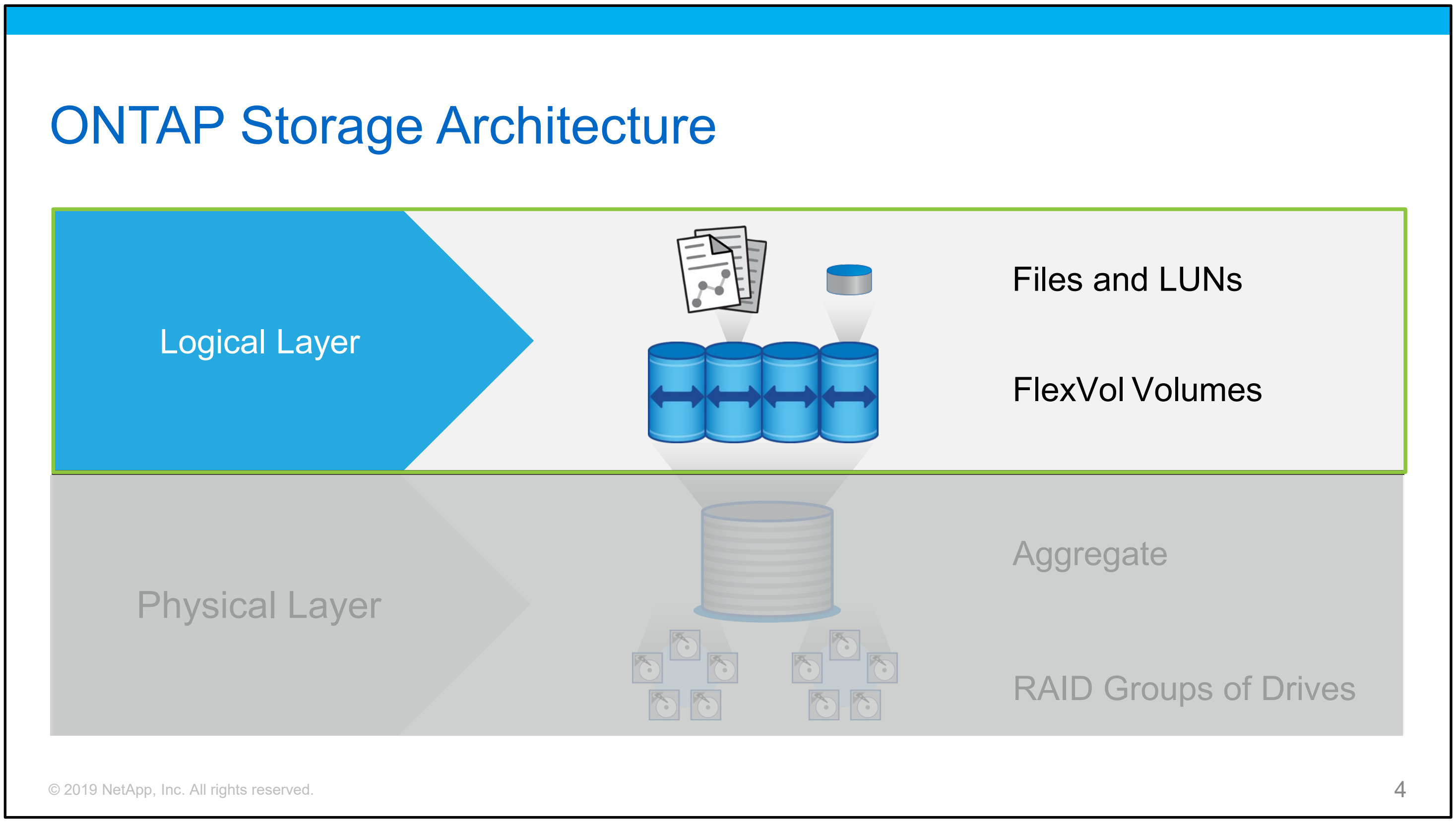
Module 6
Logical Storage Management

About This Module

This module focuses on enabling you to do the following:

- Create and manage FlexVol volumes
- Provision application-aware resources
- Move a volume within a storage virtual machine (SVM)
- Create a NetApp ONTAP FlexGroup volume

Lesson 1
Flexible Volumes



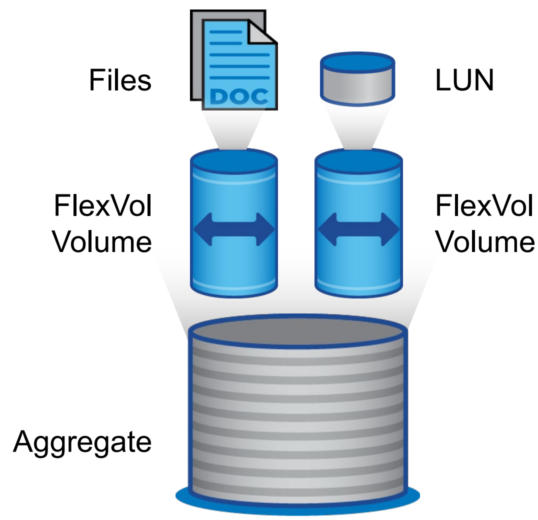
The NetApp ONTAP storage architecture uses a dynamic virtualization engine, in which data volumes are dynamically mapped to physical space.

In ONTAP software, disks are grouped into RAID groups. An aggregate is a collection of physical disk space that contains one or more RAID groups. Each aggregate has a RAID configuration and a set of assigned disks. The disks, RAID groups, and aggregates make up the physical storage layer.

Within each aggregate, you can create one or more FlexVol volumes. A FlexVol volume is an allocation of disk space that is a portion of the available space in the aggregate. A FlexVol volume can contain files or LUNs. The FlexVol volumes, files, and LUNs make up the logical storage layer.

FlexVol Volumes

- Can contain NAS, SAN, or both types of data (mixing is not recommended).
- Are contained within an aggregate, and an aggregate can hold multiple FlexVol volumes.
- Can increase or decrease in size, as needed.



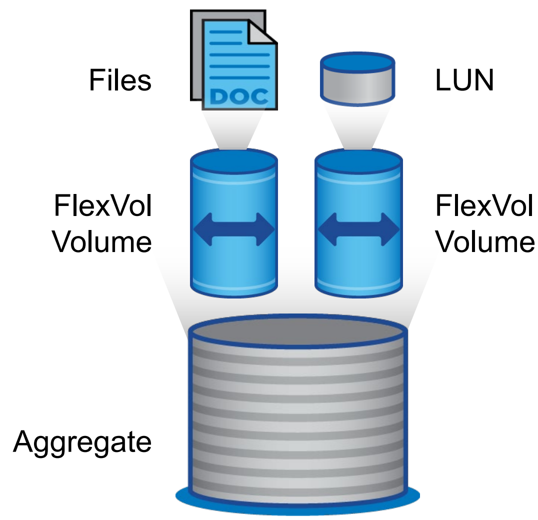
A FlexVol volume is loosely coupled to a containing aggregate, which the volume can share with other FlexVol volumes. Therefore, one aggregate can be the shared source of all the storage that is used by all the FlexVol volumes that the aggregate contains.

Because a FlexVol volume is managed separately from the aggregate, you can create small (minimum of 20MB) FlexVol volumes. You can also increase or decrease the size of FlexVol volumes in increments as small as 4KB.

FlexVol Volumes

Types

- System (or node root):
  - Typically named vol0
  - Contains only configuration and logs
  - Cannot contain user data
  - Owned by the node SVM
- SVM root volume:
  - Top level of the namespace
  - Should not contain user data
- Data:
  - **NAS:** Contains file systems for user data
  - **SAN:** Contains LUNs

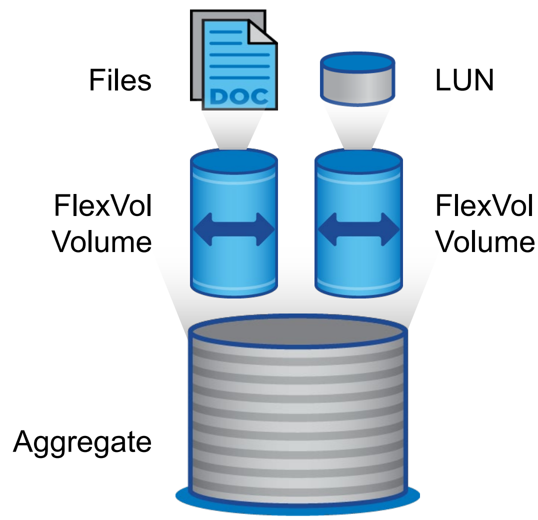


FlexVol volumes are used for the following purposes:

- As node root volumes to hold state data for the node and for the cluster
- As the root of a storage virtual machine (SVM) namespace
- To store user data within an SVM

Files and LUNs

- A file refers to any data (including text files, spreadsheets, and databases) that is exported to or shared with NAS clients.
- A LUN represents a logical drive that a SCSI protocol (FC or iSCSI) addresses:
  - Block level
  - Data accessible only by a properly mapped SCSI host



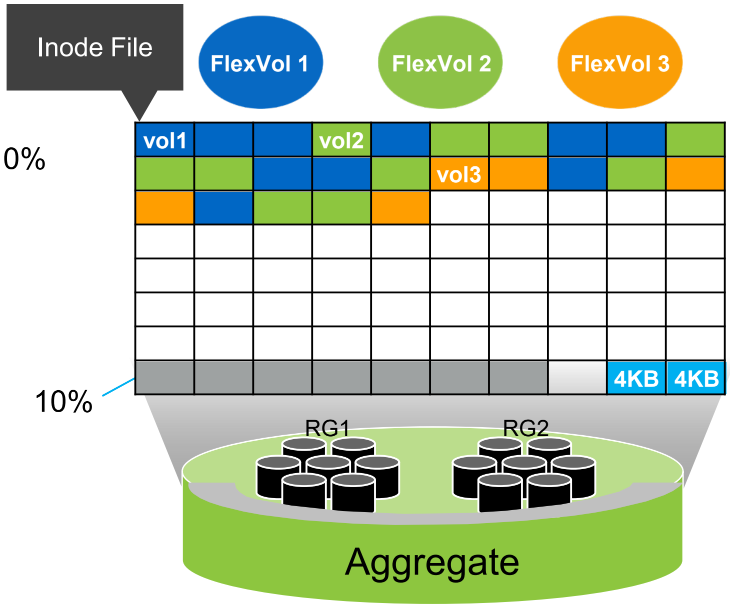
Data that is stored in a volume for a NAS environment is stored as files. Files can be documents, database files and logs, audio and video, or application data. ONTAP software manages the file system operations, and clients access the data.

Data that is stored in a SAN environment is stored in a logical container that represents a SCSI disk. The container is called a *LUN*. The LUN is presented to a host, which treats the LUN like a standard SCSI disk and writes data to the LUN in 512-byte logical blocks. Therefore, SAN is often called block-level storage—because data is stored in 512-byte SCSI blocks. ONTAP software is “unaware” of the stored files and is “aware” only of the 512-byte blocks that the host reads or writes to.

NOTE: Because SAN data (block data) and NAS data (file data) are treated differently, files and LUNs should not be placed in the same FlexVol volume.

Volumes in Aggregates

- Aggregate:
  - 4KB blocks
  - NetApp WAFL file system reserving 10%
- Volume:
  - Provisioning types:
    - **Thick:** Volume guarantee = volume
    - **Thin:** Volume guarantee = none
  - Dynamic mapping to physical space



One or more FlexVol volumes can be created in an aggregate. To understand how space is managed, examine how space is reserved in the aggregate.

The NetApp WAFL file system writes data in 4KB blocks that are contained in the aggregate. (Each 4KB block has an *inode pointer*. The inode pointers assigned to a data file are tracked in the inode file.) When the aggregate is created, the WAFL file system reserves 10% capacity for overhead. The remainder of the aggregate is available for volume creation.

FlexVol volumes are loosely tied to their aggregates. FlexVol volumes are striped across all the drives of the aggregate, regardless of the volume size. In the example, the blue block that is labeled “vol1” represents the inode file for the volume, and the other blue blocks contain the user data.

When a volume is created, the volume guarantee setting must be configured. The volume guarantee setting is the same as the space reservations. If space is reserved for the volume, the volume is thick-provisioned. If space is not reserved during creation, the volume is thin-provisioned. FlexVol volumes are dynamically mapped to physical space. Whether the volume is thick-provisioned or thin-provisioned, blocks are not consumed until data is written to the storage system.

A FlexVol volume can be as small as 20MB or as large as the controller model supports. Also, the volume can grow or shrink, regardless of the provisioning type.

Volume Properties

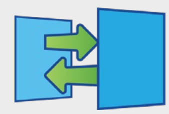
Actions that can be taken on volumes

- Create
- Edit
- Resize
- Delete
- Clone
- Move
- Rehost

Volume options

- Storage efficiency
- Storage quality of service (QoS)

Tools to protect volumes



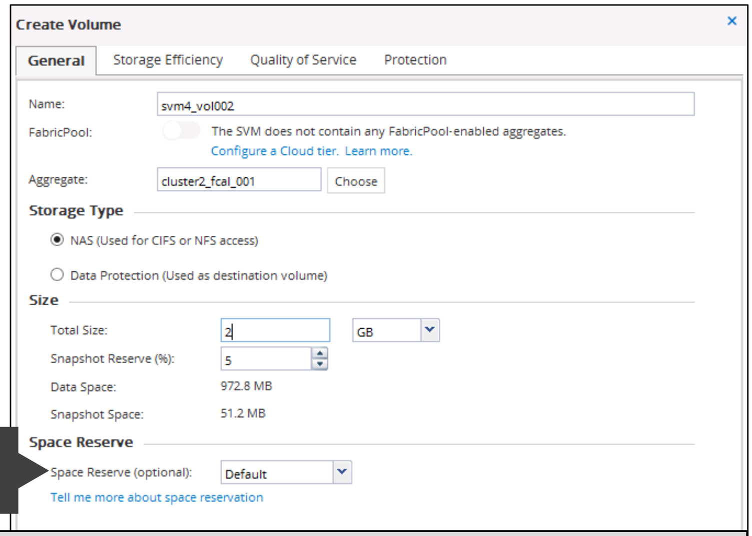
- Snapshot copies
- Mirror copies**
- Vaults**

**Covered in ONTAP DATA Protection Administration

Create a Flexible Volume in an SVM

Information to provide:

- Volume name
- Aggregate name
- Storage type
- Capacity



Discussed later

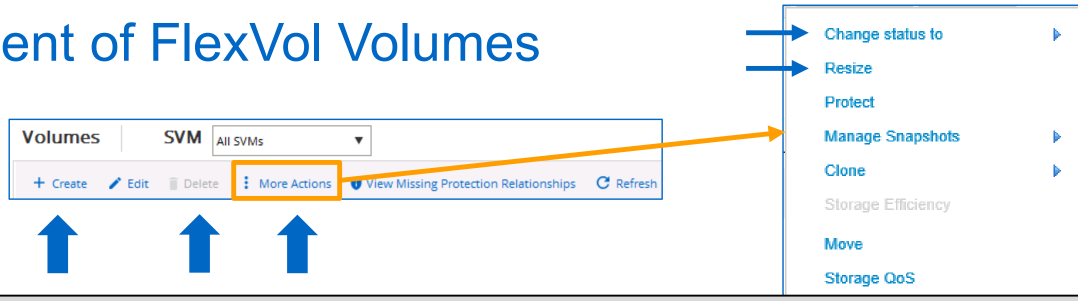
```
::> volume create -vserver svm4 -name svm4_vol_002 -aggr
cluster201_fcal_001      -junction-path /vol_002 -size 2gb
```


The storage types that are listed when you create a volume depend on the licenses that have been installed.

Examples of storage types include the following:

- NAS, when the CIFS or NFS protocol licenses are added
- SAN, when the FC or iSCSI protocol licenses are added
- Data Protection, when the SnapMirror or SnapVault licenses are added

Management of FlexVol Volumes



Create

```
::> volume create -vserver svm4 -name svm4_vol1 -aggr cluster201_fcal_001
-size 200gb
```

Resize

```
::> vol modify -vserver svm4 -name svm4_vol1 -size +10gb
```

Offline and online

```
::> vol offline -vserver svm4 -name svm4_vol1
::> vol online -vserver svm4 -name svm4_vol1
```

Destroy

```
::> vol delete -vserver svm4 -name svm4_vol1
```

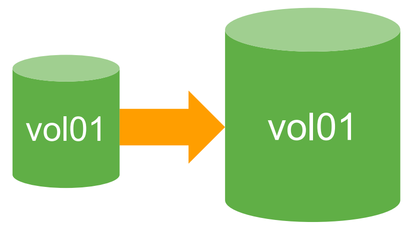
Must be offline

 11

Volume clustershell options correspond to actions on the Volumes toolbar in OnCommand System Manager.

Automatic Resizing of Volumes

- Automatic resizing of volumes enables a FlexVol volume to automatically grow or shrink the maximum space capacity of the volume.
- You can specify a mode:
  - **Off:** Volume does not grow or shrink.
  - **Grow:** Volume automatically grows when space in the volume reaches a threshold.
  - **Grow_shrink:** Volume automatically grows or shrinks in response to the amount of used space.
- In addition, you can specify the following:
  - Maximum to grow (default is 120% of volume size)
  - Minimum to shrink (default is volume size)
  - Grow and shrink thresholds



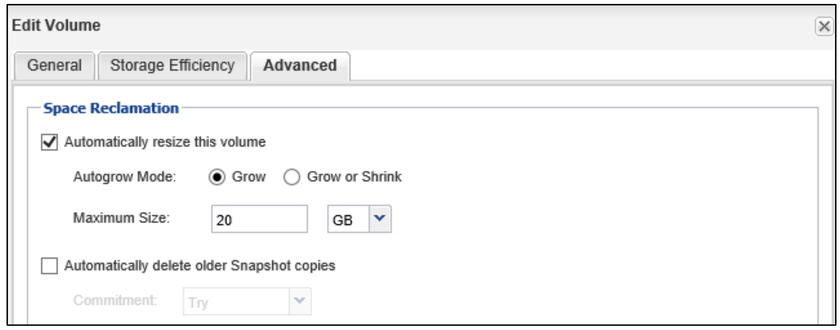
You can enable or disable automatic resizing of volumes. If you enable the capability, ONTAP software automatically increases the capacity of the volume up to a predetermined maximum size. Space must be available in the containing aggregate to support the automatic growth of the volume. Therefore, if you enable automatic resizing, you must monitor the free space in the containing aggregate and add more when needed.

The capability cannot be triggered to support Snapshot creation. If you attempt to create a Snapshot copy and the volume has insufficient space, the Snapshot creation fails, even when automatic resizing is enabled.

For more information about automatic resizing, see the *SAN Administration Guide*.

Enable Automatic Resizing

1. From Edit Volume, click the **Advanced** tab.
2. Select the **Automatically resize this volume** checkbox.
3. Select an Autogrow Mode option.
4. Specify the Maximum Size value.




```
::> volume autosize -vserver svm4 -volume svm4_vol_002 -mode grow -
maximum-size 20GB
```

ACTION: Try This Task

Using cluster1 on your exercise kit:

1. Enter the **`vol show`** command.
2. Enter the **`vol show -instance`** command.
3. Enter the **`vol show -fields comment`** command.
4. Answer the following questions:
   - What was different about the output?
   - Can you think of other reasons to use `-fields`?
   - How can you get a list of all the fields that are available for a command?

14

Review the following answers:

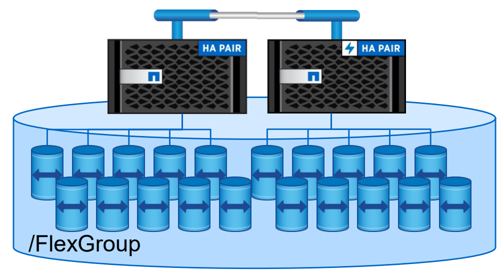
- A different amount of information is displayed about each volume.
- Use the `-fields` parameter to customize the command output for your requirements.
- Type a question mark (`?`) after the `-fields` parameter. To get a list of available fields.

What Is a FlexGroup Volume?

- A scale-out file system that is created from a group of FlexVol volumes
- A system that you and NAS clients can interact with like you interact with a FlexVol volume

FlexGroup volumes solve three problems with modern NAS in scale-out storage:

- **Performance:** FlexGroup volumes provide consistently low latency.
- **Capacity:** FlexGroup volumes provide almost unlimited capacity.
- **Management:** A FlexGroup volume looks like a FlexVol volume.



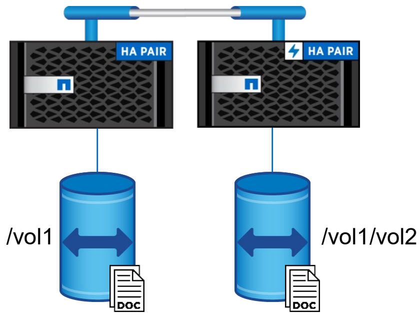
With NetApp ONTAP FlexGroup volumes, you can easily provision a massive single namespace in seconds. Like the Infinite Volume solution, a FlexGroup volume has a 20PB capacity limit. However, unlike the Infinite Volume solution, a FlexGroup volume supports as many as 400 billion files in 200 constituent volumes. The constituent volumes in a FlexGroup volume collaborate to dynamically balance load and space allocation among themselves.

A FlexGroup volume requires no maintenance or management overhead. You simply create the FlexGroup volume and share the volume with your NAS clients. ONTAP software does the rest.

For more information about FlexGroup volumes, see *NetApp FlexGroup: A Technical Overview (TR-4557)* and *Scalability and Performance Using FlexGroup Volumes Power Guide*.

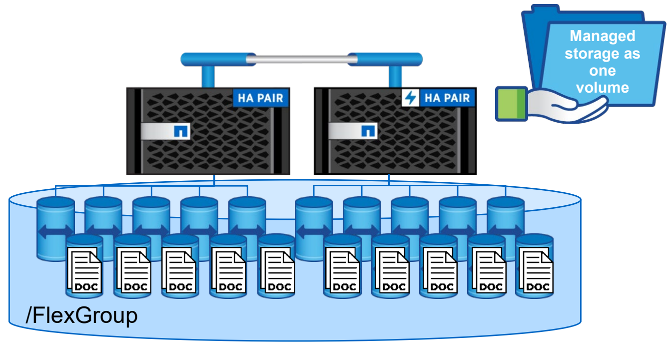
FlexVol Volumes Versus FlexGroup Volumes

How they differ at a high level



FlexVol volumes

- Owned by one node
- Span one aggregate
- Isolate reads and writes to one node and aggregate
- Are limited to storing 100TB (system-dependent)
- Are within one namespace, but with limits



FlexGroup volumes

- A shared pool of FlexVol volumes
- Component volumes span multiple aggregates
- Balance reads and writes across all nodes and aggregates
- Can store up to 20PB (200 FlexVol volumes)
- Are within one namespace, almost without limits

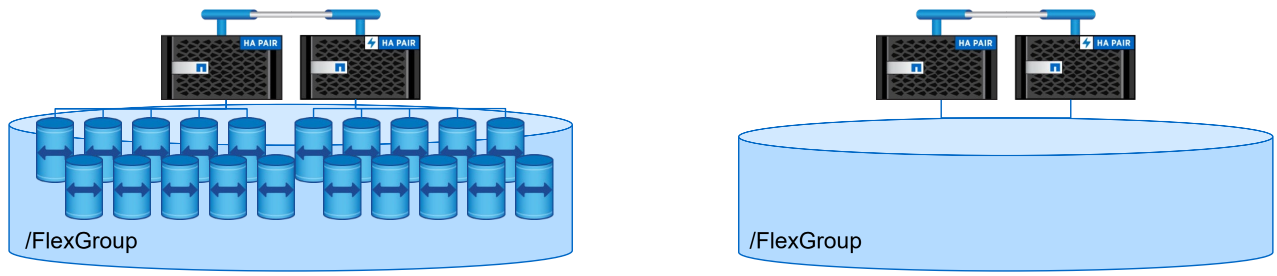
 16

Although FlexGroup volumes are positioned as a capacity feature, the volumes are also a high-performance feature. With a FlexGroup volume, you can have massive capacity, predictably low latency, and high throughput for the same storage container. A FlexGroup volume adds concurrency to workloads and presents multiple volume affinities to a single storage container, with no need for increased management.

Management of FlexGroup Volumes

You manage FlexGroup volumes like you manage FlexVol volumes.

- You create the FlexGroup volume, and ONTAP software manages the rest:
  - When you create the FlexGroup volume, you specify the size, aggregates, SVM, and file system path.
  - ONTAP software creates equally sized constituent volumes.
- If you need more space, you can add a constituent volume anywhere in the cluster.



What ONTAP Software Sees **What Clients See**

 17

At a high level, a FlexGroup volume is simply a collection of FlexVol volumes that act as one entity. NAS clients access the FlexGroup volume just as they access a FlexVol volume: from an export or a CIFS (SMB) share.

Although FlexGroup volumes are conceptually similar to FlexVol volumes, FlexGroup volumes offer several benefits that FlexVol volumes cannot match.

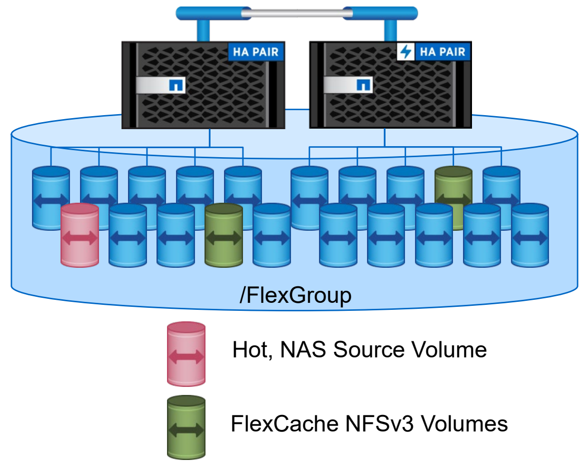
A FlexGroup volume creates files per FlexVol volume without file striping. FlexGroup volumes provide throughput gains by performing concurrent operations across multiple FlexVol volumes, aggregates, and nodes. A series of operations can occur in parallel across all hardware on which the FlexGroup volume resides. FlexGroup volumes are the perfect complement to the ONTAP scale-out architecture.

FlexCache Volumes

Accelerate hot volumes

FlexCache volumes are sparsely populated volumes, within a FlexGroup Volume, that can be cached on the same cluster or a different cluster as the origin volumes to accelerate NAS data access.

- Performance acceleration for hot NAS volumes:
  - Cache read and metadata for CPU-intensive workloads
  - Provides different mount points to avoid hot volumes
  - Cache data within the cluster (intracluster)
- FlexCache volume limitations:
  - No Snapshot copies or FlexClone support
  - No deduplication or compression
  - No volume move or volume copy
  - Supports only NFS version 3 (NFSv3) for data sharing



FlexCache volumes cache frequently accessed NAS data to reduce latency within a cluster or between clusters. For local hot volumes, FlexCache volumes provide more copies of the data to spread the I/O demands across the cluster.

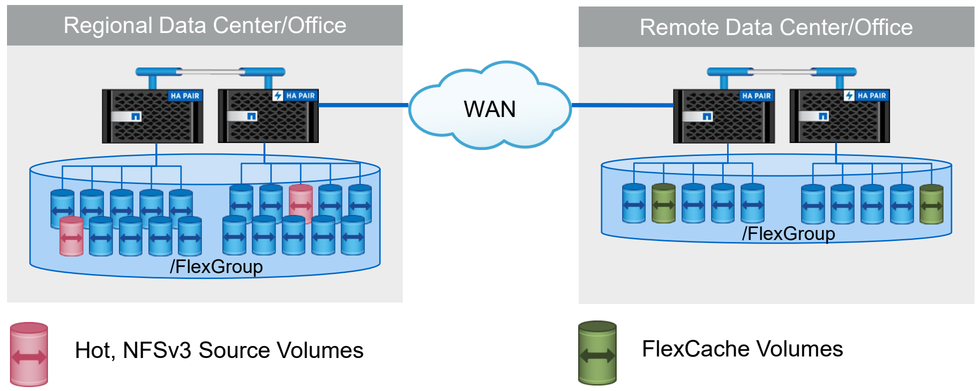
FlexCache volumes are temporary copies of some of the data in the source volume. For this reason, the volumes do not support many of the features of a typical FlexVol volume. One limitation is that although the source volume supports any NAS protocol, the FlexCache volumes share the cached data using NFS version 3 (NFSv3) only.

FlexCache Volumes

Accelerate data access to remote users

Data distribution across data centers:

- Caches across multiple data centers to reduce WAN latencies
- Brings NFSv3 data closer to compute and users
- Works between NetApp AFF, FAS, and ONTAP Select systems



? More info in Addendum

Caching frequently accessed remote data closer to the users reduces WAN traffic and latency.

In ONTAP 9.5, caching works between AFF, FAS, and ONTAP Select clusters but only for NFSv3 data.

The module addendum contains more information about FlexGroup and FlexCache volumes.

Lesson 2
Provisioning Storage Resources

Application-Aware Data Management

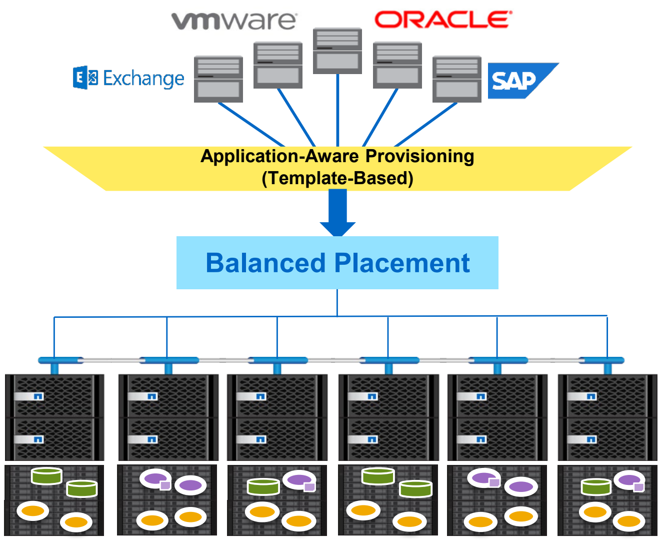
Application-aware data management enables you to describe the application that you want to deploy over ONTAP software in terms of the application rather than storage:

- Set up, manage, and monitor storage at the level of individual applications, following relevant ONTAP recommended practices for balanced placement.
- This ONTAP feature includes a set of application templates, each of which consists of a set of parameters that collectively describe the configuration of an application.
- Based on the specified parameters, ONTAP software configures storage entities such as LUNs and volumes with appropriate sizes and service levels for the application.

Application-aware data management reduces the work that is involved in planning and carving up your storage for use by widely used applications from vendors like Oracle and VMware.

Balanced Placement

Balanced LUN and volume placement based on application requirements



- Simplified provisioning
- Balanced use of cluster storage and CPU (node headroom) resources
- Balanced placement that depends on the following:
  - QoS
  - Headroom availability
- Balanced placement logic that needs the following inputs:
  - **Storage level classes:** extreme, high, or value (capacity)
  - **Protection level classes:** sync or async
  - Size of application or application components

 22

Balanced placement simplifies provisioning by eliminating questions such as the following:

- Where is the capacity to match my application I/O requirements?
- Which node or nodes have CPU headroom to take on additional work?

Balanced Placement

Storage service levels

	Application-Aligned Storage Service Levels		
Service Level	**Value**	**Performance**	**Extreme**
Workload Type	Email, web, file shares, backup	Database and virtualized applications	Latency-sensitive applications
Minimum SLA (IOPS per TB allocated)	128	2048	6144
Maximum Service-Level Objective (SLO) (QoS limit in IOPS per TB stored)	512	4096	12288
Latency (ms)	17	2	1
	Flash-Accelerated, SAN and NAS, Non-Stop Availability and Durability, Nondisruptive Movement		

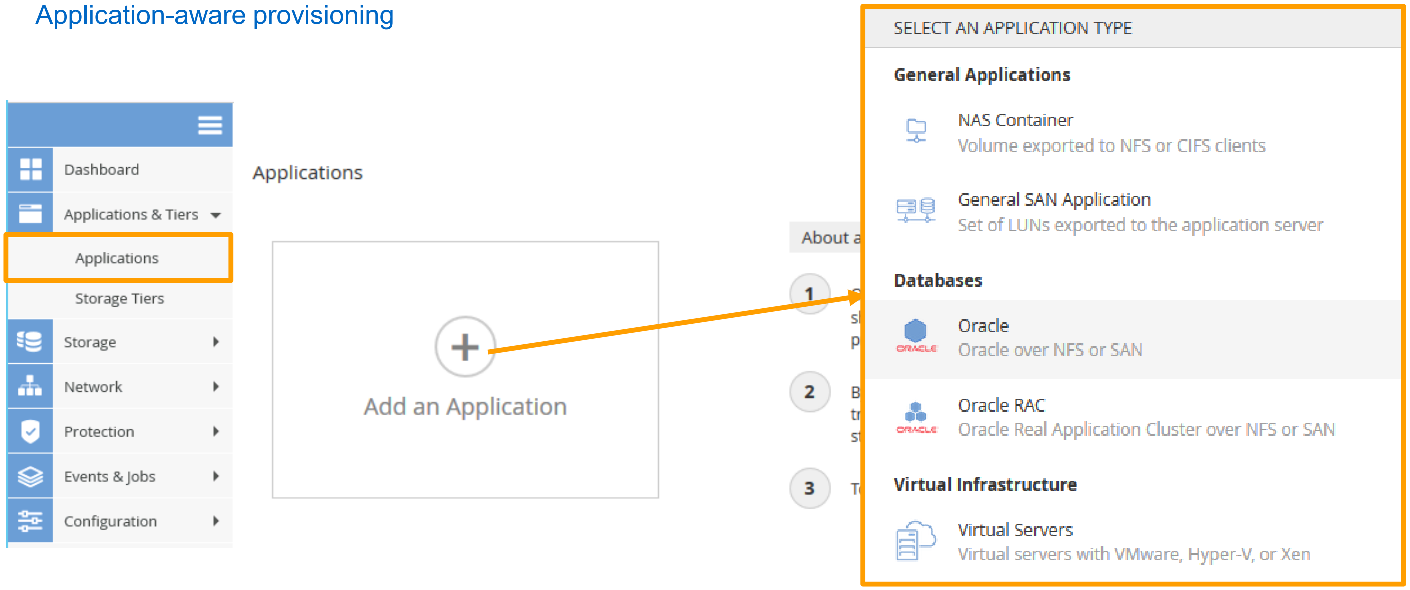
Balanced use of cluster resources

- Simplified provisioning
- Recommended placement based on size of application components, desired storage service levels, and available system resources
- Predefined storage service levels to match the media with requested performance characteristics (QoS)

Storage service levels help to ensure that limited or expensive cluster resources are dedicated to high-priority workloads. The effects are more noticeable the larger the cluster and the greater the mix of controller models and drives types in the cluster.

Balanced Placement Example

Application-aware provisioning

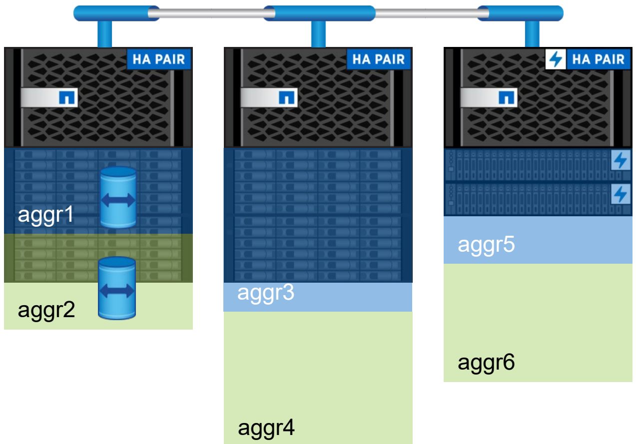


 24

Application-aware provisioning, management, and visualization in ONTAP software makes it easier to support applications following recommended practices.

Lesson 3
Moving Storage Resources

Volume Move



- Rules:
  - Move only within the SVM.
  - Move to any aggregate to which the SVM has permission.
  - Move is nondisruptive to the client.
- Use cases:
  - **Capacity:** Move a volume to an aggregate with more space.
  - **Performance:** Move to an aggregate with different performance characteristics.
  - **Servicing:** Move to newly added nodes or from nodes that are being retired.

 26

FlexVol volumes can be moved from one aggregate or node to another within the same SVM. A volume move does not disrupt client access during the move.

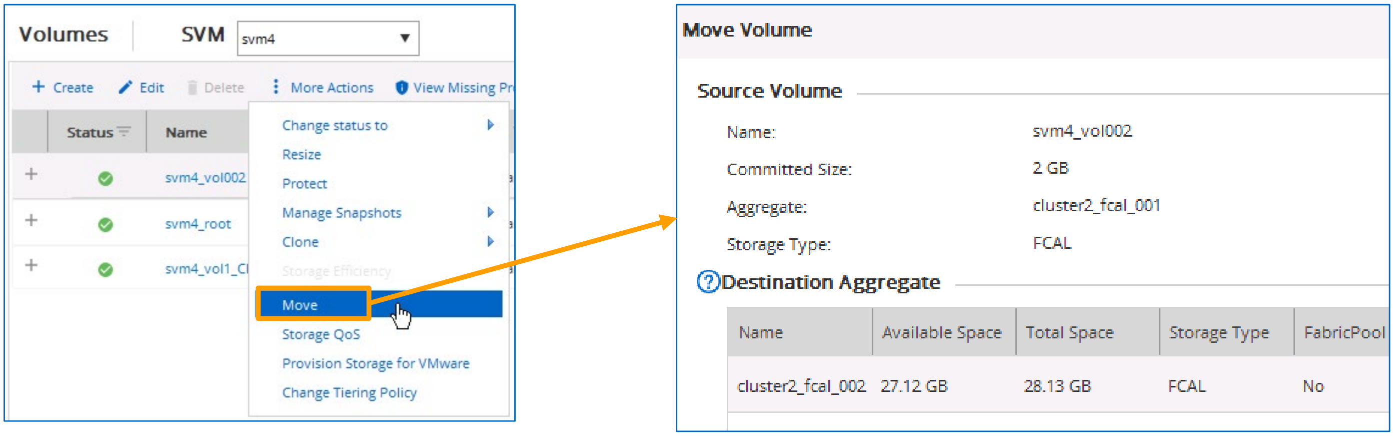
You can move volumes for capacity use, such as when more space is needed. You can move volumes to change performance characteristics, such as from a controller with HDDs to one that uses solid-state drives (SSDs). You can also move volumes during service periods.

How a Volume Move Works

1. A volume is created on the destination aggregate.
2. A Snapshot copy of the source volume is created.
3. The Snapshot copy is replicated to the destination volume.
4. When replication is complete, client access is temporarily blocked.
5. A final replication is performed to reach consistency.
6. Cutover is initiated.
7. Clients access the destination volume, and the source volume is cleaned up.

When a volume move is initiated, a Snapshot copy of the source volume is created and is used as the basis to populate the destination volume. Client systems continue to access the volume from the source destination until all data is moved. At the end of the move process, client access is temporarily blocked. Meanwhile, the system performs a final replication from the source volume to the destination volume. The system swaps the identities of the source and destination volumes and changes the destination volume to the source volume. When the move is complete, the system routes client traffic to the new source volume and resumes client access.

The `volume move` Command




```
cluster2::> vol move start -vserver svm4 -vol svm4_vol_002 -destination-
aggr cluster2_fcal_002
cluster2::> vol move trigger-cutover -vserver svm4 -vol svm4_vol_002
```


ONTAP software enables you to move a volume from one aggregate or node to another within the same SVM to use capacity, improve performance, and satisfy SLAs. The volume move is a nondisruptive operation. During the volume movement process, the original volume is intact and available for clients to access. You can move a FlexVol volume to a different aggregate, node, or both within the same SVM. The data is transferred to the destination node through the cluster interconnect.

Use the **`volume move start`** command to initiate the volume transfer. If the cutover action is defer_on_failure, and the cutover state moves to "cutover deferred," use the **`volume move trigger-cutover`** command to complete the move. To bypass any confirmation before cutover, use **`-force true`** on the **`volume move start`** command. The bypass can cause client I/O disruptions.

Autobalancing Aggregates

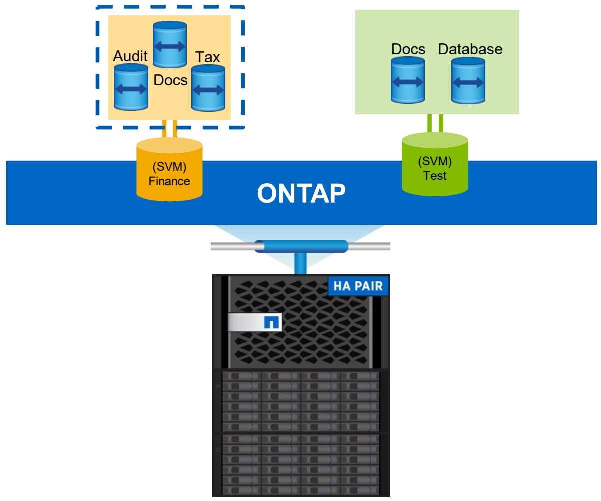
Default settings

- If you frequently move volumes to free up space, you can use the `autobalance aggregate` command to configure ONTAP software to autobalance automatically for all aggregates.
- The autobalance aggregate feature is turned off by default. See the addendum for more information.

```
::*> autobalance aggregate config show
              Is the Auto Balance Aggregate Feature Enabled: false
      Threshold When Aggregate Is Considered Unbalanced (%): 70
        Threshold When Aggregate Is Considered Balanced (%): 40
```

? More info in Addendum

Volume Rehost Within a Cluster



Destination Cluster

Steps to rehost a volume:

1. Identify the source volume and SVM.
2. Identify the destination SVM within the cluster.
3. Prevent access to the volume that is being rehosted.
4. Use the **`rehost`** command to rehost the volume to the destination SVM.
5. Configure access to the volume in the destination SVM.

The `volume rehost` command rehosts a volume from a source SVM to a destination SVM. The volume name must be unique among the other volumes on the destination SVM.

If the volume contains a LUN, you can specify that the LUN needs to be unmapped. In addition, you can specify whether you want the LUN to be automatically remapped on the destination SVM.

NOTE: Volume rehost is a disruptive operation and requires you to reconfigure access to the volume at the destination. Access to the volume must be prevented before a rehost to prevent data loss or inconsistency.

LUN Move

- The `lun move` set of commands enable you to move a LUN to a volume on another node or even the same node.
- The LUN can move only within the same SVM.
- Snapshot policies are at the volume level so do not follow to new volume. Therefore, storage efficiency features must be reapplied.
- Use the `lun move-in-volume` command to rename a LUN without moving the LUN.

To move a LUN for capacity or performance reasons, use the **`lun move`** command set rather than moving the container volume. LUNs can be moved only to another volume in the SVM. You need to set the Snapshot policies on the destination volume. Storage efficiency features, such as deduplication, compression, and compaction, are not preserved during a LUN move. The features must be reapplied after the move is completed.

If you need to rename a LUN, use the **`lun move-in-volume`** command to “move” the LUN, with a new name, to the current location.

Knowledge Check

Which of these is not a mode of the volume autoresize feature? (Choose one)

a. Off
b. Grow
c. Shrink
d. Grow_shrink

References

- ONTAP 9 Documentation Center:
  - *Logical Storage Management Guide*
  - *Volume Move Express Guide*
  - *Scalability and Performance Using FlexGroup Volumes Power Guide*
- *TR-4557: NetApp FlexGroup: A Technical Overview*
- *TR-4571-a: NetApp ONTAP FlexGroup Volumes Best Practices*
- *TR-4743: FlexCache Volumes in NetApp ONTAP*

ONTAP 9 Documentation Center:

Logical Storage Management Guide

Volume Move Express Guide

Scalability and Performance Using FlexGroup Volumes Power Guide

TR-4557: NetApp FlexGroup: A Technical Overview

TR-4571-a: NetApp ONTAP FlexGroup Volumes Best Practices

TR-4743: FlexCache Volumes in NetApp ONTAP

References

Videos

- ONTAP 9 Feature Overview: FlexGroup
  https://www.youtube.com/watch?v=Wp6jEd4VkgI
- Manage FlexGroup using OnCommand System Manager 9.4
  https://www.youtube.com/watch?v=mLpVjolI4GY

 34

ONTAP 9 Feature Overview: FlexGroup - https://www.youtube.com/watch?v=Wp6jEd4VkgI

Manage FlexGroup using OnCommand System Manager 9.4 https://www.youtube.com/watch?v=mLpVjolI4GY

Module Review

This module focused on enabling you to:

- Create and manage FlexVol volumes
- Provision application-aware resources
- Move a volume within an SVM
- Create a FlexGroup volume

ACTION: Complete an Exercise

Module 6: Managing Data Volumes

Duration: 20 minutes

Access your exercise equipment.

Use the login credentials that your instructor provided to you.

Complete the specified exercises.

- Go to the exercise for the module.
- Start with Exercise 6-1.
- Stop at the end of Exercise 6-1.

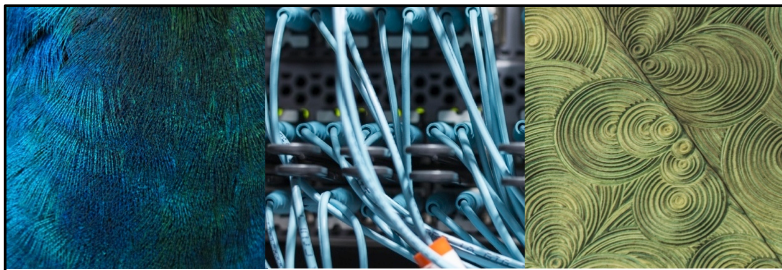
Participate in the review session.

- Share your results.
- Report issues.

Share Your Experiences

Roundtable questions for the equipment-based exercises

- Did your volume move operation disrupt the workload on the volume that you moved?



Addendum
FlexGroup and FlexCache Volumes

Pre-Deployment

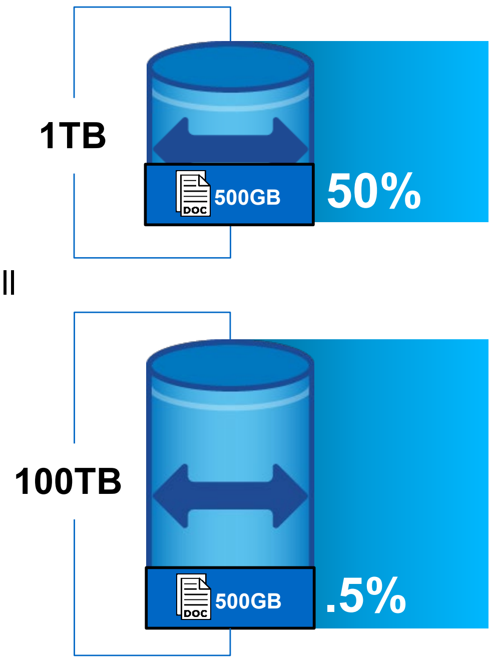
Recommended practices

- Homogenous hardware and capacity
  - Disks, nodes, and available capacity should be identical for predictable performance.
  - Relocate volumes in aggregates, using a nondisruptive volume move if necessary.
- Use a reliable network that is 10Gb or greater.
  Flow control is unnecessary across high-bandwidth networks.
- Know the average file size of the workload.
  - Avoid creating small member volumes with large file workloads.
  - Use 8 member volumes per node for low-end platforms; 16 volumes per node for higher-end platforms.
- Use two aggregates per node to maximize affinities.
  Advanced Drive Partitioning avoids concerns with wasting drive space.
- Verify that your applications can process 64-bit file IDs.
  Needed for more than 2 billion files.

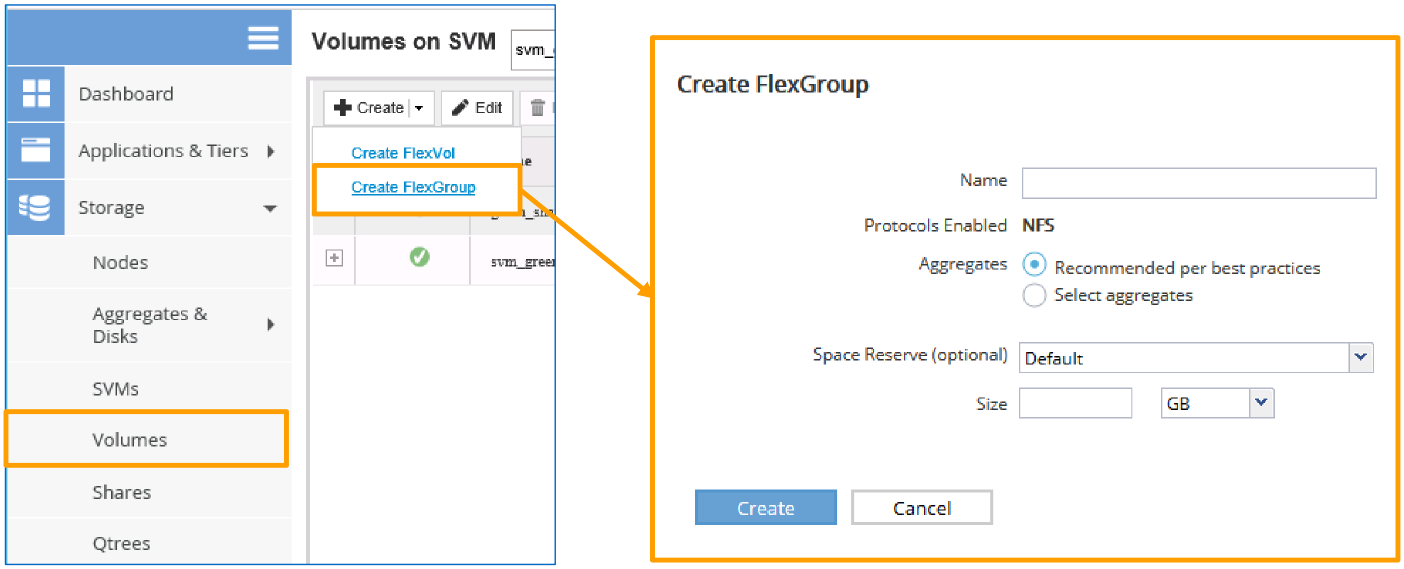
File Size Considerations

FlexGroup volumes work best with small files

- What is a “small” file? A “large” file?
  Answer: “It depends.”
- Files do not stripe across FlexGroup member volumes.
- Large files and files that grow over time can potentially fill member volumes.
- FlexGroup members that fill up prematurely can create “out of space” issues.
  “Large” files aren’t necessarily a great fit, unless you size the FlexGroup properly.



Creating FlexGroup Volumes



On the FlexGroup tab, you can manage an existing FlexGroup volume or, with two clicks, create a FlexGroup volume.

Creating a FlexGroup Volume

Navigate to the SVM that you are managing and click **Volumes** > **FlexGroups**. Then click the **Create** button. The Create FlexGroup dialog box appears. You must configure only two fields: Name and Size. The fields in the dialog box have the following features:

- **Protocols Enabled:** You cannot configure the Protocols Enabled field. Protocols are fetched from the enabled protocols for the SVM. The listing of iSCSI or FCP in the Protocols Enabled field does not mean that the FlexGroup volume supports iSCSI or FC, only that the SVM supports iSCSI or FC.
- **Aggregates:** In the Aggregates field, you define the aggregates to use with the FlexGroup volume. If you select “Recommended per best practices,” then eight constituent volumes are created per node. With AFF systems, the eight constituents are on one aggregate (there must be one aggregate per node). In other configurations, four constituents are on each aggregate (there must be two aggregates per node). If the requirements are not met, you cannot create the FlexGroup volume with the “Recommended per best practices” option and must manually select aggregates. If you want to control the layout of the FlexGroup volume by manually selecting aggregates, select the **Select aggregates** option.
- **Space Reserve:** Use the Space Reserve list to specify whether the FlexGroup volume is thin-provisioned or thick-provisioned. Thin provisioning disables the space guarantee for all constituent volumes and enables the FlexGroup volume to be overprovisioned in a cluster. Overprovisioning means that the size of the volume can be increased beyond the physical capacity of the cluster.
- **Size:** In the Size field, you specify the total size of the FlexGroup volume. The size of the constituents depends on the number of nodes and aggregates in the cluster. Constituent volumes are automatically sized equally across the FlexGroup volume. The available size depends on the total number of aggregates in the cluster. Remember that OnCommand System Manager deploys four constituent volumes per aggregate. If only two aggregates are available in the cluster, then only eight constituents are created, at a maximum of 100TB per constituent.

Creating FlexGroup Volumes

CLI

To quickly and easily deploy a FlexGroup volume, from the CLI, run the `flexgroup deploy` command:

```
::> volume flexgroup deploy ?

[-size] {<integer>[KB|MB|GB|TB|PB]}       Size of the FlexGroup
[[-vserver] <vserver name>]               Vserver Name
[ -volume <volume name> ]                 Name of the FlexGroup to Create
[ -type {RW|DP} ]                         Volume Type (default: RW)
[ -space-guarantee {none|volume} ]        Space Guarantee Style (default: volume)
[ -foreground {true|false} ]              Foreground Process (default: true)
```


NOTE: The volume `flexgroup deploy` command is supported only on clusters with 4 nodes or fewer. On clusters with more than 4 nodes, use the `volume create` command to create FlexGroups.

42

If you prefer not to use the UI or the ONTAP CLI, then you should use the new `flexgroup deploy` command.

The `flexgroup deploy` command automates the steps for deploying a FlexGroup volume, including the number and locations of constituent volumes and the space-guarantee settings.

Consider the following features when you use the `flexgroup deploy` command:

- Before you use the command, you must provision the aggregates.
- The `-vserver` parameter is also mandatory, so an SVM must also be in place.
- The Snapshot policy is set to the default. If you want to disable Snapshot copies during volume creation, use the **`volume create`** command with the **`-snapshot-policy`** option set to `none`. (After you create the volume, you can use the `volume modify` command to modify Snapshot settings.)
- The security style (UNIX, NTFS, mixed) is set to the same security style as the vsroot volume. To modify the security style for the FlexGroup volume when you create the volume, in the **`volume create`** command, use the **`-security-style`** option. (After you create the volume, you can use the `volume modify` command to modify the security style.)
- You cannot use the `flexgroup deploy` command to set the advanced-privilege NFS server option `-v3-64bit-identifiers` to `enabled`. To avoid file ID collisions, you should set the option to `enabled` for the FlexGroup volume.

Commonly Used FlexGroup Volume Options

CLI

Volume Option	What the Volume Option Does
`-aggr-list`	The option specifies the names of aggregates that contain constituent volumes. Each entry in the list creates a constituent on the specified aggregate.
`-aggr-list-multiplier`	The option specifies the number of times to iterate over the aggregates that are listed with the `-aggr-list` parameter during the creation of a FlexGroup volume.
`-max-constituent-size`	The option specifies the maximum size of a constituent volume. The default value is determined by identifying the maximum FlexVol size setting on all nodes that the FlexGroup volume uses. The smallest value that is found is selected as the default for the maximum constituent size for the FlexGroup volume.

Sometimes, `flexgroup deploy` might not be the right command to use to create a FlexGroup volume. If a cluster has more than four nodes or if you want more granular control over the design and placement of the constituent volumes, then use the **`volume create`** command. The options in the table are new options for the `volume create` command that are specific to FlexGroup creation.

Modifying a FlexGroup Volume

After you create a FlexGroup volume, to change the volume options or size, you must use the `volume modify` command.

Expanding a FlexGroup Volume

Another command that has been added to ONTAP for management of FlexGroup volumes is `volume expand`. The `volume expand` command enables you to add constituents to a FlexGroup volume. To add constituents, use the command with either the `-aggr-list` or `-aggr-list-multiplier` option. Simply specify the aggregates to which you want to add constituents and the number of constituents that you want to add to each aggregate. ONTAP does the rest.

FlexCache Software

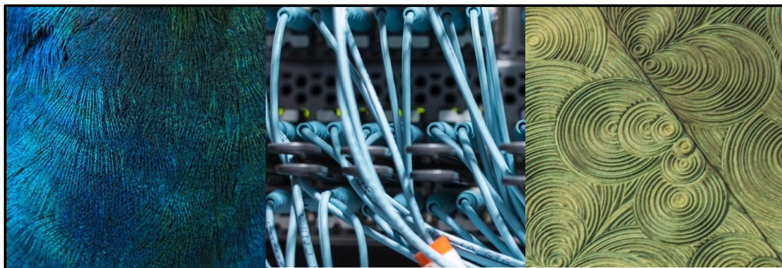
Initial support

Topology	Configuration	Platforms	Licensing
▪ Intracluster caching ▪ Within an SVM ▪ Across SVMs ▪ Cross-cluster caching	▪ Write-through caches ▪ Support for up to 10 caches per origin volume ▪ Cache volumes are FlexGroup volumes by default ▪ Protocol: NFSv3	▪ NetApp FAS ▪ NetApp AFF ▪ ONTAP Select	▪ Capacity-based licensing ▪ Only cache-volume capacity is charged ▪ Aggregated at a cluster level

Managing a FlexGroup Volume

Recommended practices

- To increase capacity, grow existing member volumes before adding new members.
  FlexGroup volumes currently do not support shrinking or renaming of volumes.
- Monitor free space and inode counts of member volumes.
  80% threshold? Take action.
- Use nondisruptive volume move to relocate member volumes to newly added nodes.
  Then, expand the FlexGroup to add more members.
- Add new members in multiples; adding single members can create hotspots.
- Consider disabling change or notify on CIFS shares if unneeded.



Addendum
Autobalance Aggregate

Autobalance Aggregate Syntax

Enable autobalancing and modify the thresholds with the following commands:

Enable the autobalance feature for the cluster:

```
::> autobalance aggregate config modify -is-enabled true
```

Modify the threshold when an aggregate is considered unbalanced:

```
::> autobalance aggregate config modify -aggregate-unbalanced-threshold-
percent <integer>
```

Modify the threshold when an aggregate is considered balanced:

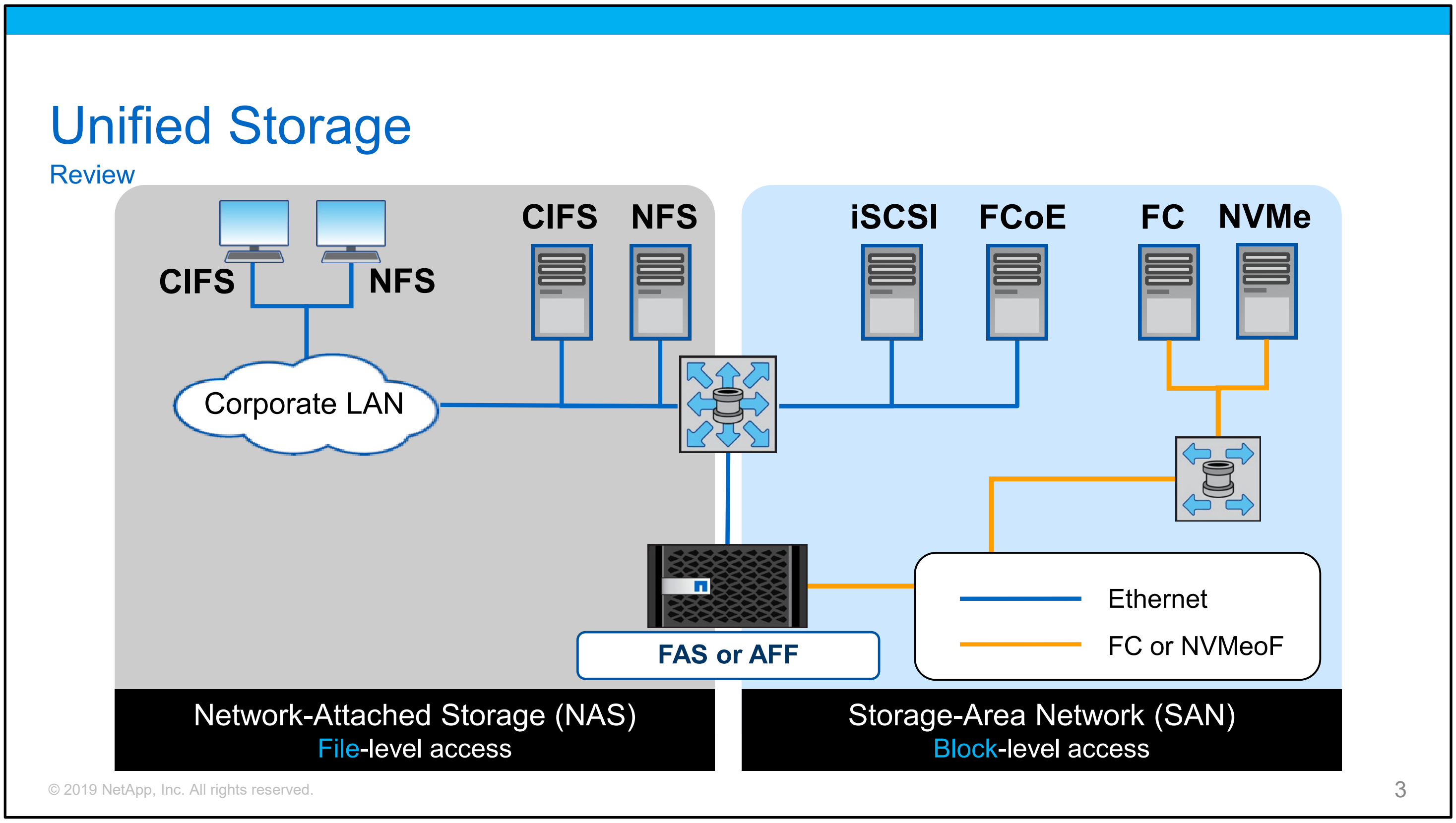
```
autobalance aggregate config modify -aggregate-available-threshold-percent
```

Module 7
Data Access

About This Module

This module focuses on enabling you to do the following:

- Use NAS protocols to access data
- Use SAN protocols to access data



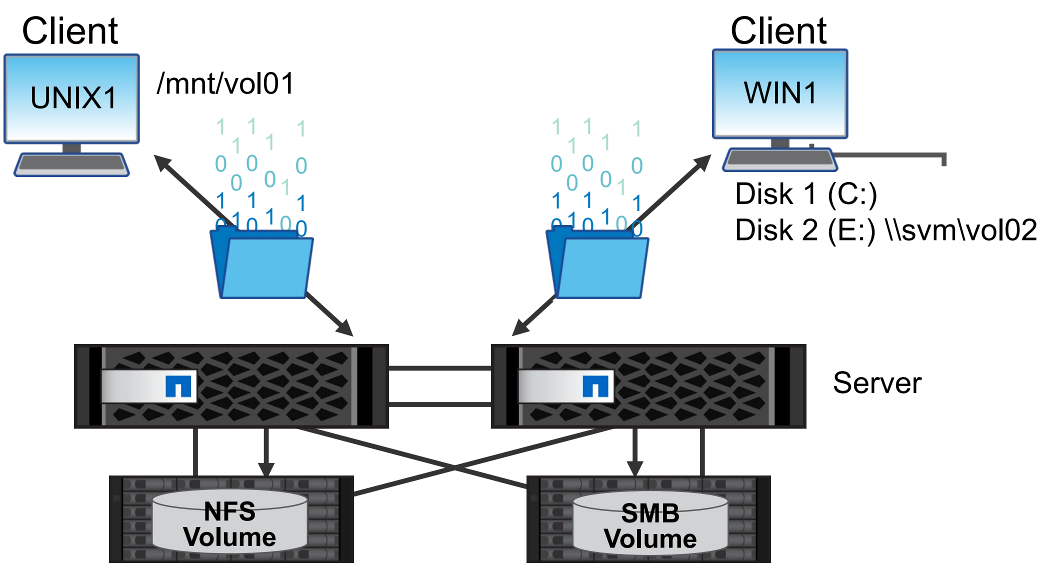
NAS is a file-based storage system that uses NFS and SMB protocols to make data available over the network. CIFS is a dialect of SMB.

A SAN is a block-based storage system that uses FC, FCoE, and iSCSI protocols to make data available over the network.

A storage system that can manage both NAS and SAN data is referred to as Unified Storage.

Lesson 1
Use NAS Protocols to Access Data

The NAS File System



 5

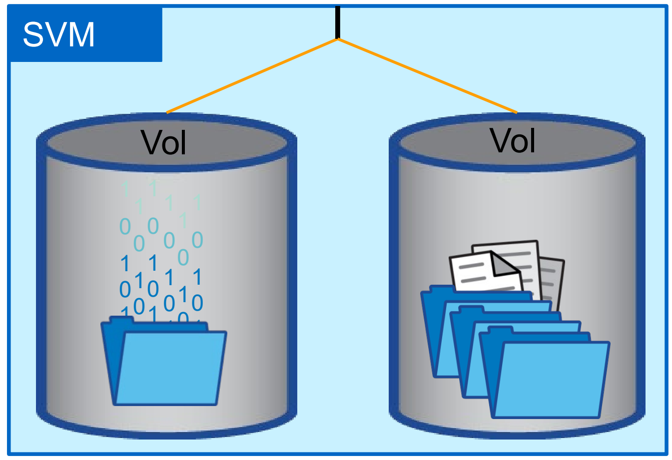
NAS is a distributed file system that enables users to access resources, such as volumes, on a remote storage system as if the resources were on a local computer system.

NAS provides services through a client-server relationship. Storage systems that make file systems and other resources available for remote access are called *servers*. The server is set up with a network address and provides file-based data storage to other computers, called *clients*, that use the server resources.

NetApp ONTAP software supports the NFS and SMB protocols.

Storage System Resources

- FlexVol Volume
  - Data containers to manage data in a storage virtual machine (SVM)
  - Exportable by mounting to namespace junction
- Qtree
  - Volume partition created on storage system
  - Exportable by mounting to namespace junction
- Directory
  - Volume partition created on the NAS client
  - Not exportable



 6

With the NAS protocols, you need to create file systems and other resources that are available to clients through either NFS or SMB.

Volumes are the highest level of logical storage object. FlexVol volumes are data containers that enable you to partition and manage your data. In a NAS environment, volumes contain file systems. The first resource to create is the volume.

In ONTAP software, the volume is associated with a storage virtual machine (SVM). The SVM is a virtual management entity, within which you create a namespace. Volumes are joined to the namespace through junctions. The junctions are exported.

Qtrees enable you to partition FlexVol volumes into smaller segments that you can manage individually. ONTAP software creates a default qtree, called qtree0, for each volume. If you do not create and put data in another qtree, all the data resides in qtree0. Qtrees enable you to partition data without incurring the overhead that is associated with creating another FlexVol volume. You might create qtrees to organize data or to manage one or more of the following factors: quotas, security style, or opportunistic lock (oplock) settings.

You can also create a directory or a file on the client in a FlexVol volume, to use as a resource to export or share. A qtree is a partition that is created on the storage system. A directory is a partition that is created on the client within a FlexVol volume.

Namespace and Junction Paths

Volumes and junctions

- Create a projects volume under the SVM root:

```
::> volume create -vserver svm4
-aggregate sas_data_23 -volume projects
-size 5GB -state online -type RW
-policy Default -security-style unix
-junction-path /projects -junction-active true
```

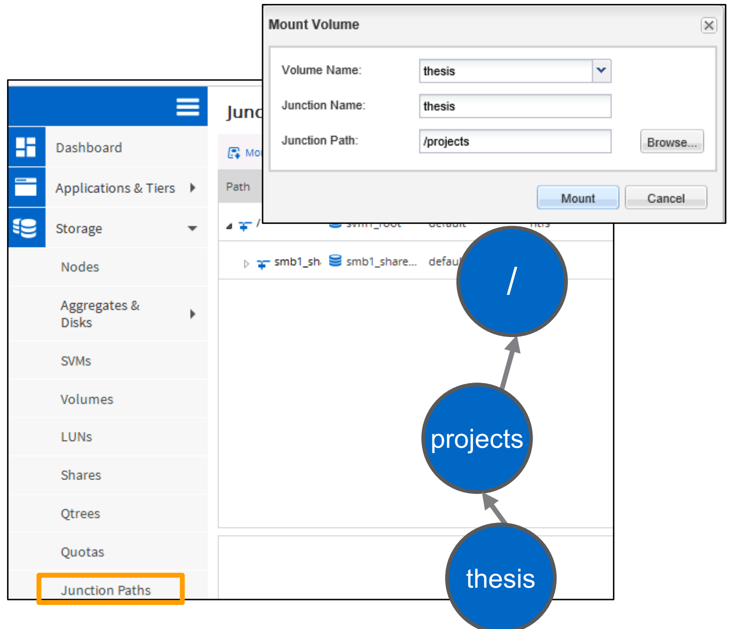
- OR -

- Create a second named project volume:

```
::> volume create -vserver svm4
-aggregate sas_data_18 -volume thesis
-size 10GB -state online -type RW
-policy Default -security-style unix
```

- Mount the second volume under /projects:

```
::> volume mount -vserver svm4 -volume thesis
-junction-path /projects/thesis
-active true -policy-override false
```



 7

Volume junctions are a way to join individual volumes into a single logical namespace. Volume junctions are transparent to CIFS and NFS clients. When NAS clients access data by traversing a junction, the junction appears to be an ordinary directory. A junction is formed when a volume is mounted to a mount point below the root and is used to create a file-system tree. The top of a file-system tree is always the root volume, which is represented by a slash mark (/). A junction points from a directory in one volume to the root directory of another volume.

A volume must be mounted at a junction point in the namespace to enable NAS client access to contained data. Specifying a junction point is optional when a volume is created. However, data in the volume cannot be exported and a share cannot be created until the volume is mounted to a junction point in the namespace. A volume that is not mounted during volume creation can be mounted after creation. New volumes can be added to the namespace at any time by mounting the volumes to a junction point.

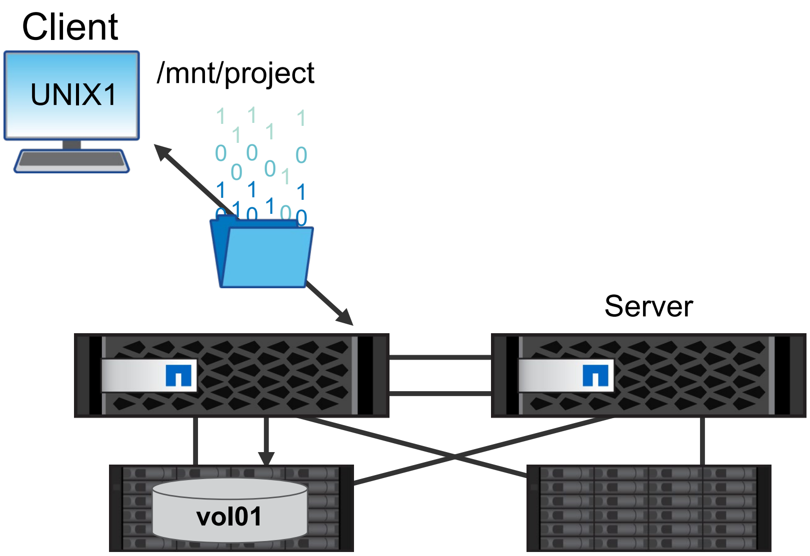
The following is an abbreviated list of parameters that are used to mount a volume:

- **Junction path of the mounting volume:** `-junction-path <junction path>`
  The junction path name is case-insensitive and must be unique within an SVM namespace.
- **Active junction path:** `[-active {true|false}]`
  The optional parameter specifies whether the mounted volume is accessible. The default setting is `false`. If the mounted path is inaccessible, the path does not appear in the SVM namespace.
- **Override the export policy:** `[-policy-override {true|false}]`
  The optional parameter specifies whether the parent volume export policy overrides the mounted volume export policy. The default setting is `false`.

ACTION: Topics for Discussion

- How do NFS and SMB clients see junctions in a namespace?

NFS



- vol01 is **exported** to UNIX1 with read/write permission.
- UNIX1 **mounts** vol01 to /mnt/project with read/write permission.

NFS is a distributed file system that enables users to access resources, such as volumes, on remote storage systems as if the resources were on a local computer system.

NFS provides services through a client-server relationship.

- Storage systems that enable the file systems and other resources to be available for remote access are called *servers*.
- The computers that use server resources are called *clients*.
- The procedure of making file systems available is called *exporting*.
- The act of a client accessing an exported file system is called *mounting*.

When a client mounts a file system that a server exports, users on the client computer can view and interact with the mounted file systems on the server, within the limits of the granted permissions.

NFSv3 Implementation Steps

1. Verify or add the NFS protocol license.
2. Enable NFS functionality on the SVM.
3. Create or identify the necessary resources.
4. Export the available resources.
5. Configure NFS authentication.
6. Authorize the user.
7. Mount the exported resources.

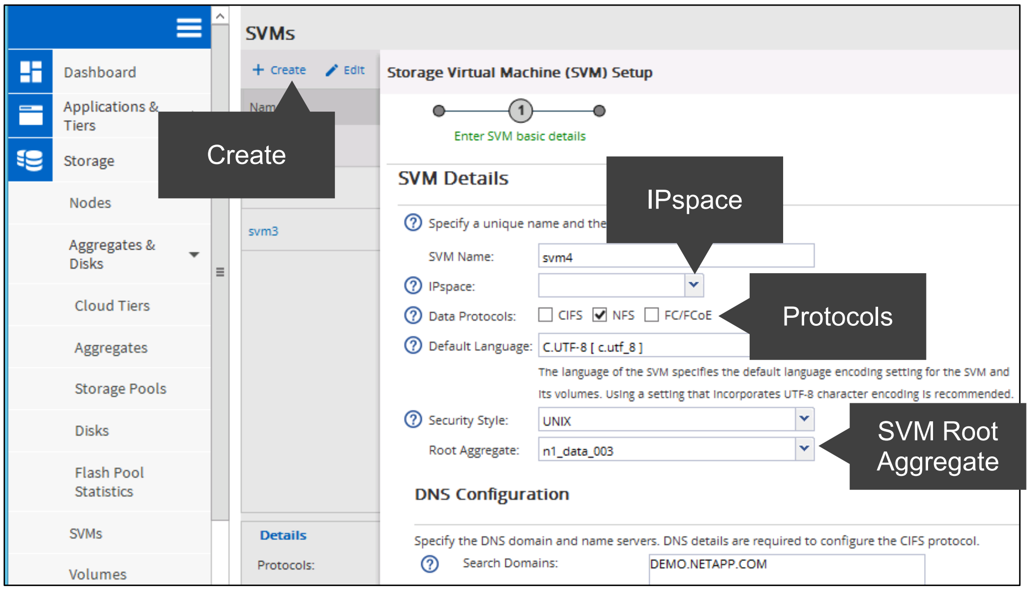
 10

The figure shows the basic process for implementing the NFS protocol between a UNIX client and an ONTAP storage system. The process consists of several steps:

- Enable NFS functionality, license NFS, and then enable the feature on the SVM.
- You need resources to export, so create volumes, qtrees, and data LIFs.
- Determine which clients have which type of access to the resources. You need a way to authenticate client access and authorize users with appropriate permissions, including read-only or read/write.
- After the client has been granted access to the exported resource, the client mounts the resource and grants access to the users.

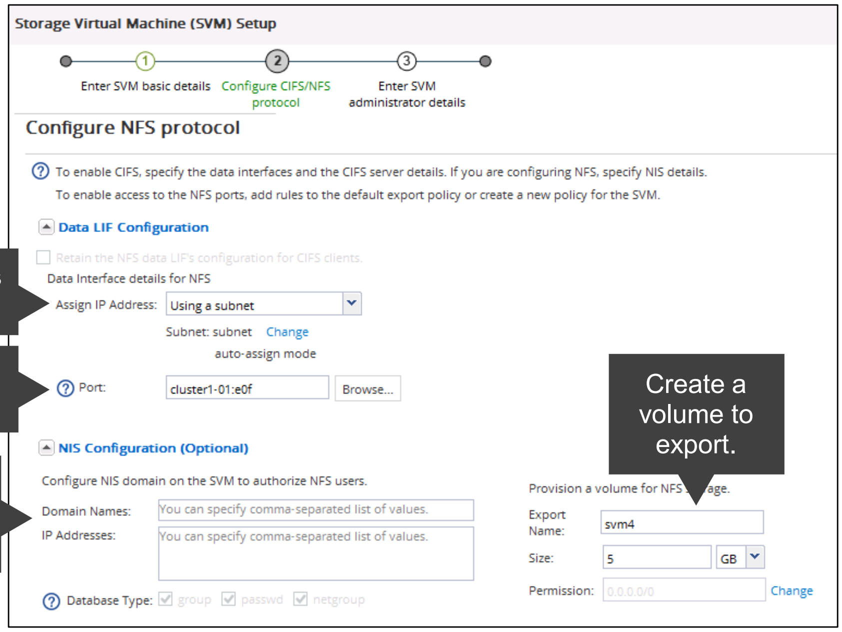
SVM Create Wizard: NFS

SVM basic details



SVM Create Wizard: NFS

Configure the NFS protocol



Select an IP address from the subnet?

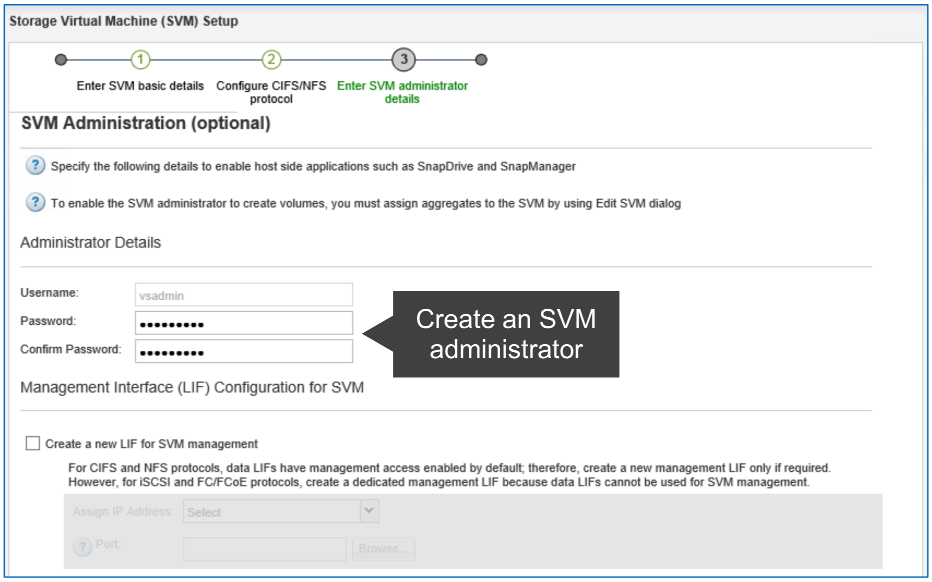
Network Port

(Optional) Network Information Service (NIS) information

Create a volume to export.

SVM Create Wizard: NFS

SVM administrator details



Mounts

Use the UNIX `mount` command on the client to mount an exported NFS resource from the storage system.

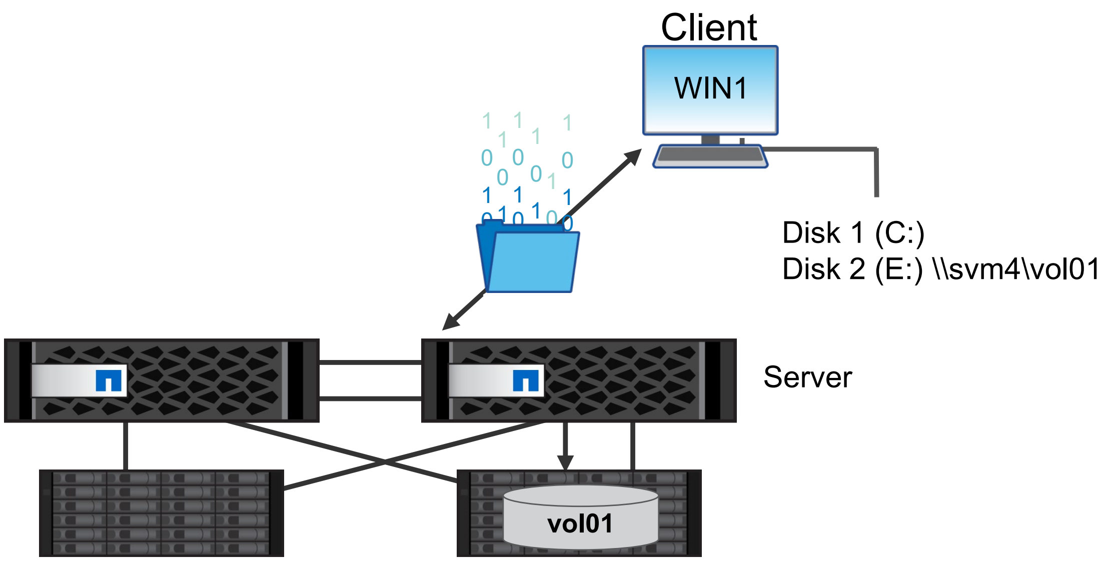
```
unix1# mkdir /mnt/project1

unix1# mount <SVM LIF IP>:/project/pro1 /mnt/project1
```


NOTE: The junction path is /project/pro1.

To enable an NFS client, mount a remote file system after NFS starts. Usually, only a privileged user can mount file systems with NFS. However, if the `user` option is set in /etc/fstab, you can enable users to mount and unmount selected file systems by using the `mount` and `unmount` commands. The setting can reduce traffic by having file systems mounted only when they are needed. To enable user mounting, create an entry in /etc/fstab for each file system to be mounted.

SMB



SMB is an application-layer network file-sharing protocol that the Microsoft Windows OS uses. SMB enables users or applications to access, read, and write to files on remote computers like they would on a local computer. For the purposes of this course, the terms SMB and CIFS are used interchangeably (although the definitions of the two terms are not strictly the same).

A user or application can send network requests to read and write to files on remote computers. Messages travel from the network interface card (NIC) of the user's computer, through the Ethernet switch, to the NIC of the remote computer.

SMB provides access to files and directories that are stored on the remote computer, through sharing resources. The rules of network protocols such as IPv4 and IPv6 control the network read and write process, which is also called network I/O.

SMB Implementation Steps

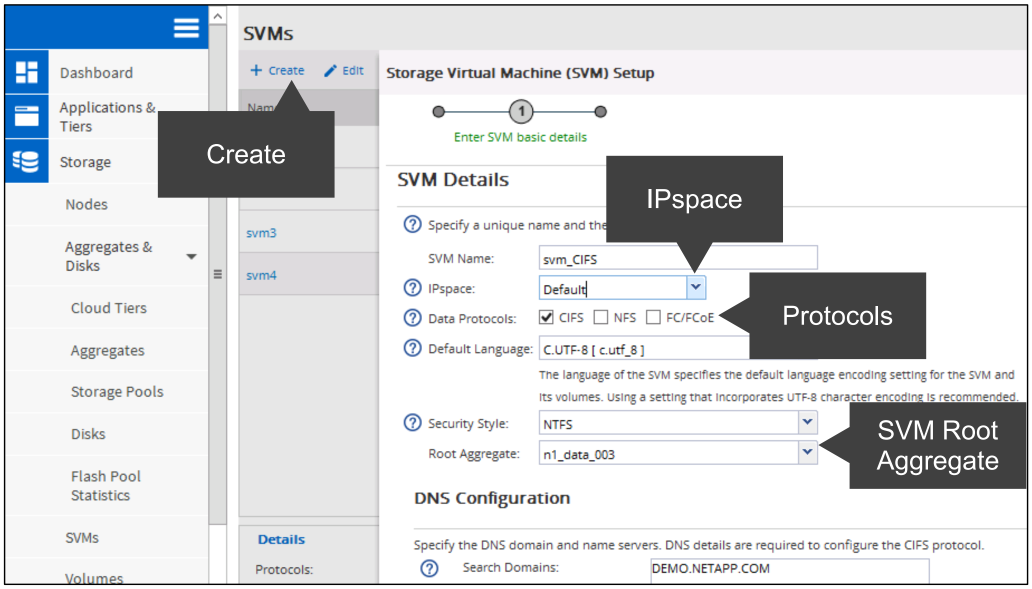
1. Verify or add the CIFS protocol license.
2. Enable SMB functionality on the SVM.
3. Create or identify the necessary resources.
4. Share the available resources.
5. Configure SMB authentication.
6. Authorize the user.
7. Map the shared resources.

The figure shows the basic process for implementing the SMB protocol between a Windows client and an ONTAP storage system. The process consists of several steps:

- Enable the SMB functionality, license CIFS, and then enable the feature on the SVM.
- Create volumes, qtrees, and data LIFs.
- Determine which clients have which type of access to the resources. You need a way to authenticate client access and authorize users with appropriate permissions, including read-only or read/write.
- After the client has been granted access to the shared resource, the client maps the resource and grants access to the users.

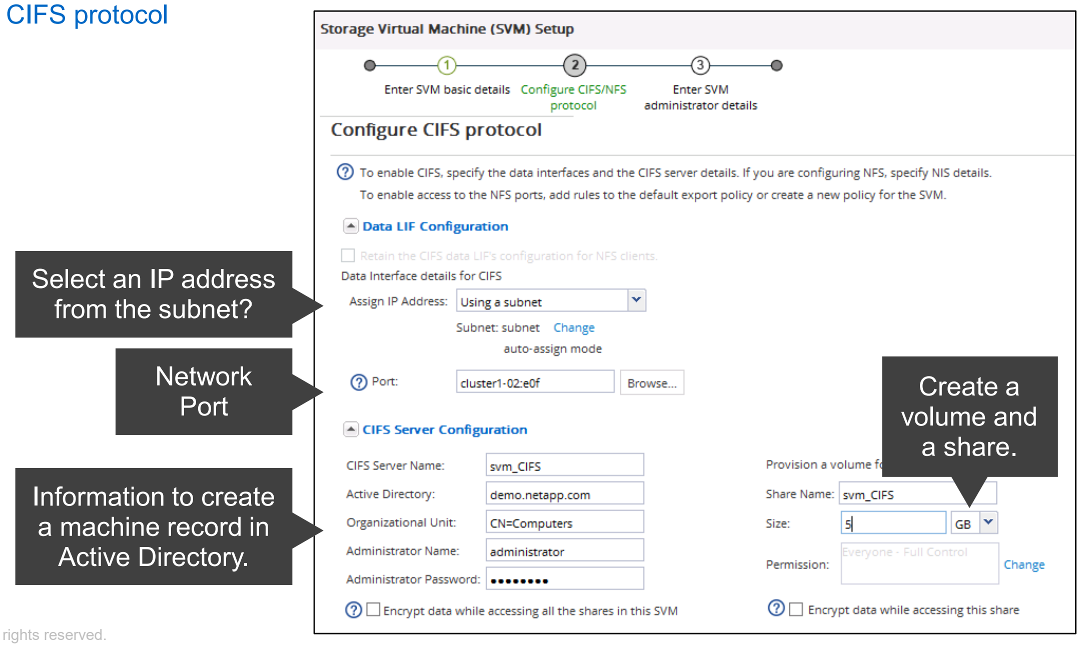
SVM Create Wizard: CIFS

SVM basic details



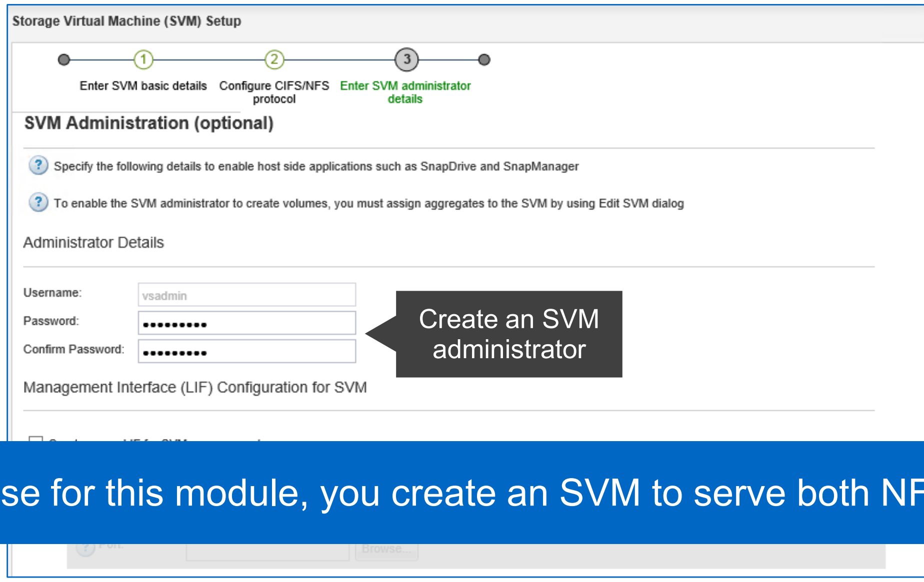
SVM Create Wizard: CIFS

Configure the CIFS protocol



SVM Create Wizard: CIFS

SVM administrator details



In an exercise for this module, you create an SVM to serve both NFS and SMB.

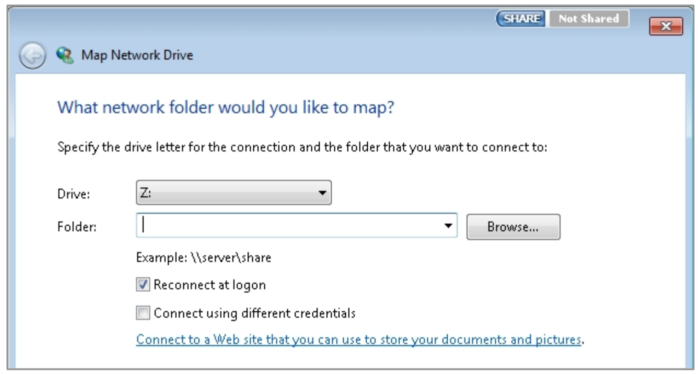
ACTION: Topics for Discussion

- You assign exports to volumes and qtrees. Which resources can you share through SMB?

SMB shares are associated with paths within the namespace. Because junctions, qtrees, and directories construct the namespace, shares can be associated with any resources.

Mapping a Share to a Client

- CLI:
  - C:\> **net view \\svm4**
  - C:\> **net use e: \\svm4\DOCS /user:marketing\jdoe**
- UI:
  - Use the Run dialog box.
  - Map a drive.



21

The net view command displays a list of computers with shared resources that are available on the specified computer.

To use the net view command, use the following steps:

1. Click the **Start** button, point to **Programs**, and then click the **MS-DOS** prompt.
2. At the command prompt, type **net view \\<*computer_name*>**, where <*computer_name*> is the name of a computer with resources that you want to view.

You can connect or disconnect a computer from a shared resource, or you can display information about computer connections. The command also controls persistent net connections. Used without parameters, the net use command retrieves a list of network connections.

You can also use Windows to map a share to a client.

Additional NAS Learning

Where can I learn about advanced topics like protocol versions and features, export policies and rules, shares, authentication, and permissions, using multiple protocols, and managing scalable NAS container?

- ONTAP NAS Fundamentals (online course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022332
- ONTAP NFS Administration (virtual/instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000015071
- ONTAP SMB Administration (virtual/instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000015070

 22

ONTAP NAS Fundamentals (online course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022332

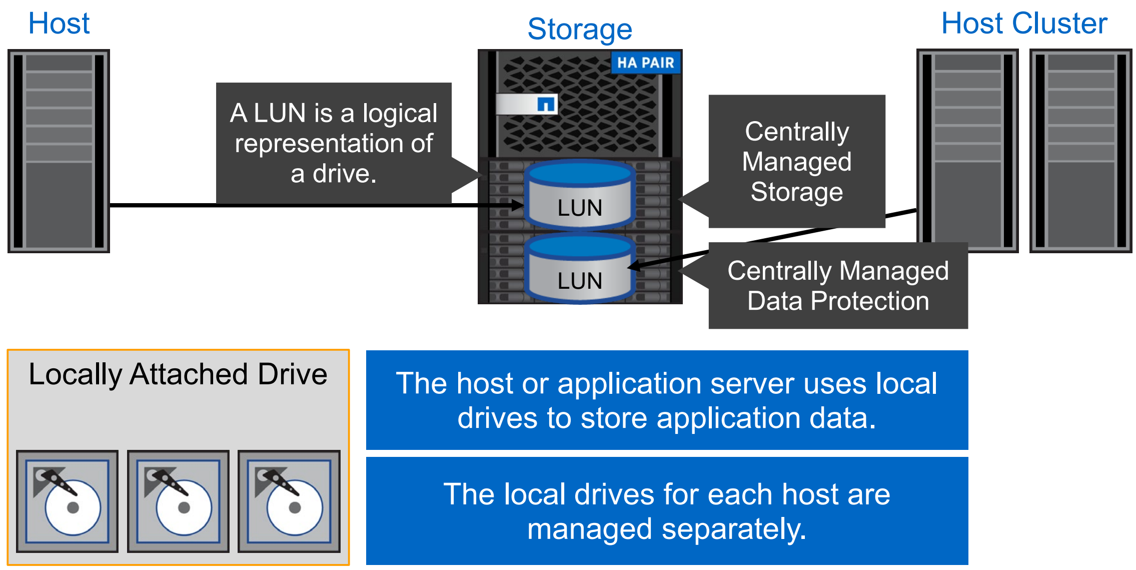
ONTAP NFS Administration (virtual/instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000015071

ONTAP SMB Administration (virtual/instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000015070

Note: Fundamentals and Administration courses are updated at least once a year. The URLs may change but the names rarely do. Use the search engine in the Learning Center to find the most recent version of the courses and offerings.

Lesson 2
Use SAN Protocols to Access Data

SAN



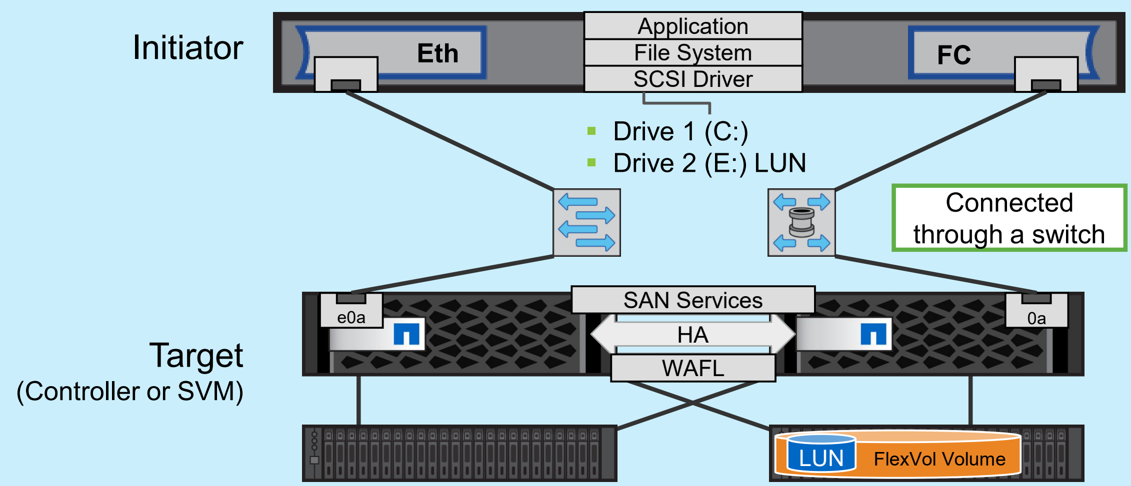
HA Pair = High-Availability Pair

In an application server environment, locally attached drives, also called direct-attached storage (DAS), are separately managed resources. In an environment with more than one application server, each server storage resource also needs to be managed separately.

A SAN provides access to a LUN, which represents a SCSI-attached drive. The host operating system partitions, formats, writes to, and reads from the LUN as if the LUN were any other locally attached drive. The advantages of using SAN storage include support for clustered hosts, where shared drives are required, and centrally managed resources. In the example, if the administrator did not use a SAN, the administrator would need to manage separate resources for each application server and host cluster. As well as enabling centrally managed resources, SAN uses ONTAP Snapshot copy technology to enable centrally managed data protection.

Connecting Initiator to Target

How can you connect an initiator to a target?



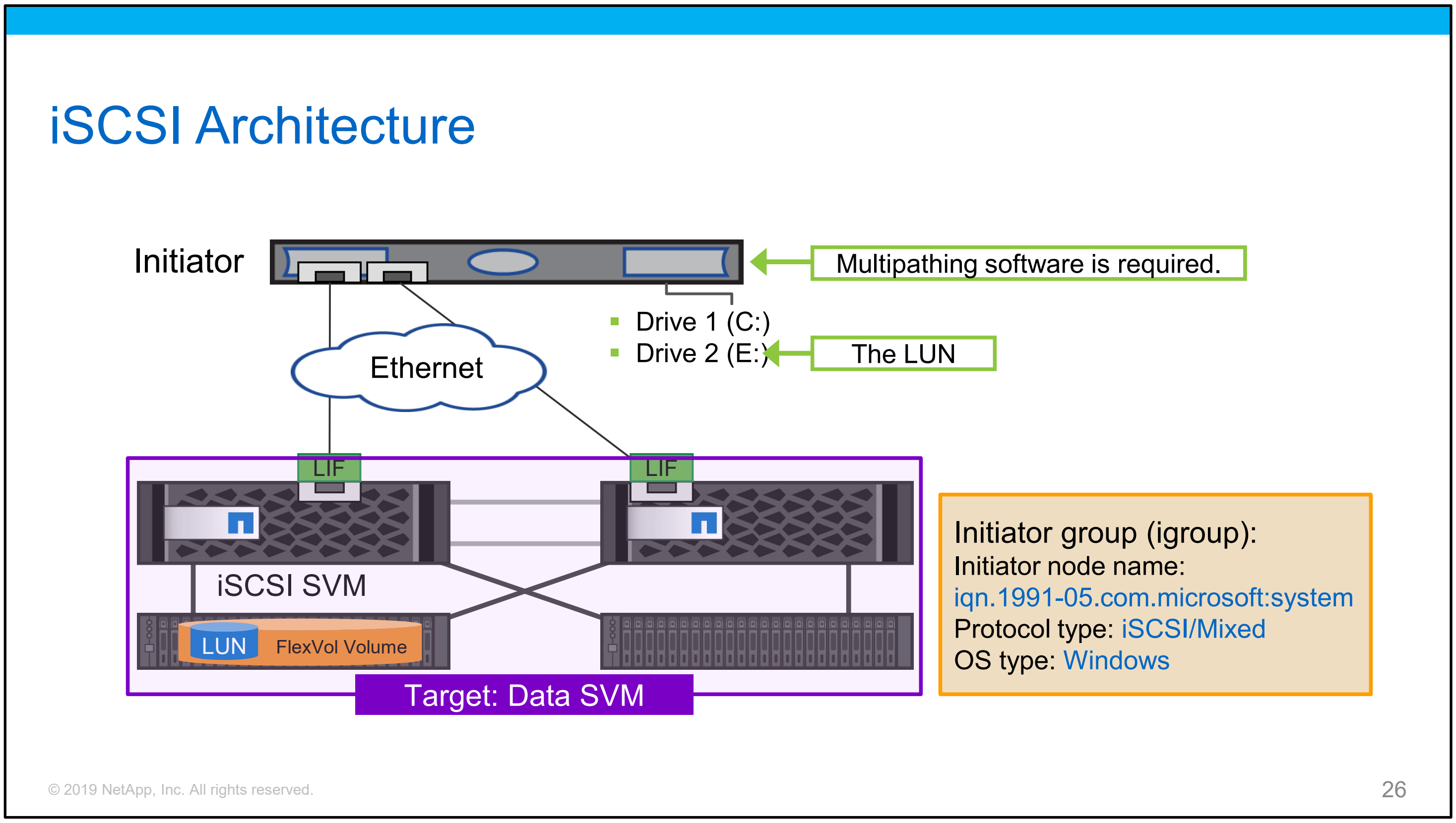
ONTAP supports the iSCSI, FC, FCoE, and NVMe over Fibre Channel (NVMe/FC) protocols. This course uses only the iSCSI protocol.

Data is communicated over ports and LIFs.

- In an Ethernet SAN, the data is communicated by using Ethernet ports.
- In an FC SAN and NVMe/FC SAN, the data is communicated over FC ports.
- For FCoE, the initiator has a converged network adapter (CNA), and the target has a unified target adapter (UTA).
- SAN data LIFs do not migrate or fail over the way that NAS does. However, the LIFs can be moved to another node or port in the SVM.

The following are NetApp recommended practices:

- Use at least one LIF per node, per SVM, per network.
- Use redundant connections to connect the initiator to the target.
- Use redundantly configured switched networks to ensure resiliency if a cable, port, or switch fails.



Initiator groups (igroups) are tables of FC protocol host worldwide port names (WWPNs) or iSCSI host node names. You can define igroups and map the igroups to LUNs to control which initiators have access to LUNs. In the example, the initiator uses the iSCSI protocol to communicate with the target.

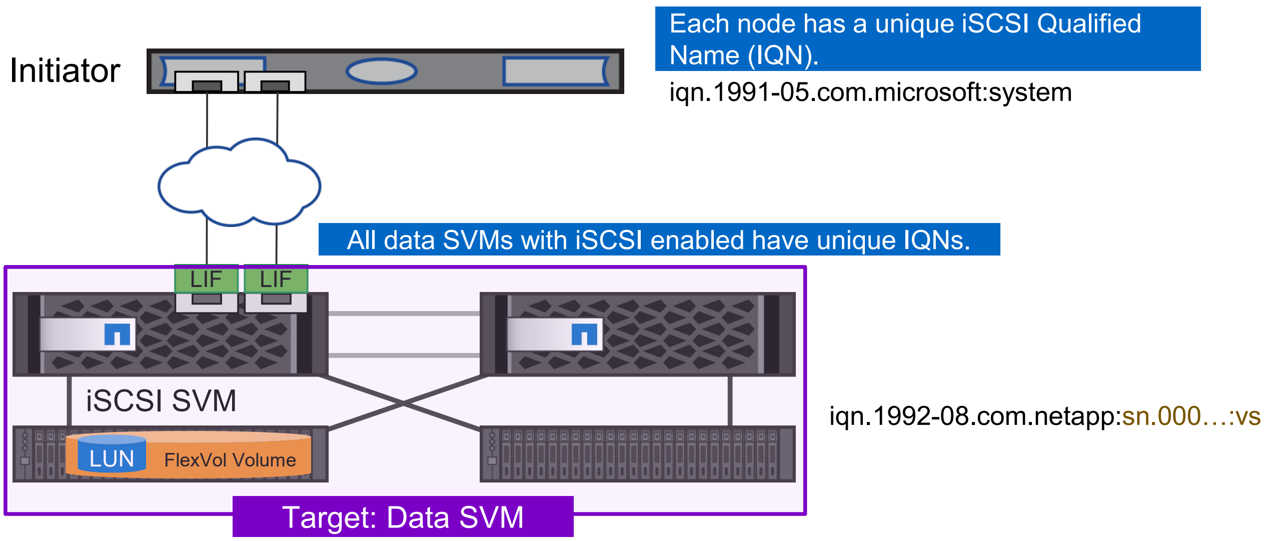
Typically, you want all the host initiator ports or software initiators to have access to a LUN. The example shows a single host. The iSCSI Software Initiator iSCSI Qualified Name (IQN) is used to identify the host.

An igroup can have multiple initiators, and multiple igroups can have the same initiator. However, you cannot map a LUN to multiple igroups that have the same initiator. An initiator cannot be a member of igroups of differing OS types. In the example, the initiator runs Windows.

When multiple paths are created between the storage controllers and the host, the LUN is seen once through each path. When a multipath driver is added to the host, the multipath driver can present the LUN as a single instance.

The figure illustrates two paths. The multipath driver uses asymmetric logical unit access (ALUA) to identify the path to the node where the LUN is located as the active *direct data path*. The direct data path is sometimes called the *optimized path*. The active path to the node where the LUN is not located is called the *indirect data path*. The indirect data path is sometimes called the *nonoptimized path*. Because indirect data paths must transfer I/O over the cluster interconnect, which might increase latency, ALUA uses only direct data paths, unless none is available. ALUA never uses both direct and indirect data paths to a LUN.

iSCSI Node Names



Each SVM is a separate target. Each SVM is assigned a unique node name:

- iSCSI uses an IQN.
- FC and FCoE use a worldwide node name (WWNN).

iSCSI Implementation Steps

1. Verify or add the iSCSI protocol license.
2. Enable iSCSI functionality on the SVM.
3. Create or identify the necessary resources.
4. Map the LUN to the appropriate igroup.
5. Locate the LUN on the host computer and prepare the drive.

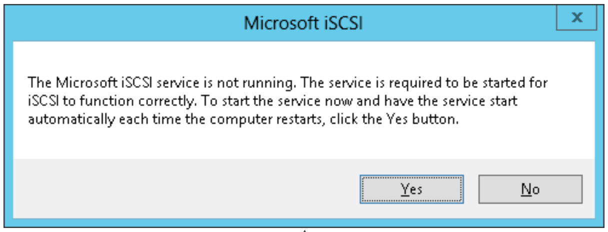
 28

The figure shows the basic process for implementing the iSCSI protocol between an initiator and an ONTAP storage system. The process consists of several steps:

- Enable iSCSI functionality, license iSCSI, and then enable the feature on the SVM. You must also identify the software initiator node name.
- Create a volume, LUN, igroup, and data LIFs.
- Determine which hosts have access to the resources, and map the hosts to the LUN.
- The LUN is discovered on the host and prepared.

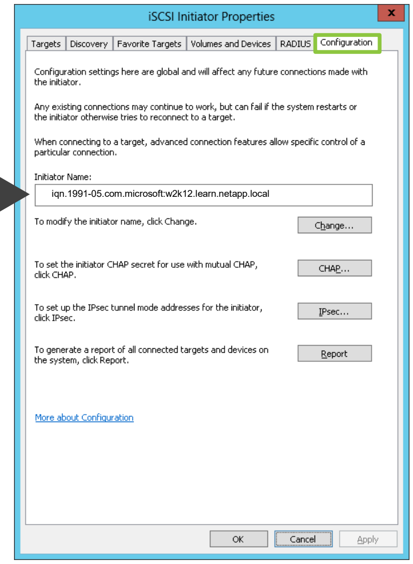
Windows iSCSI Implementation

Identify the iSCSI node name



The prompt might appear the first time that you start the iSCSI initiator.

iSCSI Initiator Name

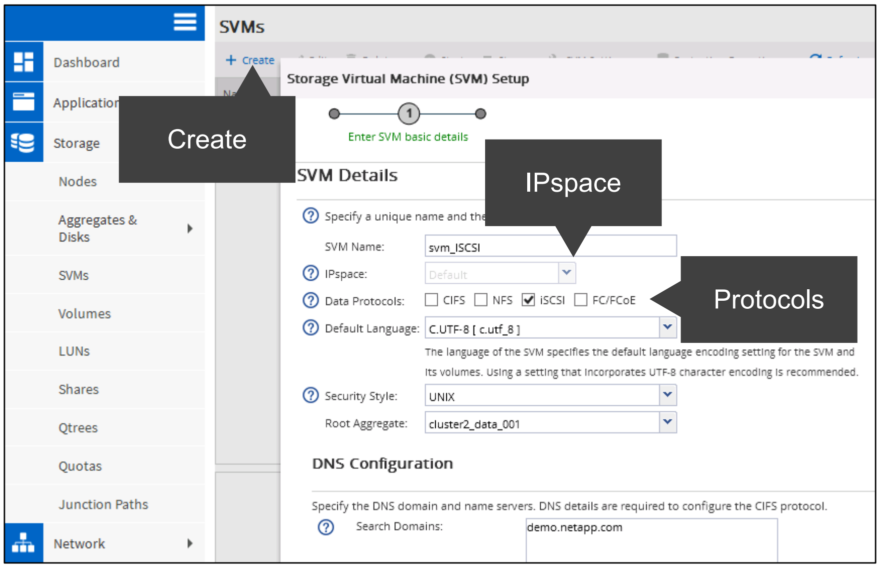


The iSCSI Software Initiator creates the iSCSI connection on the Windows host. The iSCSI Software Initiator is built in to Windows Server 2008 and Windows Server 2012.

If the system has not yet used an iSCSI Software Initiator, a dialog box appears and requests that you turn on the service. Click **Yes**. The iSCSI Initiator Properties dialog box then appears. You need to identify the iSCSI initiator name before you start the SVM creation wizard.

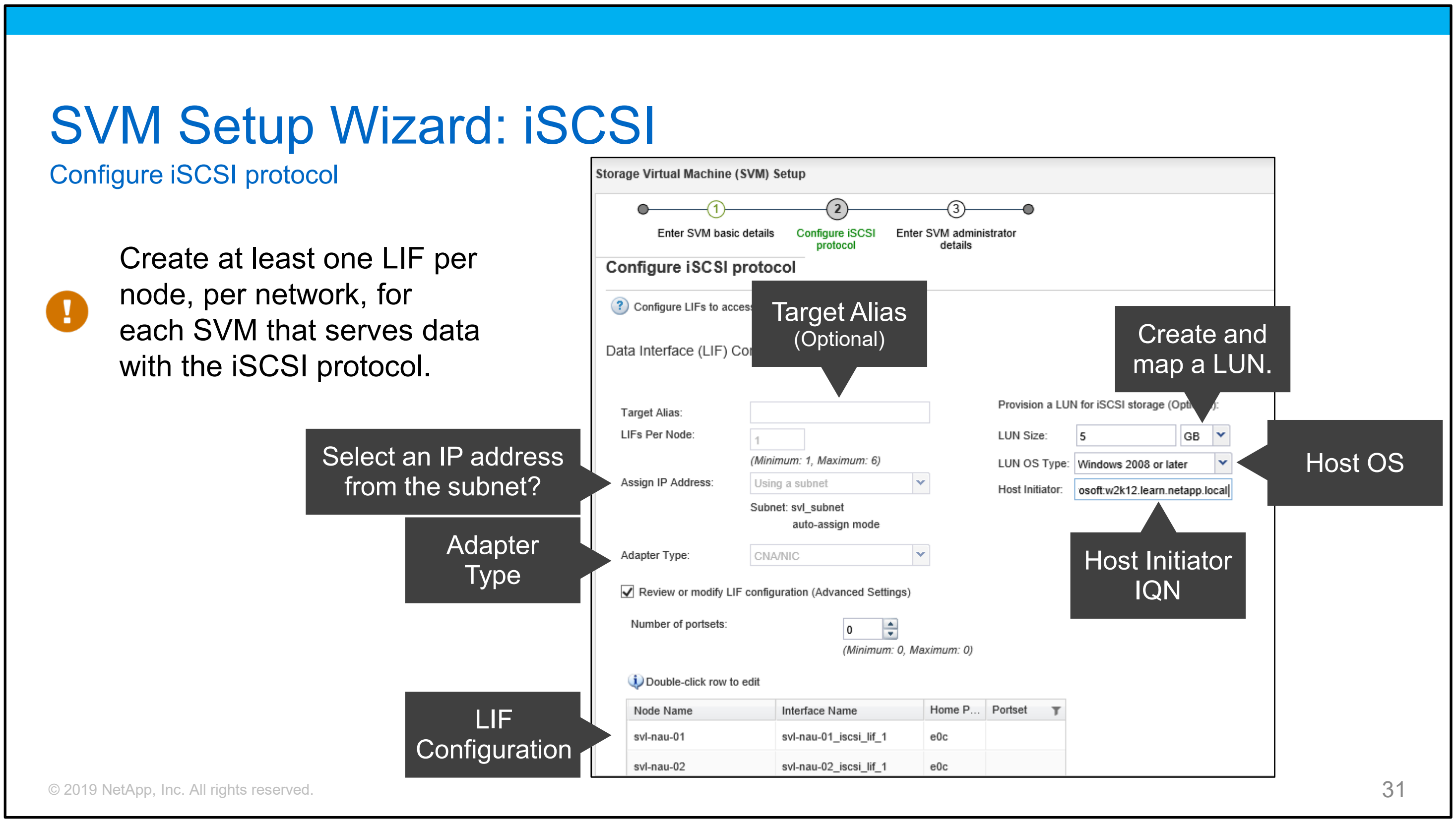
SVM Setup Wizard: iSCSI

SVM basic details



View the steps to create an SVM for an iSCSI environment.

You can enable the iSCSI protocol on an existing SVM by using NetApp OnCommand System Manager or the `vserver iscsi create -vserver <vserver_name>` command. Verify that the operational status of the iSCSI service on the specified SVM is up and ready to serve data.



The SVM creation wizard automatically creates a LIF on each node of the cluster. IP addresses can be assigned manually or automatically by selecting a subnet. To verify or modify the LIF configuration, select the **Review or modify LIF configuration** checkbox.

To create an iSCSI LIF manually, using either System Manager or the CLI, you must specify the `-role` parameter as `data` and the `–data-protocol` parameter as `iscsi`.

CLI LIF creation example:

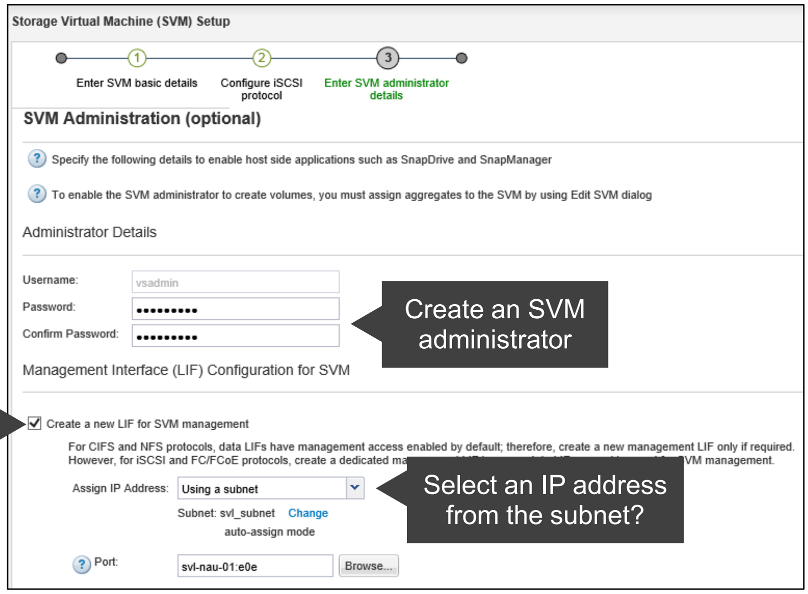
```
rtp-nau::> network interface create -vserver svm_black -lif black_iscsi_lif1    -role
data -data-protocol iscsi -home-node rtp-nau-01 -home-port e0e –subnet snDefault
```

The SVM creation wizard also enables you to provision a LUN for iSCSI storage. Enter the size, the LUN OS type, and the IQN for the host initiator.

NOTE: You should create at least one LIF for each node and each network on all SVMs that serve data with the iSCSI protocol. NetApp recommends having network redundancy through either multiple networks or link aggregation.

SVM Setup Wizard: iSCSI

SVM administrator details



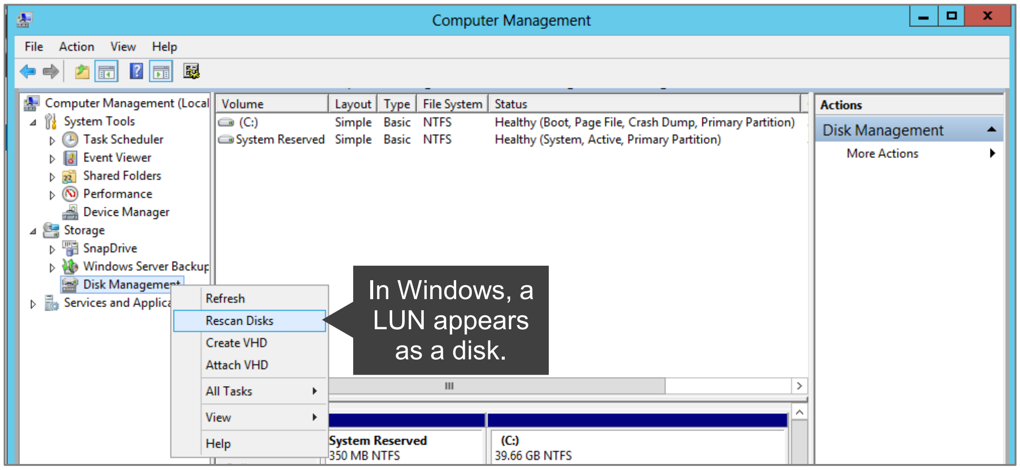
Create an SVM administrator

Create an SVM management LIF.

Select an IP address from the subnet?

Windows LUN Implementation

Discover LUN



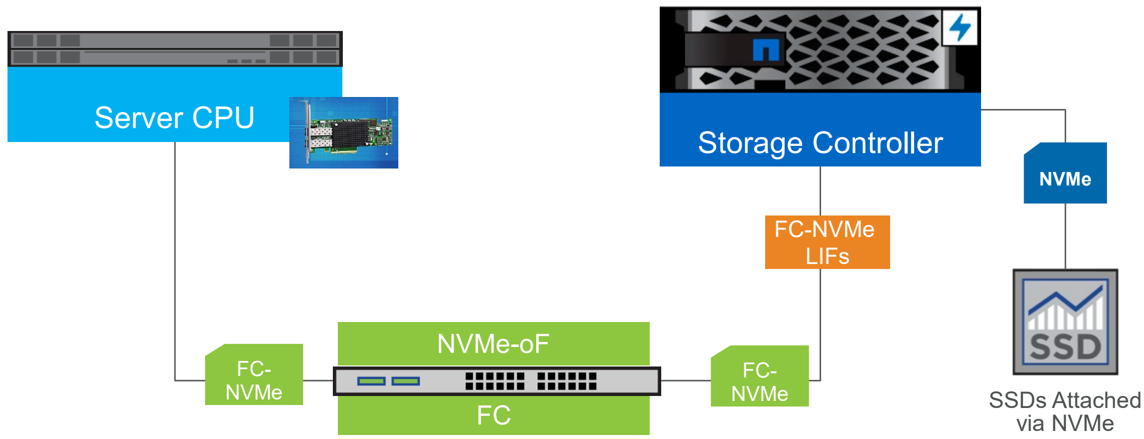
To configure the LUN with NTFS, first discover the LUN by selecting **Disk Management > Rescan Disks**.

 33

You can discover and prepare the LUN in Windows in many ways. Each version of Windows might have slightly different tools that you can use. This module illustrates the most often used method. In Windows, a LUN appears as a disk and is labeled as a disk.

1. Open Computer Management.
2. Select Disk Management.
3. If the LUN that you created is not displayed, rescan disks by right-clicking **Disk Management** or, from the Action menu, select **Rescan Disks**.

NVMe over Fibre Channel



More info in Addendum

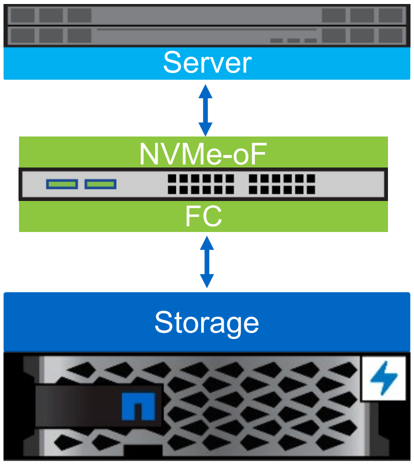
NVMe/FC = NVMe over Fibre Channel | SSD = solid-state drive

34

NVMe/FC is a new block-access protocol that was first supported in ONTAP 9.4. The NetApp AFF A800 all-flash array was the first NetApp system to support NVMe/FC. The NVMe protocol can use an existing FC network to provide block access to LUNs that reside on nonvolatile disks in the cluster. The protocol uses NVMe-FC LIFs rather than FC LIFs. Review the Hardware Universe to determine whether your storage controller has been added to the list of supported models.

NVMe over Fibre Channel

Supported features in ONTAP software



ONTAP 9.4

- Application-based high availability only
  - No storage path failover
  - Use with applications that provide failover (for example, Oracle RAC, MongoDB, Splunk)
- SUSE Enterprise Linux 12 SP3 support

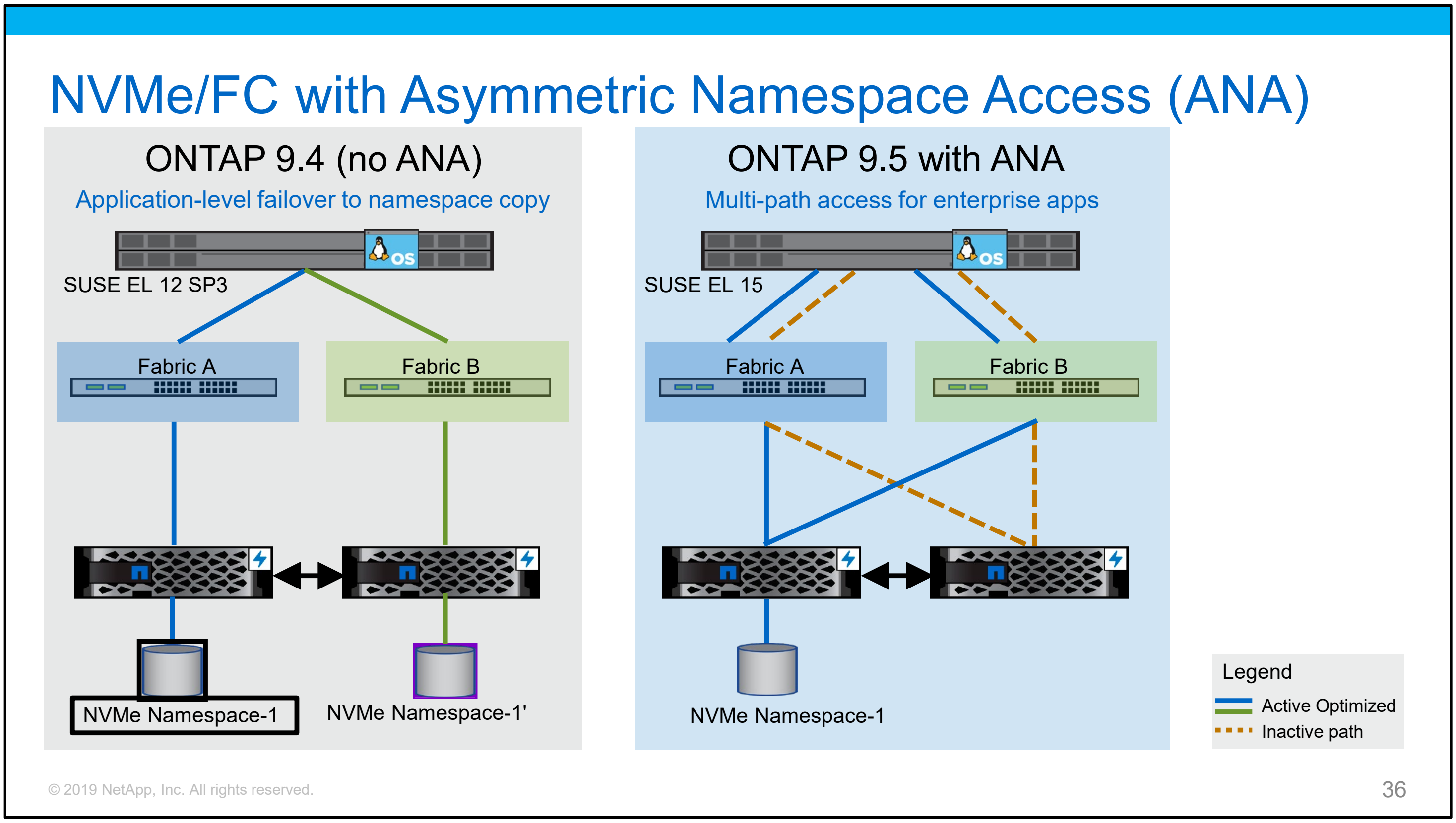
ONTAP 9.5

- Multipath (storage path) failover with asynchronous namespace access (ANA)
  - ANA is similar to asymmetric logical unit access (ALUA) for FC
  - Supported first with SUSE Enterprise Linux 15
  - SPC-1 benchmark planned
- Red Hat Enterprise Linux 7.6 support (without ANA)

See NetApp Interoperability Matrix Tool (IMT) for host bus adapter (HBA), switches, and host software support:
https://mysupport.netapp.com/matrix/#welcome

SAN Multipath

Unlike Ethernet connections for NAS protocols, SAN connections are point-to-point. A failure anywhere in the path takes the connection offline. Therefore, LUNs need at least two paths between the host and the storage, an approach referred to as Multipath I/O (MPIO). ALUA is an industry-standard protocol for identifying optimized MPIO paths between a storage system and a host and manages the switching between primary and secondary routes. In a high-availability (HA) and cluster configuration, the primary and secondary paths are generally on different nodes, to provide fault tolerance. Asynchronous Namespace Access (ANA) performs a similar function for NVMe/FC as ALUA does for FC.



NVMe/FC relies on the ANA protocol to provide multipathing and path management necessary for both path and target failover. The ANA protocol defines how the NVMe subsystem communicates path and subsystem errors back to the host so that the host can manage paths and failover from one path to another. ANA fills the same role in NVMe/FC that ALUA does for both FCP and iSCSI protocols.

ANA categorizes paths as active or inactive. Active paths are both preferred and functional. Inactive paths are neither preferred or functional. An Inactive path will only become active in the event of a controller failover, this means there is no remote path support in ONTAP’s current ANA implementation.

ONTAP 9.4: NVMe/FC (no ANA): In 9.4 the host is connected to a fabric to a single SVM through a single LIF. The namespace can be only accessed through the designated LIF. There is no remote IO in 9.4, as a result there is no failover support from the storage stack. In case of a path or controller failover, the enterprise applications with built in application failover accesses the stored copy of data (Namespace-1’) through the fabric (green) as shown in the picture.

ONTAP 9.5: NVMe/FC (with ANA): In 9.5 the host is connected to both the fabrics and has multipath access to the namespace through two LIFs (one from each fabric - Blue). These paths are active optimized. The host is also connected to the namespace through an Inactive path as shown in the figure with dashed amber lines. In case of a path failure or controller failover, partner takeover occurs, and the inactive path is turned to an active optimized path for the host to access the data from the namespace. For ex: When there is a failure in the path or controller attached to Fabric A, the controller failover notification is sent, and controller B takes over. The inactive path from host to Fabric A & B are turned into an active optimized state and the host can access the data through the controller B.

Knowledge Check: Question

A volume called svm1_vol2 is created on the aggr2 aggregate and mounted to the junction path /svm1/vol2. An administrator moves the volume to the aggr1 aggregate.

After the move, what is the path to the volume?

a. /aggr1/svm1/svm1_vol2
b. /svm1/vol2
c. /vol/svm1_vol2
d. /aggr1/svm1_vol2

Additional SAN Learning

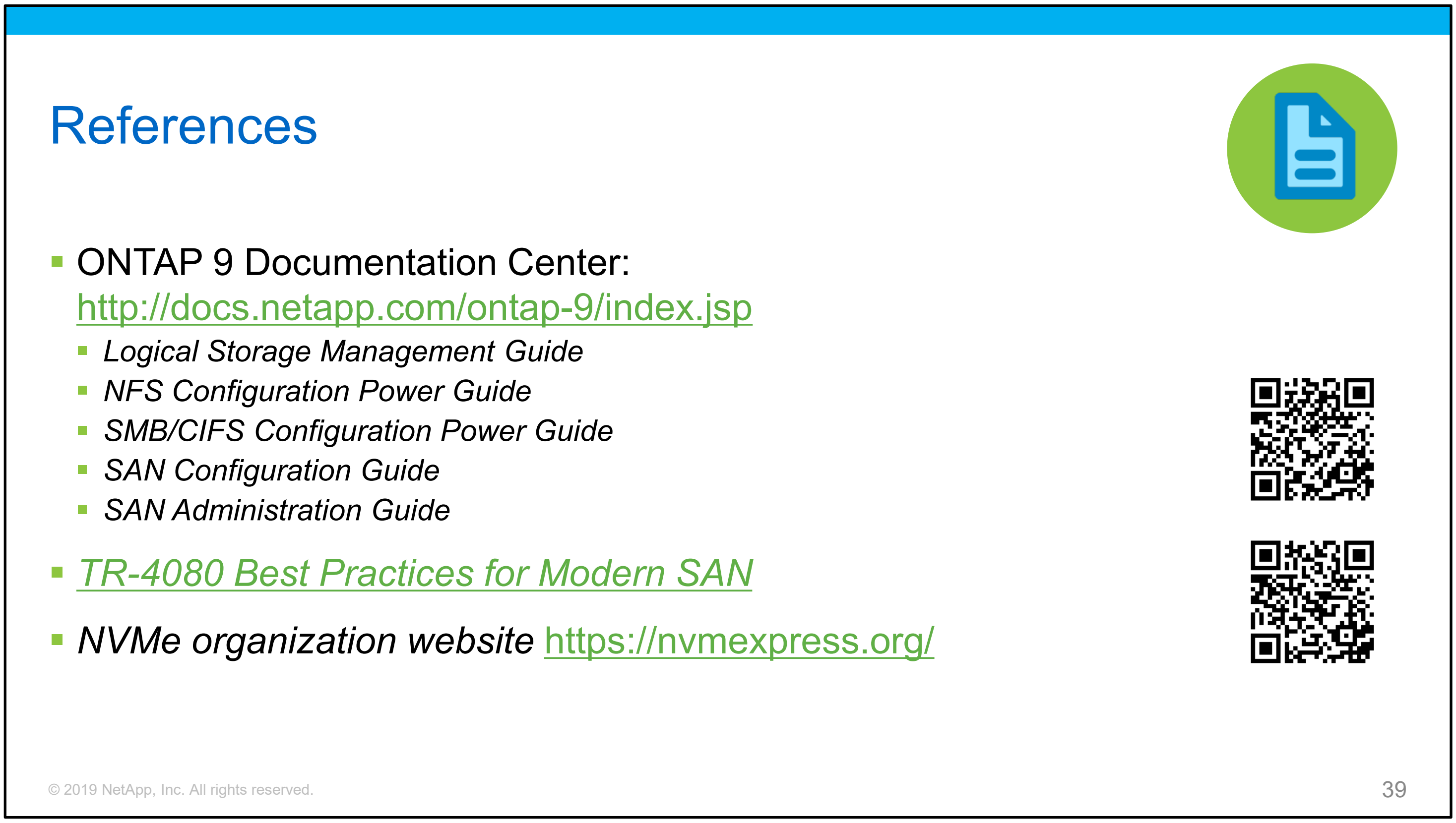
Where can I learn about advanced topics like FC and FCoE protocols, implementing Windows and Linux initiators, and LUN management and mobility enhancements?

- ONTAP SAN Fundamentals (online course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000018109
- Data ONTAP SAN Administration (virtual/instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000015072

ONTAP SAN Fundamentals (online course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000018109

Data ONTAP SAN Administration (virtual/instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000015072

Note: Courses are regularly updated and revised. Check the Learning Center for the latest version and offerings.



ONTAP 9 Documentation Center:

http://docs.netapp.com/ontap-9/index.jsp

- *Logical Storage Management Guide*
- *NFS Configuration Power Guide*
- *SMB/CIFS Configuration Power Guide*
- *SAN Configuration Guide*
- *SAN Administration Guide*

TR-4080 Best Practices for Modern SAN

NVMe organization website https://nvmexpress.org/

Module Review

This module focused on enabling you to:

- Use NAS protocols to access data
- Use SAN protocols to access data

ACTION: Complete an Exercise

Module 7: Configuring NAS Protocols and iSCSI in an SVM

Duration: 45 minutes

Access your exercise equipment.

Use the login credentials that your instructor provided to you.

Complete the specified exercises.

- Go to the exercise for the module.
- Start with Exercise 7-1.
- Stop at the end of Exercise 7-2.

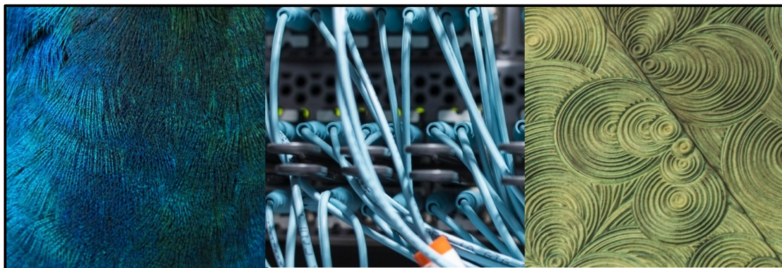
Participate in the review session.

- Share your results.
- Report issues.

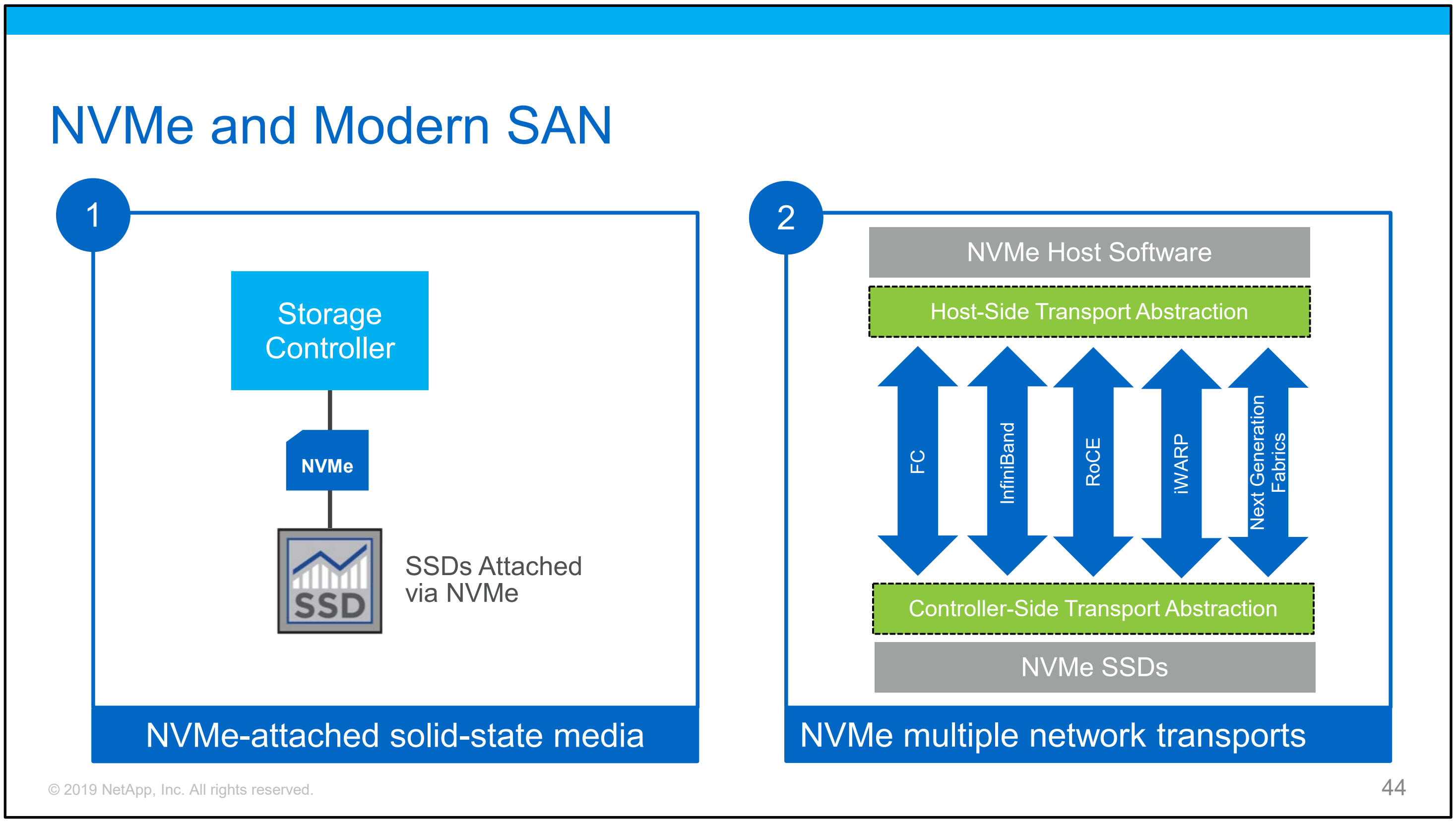
Share Your Experiences

Roundtable questions for the equipment-based exercises

1. Were you able to use both the SMB and NFS protocols to access the same volume in the namespace?
2. How does partitioning and formatting a LUN from the Windows host differ from partitioning and formatting a physical disk in Windows?
3. Why do you need FlexVol volumes?
4. Why should you not place data directly on the aggregate?



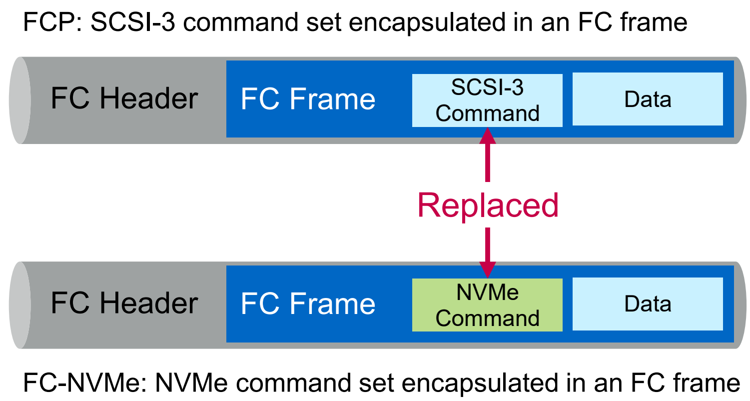
Addendum
NVMe and NVMe/FC



NVMe is most often used for attaching disks and disk shelves. Implementing end-to-end NVMe requires NVMe-attached solid-state media and NVMe transport from the storage controller to the host server. NVMe over Fabrics (NVMe-oF) adds NVMe as a new block storage protocol type. NVMe-oF defines and creates specifications for how to transport NVMe over various network storage transports such as FC, InfiniBand, and others.

NVMe/FC and FC Frames

- Share common hardware and fabric components.
- Can coexist on the same optical fibers, ports, switches, and storage controllers.
- NVMe/FC and FCP look similar.



 45

FCP and NVMe share hardware and fabric components and can coexist on the same optical fibers, ports, switches, and storage controllers. If you own the necessary hardware to run NVMe/FC, you can start using NVMe/FC with a simple software upgrade to ONTAP 9.4 or later. NVMe/FC implementations can use existing FC infrastructure, including host bus adapters (HBAs), switches, zones, targets, and cabling.

See the NetApp Interoperability Matrix Tool (IMT) to verify the latest supported solution stack for ONTAP software.

NVMe/FC and FC look similar. FC encapsulates SCSI-3 Command Descriptor Block (CDB) inside FC frames while NVMe/FC swaps out the SCSI-3 CDB for the new NVMe command set, thus offering substantial improvements to throughput and latency.

NVMe and FC Naming

NVMe terminology

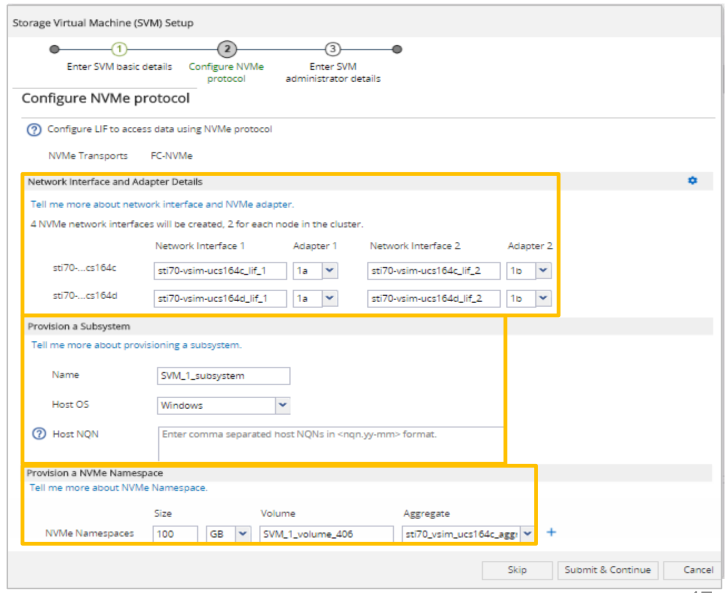
FC	NVMe/FC
Worldwide port name (WWPN)	NVMe qualified name (NQN)
LUN	Namespace
LUN mapping/LUN masking/igroup	Subsystem
Asymmetric logical unit access (ALUA)	Asynchronous namespace access (ANA)

NVMe adds some new names for some common structures. The table maps some structures that have different names than those used in FC.

An NVMe qualified name (NQN) identifies an endpoint and is similar to an IQN. A namespace is analogous to a LUN; both represent an array of blocks presented to an initiator. A subsystem is analogous to an igroup and is used to mask an initiator so that it can see and mount a LUN or namespace. ANA is a new protocol feature for monitoring and communicating path states to the host operating system's MPIO or multipath stack, which uses information communicated through ANA to select and manage multiple paths between the initiator and target.

Setting up NVMe

1. Configure an SVM for NVMe.
2. Create namespaces and subsystems.
3. Configure an FC-NVMe LIF.
4. Map the namespace to the subsystem.



47

To set up the NVMe protocol in your SAN environment, you must configure an SVM for NVMe. You must also create namespaces and subsystems, configure an FC-NVMe LIF, and then map the namespaces to the subsystems. You can use System Manager to set up NVMe.

For systems that use the NVMe protocol, you must configure NVMe LIFs and create one or more NVMe namespaces and subsystems. Each namespace can then be mapped to an NVMe subsystem to enable data access from your host system.

Module 8
Data Protection

About This Module

This module focuses on enabling you to:

- Manage Snapshot copies
- Restore data from Snapshot copies
- Back up and replicate data
- Use encryption to prevent unauthorized access to data

Lesson 1
Manage Snapshot Copies

Snapshot Copies

- A Snapshot copy is a read-only, point-in-time image of a FlexVol volume.
- The image consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the most recent Snapshot copy was made.
- Snapshot copies owe their efficiency to the NetApp WAFL file system, which uses metadata to point to blocks on disk and writes to a new block rather than overwrite existing blocks.
- Instead of moving old blocks to a pool of space for Snapshot copies, old blocks remain in place. Only the pointers move from the active file system to the Snapshot copies.

 4

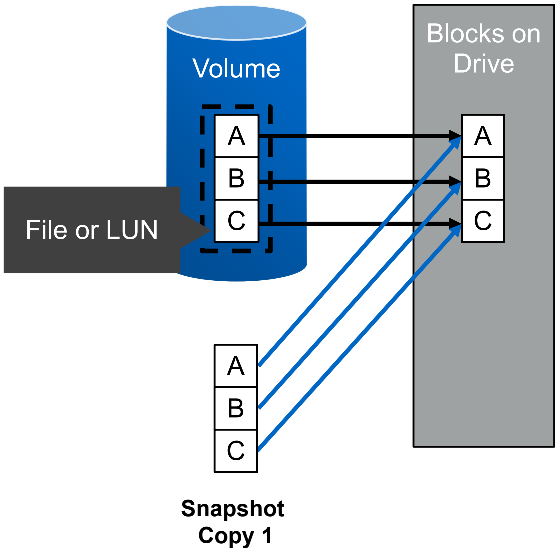
Understanding the technology that is used to create a Snapshot copy helps you to understand how space is used. Furthermore, understanding the technology helps you to understand features such as FlexClone technology, deduplication, and compression.

A Snapshot copy is a local, read-only, point-in-time image of data. Snapshot copy technology is a built-in feature of NetApp WAFL storage virtualization technology and provides easy access to old versions of files and LUNs.

Snapshot technology is highly scalable. A Snapshot copy can be created in a few seconds, regardless of the size of the volume or the level of activity on the NetApp storage system. After the copy is created, changes to data objects are reflected in updates to the current version of the objects, as if the copy did not exist. Meanwhile, the Snapshot copy of the data remains stable. A Snapshot copy incurs no performance overhead. Users can store as many as 255 Snapshot copies per volume. All the Snapshot copies are accessible as read-only and online versions of the data.

Snapshot Copy Technology

Create Snapshot copy 1

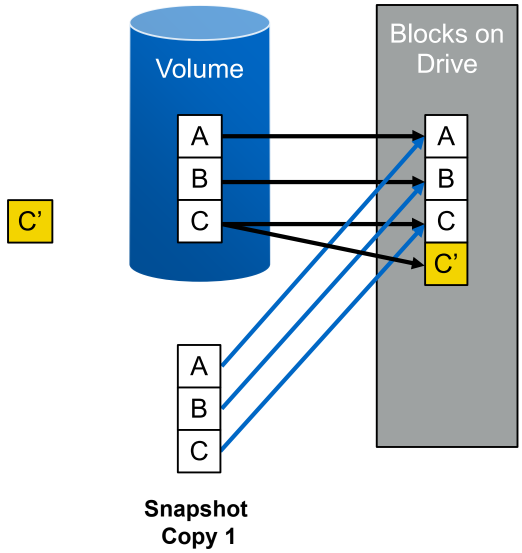


1. Create Snapshot copy 1:
   - Pointers are copied.
   - No data is moved.

When NetApp ONTAP creates a Snapshot copy, ONTAP starts by creating pointers to physical locations. The system preserves the inode map at a point in time and then continues to change the inode map on the active file system. ONTAP then retains the old version of the inode map. No data is moved when the Snapshot copy is created.

Snapshot Copy Technology

Continue writing data



1. Create Snapshot copy 1.
2. Continue writing data:
   - Data is written to a new location on the disk.
   - Pointers are updated.

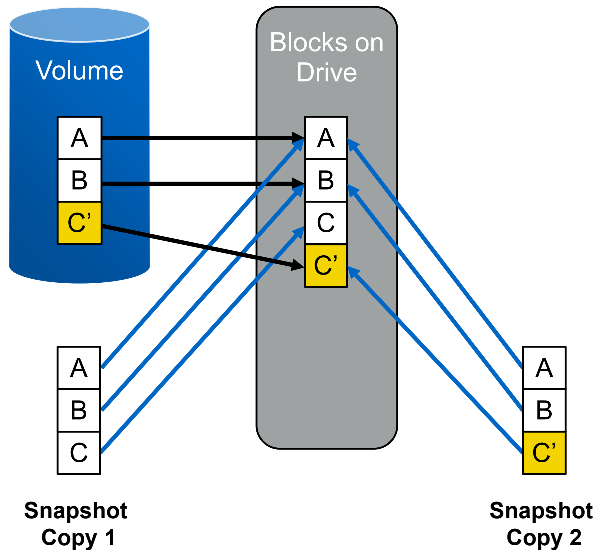
 6

When ONTAP writes changes to disk, the changed version of block C is written to a new location. In the example, C' is the new location. ONTAP changes the pointers rather than moving data.

The file system avoids the parity update changes that are required if new data is written to the original location. If the WAFL file system updated the same block, then the system would need to perform multiple parity reads to update both parity disks. The WAFL file system writes the changed block to a new location, writing in complete stripes and without moving or changing the original data blocks.

Snapshot Copy Technology

Create Snapshot copy 2



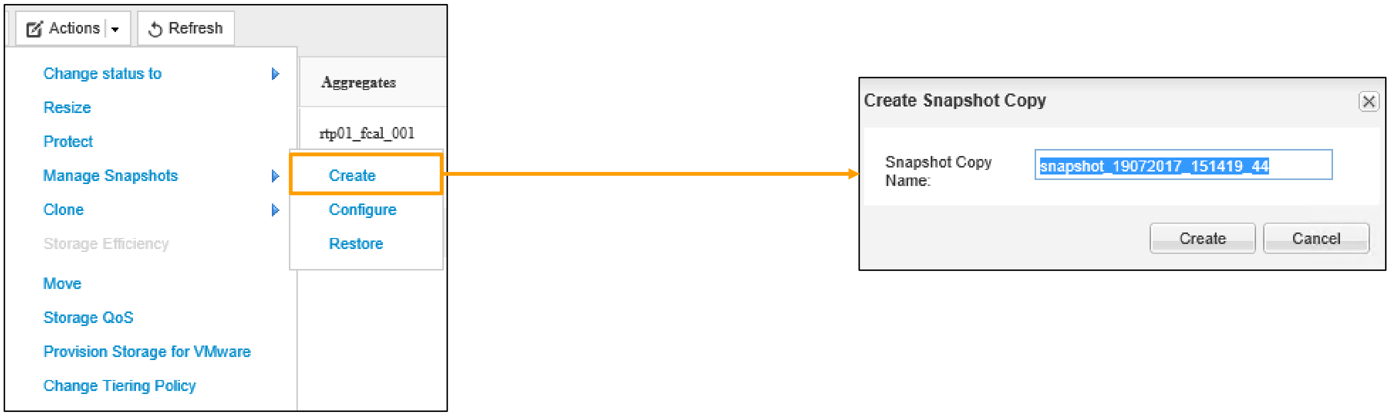
1. Create Snapshot copy 1.
2. Continue writing data.
3. Create Snapshot copy 2:
   - Pointers are copied.
   - No data is moved.
   - Block C consumes Snapshot space because the active file system no longer references Block C.

 7

When ONTAP creates another Snapshot copy, the new Snapshot copy points only to the unchanged blocks A and B and to block C'. Block C' is the new location for the changed contents of block C. ONTAP does not move any data; the system keeps building on the original active file system. The method is simple and good for disk use. Only new and updated blocks use additional block space.

When Snapshot copy 1 is created, the copy consumes no space because the copy holds only pointers to blocks on disk. When C' and Snapshot copy 2 are created, the primary pointer from block C changes from the active file system to Snapshot copy 1. Snapshot copy 1 now owns the block and the space the block consumes. If Snapshot copy 1 is deleted, the C block will have no more pointers referencing it. The block will be returned to the available free space.

Create a Snapshot Copy




```
cluster1::> snapshot create -vserver svm4 -volume svm4_vol002
```


You can use NetApp OnCommand System Manager or clustershell to create, schedule, and maintain Snapshot copies for volumes and aggregates.

Snapshot Copy Design

- Do not create more Snapshot copies than necessary.
- Check and adjust the volume Snapshot copy reserve defaults.
- To control storage consumption, configure Snapshot copy automatic deletion and volume automatic increase.
- Consult TR-4678 for guidance on planning Snapshot copies of NetApp FlexGroup volumes.

Snapshot copies are the first line of defense against accidental data loss or inconsistency.

To provide efficient use of drive space, deploy only the required number of Snapshot copies on each volume. If you deploy more Snapshot copies than are required, the copies consume more drive space than necessary.

You might need to adjust default settings for the Snapshot copy reserve for volumes:

- The Snapshot copy reserve guarantees that you can create Snapshot copies until the reserved space is filled.
- When Snapshot copies fill the reserved space, the Snapshot blocks compete for space with the active file system.

NetApp ONTAP FlexGroup volumes have special considerations for taking a Snapshot copy. All FlexGroup volumes must temporarily halt data access to help ensure a crash-consistent state. If the Snapshot copy does not complete in 10 seconds, the copy fails. Technical report TR-4678 covers the process of configuring FlexGroup Snapshot copies for use by ONTAP Snap and Flex features. Consult the References page for the URL and QR code link to the technical report.

Naming Conventions for Snapshot Copies

- A Snapshot copy name can have a prefix or schedule name, timestamp, comment, and label:

```
vserver     volume               snapshot
-------     ----------------     ------------------------------
svm4        svm4_vol002          2HourSnapshot.2016-07-11_1030
```

$\underbrace{\texttt{2HourSnapshot}}_{\text{(Prefix)}}.\underbrace{\texttt{2016-07-11\_1030}}_{\text{(Timestamp)}}$

- Snapshot copy names cannot be longer than 255 characters.

 10

Administrators can use the Snapshot copy prefix, timestamp, and comment features to quickly determine why a Snapshot copy was created.

The Prefix or Schedule

- The prefix is an optional string of characters that you can specify for an automatic Snapshot copy. If a prefix is specified, the Snapshot name is made up of the *prefix* and *timestamp*. Prefix names must be unique within a policy.
- A schedule cannot have more than one prefix. The number of characters in the prefix counts toward the 255-character limit on the Snapshot name.

If a prefix is specified in the Snapshot schedule, the schedule name is not used. The schedule name is used if the prefix is not specified for a Snapshot schedule:

```
volume snapshot policy add-schedule -policy <snapshot_policy> -schedule <text> -count <integer> [-prefix <text>]
```

The Comment

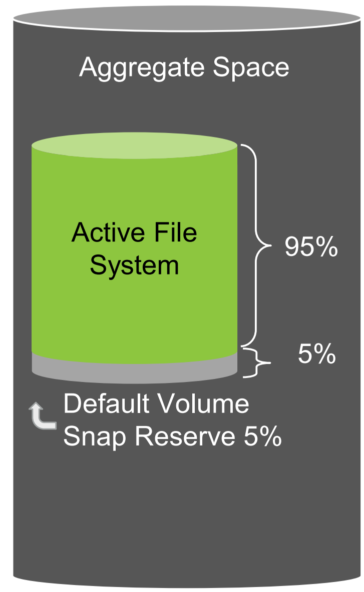
Use the `volume snapshot modify` command to change the text comment that is associated with a Snapshot copy.

The Label

The vaulting subsystem uses the SnapMirror label when you back up Snapshot copies to the vault destination. If an empty label ("") is specified, the existing label is deleted.

The Snapshot Copy Reserve

- The Snapshot reserve is a storage space set aside inside a volume.
  - Often depicted as a partition
  - Actually a soft quota
- The reserve holds blocks that are no longer in the active file system but are still referenced by Snapshot copies.
- The reserve is not used for file system writes.
- The reserve can be increased or decreased.



11

The `snap reserve` command displays the percentage of storage space that has been set aside for Snapshot copies.

Use the `snap reserve` command to change the percentage of storage space that is set aside for the Snapshot copies of a volume. For example, to increase the Snapshot copy reserve from 5% to 10% for the volume named *engineering*, enter the following command:

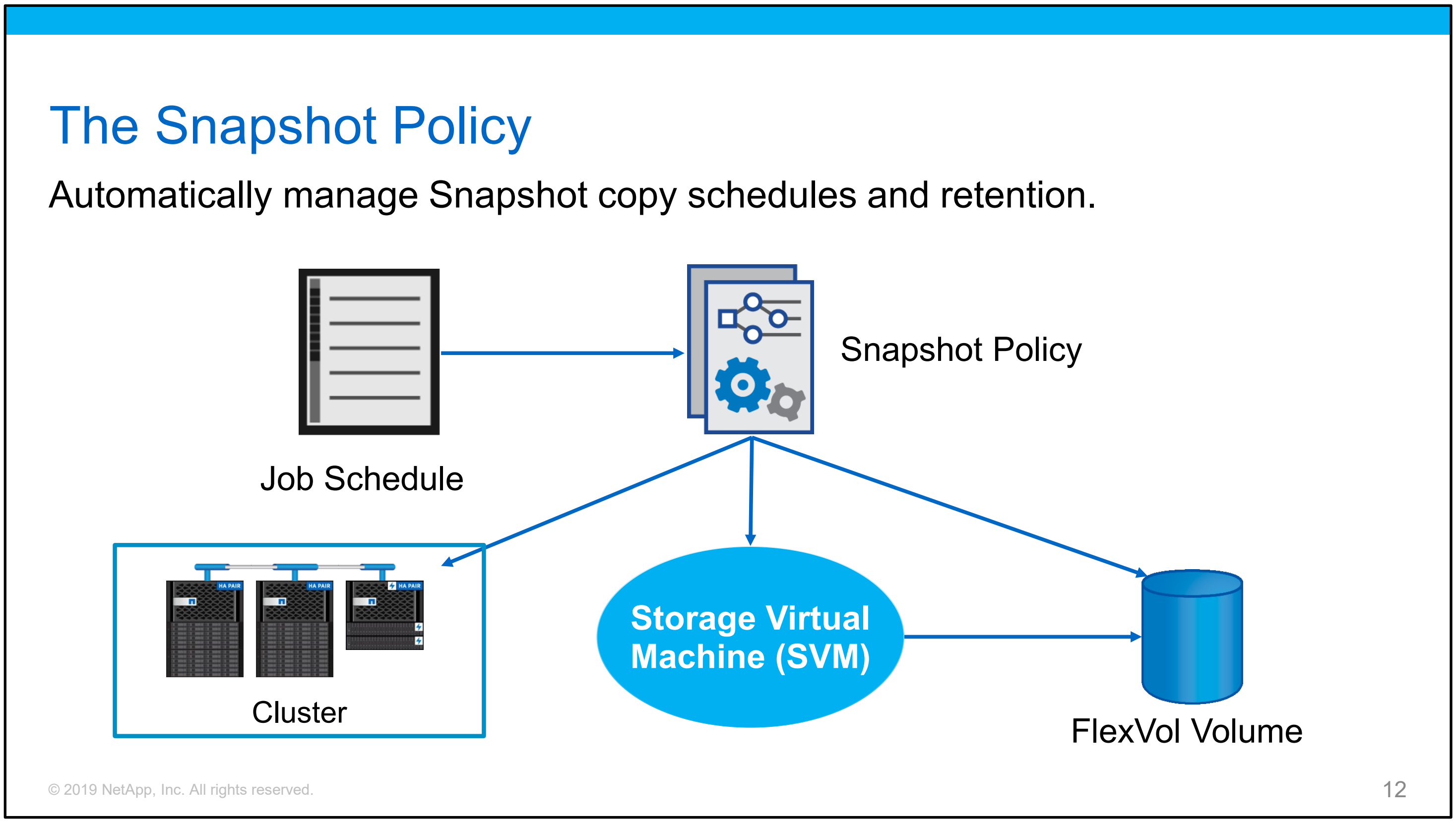
```
snap reserve engineering 10
```

By default, volume Snapshot copies are stored in the Snapshot copy reserve storage space. The Snapshot copy reserve space is not counted as part of the volume disk space that is allocated for the active file system. (For example, when you enter the df command for a volume, the amount of available disk space shown does not include the amount of disk space that is reserved by the `snap reserve` command.)

When a Snapshot copy is first created, none of the Snapshot copy reserve is consumed. The Snapshot copy protects the active file system at a point in time when the Snapshot copy was created. As the Snapshot copy ages, and the active file system changes, the Snapshot copy begins to own the data blocks that the current active file system deleted or changed. The Snapshot copy begins to consume the Snapshot copy reserve space. The amount of disk space that Snapshot copies consume can grow, depending on the length of time that a Snapshot copy is retained and the rate of change of the volume.

Sometimes, if the Snapshot copy is retained for a long period and the active file system has a high rate of change, the Snapshot copy can consume 100% of the Snapshot copy reserve. If the Snapshot copy is not deleted, then the copy can consume a portion of the drive space that is intended for the active file system. Monitor and manage Snapshot copies so that drive space is properly managed.

NOTE: Even if the Snapshot copy reserve is set to 0%, you can still create Snapshot copies. If no Snapshot copy reserve exists, then over time, Snapshot copies consume blocks from the active file system.



A Snapshot policy enables you to configure the frequency and maximum number of Snapshot copies that are created automatically:

- You can create Snapshot policies as necessary.
- You can apply one or more schedules to the Snapshot policy.
- The Snapshot policy can have zero schedules.

When you create a storage virtual machine (SVM), you can specify a Snapshot policy that becomes the default for all FlexVol volumes that are created for the SVM. When you create a FlexVol volume, you can specify which Snapshot policy you want to use, or you can enable the FlexVol to inherit the SVM Snapshot policy.

The default Snapshot policy might meet your needs. The default Snapshot copy policy is useful if users rarely lose files.

The default Snapshot policy specifies the following:

- Weekly schedule to keep two weekly Snapshot copies
- Daily schedule to keep two daily Snapshot copies
- Hourly schedule to keep six hourly Snapshot copies

However, if users often lose files, then you should adjust the default policy to keep Snapshot copies longer:

- Weekly schedule to keep two weekly Snapshot copies
- Daily schedule to keep six daily Snapshot copies
- Hourly schedule to keep eight hourly Snapshot copies

For typical systems, only 5% to 10% of the data changes each week: six daily and two weekly Snapshot copies consume 10% to 20% of disk space. Adjust the Snapshot copy reserve for the appropriate amount of disk space for Snapshot copies.

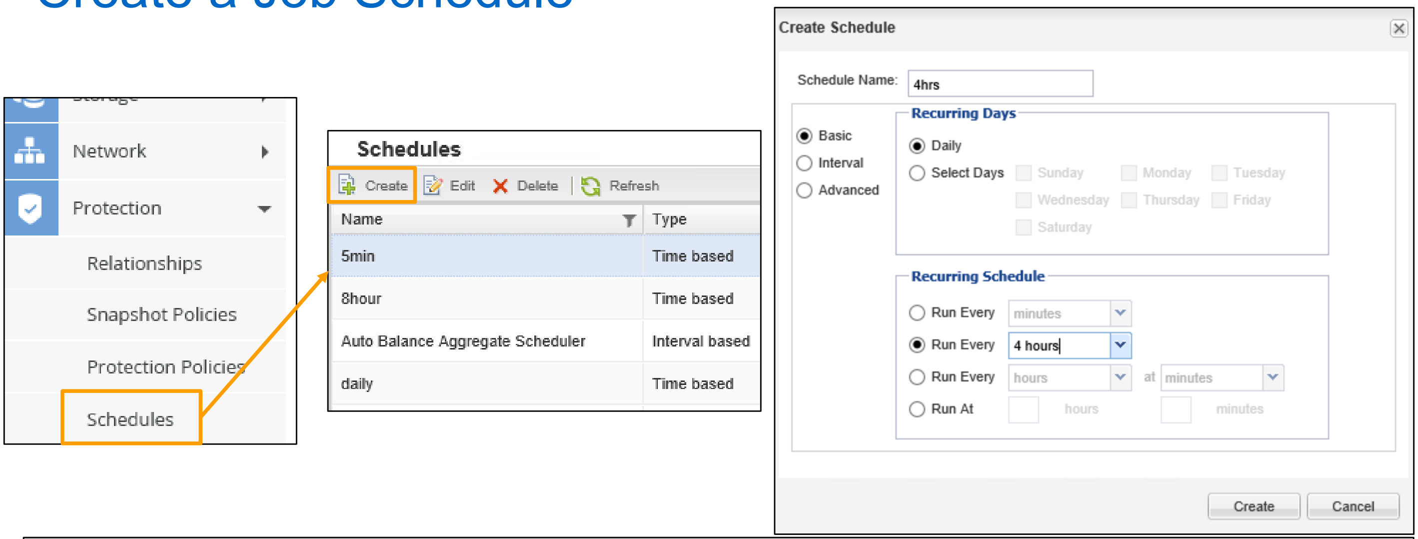
Each volume on an SVM can use a different Snapshot copy policy. For active volumes, create a Snapshot schedule that creates Snapshot copies every hour and keeps them for just a few hours, or turn off the Snapshot copy feature.

You back up Snapshot copies to the vault destination. If an empty label ("") is specified, the existing label is deleted.

Typical Workflow

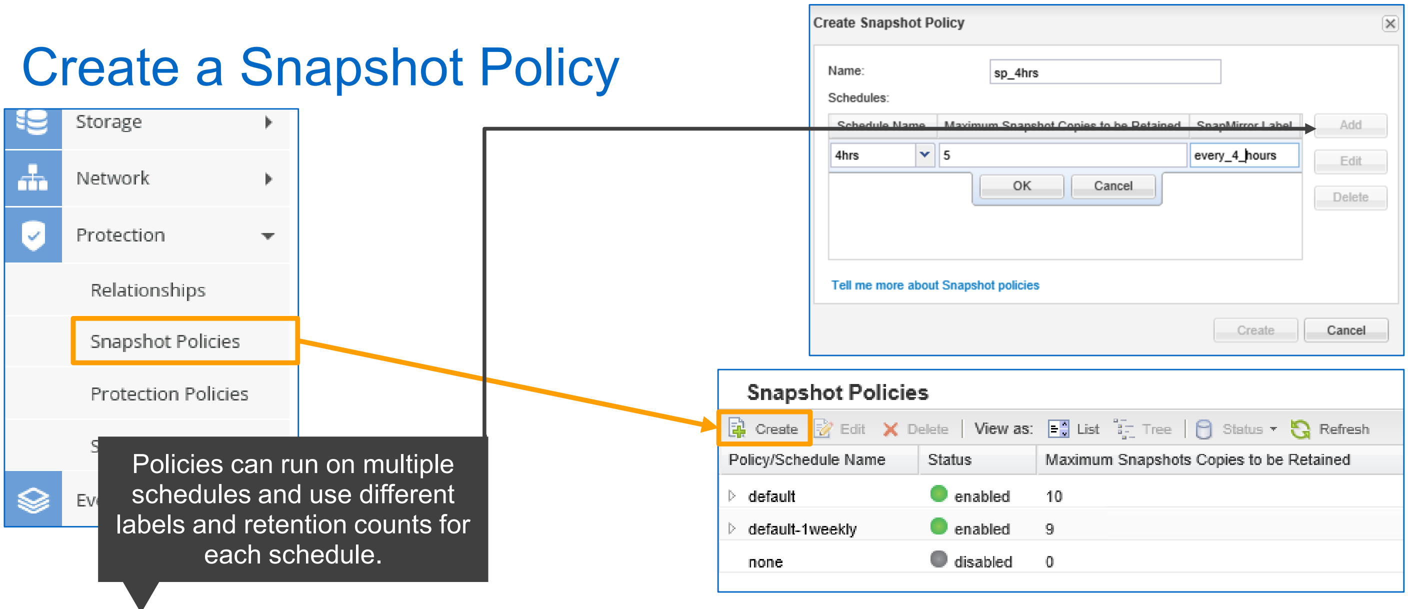
1. Create a job schedule, or use the default.
2. Create a Snapshot policy, and then specify the job schedule.
3. Assign the Snapshot policy to a FlexVol volume, or inherit a Snapshot policy from the SVM.

Create a Job Schedule



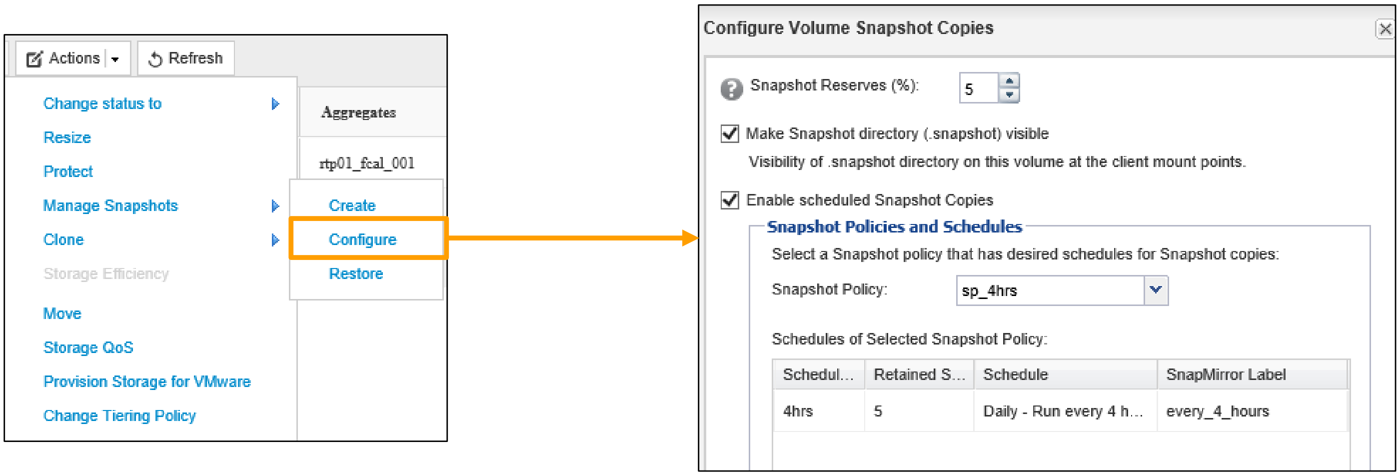

```
::> job schedule cron create -name 4hrs -dayofweek all
  -hour 4,8,12,16,20 -minute 0
```

Create a Snapshot Policy




```
::> volume snapshot policy create -vserver svm4 -policy sp_4hrs     -
schedule1 4hrs -count1 5 -prefix1 every_4_hrs
```

Apply a Snapshot Policy to a Volume




```
::> vol modify -vserver svm4 -volume svm4_vol002 -snapshot-policy sp_4hrs
```

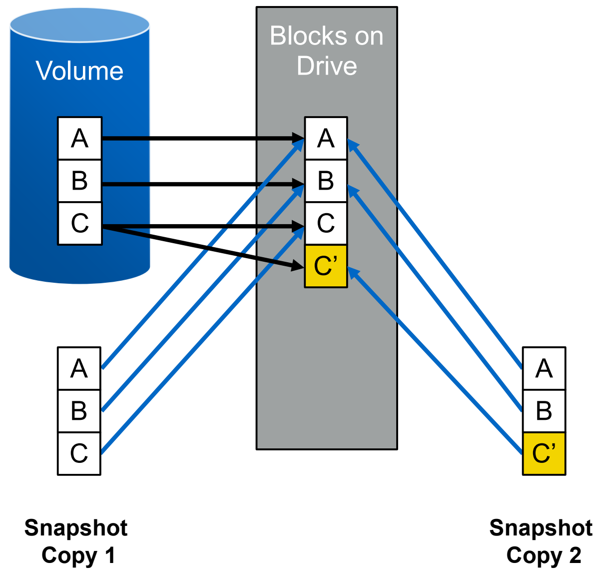
ACTION: Topics for Discussion

- Should all hourly Snapshot copies run on the hour?
- Why or why not?

Lesson 2
Restore Data from a Snapshot Copy

Snapshot Copy Technology

Restore from a Snapshot copy



- To restore a file or LUN from Snapshot copy 1, use SnapRestore data recovery software.
- Snapshot copies that were created after Snapshot copy 1 are deleted.
- Unused blocks on drives are made available as free space.

 19

Suppose that after the Snapshot copy is created, the file or LUN becomes corrupted, which affects logical block C'. If the block is physically bad, RAID can manage the issue without recourse to the Snapshot copies. In the example, block C' becomes corrupted because part of the file is accidentally deleted. You want to restore the file.

To easily restore data from a Snapshot copy, use the SnapRestore feature. SnapRestore technology does not copy files. SnapRestore technology moves pointers from files in the good Snapshot copy to the active file system. The pointers from the good Snapshot copy are promoted to become the active file system pointers. When a Snapshot copy is restored, all Snapshot copies that were created after that Snapshot copy are destroyed. The system tracks links to blocks on the WAFL system. When no more links to a block exist, the block is available for overwrite and is considered free space.

Because a SnapRestore operation affects only pointers, the operation is quick. No data is updated, nothing is moved, and the file system frees any blocks that were used after the selected Snapshot copy. SnapRestore operations generally require less than one second. To recover a single file, the SnapRestore feature might require a few seconds or a few minutes.

Recovering Data

Recover Snapshot Data	Copy from a Snapshot Copy	Use SnapRestore Technology*
▪ Copy data from Snapshot data. ▪ Use SnapRestore data recovery software. ▪ Use the Windows Previous Versions feature.	▪ Locate the Snapshot copy. ▪ Copy the file to the original location. ▪ Copy the file to a new location.	▪ Restore an entire volume. ▪ Quickly restore large files.

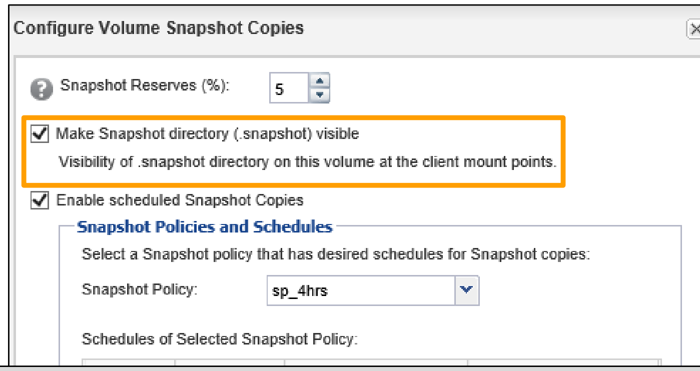
* Requires a SnapRestore license

You can use Snapshot copies to recover data in two ways:

- **Copy a file from a Snapshot directory:** To copy a lost or corrupted file from a Snapshot copy, navigate to the Snapshot directory on the client host. Locate the Snapshot copy that contains the correct version of the file. You can copy the file to the original location and overwrite existing data or copy the file to a new location.
- **Use the SnapRestore feature to recover data:** To revert a volume or a file from a Snapshot copy, you need the SnapRestore license. You can revert a volume or file from the storage CLI or from the System Manager interface.

Snapshot Visibility to Clients

Enable client access to a Snapshot directory.




```
::> vol modify -vserver svm4 -volume svm4_vol_002 -snapdir-access true
::> vserver cifs share modify -vserver svm4 -share-name svm4_vol2     -
share-properties showsnapshot
```


CLI commands are available to control visibility from NAS clients of Snapshot directories on a volume.

NOTE: Show Hidden Files and Folders must be enabled on your Windows system.

Access to .snapshot and ~snapshot is controlled at the volume level by setting the `-snapdir-access switch`. You can also control access to ~snapshot from CIFS clients at the share level with the `showsnapshot` share property.

ACTION: Topic for Discussion

- What are the advantages and disadvantages of enabling clients to restore their own data?

Snapshot View from a UNIX Client

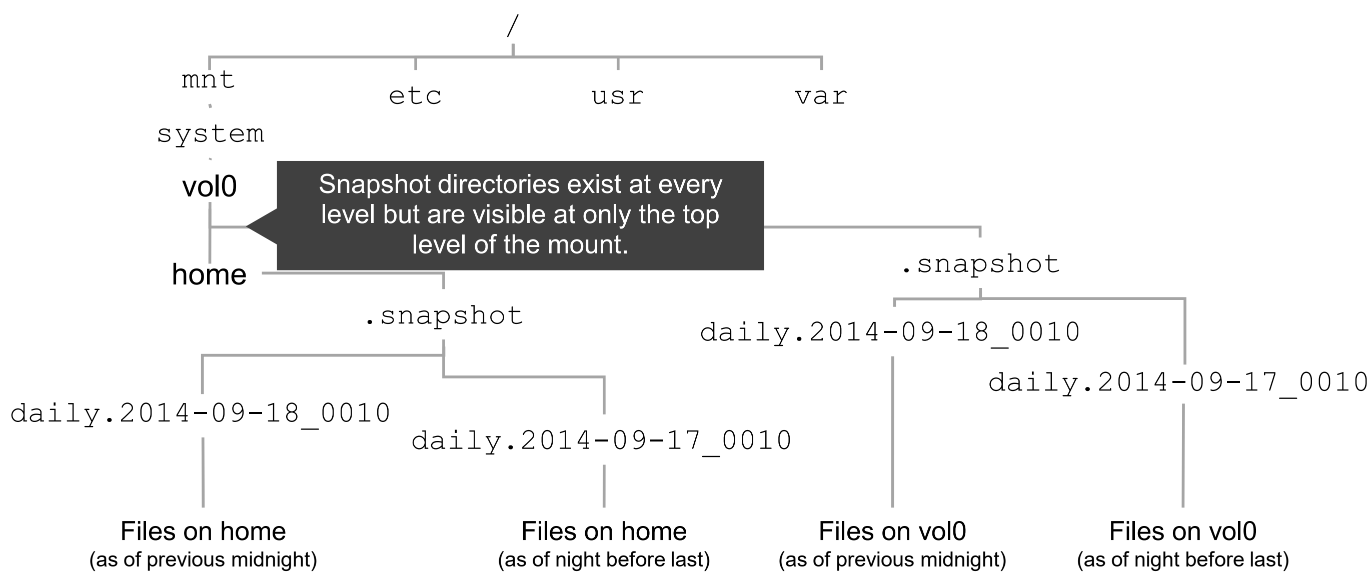
```
# ls /system/vol01/.snapshot
weekly.2014-09-15_0015  daily.2014-09-18_0010
daily.2014-09-19_0010   hourly.2014-09-19_0605
hourly.2014-09-19_0705  hourly.2014-09-19_0805
hourly.2014-09-19_0905  hourly.2014-09-19_1005
hourly.2014-09-19_1105  hourly.2014-09-19_1205
snapmirror.3_2147484677.2014-09-19_114126
```


Every volume in your file system contains a special Snapshot subdirectory that enables users to access earlier versions of the file system, to recover lost or damaged files.

The Snapshot directory appears to NFS clients as .snapshot. The .snapshot directory is usually hidden. The directory is not displayed in directory listings, unless you use the `ls` command with the `-a` option.

When client Snapshot directories are listed, the timestamp is usually the same for all directories. To find the actual date and time of each Snapshot copy, use the `snap list` command on the storage system.

Recovering Files from the .snapshot Directory of a UNIX Host



 24

The .snapshot directory is at the root of a storage system volume.

In the example, the directory structure is shown for an NFS client that has mounted vol0 of a storage system to the mount point `/mnt/system` on the UNIX host.

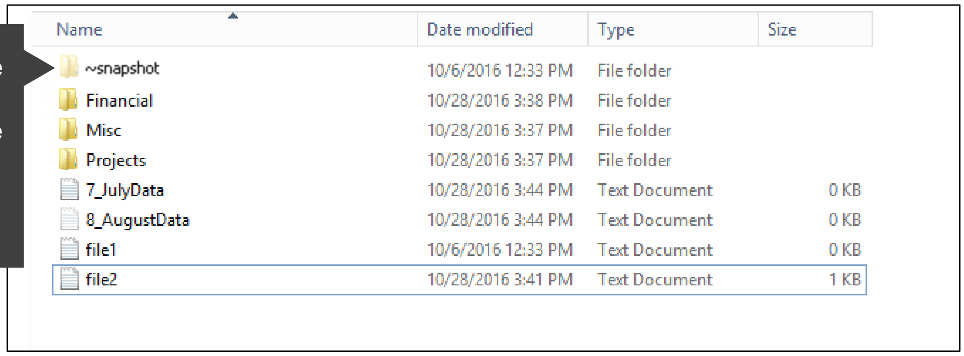
The home directory and the .snapshot directory are visible at the root of the vol0 mount.

You can open the .snapshot directory and access the files in the two Snapshot copies that are subdirectories of the .snapshot directory.

To restore a file from the .snapshot directory, rename or move the original file, then copy the file from the .snapshot directory to the original directory.

Recovering Files from the ~snapshot Directory

Snapshot copies are visible to Windows clients that have File Explorer configured to display hidden files.



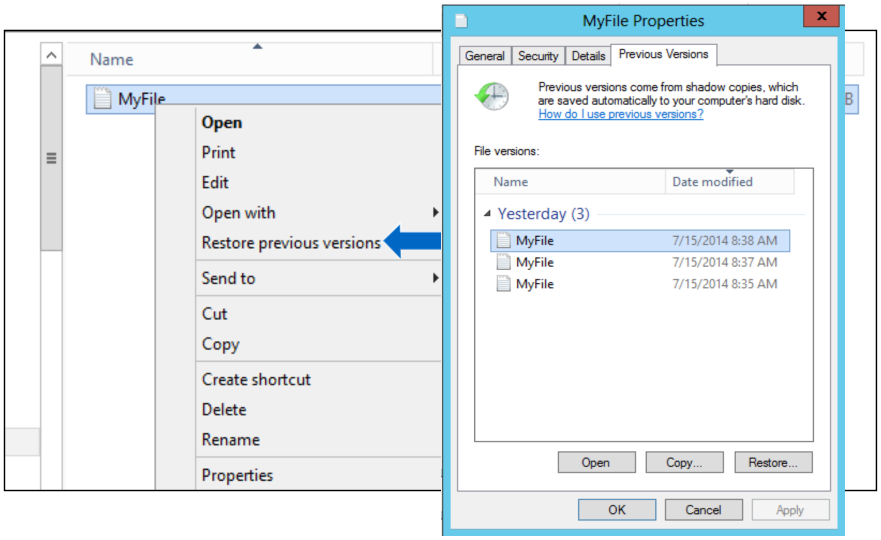
 25

Snapshot directories are hidden on Windows clients. To view them, you must first configure File Explorer to display hidden files. Then, navigate to the root of the CIFS share and find the directory folder.

The subdirectory for Snapshot copies appears to CIFS clients as ~snapshot. Both automatic and manually created Snapshot copies are listed.

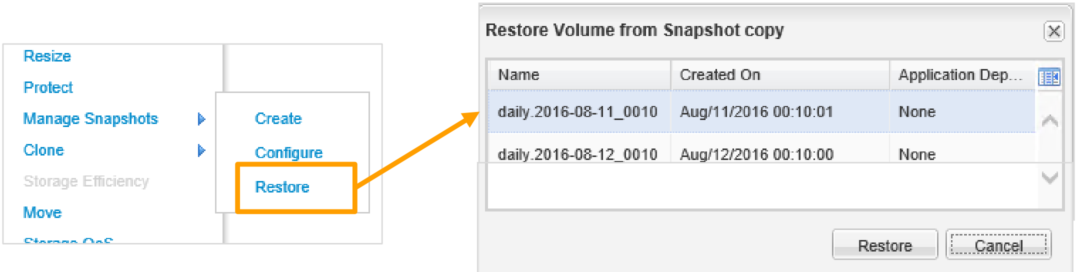
To restore a file from the ~snapshot directory, rename or move the original file, and then copy the file from the ~snapshot directory to the original directory.

Restoring Previous Versions in Windows



In Windows, right-click the file, and then select **Restore previous versions**.

Reverting and Restoring a File



1. Verify that the volume is online and writable.
2. List the Snapshot copies in the volume.

```
::> volume snapshot show -vserver svm4 -volume svm4_vol_002
```

3. Notify network users about the reversion.
4. Identify the names of the Snapshot copy and the file to restore and initiate the reversion.

```
::> volume snapshot restore-file -vserver svm4 -volume svm4_vol_002 -
snapshot svm4_vol_002_snap -path /svm4_vol2/myfile.txt
```


After you complete the steps to revert a file, ONTAP software displays a warning message and prompts you to confirm your decision to revert the file. Press **Y** to confirm that you want to revert the file. If you do not want to proceed, press **Ctrl+C** or press **N**.

If you confirm that you want to revert a file in the active file system, the file is overwritten by the version in the Snapshot copy.

SnapRestore Technology Versus Copying

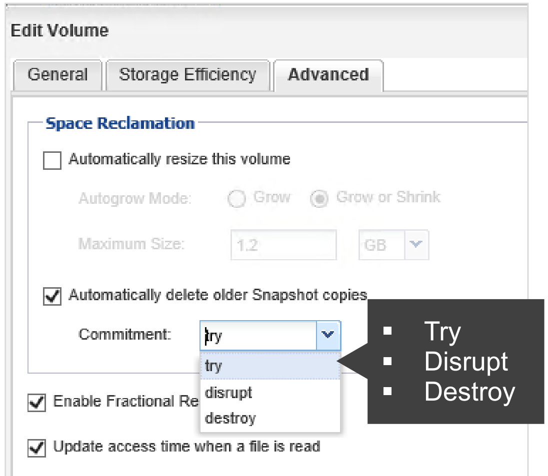
If a file is large (such as a database), you should use SnapRestore technology to revert instead of copying the file:

- Copying requires double the storage and time.
- Reverting saves time and reinstates the data.
- For reliability, NetApp recommends SnapRestore technology rather than alternative technologies.

 28

Whether you restore by copying files from a Snapshot directory or from tape, copying large quantities of data can be time consuming. Instead, use the SnapRestore function to restore by reverting the volume or file.

Snapshot Automatic Delete




```
::> volume snapshot autodelete modify -vserver svm4 -volume svm4_vol_002 -
enabled true
```


Snapshot automatic delete determines when or whether Snapshot copies are automatically deleted. The option is set at the volume level.

When set to *try*, the Snapshot copies (which are not locked by any application) and the LUN, NVMe namespace, or file clones that are not configured as preserved are deleted.

When set to *disrupt*, the Snapshot copies that are not locked by data-backing functionalities (such as volume clones, LUN clones, NVMe namespace clones, and file clones), LUN, NVMe namespace, or file clones (which are not configured as preserved) are deleted. In the *disrupt* mode, the Snapshot copies that are locked by data protection utilities such as SnapMirror software and Volume Move can be deleted. If such a locked Snapshot copy is deleted during the data transfer, the transfer is aborted.

When set to *destroy*, the Snapshot copies locked by the data backing functionalities are deleted. In addition, all the LUN, NVMe namespace or file clones in the volume are deleted.

Lesson 3
Back up and Replicate Data

Disaster Recovery and Business Continuance

There are two reasons for backing up and replicating data:

- **Disaster Recovery.** The ability to recover data that has been deleted, corrupted, infected by a virus, or physically lost due to a disaster.
  - Network Data Management Protocol (NDMP) backup
  - SnapVault
- **Business Continuance.** Using up-to-date replicas of data to keep a business operating despite a disaster.
  - SnapMirror
  - MetroCluster cluster configuration
- Both are constrained by Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

 31

Regardless of how resilient a storage system is, there are some events which can result in the corruption or loss of data. To reduce the impact of these events, you make backup copies and replicas of the data. Whether you do both or only one is determined by your business needs. The two primary business needs are disaster recovery and business continuance.

For disaster recovery, the primary goal is the ability to restore the data. The amount of time required to recover the data is secondary. Disaster recovery is the least expensive option so is often used by companies with limited budgets or less reliance on data. The two primary ONTAP feature used to create disaster recovery backups are Network Data Management Protocol (NDMP) backups and SnapVault.

For business continuance, the primary goal is for the company to continue doing business while recovery from a disaster. Business continuance is expensive because it generally requires the duplication of the production compute, storage, and network infrastructure. SnapMirror is the primary ONTAP feature used to accomplish business continuance. MetroCluster configurations are hardware and software solution to provide business continuance.

RTO

The RTO is the amount of time within which the service, data, or process must be made available again to avoid undesirable outcomes. Essentially, how long the business can tolerate an outage.

RPO

The RPO is a point to which data must be restored or recovered to be acceptable to the organization's acceptable data loss policy. Essentially, how much data the business can tolerate to lose.

NDMP Backup

NDMP is the industry standard protocol that third-party backup applications use to back up data to physical or virtual tape devices. Two NetApp ONTAP features use NDMP:

- **Dump**. Dump is a Snapshot copy-based backup for entire volumes down to a single file. Dump supports baseline, differential, and incremental backups. Dump is the primary method for performing backups.
- **SMTape**. SMTape (formerly called SnapMirror-to-Tape) is a Snapshot copy-based solution that backs up blocks of data to tape. SMTape works only at the volume level but supports baseline, differential, and incremental backups. SMTape is used primarily to back up Snapshot copies and to *seed* SnapMirror destination volumes.

 32

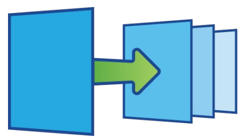
NDMP is an industry standard protocol for communication between storage devices and backup devices, such as tape drives. ONTAP software has two features that use NDMP for data backup: Dump and SMTape.

Dump is a backup application that traces its roots to the UNIX file system. In ONTAP software, Dump can use a Snapshot copy as its source to back up an entire volume or a single file. Through third-party backup applications, Dump can be used to create baseline, incremental, and differential backups.

SMTape uses the SnapMirror engine, discussed a little later, to back up blocks of data rather than files. (Think of SMTape as a SAN protocol and Dump as a NAS protocol.) Although SMTape can be used for daily backup, the feature is most frequently used to seed a remote SnapMirror destination for large volumes. Rather than send a large amount of data over the network to the destination, SMTape creates a set of tapes that is shipped to the destination and recovered locally onto the destination volumes. SnapMirror replication is then initiated, and only the blocks that are new or changed since the tapes were created are transferred over the network.

SnapVault

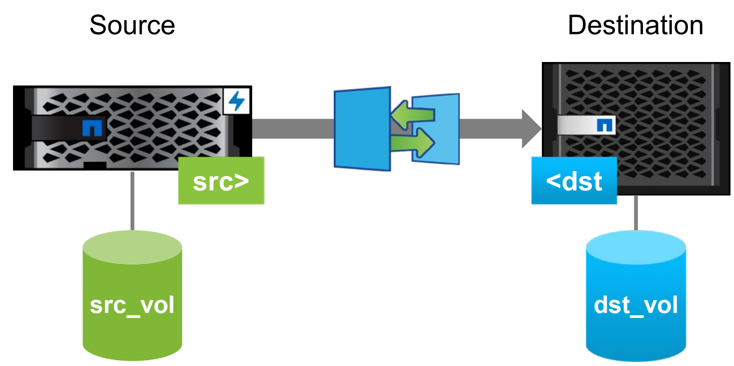
- SnapVault creates read-only backup copies on a destination volume.
- SnapVault is frequently used to backup multiple production clusters to a few remote high-capacity disaster recovery clusters.
- Reasons for using SnapVault instead of NDMP dump backups:
  - Data is stored on drives so faster to access and to recover
  - Can store hundreds of daily backups often for lower costs than tape



SnapVault provides a backup function similar to a backup to tape. On a scheduled basis, a volume Snapshot copy is backed up over the network to a destination volume. Just like tapes, multiple copies can be retained to store all the changes made to files in the volume. SnapVault is frequently used to consolidate the backup of small, remote office storage systems to a storage system with a high storage capacity. Although SnapVault is similar to dump backups to tape, it has two signification advantages. The first advantage is the backed-up data is always online and available. The second is the economies of scale often make it less expensive than using tapes. Tapes have the cost of media, the administrative overhead to load and remove them from the tape libaries, and ongoing expenses for the physical transport and storage costs at archive facilities like Iron Mountain.

SnapMirror Technology

SnapMirror technology enables the mirroring of volumes to other local or geographically remote AFF or FAS storage systems or to tape drives.



SnapMirror technology is an ONTAP feature that enables you to replicate data for business continuance. SnapMirror technology enables you to replicate data from specified source volumes to specified destination volumes.

You can use SnapMirror technology to replicate data within the same storage system or between different storage systems.

After the data is replicated to the destination storage system, you can access the data on the destination to perform the following actions:

- Provide users immediate access to mirrored data if the source fails
- Restore the data to the source to recover from disaster
- Archive the data to tape
- Balance resource loads
- Back up or distribute the data to remote sites

SnapMirror Features and Benefits

- The SnapMirror destination is a replica. Changes to the source are mirrored to the destination.
- Updates to the destination can be made frequently because only new and changed data blocks, rather than entire files, are sent.
- SnapMirror technology uses deduplication and compression and supports multiple paths (Ethernet or FC) to keep latency low and network bandwidth needs to a minimum.
- For backup and recovery, NetApp SnapCenter software manages application and database consistent backups, verification, cloning, and recovery.

Unlike a Dump or SnapVault backup, which requires a backup window, SnapMirror replicas can be created and updated as frequently as every five minutes. Only the new or changed blocks in a file, rather than the entire file, are sent to the destination. Deduplication and compression provide further efficiencies. Applications like databases cannot be easily recovered by simply copying their files from a backup. The data must be *quiet* during the backup, and the state of the application must be preserved to create what is known as a *crash consistent* backup. NetApp SnapCenter software automates the work of creating and recovering crash consistent backups or replicas.

MetroCluster Configuration

- A MetroCluster configuration geographically separates the partners in HA pairs.
- If a disaster damages the physical storage hardware or network access to the hardware, the cluster can continue to serve data.
- MetroCluster configuration is not an add-on feature or upgrade.
  Clusters must be physically installed and configured in a MetroCluster configuration.

Earlier, the course discussed cluster configurations and MetroCluster cluster configurations. In a standard cluster configuration, the partners in an HA pair are often physically located in the same cabinet. If the cabinet is destroyed by a fire or earthquake, the entire HA pair is lost. In a MetroCluster cluster configuration, the HA partners are geographically separated to reduce the likelihood of a disaster taking down both partners. Because of the complexity and physical requirements of a MetroCluster configuration, this type of cluster configuration must be decided on when the cluster is purchased. MetroCluster configurations are popular in regions where geography, politics, and national borders make the use of remote disaster-recovery locations difficult.

Lesson 4
Compliance

SnapLock

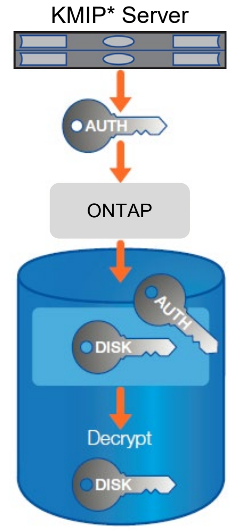
- SnapLock is a high-performance compliance solution for organizations that use WORM (Write Once Read Many) storage to retain files in unmodified form for regulatory and governance purposes.
- Files are locked from modification for an administrator-defined length of time.
  - Files in Snapshots and SnapMirror destinations are also locked until the time limit for all files expires.
- Requires a license
- Can be used in conjunction with storage encryption.
- Recommended Practice: Learn and practice using SnapLock on a simulator before implementing it because some mistakes are not reversible.

SnapLock is a licensed feature that allows you to lock files down so they cannot be altered in any way for pre-determined amount of time. Companies that handle insurance, mortgage and other legal and financial documentation use SnapLock to ensure digital files cannot be altered and therefore legally indefensible. SnapLock has a learning curve and mistakes can result in files, or entire aggregates, that cannot be deleted until the lock expires (locks are often set for many years). If you plan to implement SnapLock, or take over administration of cluster using SnapLock, practice on a sim before making any changes to a production cluster.

Lesson 5
Storage Encryption

What Is NetApp Storage Encryption (NSE)?

- NSE is an ONTAP feature that provides support for self-encrypting drives (SEDs).
- SEDs protect data when it is at rest (when the drive is powered off).
- NSE manages the authorization process with a key management server to grant storage controllers access to the encrypted data on the drives.
- The encryption process is transparent to end users and has a minimal impact on performance.



* KMIP: Key Management Interoperability Protocol

A standard drive stores data unencrypted. If the drive is lost or stolen, the data is vulnerable to unauthorized access. Theft of storage devices is a very real threat for financial, healthcare, and government institutions. To solve this issue, drive manufacturers created drives with built-in encryption called self-encrypting drives (SEDs). All data written to SEDs is encrypted and can be read only by systems that have successfully completed an authentication process with a key management server. NetApp Storage Encryption (NSE) is an ONTAP feature to support the use of self-encrypting drives.

After NSE is enabled and an authorization key is created, a FAS or AFF system must send a password to the key server to allow access to the encrypted drives. When the storage system is running and the drives are powered on, the process is transparent to end users, and performance is barely affected. Only when the drives are offline or not connected to an authenticated system is the data indecipherable.

The one caveat of NSE is that all drives attached to a standalone system or an HA pair of systems must be self-encrypting drives. Mixing of encrypting and non-encrypting drives is not supported. Multi-node clusters do support mixing HA pairs use SEDs and HA pairs with standard drives.

Onboard Key Management

- The Onboard Key Manager (OKM) is a less expensive alternative to external KMIP servers. With onboard key management, the storage servers manage their own authentication to the NSE drives.
- You should not use OKM if any of the following conditions are true:
  - Your storage systems must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
  - You need a centralized, multicluster solution. OKM works only for the cluster that hosts the keys.
  - Your business requires the added security of storing authentication keys separate from the encrypted data.

41

A low-cost alternative to key management servers is to enable Onboard Key Manager (OKM). With OKM, the storage systems manage the authentication keys that unlock the NSE drives. This approach helps to ensure that encryption protects data at rest. However, OKM is not compliant with Federal Information Processing Standards (FIPS) and does not work with more than one cluster. OKM also has a physical security flaw: Unauthorized users with physical access to the storage systems and disks can access the encrypted data.

NetApp Volume Encryption (NVE)

- Software-based, data-at-rest encryption solution:
  - Encrypts sensitive data, without relying on NSE drives
  - Uses Advanced Encryption Standard (AES)-256 encryption
  - Requires a license
- Each data volume has a unique encryption key:
  Decide which volumes to encrypt and which to leave unencrypted.
- Encryption requires zero management:
  Snapshot copies and FlexClone volumes are also encrypted.

NSE has some caveats that can be problematic in environments where not all data needs to be encrypted. NetApp Volume Encryption (NVE) provides a flexible solution. Using onboard key management, you can select a volume to encrypt and assign the volume a unique encryption. Because the data blocks in the volume are encrypted, the encryption follows the blocks into Snapshot copies and FlexClone volumes.

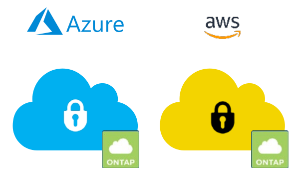
Additional Storage Security Features

Honor "right to be forgotten."

Manage new data-compliance regulations better with crypto-shredding of data via secure purge.

Protect systems in transit.

Protected controller reboot and secure Unified Extensible Firmware Interface (UEFI) boot prevent unwanted access of systems outside the data center.



Worry less about cloud security.

NVE support for NetApp Cloud Volumes ONTAP provides FIPS 140-2 certified encryption in the cloud.

? More info in Addendum

Secure purge shreds data in the volume and Snapshot copies to meet data-compliance regulations.

For systems that move between data centers, protected controller reboot prevents unauthorized access if the storage hardware is stolen.

NVE also works to protect data in the cloud.

Learn more about secure purge and secure boot in the module Addendum.

Knowledge Check: Question

True or False: Data can be written to a Snapshot copy.

a. True
b. False

Additional Data-Protection Learning

Learn about advanced topics like configuration of intercluster replication, fan-in and fan-out strategies, and NetApp data-protection interfaces.

- ONTAP Data Protection Fundamentals (online course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000024323
- ONTAP Data Protection Administration (two-day instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022724
- ONTAP Compliance Solutions Administration (one-day instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000024832
- ONTAP MetroCluster Installation (two-day instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022663

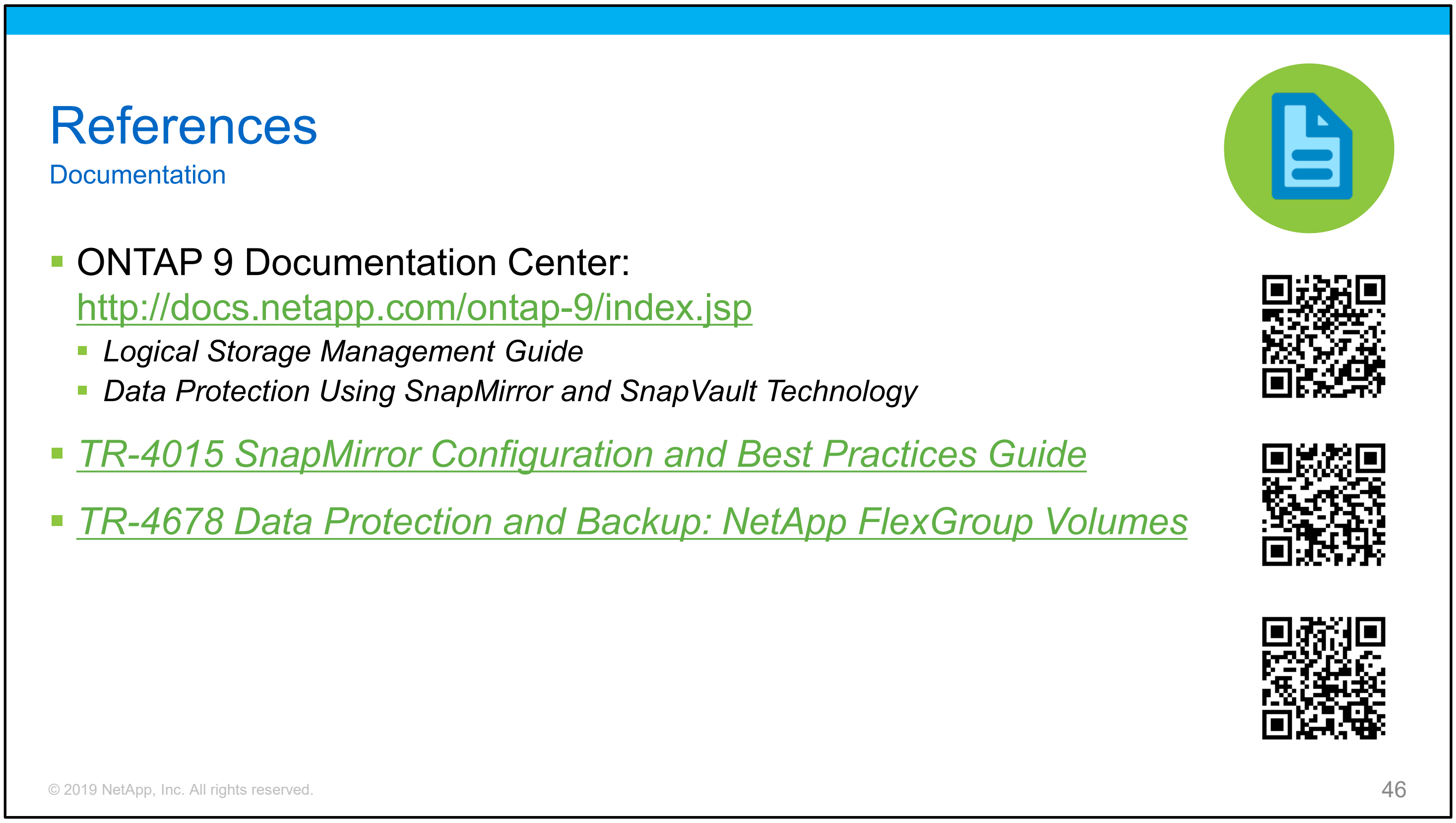
ONTAP Data Protection Fundamentals (online course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000024323

ONTAP Data Protection Administration (two-day instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022724

ONTAP Compliance Solutions Administration (one-day instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000024832

ONTAP MetroCluster Installation (two-day instructor-led course)
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022663

NOTES: Courses are regularly revised and updated. Check the Learning Center for the latest versions of the courses and offerings.



ONTAP 9 Documentation Center:

http://docs.netapp.com/ontap-9/index.jsp

Logical Storage Management Guide

Data Protection Using SnapMirror and SnapVault Technology

TR-4015 SnapMirror Configuration and Best Practices Guide

TR-4678 Data Protection and Backup: NetApp FlexGroup Volumes

References

Videos

- NetApp SnapCenter Backup Management Software
  https://www.youtube.com/watch?v=ejsq7nNawI4
- ONTAP Data Security Overview
  https://www.youtube.com/watch?v=cY_iuayAL2M
- How to Use SnapLock feature in ONTAP 9
  https://www.youtube.com/watch?v=JUYtta3Ymdw

NetApp SnapCenter Backup Management Software https://www.youtube.com/watch?v=ejsq7nNawI4

ONTAP Data Security Overview https://www.youtube.com/watch?v=cY_iuayAL2M

How to Use SnapLock feature in ONTAP 9 https://www.youtube.com/watch?v=JUYtta3Ymdw

Module Review

This module focused on enabling you to:

- Manage Snapshot copies
- Restore data from Snapshot copies
- Back up and replicate data
- Use encryption to prevent unauthorized access to data

ACTION: Complete an Exercise

Module 8: Managing Snapshot Copies and Encrypting a Volume

Duration: 45 minutes

Access your exercise equipment.

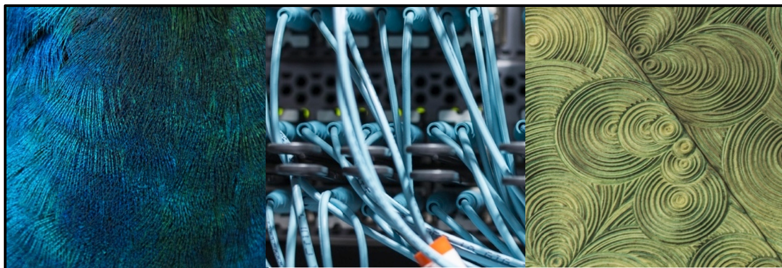
Use the login credentials that your instructor provided to you.

Complete the specified exercises.

- Go to the exercise for the module.
- Start with Exercise 8-1.
- Stop at the end of Exercise 8-2.

Participate in the review session.

- Share your results.
- Report issues.



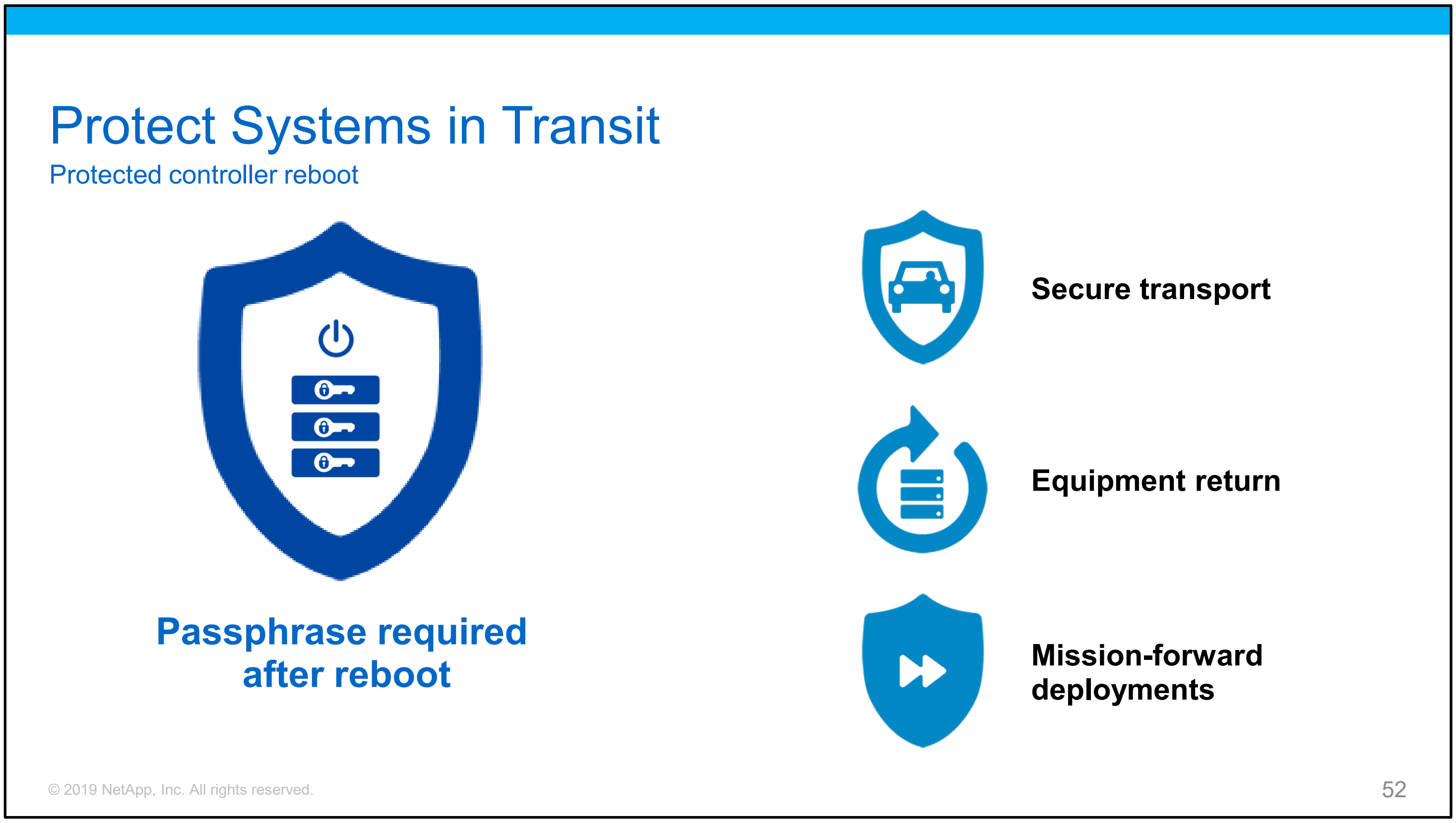
Addendum
Secure Purge and Secure Boot

Manage Data Spillage and Right to Erasure via Secure Purge

NVE for General Data Protection Regulation (GDPR) and US Public Sector

- Immediate need to destroy data:
  - When data with different classification levels accidentally ends up in the same volume
  - To delete user data cryptographically to satisfy GDPR requirements
- Cryptographically shred a single file from an encrypted volume when the file is not recoverable from the drives because the key has been deleted.

Secure purge enables storage administrators to selectively destroy data blocks rather than the entire LUN or volume, to meet security and compliance requirements.

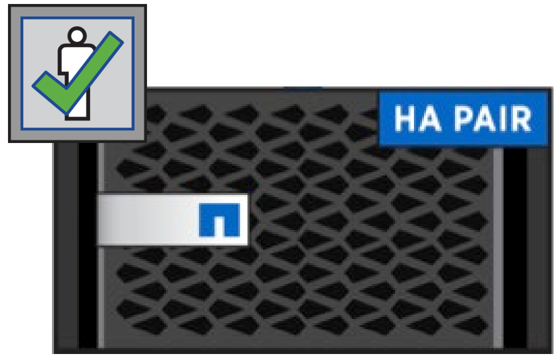


For customers like the military, which has clusters on mobile platforms (trucks, ships, aircraft), the data on the system must not be accessible if unauthorized users gain access to the storage system. NSE disk and volume encryption serves as a first line of defense. However, that defense can be overcome by physically hacking the storage. Protected controller reboot renders the hardware inoperable until the correct passphrase is supplied.

Secure Boot on Next-Generation Platforms

UEFI

- **Verifies** that software is **genuine NetApp ONTAP software during boot**
- **Prevents hacked or pre-release versions** of ONTAP software any time the system boots
- Signed ONTAP images are **verified by the boot loader**
- Supported platforms: NetApp AFF A800, AFF A220, FAS2750, FAS2720, and newer



Secure boot is another security feature that is designed to protect all new AFF and FAS systems from use or exploitation via hacked or pre-release versions of ONTAP. The feature protects customers from purchasing gray-market or stolen hardware.

Module 9
Storage Efficiency

About This Module

This module focuses on enabling you to:

- Implement storage-efficiency features
- Use FlexClone software volumes

Lesson 1
Thin Provisioning

Thick and Thin Provisioning of Volumes

- Thick provisioning of volumes (guarantee = volume):
  - Requires reserved space within the aggregate for volume creation
  - Helps to prevent overcommitment of an aggregate
  - Simplifies storage management
- Thin provisioning of volumes (guarantee = none):
  - Does not require reserved space within the aggregate for volume creation
  - Enables more aggressive allocation
  - Does not prevent overcommitment of an aggregate
  - Requires more complex storage management

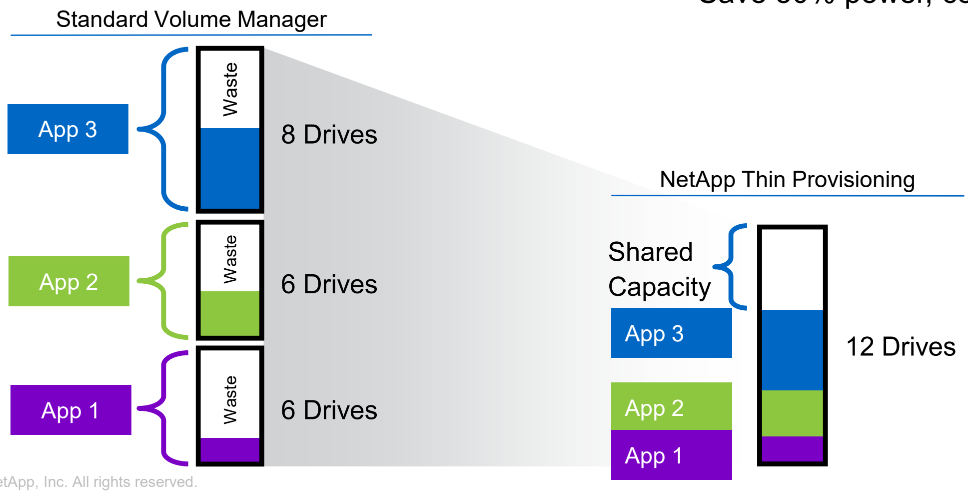
Administrators can manage storage systems by allocating volumes in one of two ways:

- Thick provisioning of volumes uses a space guarantee for a volume or file. A volume guarantee requires reserved space in the aggregate when the volume is created. A file guarantee provides guaranteed space for LUNs in the volume. Thick provisioning is a conservative approach that prevents administrators from overcommitting space to an aggregate. Thick provisioning simplifies storage management at the risk of wasting unused space.
- Thin provisioning of volumes uses a space guarantee of none, meaning that no space within the aggregate is reserved for the volume when the volume is created.

NOTE: As of NetApp Data ONTAP 8.3, the file guarantee is no longer supported.

Thin Provisioning

- Typical: Only 40% of provisioned storage is used.
- NetApp: More than 70% is used.
  - Buy 50% less storage.
  - Save 50% power, cooling, and space.

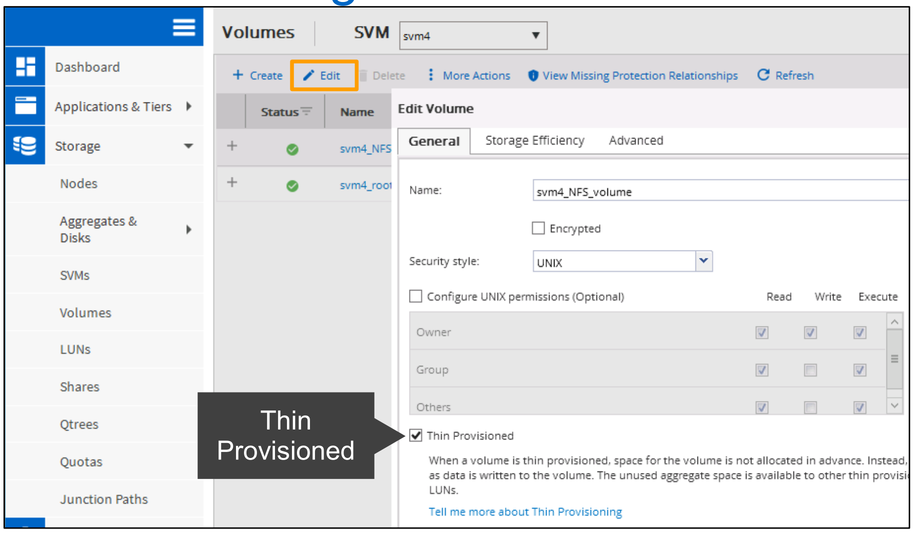


 5

When you compare the NetApp storage use approach to competing approaches, one feature stands out. Flexible dynamic provisioning with FlexVol technology provides high storage-use rates and enables customers to increase capacity without the need to physically reposition or repurpose storage devices. NetApp thin provisioning enables users to overcommit data volumes, resulting in high-use models. You can think of the approach as “just-in-time” storage.

To manage thin provisioning on a cluster, use the volume command.

Enable Thin Provisioning




```
::> volume modify -vserver svm4 -volume svm4_vol_002 -guarantee none
```

Lesson 2
Deduplication and Compression

Volume Efficiency

Deduplication

- Elimination of duplicate data blocks
- Inline or postprocess options
- Inline deduplication for AFF and Flash Pool systems to reduce the number of writes to solid-state drives (SSDs)

Data compression

- Compression of redundant
- data blocks
- Inline or postprocess options
- Two compression methods:
  - **Secondary:** 32KB compression groups
  - **Adaptive:** 8KB compression groups, which improve read performance

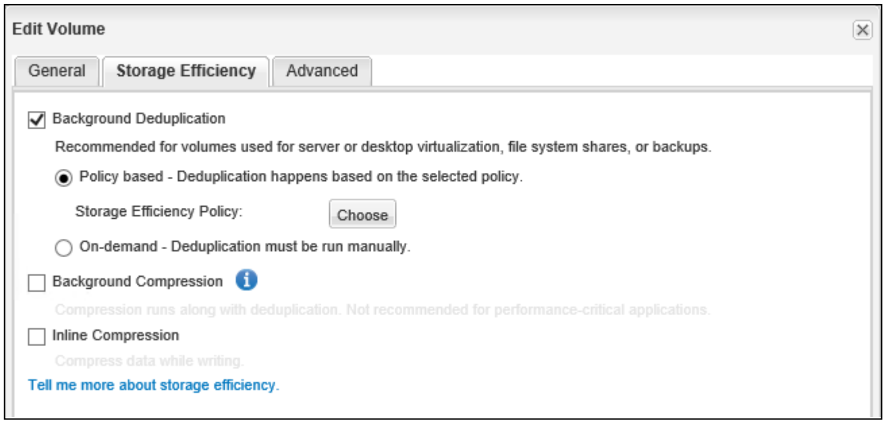
ONTAP software provides two features that can increase volume efficiency: deduplication and data compression. You can run deduplication and data compression together or independently on a FlexVol volume to reduce the amount of physical storage that the volume requires.

To reduce the amount of physical storage that is required, deduplication eliminates the duplicate data blocks and data compression compresses redundant data blocks. Depending on the version of ONTAP software and the type of drives that are used for the aggregate, the volume efficiency features can be run inline or postprocess.

Inline deduplication can reduce writes to solid-state drives (SSDs). Starting with Data ONTAP 8.3.2, inline deduplication is enabled by default on all new volumes that are created on AFF systems. Inline deduplication can also be enabled on new and existing Flash Pool volumes.

Data compression combines multiple 4KB NetApp WAFL blocks into compression groups before compression. Starting with Data ONTAP 8.3.1, two data compression methods can be used: secondary and adaptive.

Enable Deduplication




```
::> volume efficiency on -vserver svm4 -volume svm4_vol_002
```


Deduplication improves the efficiency of physical storage space by eliminating redundant data blocks within a FlexVol volume. Deduplication works at the block level on an active file system and uses the NetApp WAFL block-sharing mechanism. Each block of data has a digital signature that is compared with all the other blocks in the data volume. If an exact match is identified, the duplicate block is discarded. A data pointer is modified so that the storage system references the copy of the data object that is stored on disk. The deduplication feature works well with datasets that have large quantities of duplicated data or white space. You can configure deduplication operations to run automatically or according to a schedule. You can run deduplication on new or existing data on any FlexVol volume.

Characteristics of Data Compression

- Inline compression:
  - Parallelism increases.
  - Path length decreases.
  - On FAS systems, latency increases.
- Postprocess compression:
  - Uncompressed data is compressed during idle time.
  - Only previously uncompressed blocks are compressed.
  - Compression occurs before deduplication.
  - ONTAP software can detect incompressible data before wasting cycles.

For more information, see TR-4476: *NetApp Deduplication, Compression, and Compaction Deployment and Implementation Guide*.

 10

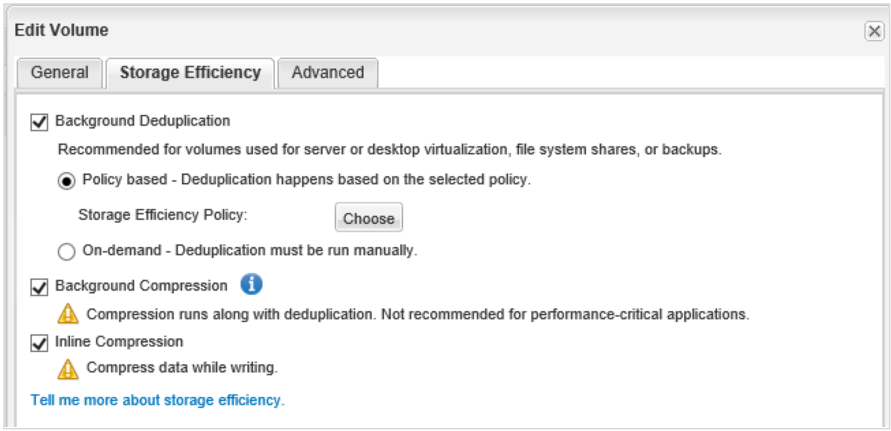
There are two types of data compression: inline and postprocess.

With inline compression, all writes to a volume are compressed immediately before being written to the volume. Inline compression increases parallelism because all compression and decompression algorithms are multiprocessor-capable and because writes are compressed outside the consistency point. Because operations do not need to be suspended and resumed, inline compression also reduces path length. However, because processing is required for compression and decompression, latency affects performance on FAS systems due to mechanical operations in hard drives.

Postprocess compression runs as a background task. Uncompressed data that is written after deduplication is compressed and rewritten to the volume when the controller is not busy. If inline and postprocess compression are enabled for the same volume, postprocess compression compresses only the blocks on the volume that were not compressed previously. If compression and deduplication are enabled, compression always occurs before deduplication.

For more information, see TR-4476: *NetApp Deduplication, Compression, and Compaction Deployment and Implementation Guide*.

Configuring Data Compression




```
::> volume efficiency modify -vserver svm4 -volume svm4_vol002   -
compression true -inline-compression true
```

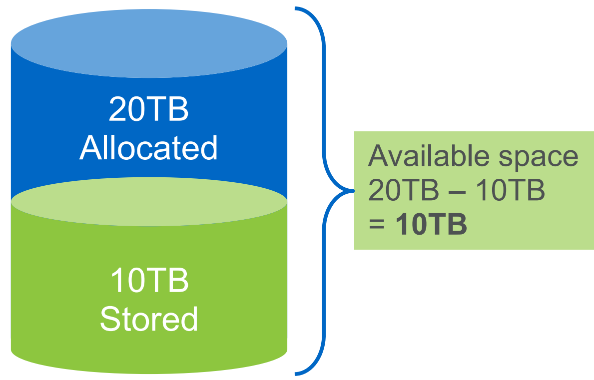

Data compression enables you to reduce the physical capacity that is required to store data on a cluster, by compressing data blocks within a FlexVol volume. Data compression is available only on FlexVol volumes that are created on 64-bit aggregates. Data compression optimizes the storage space and bandwidth that are required to replicate data during volume operations, such as moving volumes and performing SnapMirror transfers. You can compress standard data files, virtual disks, and LUNs. You cannot compress file system internal files, alternate data streams, or metadata.

To manage compression on a cluster, use the `volume efficiency` command.

The Storage Service Provider Conflict

Charge for data stored

Storage service providers want to charge customers for the amount of data that they store.

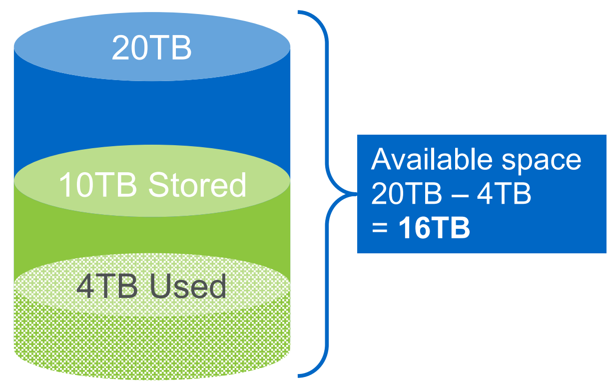


Assume that, as a service provider, you have provisioned a 20TB volume to a customer and the customer stores 10TB of data in the volume. As the provider, you want to charge the customer for storing 10TB of data.

The Storage Service Provider Conflict

Storage efficiencies provide more space

- Storage efficiencies gave customers more storage space than they paid for.
- Before ONTAP 9.4, ONTAP software provided reporting only for consumed physical storage. Storage service providers could charge only for space consumed, not for the amount of data stored.



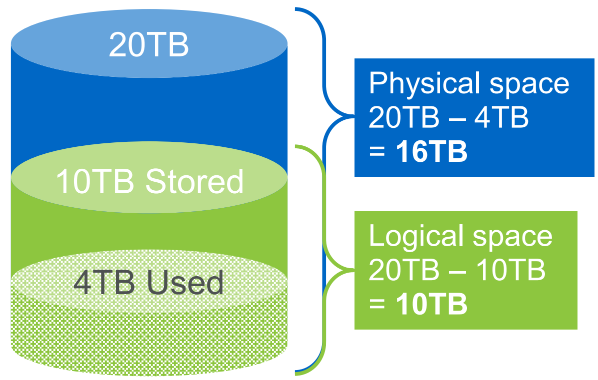
 13

With ONTAP efficiency technologies, if the 10TB of data is reduced to 4TB, the actual space used in the volume is shown as 4TB.

The customer sees that the available space is 16TB. This does not help you charge the customer based on the actual amount of data stored regardless of storage efficiencies.

Logical Space Reporting

Volume option: `-is-space-reporting-logical [true | false]` shows customers the consumed logical space rather than the consumed physical space.



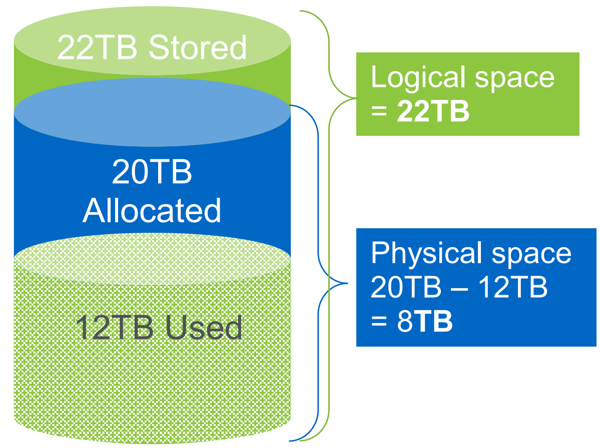

```
volume modify -vserver SVM-name -volume volume-name -size volume-size -is-space-reporting-logical true
```


Logical space enforcement and reporting enable service providers and large enterprises with multiple business units to use chargeback mechanisms to charge their customers and business units.

ONTAP 9.4 software introduced the logical space reporting feature. The feature enables service providers and larger enterprises to report to customers the logical space used instead of the physical space used. With the feature, the storage efficiencies are hidden from customers, who see the available physical space.

Logical Space Enforcement

- Storage efficiencies enable customers to store more data than the physical space that is allocated.
- Volume option: `is-space-enforcement-logical [true | false]` ensures that customers cannot store more than the logical space that is allocated, regardless of the physical space that is consumed.
  Error messages are generated when stored data reaches 95%, 98%, and 100% of logical space limits.



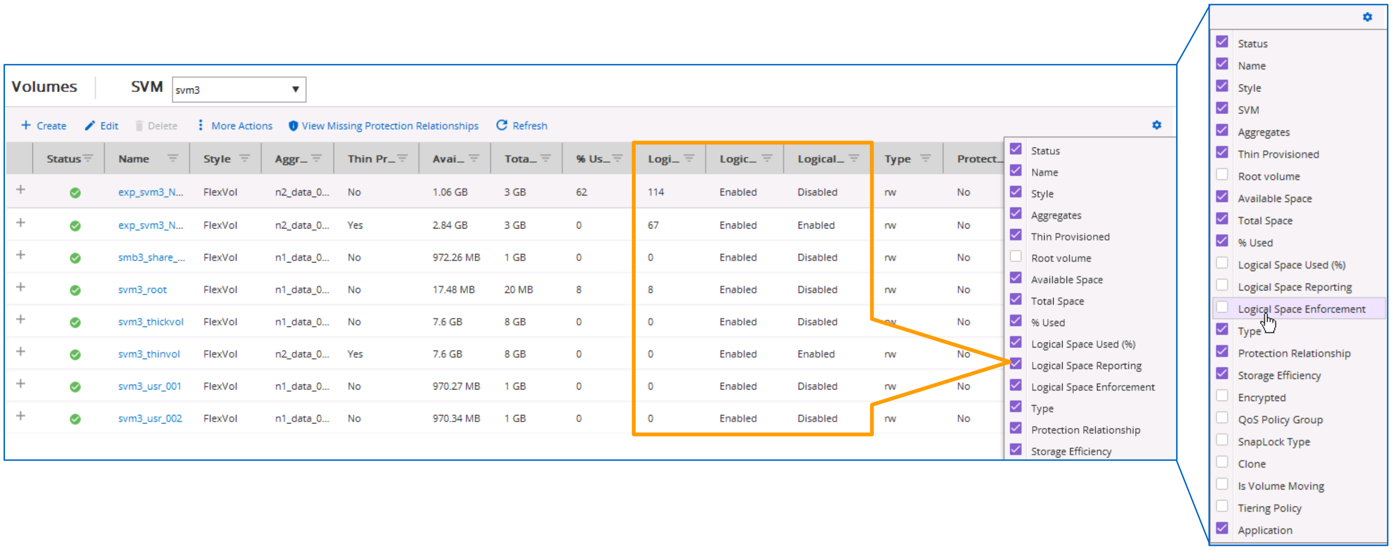
With ONTAP storage efficiencies, the customer can store more data than the logical available space. The logical space reporting shows that the customer is using more than the volume size that is provisioned.

To overcome this issue, ONTAP 9.5 software introduces the enforcement of logical space. With the logical space enforcement feature, customers cannot store data into a volume if the logical space limit is reached. Thus, the customer cannot store beyond 20TB of data even though physical space is available. ONTAP systems trigger error messages as the customer reaches the logical space limit at 95%, 98%, and 100%. These space limits are predefined and nonconfigurable. Use an external monitoring application to set alerts for custom space limits.

Any new writes to the volume when the logical space used is 100% return an ENOSPC (out of space) error message.

Logical Space Report in OnCommand System Manager

Default columns



16

Beginning with ONTAP 9.5, you can use System Manager to enable the display to users of the logical space used in a volume and how much storage space remains in a volume.

The percentage of logical space used is shown in the Logical Space Used (%) column of the Volumes on SVM page in System Manager.

When you enable the logical space reporting feature in ONTAP, System Manager displays the amount of used and available space in addition to the total space on a volume.

When used, logical space reporting shows the following columns to users in System Manager:

- Logical Space Used (%): the amount of physical space currently available on the volume
- Logical Space: whether the logical space reporting feature is enabled

The Total column, which shows the amount of used and available space, can appear greater than the provisioned space on the volume. The discrepancy occurs because the Total column includes any block savings that are achieved through deduplication, compression, and other space-saving capabilities.

NOTE: Logical space reporting is not enabled by default.

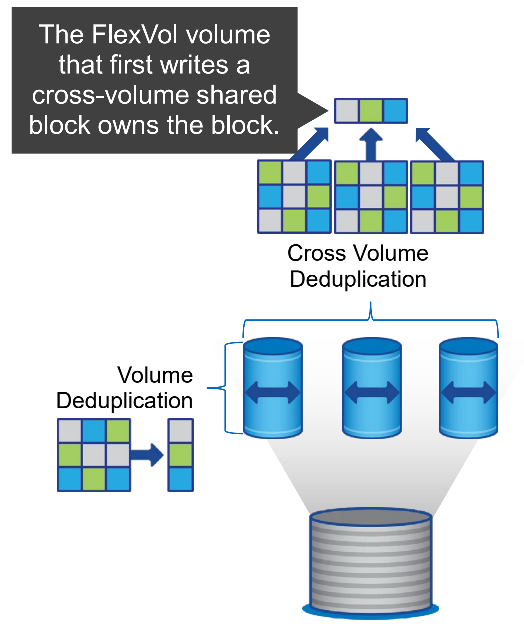
Lesson 3
Flash Efficiency

Aggregate Inline Deduplication

Overview

Aggregate inline deduplication enables block sharing across multiple volumes within an aggregate:

- Only available on AFF systems
- Uses the volume efficiency parameter:
  `-cross-volume-inline-dedupe`
- The FlexVol volume that first writes a cross-volume shared block owns the block.



More info in Addendum

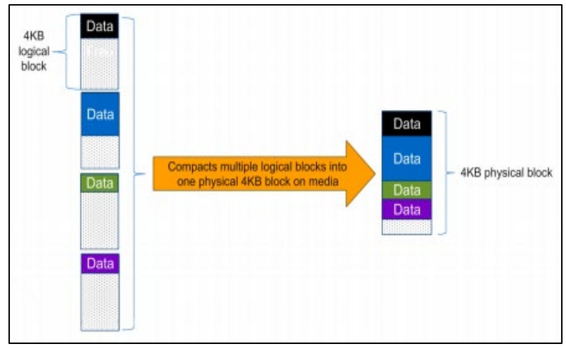
NOTE: Compressed and compacted blocks cannot be shared.

Aggregate inline deduplication is available only on AFF systems and is enabled by default . The feature can be enabled and disabled by using the volume efficiency parameter `-cross-volume-inline-dedupe`. Cross-volume blocks are owned by the FlexVol volume that wrote to the block first. Blocks that have been compressed or compacted cannot be shared.

For information about feature support, see the *Logical Storage Management Guide*.

Inline Data Compaction

- Writes multiple logical data blocks in the same volume to one 4KB block on storage:
  - Compaction occurs during the consistency point (CP) operation just before the write to media.
  - Compaction occurs after inline adaptive compression and inline deduplication.
- Provides additional space savings with highly compressible data
- Is enabled by default for new AFF systems but is disabled on FAS systems:
  - Optional policy for Flash Pool aggregates
  - Optional policy for hard disk-only aggregates



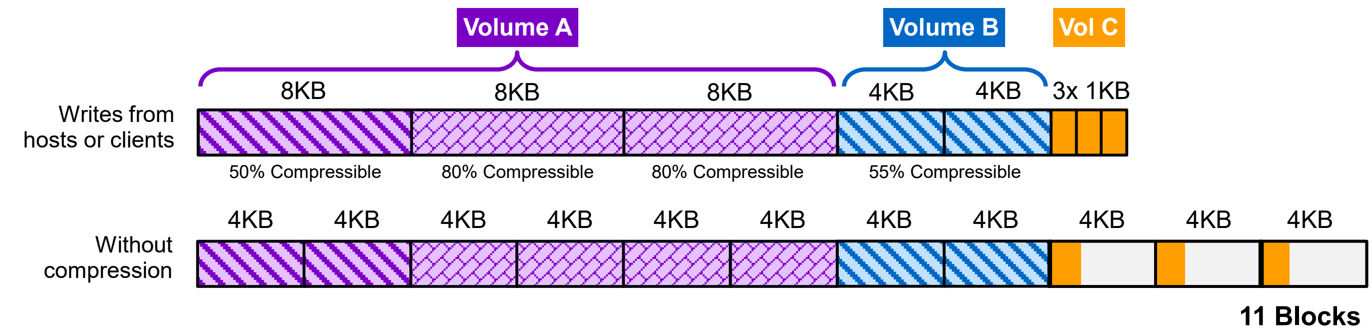
? More info in Addendum

 19

You can control inline data compaction on FAS systems with Flash Pool (hybrid) aggregates or HDD aggregates at the volume or aggregate level by using the `wafl compaction enable node shell` command. Data compaction is disabled by default for FAS systems. If you enable data compaction at the aggregate level, data compaction is enabled on any new volume that is created with a volume space guarantee of none in the aggregate. Enabling data compaction on a volume on an HDD aggregate uses additional CPU resources.

Storage Consumption

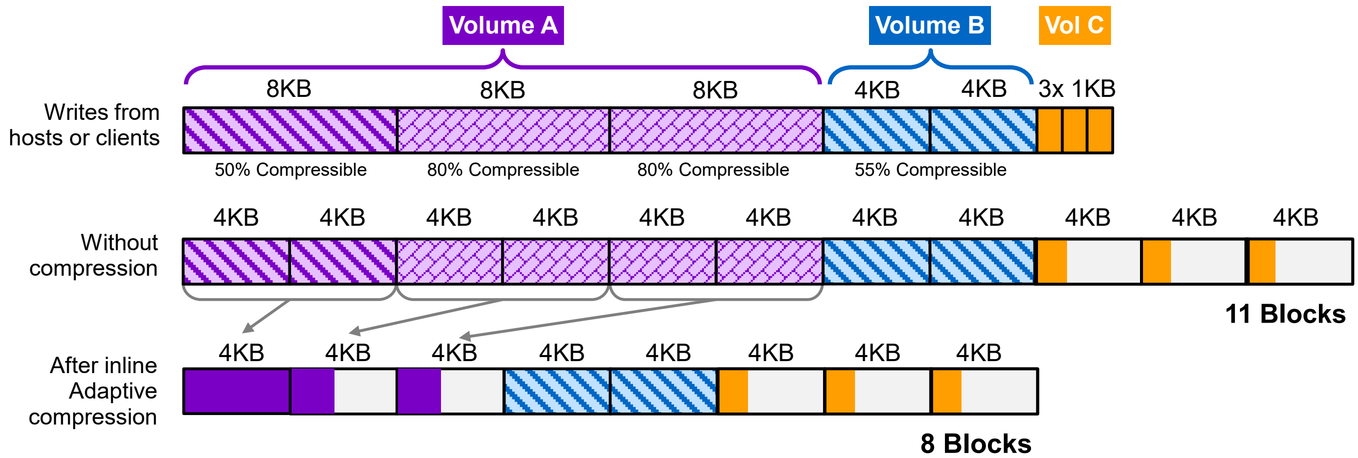
No inline storage efficiency



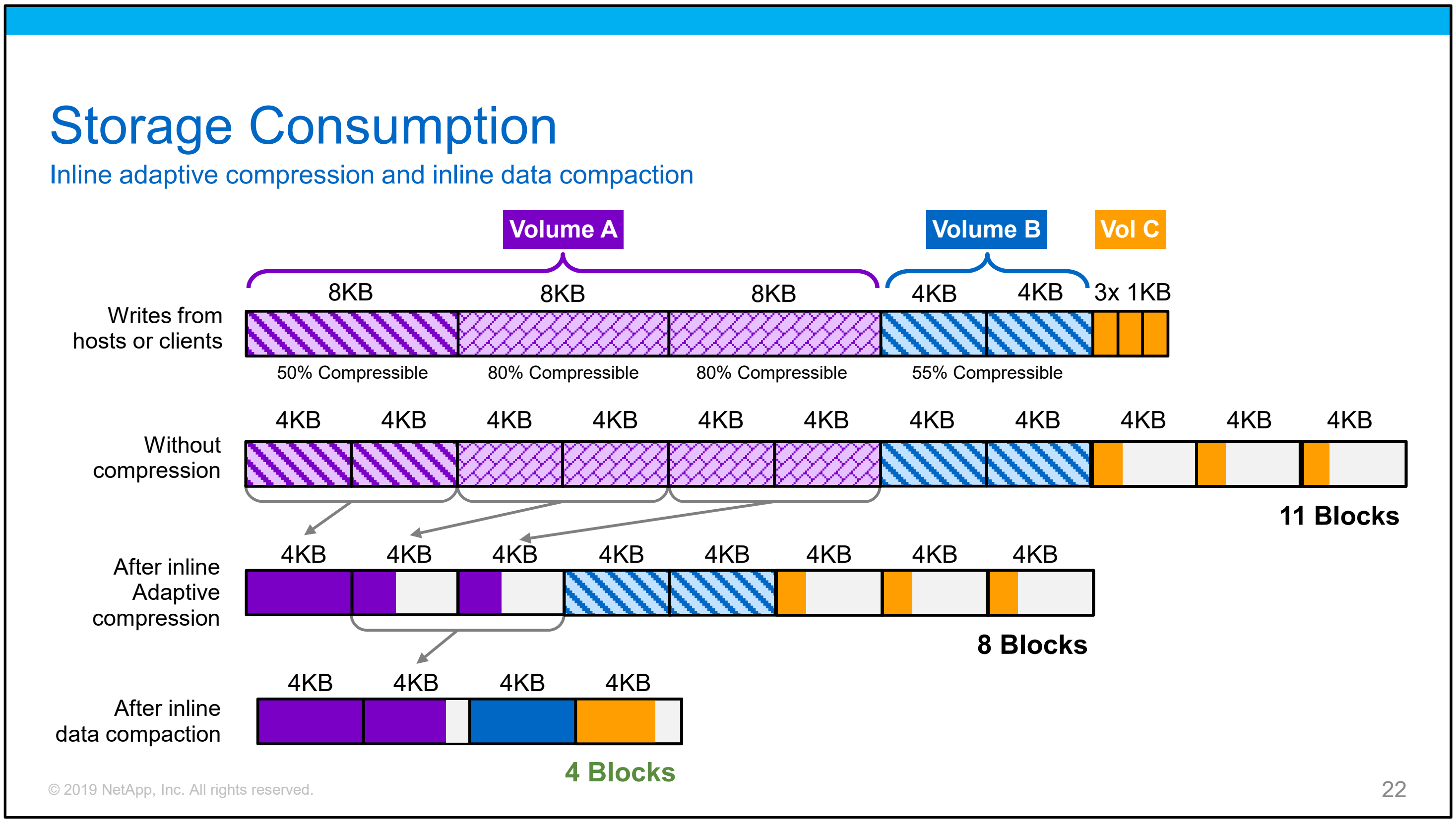
The figure shows the writes for a host or client and the amount of space on disk when no efficiency features are enabled.

Storage Consumption

Inline adaptive compression



The figure shows the default policy for AFF systems that run Data ONTAP 8.3.1 software and later.



The figure shows the default policy for AFF systems that run ONTAP 9 software.

Data compaction is an inline operation and occurs after inline compression and inline deduplication. On an AFF system, the order of execution is as follows:

1. Inline zero-block deduplication: All zero blocks are detected. No user data is written to physical storage. Only metadata and reference counts are updated.
2. Inline adaptive compression: 8KB logical blocks are compressed into 4KB physical blocks. Inline adaptive compression efficiently determines the compressibility of the data and doesn’t waste many CPU cycles trying to compress incompressible data.
3. Inline deduplication: Incoming blocks are opportunistically deduplicated to existing blocks on physical storage.
4. Inline adaptive data compaction: Multiple logical blocks of less than 4KB are combined into a single 4KB physical block, which maximizes savings. Also, 4KB logical blocks that inline compression skips are compressed to improve compression savings.

AFF Inline Storage Efficiency

ONTAP workflow

Inline Zero Block Deduplication

The process detects all zero blocks and eliminates those blocks first.

Inline Adaptive Compression

The data is scanned and compressed.

Inline Deduplication

The compressed blocks are scanned to identify duplicates:

- Duplicates within a volume
- Duplicates across volumes within an aggregate (if no duplicates are found within a volume)

Inline Data Compaction

Inline deduplication blocks are not compacted.

Other blocks (either compressed or uncompressed) are compacted, where possible.

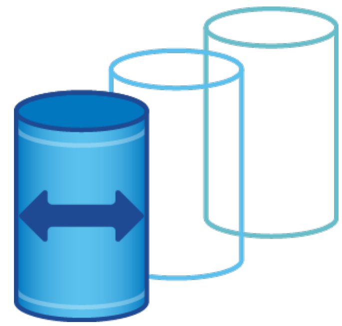
 23

Aggregate inline deduplication works seamlessly with other efficiency technologies, such as compression and inline zero-block deduplication.

Lesson 4
Volume and File Clones

FlexClone

- FlexClone uses blocks pointers to enable you to create multiple, instant dataset clones (files, LUNs, or entire volumes) with no storage overhead.
- FlexClone provides dramatic improvement for application testing and development environments:
  - Create an instantaneous replica of a file or LUN (such as an entire database).
  - Provision thousands of virtual machines (VMs) in seconds by cloning *golden images*.
- Clones can be split from the source but then make copies of all source blocks and consume an equal amount of storage space.



 25

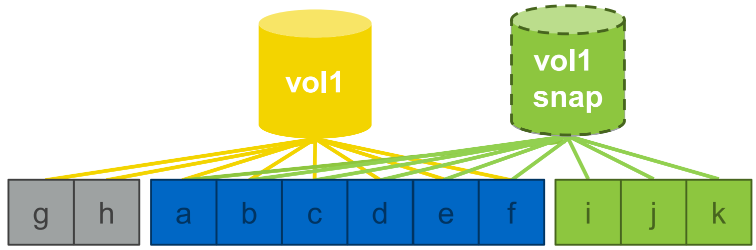
FlexClones are often referred to as *writable Snapshot copies*. By leveraging blocks pointers, you can create multiple, instant dataset clones—files, LUNs, or entire volumes—with no initial storage overhead. Only when data is added or changed in a clone is storage space consumed.

Clones are especially useful in test and development environments. Data can be replicated numerous times within seconds and used just like the source data, without concerns of damaging or destroying the source data. FlexClone software is also useful in virtual environments, where golden images of virtual machines can be cloned thousands of times.

Clones can be split from the source, but then make copies of all source blocks and consume an equal amount of storage space. This behavior is useful for upgrading or patching an application in a clone and then rolling it out by splitting off the clone and promoting it to production. Rollbacks can be as simple as promoting the source back into production.

How Cloning Works

- Make a Snapshot copy of the volume.
- Create a clone by adding another pointer to the blocks in the Snapshot (blocks A–H):
  - Modifications to the original volume are separate from modifications to the cloned volume (blocks G and H).
  - Modifications to the clone are separate from the original volume (blocks I – K) These blocks are the only drive space consumed by the clone.



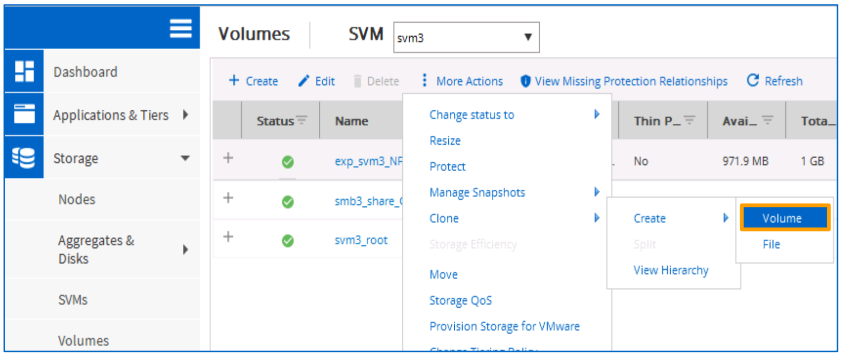
FlexClone volumes are managed similarly to regular FlexVol volumes, with a few key differences. FlexClone volumes have the following features:

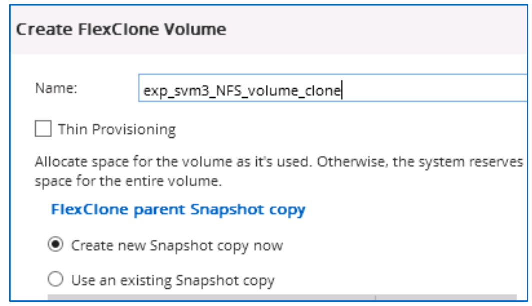
- FlexClone volumes are point-in-time, writable copies of parent volumes. The FlexClone volume does not reflect changes that are made to the parent volume after the FlexClone volume is created.
- FlexClone volumes are fully functional volumes that are managed, as with the parent volume, by using the vol command. As with parent volumes, FlexClone volumes can be cloned.
- FlexClone volumes are always in the same aggregate as parent volumes.
- FlexClone volumes and parent volumes share the same drive space for common data. This means that the process of creating a FlexClone volume is instantaneous and requires no additional drive space (until changes are made to the clone or parent).
- A FlexClone volume is created with the same space guarantee as the parent.
- You can sever the connection between the parent and the clone. This is called *splitting* the FlexClone volume. Splitting removes all restrictions on the parent volume and causes the FlexClone volume to use its own storage.

NOTE: When you split a FlexClone volume from its parent volume the following occurs:

- All existing Snapshot copies of the FlexClone volume are deleted.
- Creation of new Snapshot copies is disabled while the splitting operation is in progress.
- Quotas that are applied to a parent volume are not automatically applied to the clone.
- When a FlexClone volume is created, existing LUNs in the parent volume are also present in the FlexClone volume, but these LUNs are unmapped and offline.

Clone a Volume

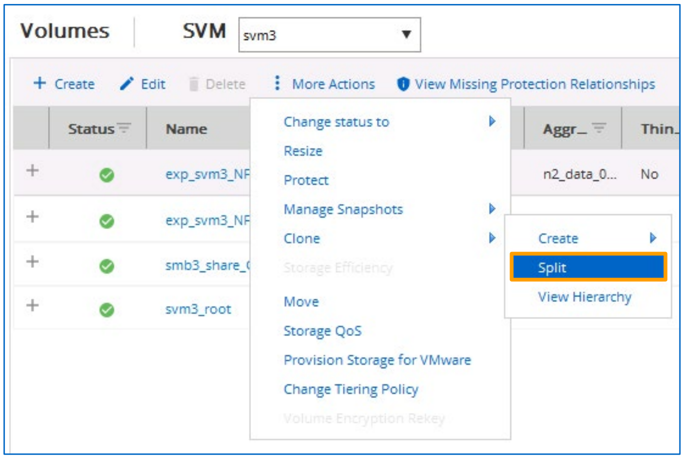


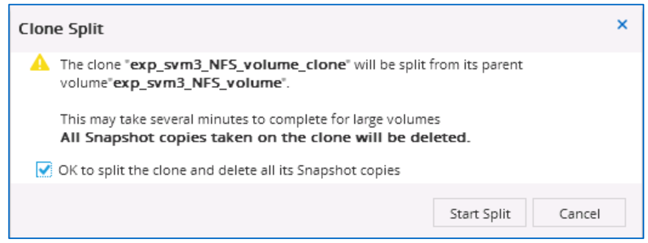



```
cluster2::> volume clone create -vserver svm3 -flexclone
exp_svm3_NFS_volume_clone -parent-volume exp_svm3_NFS_volume
```


To create a FlexClone volume, use the `volume clone create` command.

Split a Cloned Volume



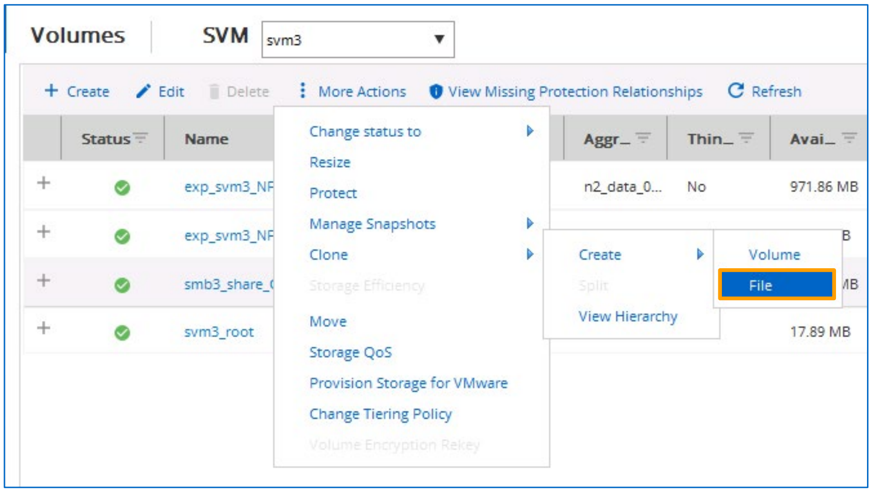



```
::> volume clone split start -vserver svm5 -flexclone svm5_vol_002_clone
```


28

To initiate a split of the clone from the parent, use the `volume clone split start` command.

Clone a File or LUN




```
cluster2::> volume file clone create -vserver svm5 -volume
svm5_vol_002/file1 -destination-path svm5_vol_002/file1_clone
```


FlexClone can also be used to clone individual files or LUNs. This is useful in application testing. Unlike FlexClone volumes, cloning of files and LUNs does not require a backing Snapshot copy.

Knowledge Check: Questions

1. Which types of data compression are available in ONTAP software?
    a. inline and external
    b. inline and preprocess
    c. inline and postprocess
    d. inline and reclaimable

Knowledge Check: Questions

2. True or False: Data can be written to a FlexClone volume.
   a. True
   b. False

Knowledge Check: Questions

3. True or False: A FlexClone volume, by definition, shares no data blocks with the parent volume.
   a. True
   b. False

References

- NetApp Hardware Universe: http://hwu.netapp.com
- ONTAP 9 Documentation Center: http://docs.netapp.com/ontap-9/index.jsp
  - *Cluster Management Using OnCommand System Manager*
  - *Logical Storage Management Guide*
- TR-4476: NetApp Deduplication, Compression, and Compaction.

NetApp Hardware Universe: http://hwu.netapp.com

ONTAP 9 Documentation Center:
http://docs.netapp.com/ontap-9/index.jsp

Cluster Management Using OnCommand System Manager

Logical Storage Management Guide

TR-4476: NetApp Deduplication, Compression, and Compaction

Storage Efficiency Video: How NetApp FlexClone Works

https://www.youtube.com/watch?v=c8VI_L5K8VM

How to efficiently search the event log in clustered Data ONTAP

https://www.youtube.com/watch?v=5qu8hJYfKm8

Module Review

This module focused on enabling you to do the following:

- Implement storage-efficiency features
- Use FlexClone software volumes

ACTION: Complete an Exercise

Module 9: Managing Storage Efficiency and FlexClone Volumes

Duration: 30 minutes

Access your exercise equipment.

Use the login credentials that your instructor provided to you.

Complete the specified exercises.

- Go to the exercise for the module.
- Start with Exercise 9-1.
- Stop at the end of Exercise 9-2.

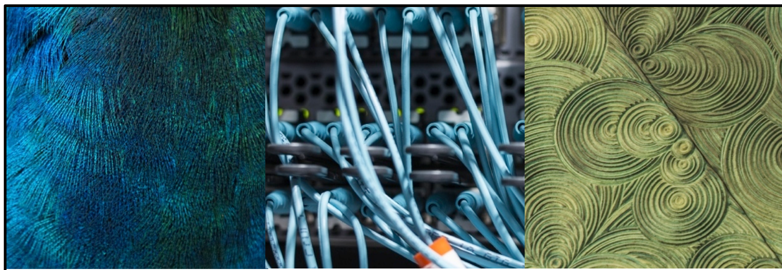
Participate in the review session.

- Share your results.
- Report issues.

Share Your Experiences

Roundtable questions for the equipment-based exercises

- Were you able to observe storage-efficiency benefits in your exercise environment?
- What are some popular uses for FlexClone volumes?



Addendum
Inline Deduplication Status

Aggregate Inline Deduplication

Status

Volume Status

```
::> volume efficiency show -vserver svm4 -volume svm4_vol003     -fields
cross-volume-inline-dedupe
vserver   volume       cross-volume-inline-dedupe
--------- ------------ --------------------------
Svm4      svm4_vol003  true
```

Aggregate Status

```
::> run local aggr cross_vol_share status cluster1_ssd_001
```


You can display the aggregate inline deduplication status for a volume by using the `volume efficiency show` command. You can display the status for an aggregate by using the `run local aggr cross_vol_share status` command.

You can enable or disable aggregate inline deduplication for a volume by using the `volume efficiency modify –cross-volume-inline-dedupe {true|false}` command. You can enable or disable aggregate inline deduplication for an aggregate by using the `run local aggr cross_vol_share {on|off}` command.

NOTE: If you try to enable aggregate inline deduplication on a node that is not an AFF node, the following error appears:

```
::> run local aggr cross_vol_share on SSD_AGGR1
aggr cross-volume-sharing: Operation is not permitted.
ERROR: Cannot enable cross volume deduplication on aggregate "SSD_AGGR1" residing on non
AFF node.
```

Aggregate Inline Deduplication

Savings

Aggregate Savings

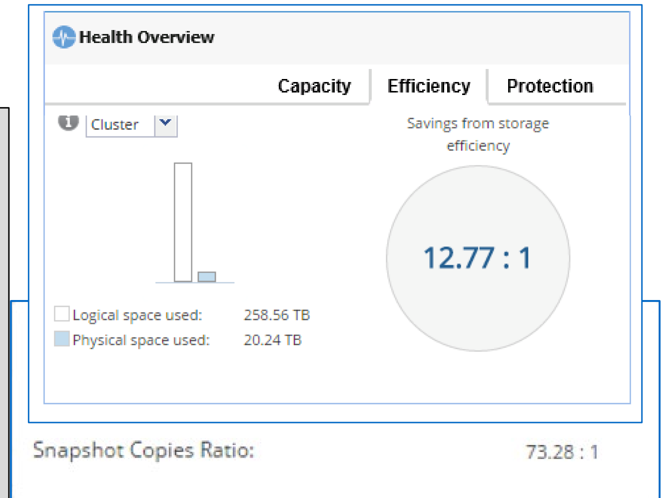
```
::> aggr show-efficiency -details

Aggregate: cluster1_ssd_001
     Node: cluster1-01

Total Storage Efficiency Ratio:       25.22:1
Total Data Reduction Ratio:           2.57:1

Aggregate level Storage Efficiency
(Aggr Dedupe and Data Compaction):    1.33:1
Volume Dedupe Efficiency:             1.40:1
Compression Efficiency:               1.29:1

Snapshot Volume Storage Efficiency:   27.14:1
FlexClone Volume Storage Efficiency:  -
```



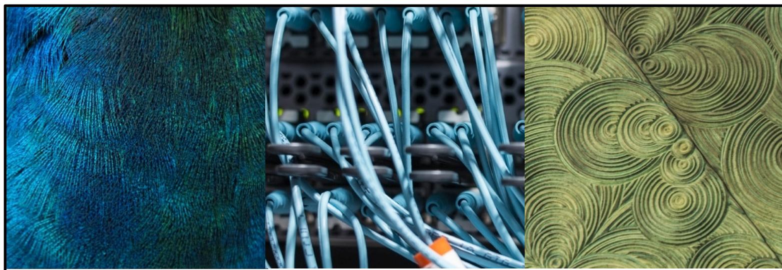
The overall ratio and data-reduction ratio include aggregate inline deduplication savings.

Aggregate inline deduplication savings and data compaction savings are combined and reported as a single ratio percentage.

The existing ONTAP API includes aggregate inline deduplication savings:

- CLI: `df -A -S, aggr show-efficiency`
- System Manager: Efficiency Dashboard, Efficiency tab in Hardware and Diagnostics, on the Aggregates page
- My AutoSupport: Aggregates tab under AFF Efficiency calculator

NOTE: At the aggregate level, aggregate inline deduplication savings and data compaction are combined and reported as deduplication savings.



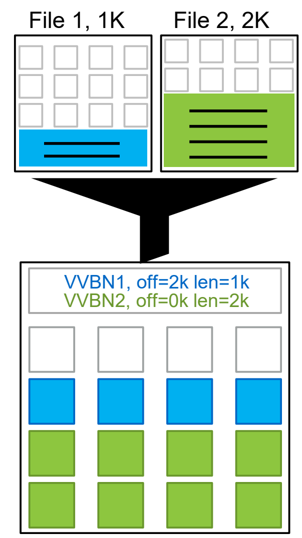
Addendum
Inline Data Compaction

Reading Multiple Files in One Data Block

Virtual Volume Block Number (VVBN)

How does WAFL read a single file in a compacted data block when the compacted files share the same Physical Volume Block Number (PVBN)?

- A header inside compacted blocks stores a VVBN for each file inside the block.
- The VVBN stores the offset for the start of the file and the length of the data.
- When a READ request for file1 is made, WAFL identifies the PVBN first and then references the VVBN to provide only the contents of file1 to the client.



The bytes that make up a file inside a FlexVol volume are stored in 4K blocks. Each block is assigned a Physical Volume Block Number (PVBN). Most files are composed of multiple physical blocks, which WAFL maintains a directory of. When inline data compaction finds small files that reside in a single 4KB block, compaction tries to squeeze the data from multiple small files into a single block. Now, the small files share the same PVBN. How does WAFL send the data for a single file only and not all the data in the 4KB block? By creating a miniature file system inside the compacted block.

Some space inside the compacted data block is used as a header to store metadata. Each file within the compacted block is assigned a Virtual Volume Block Number (VVBN). The header also stores the offset for where the first byte of the file starts. And the header stores the length of the file, or where the last byte of the file is located.

In the diagram, WAFL has compacted a 1KB and a 2KB file together. The metadata for file 1 indicates that the start of the file is offset by 2KB and uses 1KB of space. The metadata itself consume some space so not all 4KB can be used for data. For the purposes of this example, assume that the metadata requires 1KB of space. Any combination of small files that add up to 3KB could then be compacted into this block.

Module 10
Cluster Maintenance

About This Module

This module focuses on enabling you to:

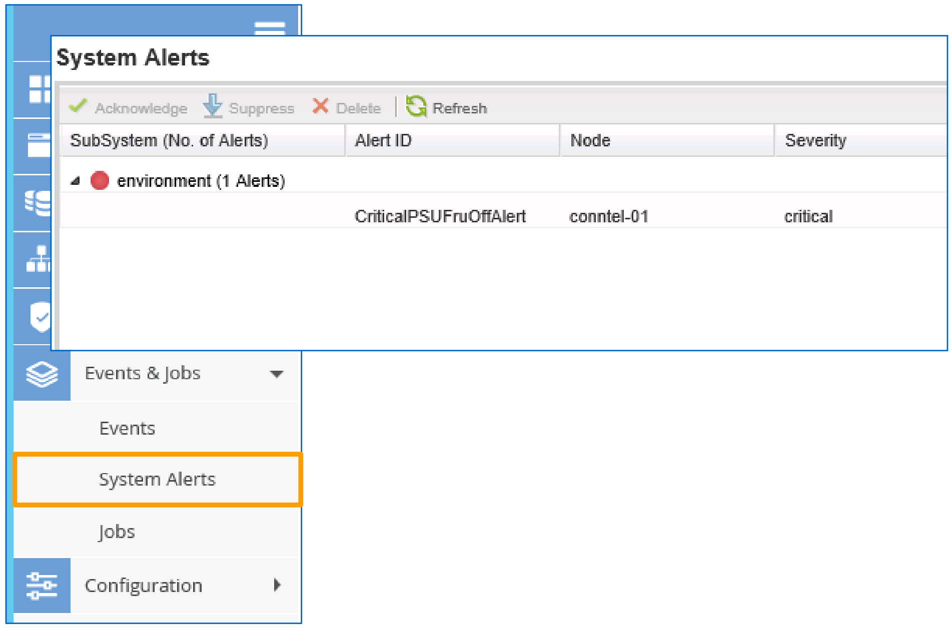
- Navigate the NetApp Active IQ customer dashboard
- Plan for NetApp ONTAP software upgrades
- Follow recommended practices for peak performance
- Configure event notifications and alerts
- Prepare to engage NetApp Technical Support
- Perform cluster maintenance

Lesson 1
Data Collection, Monitoring, and Automation Tools

Alerts

Tools for monitoring the system:

- AutoSupport
- Event management system (EMS)
- OnCommand System Manager
- OnCommand Unified Manager

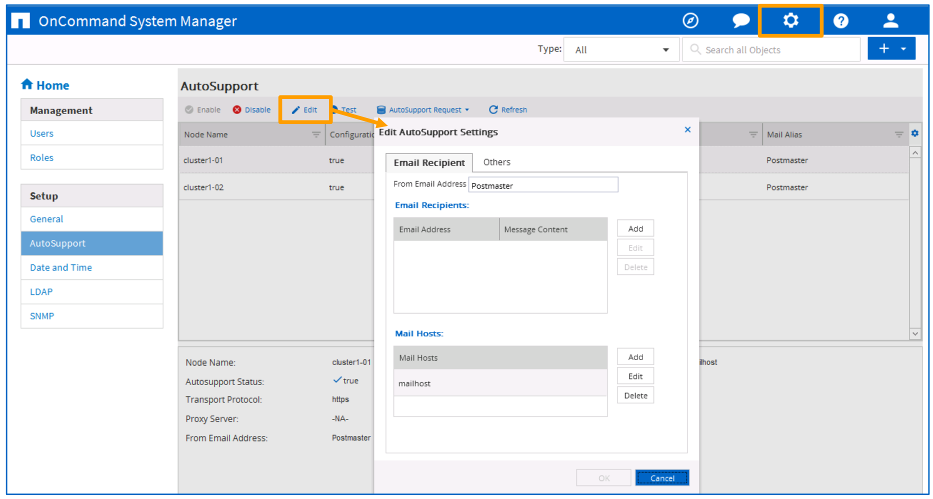


Monitoring your system regularly is a best practice.

In the example, a notification from NetApp OnCommand System Manager needs to be diagnosed. When there is an alert or event, first try the solution that the monitoring software suggests.

AutoSupport

- Is an integrated monitoring and reporting technology
- Checks the health of NetApp systems
- Should be enabled on each node of a cluster



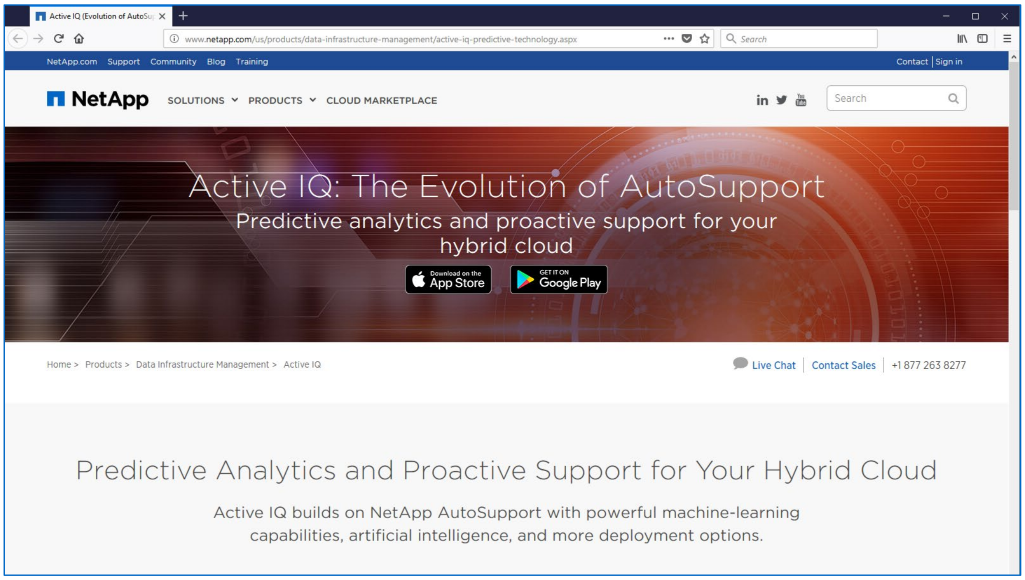
 5

AutoSupport is an integrated and efficient monitoring and reporting technology that, when enabled on a NetApp system, checks the system health on a continual basis. AutoSupport should be enabled on each node of the cluster.

AutoSupport can be enabled or disabled. To configure AutoSupport, click the gear icon in the UI menu. Select **AutoSupport**, click **Edit**, and then enter your configuration information.

Active IQ

The evolution of AutoSupport



- Actionable intelligence
- Predictive, self-healing care
- Global analytics at your fingertips

 6

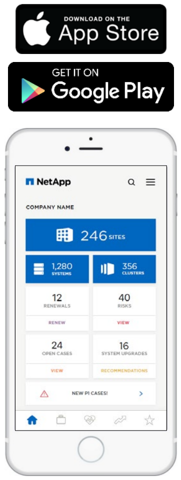
NetApp Active IQ is a suite of web-based applications that are hosted on the NetApp Support site and are accessible via your web browser. Active IQ uses data from the AutoSupport support tool. Active IQ proactively identifies storage infrastructure issues through a continuous health-check feature. Active IQ also automatically provides guidance about remedial actions that help to increase uptime and avoid disruptions to your business.

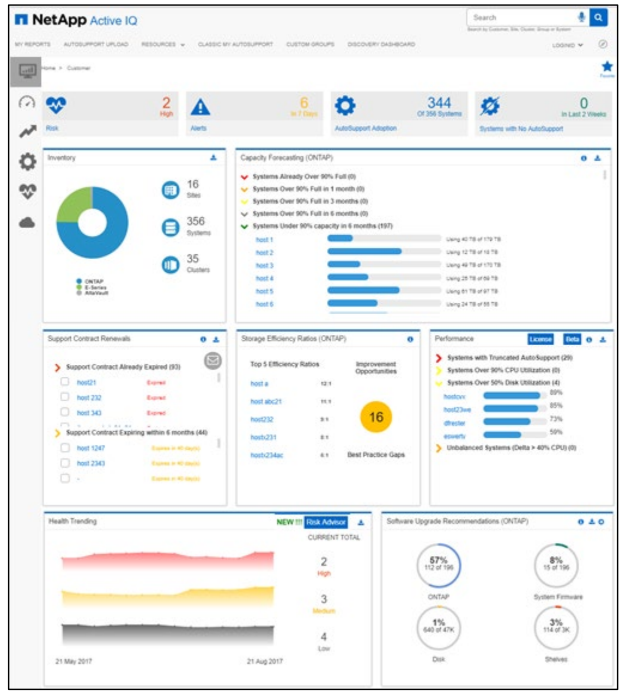
For example, Active IQ might find a configuration issue, a bad disk, or version incompatibility on your system. Or Active IQ might notify you about end-of-life (EOL) issues or an upcoming support contract expiration date.

If you plan any changes to your controllers, you should manually trigger an AutoSupport message before you make the changes. The message provides a “before” snapshot for comparison, in case a problem arises later.

Active IQ

- Dashboard
  - Inventory of NetApp systems
  - Health summary and trends
  - Upgrade Advisor
  - Storage efficiency and risk advisors
- Mobile app for iOS and Android





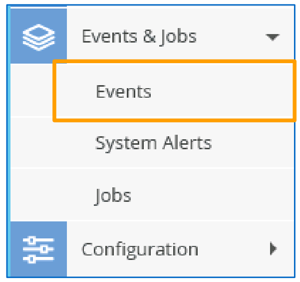
Active IQ provides predictive analytics and proactive support for the hybrid cloud. Along with an inventory of NetApp systems, Active IQ provides a predictive health summary and trends. You also get improved storage efficiency information and a system risk profile.

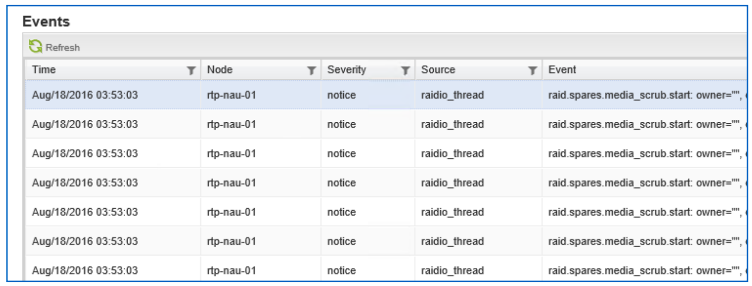
Access Active IQ either from the NetApp Support site or from the Active IQ mobile app.

EMS

- EMS does the following:
  - Writes events to the event log
  - Sends and routes notifications of events
  - Collects events throughout the cluster
  - Can view events of all nodes from any node

    `rtp-nau::> event log show`
- Each event contains the following:
  - Message name
  - Severity level
  - Description
  - Corrective action, if applicable




Events

Refresh

Time	Node	Severity	Source	Event
Aug/18/2016 03:53:03	rtp-nau-01	notice	raidio_thread	raid.spares.media_scrub.start: owner="",
Aug/18/2016 03:53:03	rtp-nau-01	notice	raidio_thread	raid.spares.media_scrub.start: owner="",
Aug/18/2016 03:53:03	rtp-nau-01	notice	raidio_thread	raid.spares.media_scrub.start: owner="",
Aug/18/2016 03:53:03	rtp-nau-01	notice	raidio_thread	raid.spares.media_scrub.start: owner="",
Aug/18/2016 03:53:03	rtp-nau-01	notice	raidio_thread	raid.spares.media_scrub.start: owner="",
Aug/18/2016 03:53:03	rtp-nau-01	notice	raidio_thread	raid.spares.media_scrub.start: owner="",
Aug/18/2016 03:53:03	rtp-nau-01	notice	raidio_thread	raid.spares.media_scrub.start: owner="",

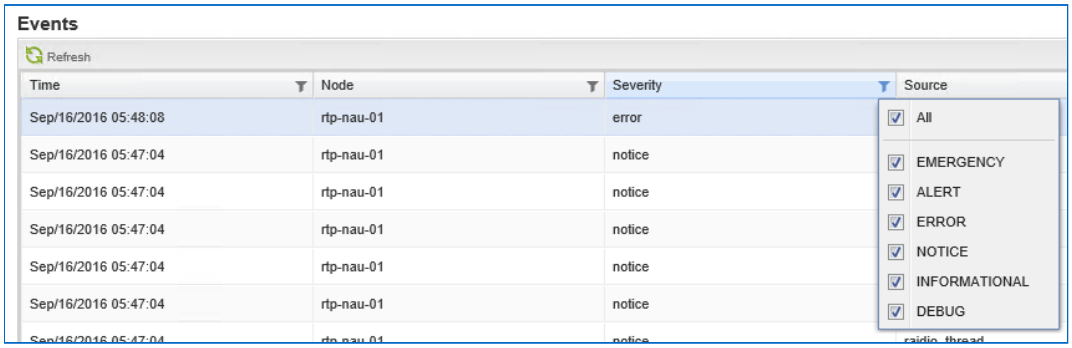
 8

The event management system (EMS) collects and displays information about events that occur in a cluster. You can manage the event destination, event route, mail history records, and SNMP trap history records. You can also configure event notification and logging.

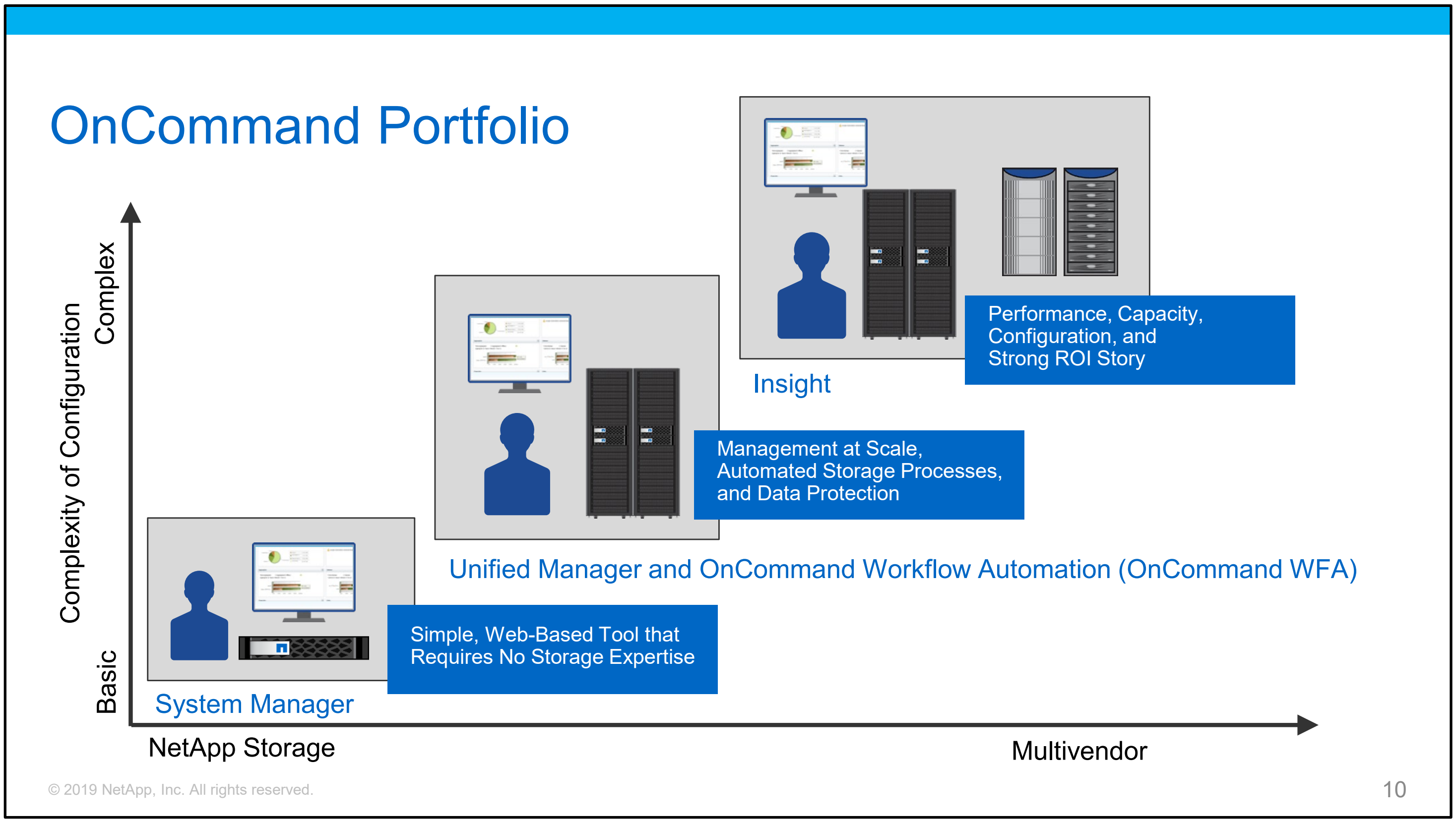
Event Log Filtering

Filter EMS log messages by severity, time, message name, and other criteria.

```
::> event log show -severity {EMERGENCY|ALERT|ERROR|NOTICE|INFORMATIONAL|DEBUG}
::> event log show -time "08/30/2016 10:00:00".."08/30/2016 11:30:00"
::> event log show -severity informational -message-name kern.uptime.filer
```



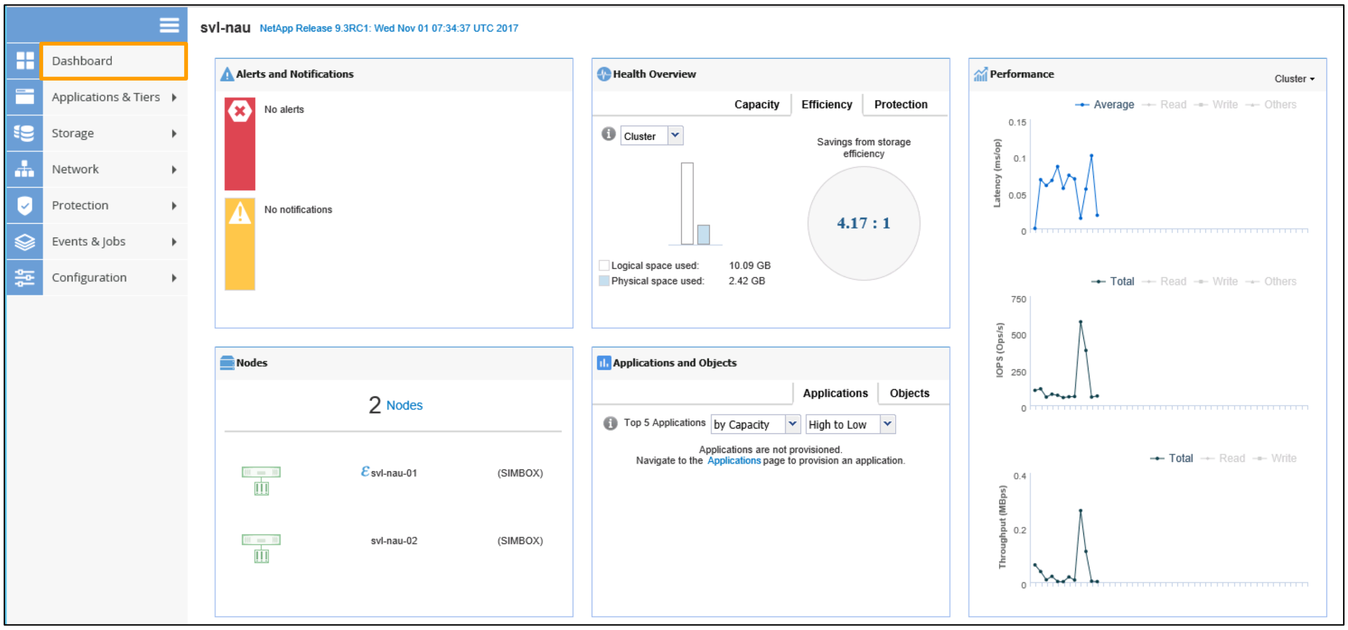

```
::> event log show ?
  [ -detail | -detailtime | -instance | -fields <fieldname>, ... ]
  [[-node] <nodename>]                                                  Node
  [[-seqnum] <Sequence Number>]                                         Sequence#
  [ -time <"MM/DD/YYYY HH:MM:SS"> ]                                     Time
  [ -severity {EMERGENCY|ALERT|ERROR|NOTICE|INFORMATIONAL|DEBUG} ]  Severity (default:
<=ERROR)
  [ -source <text> ]                                                    Source
  [ -message-name <Message Name> ]                                      Message Name
  [ -event <text> ]                                                     Event
  [ -action <text> ]                                                    Corrective Action
  [ -description <text> ]                                               Description
  [ -filter-name <text> ]                                               Filter Name
```



You can choose from many management tools.

Although System Manager provides simplified device-level management, and OnCommand Unified Manager can be used to monitor cluster resources at scale, both products are used to monitor only ONTAP storage systems. NetApp OnCommand Insight enables storage resource management, including configuration and performance management and capacity planning, along with advanced reporting for heterogeneous environments.

System Manager Dashboard

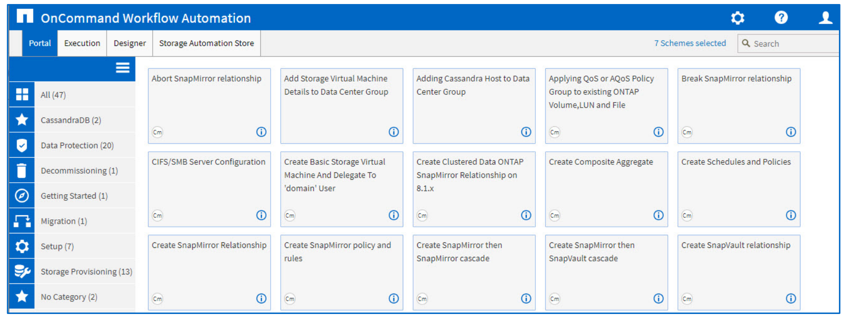


The System Manager dashboard shows at-a-glance system status for a storage system. The dashboard displays vital storage information, including efficiency and capacity use for various storage objects, such as aggregates and volumes.

OnCommand WFA

What is OnCommand WFA?

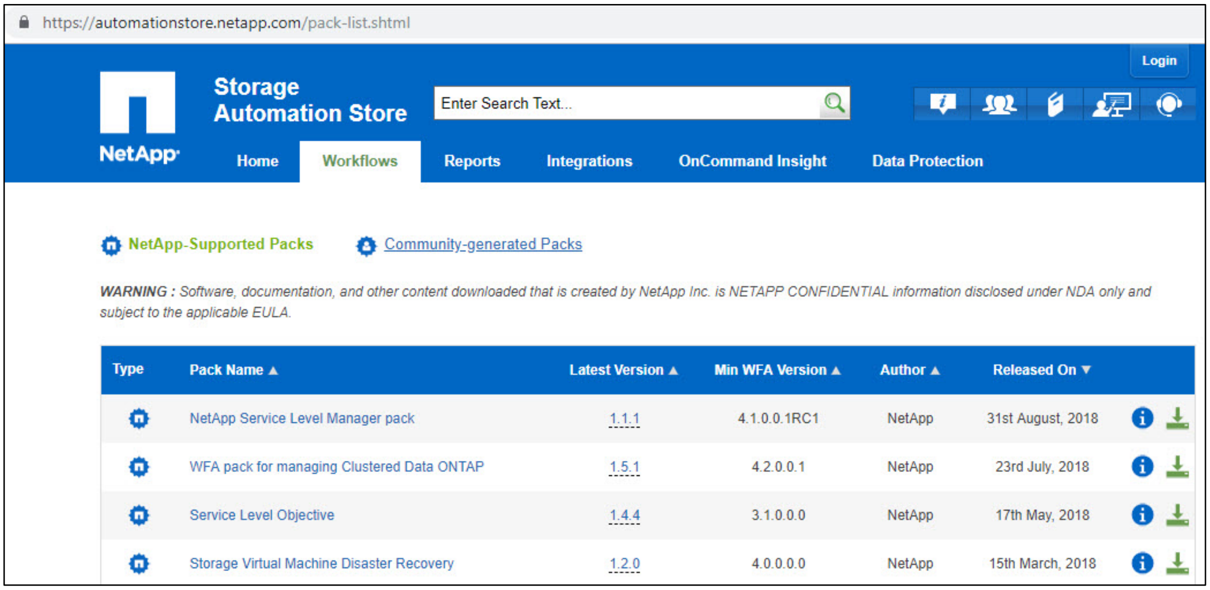
- Highly flexible automation framework
  Enables automation of simple to complex storage processes
- Operations portal
  - One click to perform common tasks, with more than 45 built-in workflows
  - Authentication and authorization
- Point of integration
  - Initiate third-party actions
  - Drive OnCommand WFA from web services



OnCommand WorkFlow Automation (OnCommand WFA) reduces the time to perform common, repetitive storage administration tasks. OnCommand WFA also simplifies the push of some system administration tasks to storage virtual machine (SVM) administrators or smart end users.

Storage Automation Store

Additional workflows can be downloaded

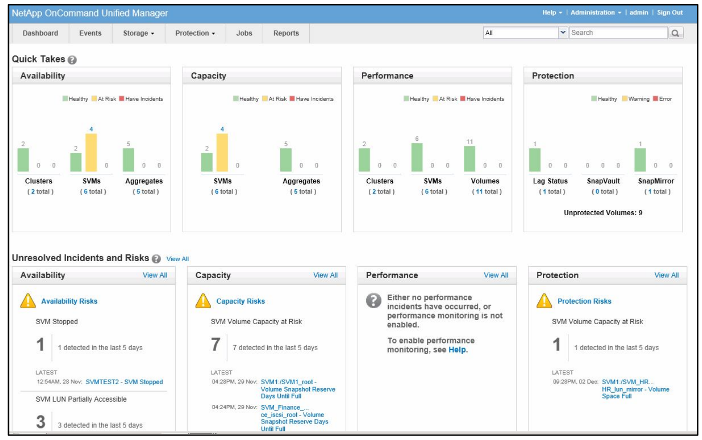


Type	Pack Name ▲	Latest Version ▲	Min WFA Version ▲	Author ▲	Released On ▼
	NetApp Service Level Manager pack	1.1.1	4.1.0.0.1RC1	NetApp	31st August, 2018
	WFA pack for managing Clustered Data ONTAP	1.5.1	4.2.0.0.1	NetApp	23rd July, 2018
	Service Level Objective	1.4.4	3.1.0.0.0	NetApp	17th May, 2018
	Storage Virtual Machine Disaster Recovery	1.2.0	4.0.0.0.0	NetApp	15th March, 2018

The larger NetApp community has created and shared dozens of workflows for OnCommand WFA to automate many storage administration tasks. You can download the workflows for free at https://automationstore.netapp.com/.

Unified Manager

- NetApp-centric application for managing multiple NetApp storage systems.
- Works with OnCommand System Manager on each storage system.
- Supports plug-in modules to extend functionality.



To learn more about Unified Manager and how it integrates with OnCommand WFA, enroll in the instructor-led course **Administration of OnCommand Unified Manager and Integrated Solutions.**

 14

Think of Unified Manager as the big brother of OnCommand System Manager. Unified Manager can manage multiple clusters and opens System Manager when you navigate to a specific node.

Unified Manager has two UIs: one for managing the operation of the Unified Manager server and one for troubleshooting data-storage capacity and availability and protection issues. These two UIs are the Unified Manager web UI and the maintenance console.

Unified Manager Web UI

The Unified Manager web UI enables a storage administrator, cluster administrator, or SVM administrator to monitor and troubleshoot cluster or SVM issues that relate to data-storage capacity, availability, performance, and protection.

Maintenance Console

The maintenance console enables an administrator to monitor, diagnose, and address operating system, version upgrade, user access, and network issues that relate to the Unified Manager server. If the Unified Manager web UI is unavailable, the maintenance console is the only form of access to Unified Manager.

A connection between an OnCommand Performance Manager server and the Unified Manager server enables you to use the Unified Manager web UI to monitor performance issues that the Performance Manager server detects.

For the user guide, see https://library.netapp.com/ecm/ecm_download_file/ECMP1653271. NetApp University offers courses that focus on the configuration and use of the OnCommand suite of products.

OnCommand Insight

- Provides proactive monitoring of your entire storage infrastructure: NetApp and competitor storage, SAN fabric switches, virtualization servers, and VM hosts.
- Provides reports on:
  - Inventory
  - Capacity
  - Performance
  - Showback and chargeback
- Is highly customizable through APIs and scripting

To learn more, enroll in the online course **OnCommand Insight: Fundamentals.**

OnCommand Insight is a monitoring and reporting tool that you can use for your entire data center. Insight is even popular with customers who do not own NetApp storage.

NetApp University has multiple courses covering all the features and functionality of Insight. You should start with the Fundamentals course:
https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000026950

NetApp OneCollect

- Collects data from a wide array of data center components
- Performs data collection on:
  - Hybrid, FC, and Ethernet switches
  - Windows, Linux, Solaris, HPUX, ESXi, AIX, KVM, XenServer, and Oracle VM Manager host types
  - NetApp ONTAP software, ONTAP operating in 7-Mode, E-Series, and EMC Isilon storage controllers
  - NetApp SnapCenter software
  - Hyper converged infrastructure (HCI) components including NetApp SolidFire, ONTAP Select, and VMware vCenter
- Uses an interface like the Config Advisor UI

You can use NetApp OneCollect to gather the most critical log files and configuration information from a wide array of data center components. These components can include network switches, operating systems and hypervisors, storage controllers, SnapCenter software, and hyper converged infrastructure (HCI) elements. The collected data can be used for troubleshooting, solution validation, migration, and upgrade assessments.

Lesson 2
Backing up and Restoring Your Cluster Configuration

Cluster Configuration Backup Files

Backing up the cluster configuration enables you to restore the configuration of any node or the cluster in the event of a disaster or emergency.

- Configuration backup files are archive files (.7z) that contain information for all configurable options that are necessary for the cluster and cluster nodes to operate properly.
- Two types of configuration backup files:
  - Node configuration backup file
  - Cluster configuration backup file
- Configuration backup files do not include any user data.

18

Configuration backup files are archive files (.7z) that contain information for all configurable options that are necessary for the cluster, and the nodes within it, to operate properly.

These files store the local configuration of each node, plus the cluster-wide replicated configuration. You use configuration backup files to back up and restore the configuration of your cluster.

There are two types of configuration backup files:

Node configuration backup file

Each healthy node in the cluster includes a node configuration backup file, which contains all of the configuration information and metadata necessary for the node to operate healthy in the cluster.

Cluster configuration backup file

These files include an archive of all of the node configuration backup files in the cluster, plus the replicated cluster configuration information (the replicated database, or RDB file). Cluster configuration backup files enable you to restore the configuration of the entire cluster, or of any node in the cluster. The cluster configuration backup schedules create these files automatically and store them on several nodes in the cluster.

NOTE: Configuration backup files contain configuration information only. They do not include any user data. For information about restoring user data, see the *Data Protection Power Guide*.

Cluster Backup Scheduling

- ONTAP automatically creates the configuration backup files every 8 hours, daily, and weekly.
- Use the `system configuration backup` commands to manage cluster and node configuration backup files, backup schedules, and to perform a configuration restore.
- Before you restore a node or cluster configuration, always refer to the ONTAP 9.5 *Storage Administration Reference Guide* and contact technical support.
  - There may be discrepancies between the configuration backup file and the configuration present in the cluster.

 19

Three separate schedules automatically create cluster and node configuration backup files and replicate them among the nodes in the cluster.

The configuration backup files are automatically created according to the following schedules:

- Every 8 hours
- Daily
- Weekly

At each of these times, a node configuration backup file is created on each healthy node in the cluster. All of these node configuration backup files are then collected in a single cluster configuration backup file along with the replicated cluster configuration and saved on one or more nodes in the cluster.

For single-node clusters (including Data ONTAP Edge systems), you can specify the configuration backup destination during software setup. After setup, those settings can be modified using ONTAP

commands.

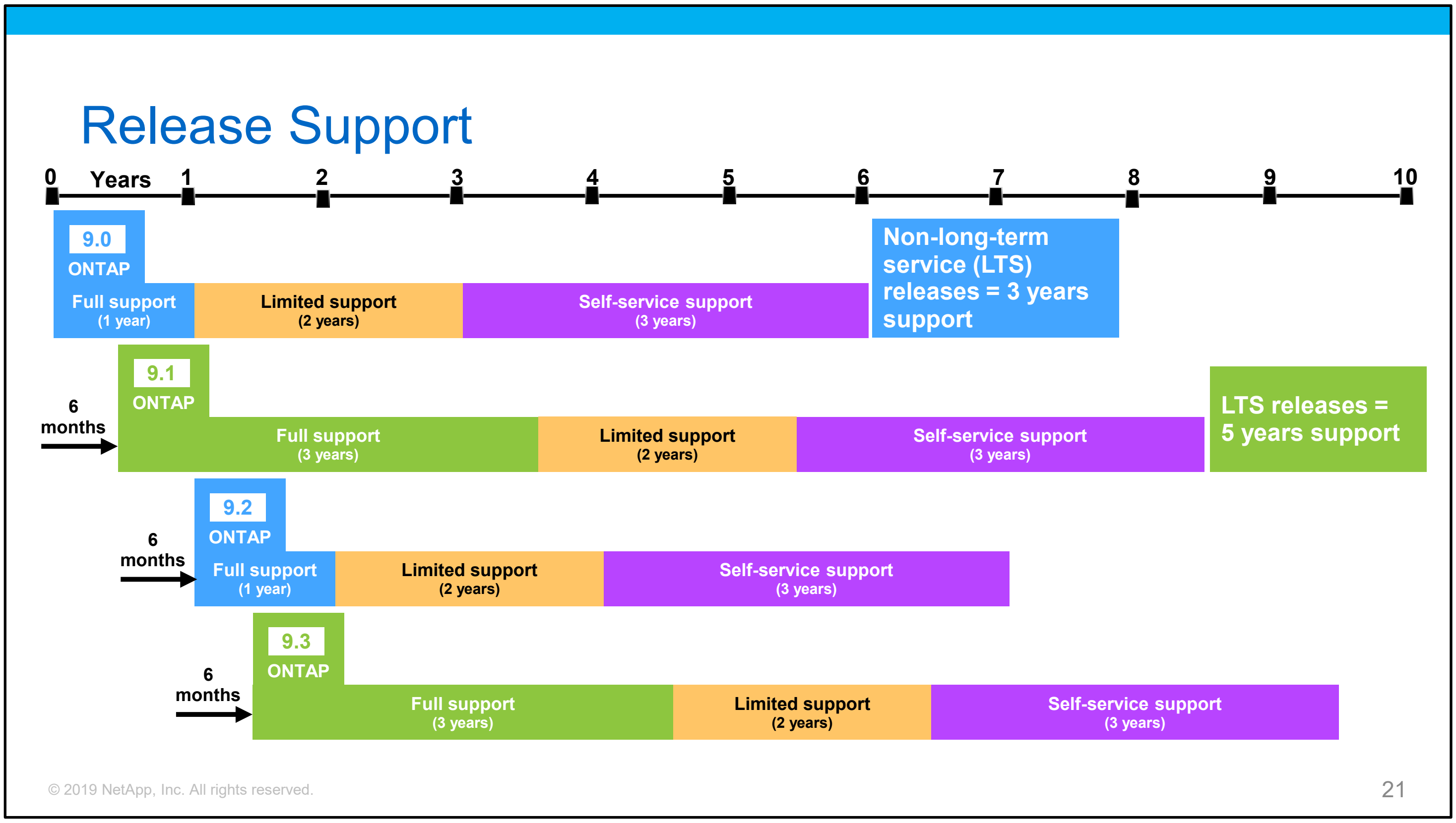
You use the 'system configuration backup' commands to manage cluster and node configuration backup files, backup schedules, and to perform a configuration restore.

You should only perform this task to recover from a disaster that resulted in the loss of the cluster's configuration.

Attention: If you are re-creating the cluster from a configuration backup file, you must contact technical support to resolve any discrepancies between the configuration backup file and the

configuration present in the cluster.

Lesson 3
Upgrading Your Cluster



Starting with ONTAP 9.0 software, a new software version support policy exists for ONTAP software:

- The NetApp release model delivers two feature releases each calendar year: the first in Q2CY and the second in Q4CY.
- NetApp supports designated long-term service (LTS) feature versions for five years after the feature version is designated with general availability (GA) for customers. NetApp provides full support for 36 months following the GA designation and then limited support for the remaining two of the five years.
- NetApp supports all feature versions that are not designated LTS for three years after the feature version is designated GA to customers. NetApp provides full support for 12 months following the GA designation and then limited support for the remainder of the three years.
- Following limited support, a feature version transitions to self-service support and is no longer supported by NetApp. However, documentation remains available for three years on the NetApp Support site. Customers are encouraged to upgrade to a supported version of the product for support coverage before the limited support period expires.
- After the self-service support period has elapsed, the version becomes obsolete.

Support definitions:

- **Full support:** The period during which NetApp provides full support for a version of a software product. Full support includes technical support, root cause analysis, online availability of documentation and software, maintenance, and service updates (such as patch releases).
- **Limited support:** The period during which NetApp provides partial support for a version of a software product. Limited support includes technical support, root cause analysis, and online availability of documentation and software. Service updates, maintenance, and patch releases are not provided for versions under limited support.
- **Self-service support:** The period during which NetApp does not support a version of a software product, but during which related documentation is still available on the NetApp Support site.
- Following the self-service support period, the release is considered obsolete, which means that support and information about the version of the software product are no longer available.

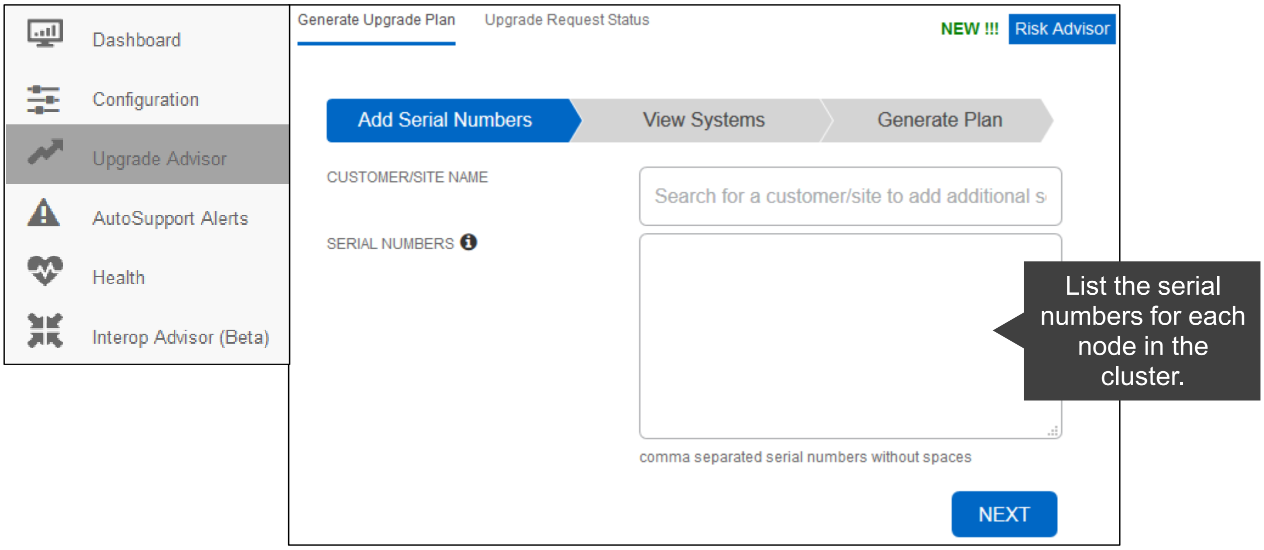
For more information about the software version support policy for ONTAP 9.0 software and later, see http://mysupport.netapp.com/info/web/ECMP1147223.html#_Data%20ONTAP%209.0%20and%20later%20Software%20Version%20Support%20Policy.

Learning About New ONTAP Features

- The new Release and Support model requires ONTAP upgrades every few years.
- How can you learn what has changed since your current running version?
  - The release notes in the ONTAP documentation
  - The *What Is New in ONTAP <version #>* online courses
  - The CLI Comparison Tool:
    https://mysupport.netapp.com/NOW/products/support/cli-comparison.shtml

Depending on the ONTAP version that your runs, you might need to upgrade to maintain a full level of support. Even numbered releases have full support only for the first year. Before deciding to upgrade, do your due diligence and learn whether any changes will affect your environment, either positively or negatively. Each major version of ONTAP software maintains a set of release notes, which is expanded with each minor release. For a short overview of the key new features and changes in a release, take the associated What's New online course, available through NetApp University. If you use the command line extensively, the CLI Comparison Tool is a great resource for comparing changes made to commands between releases.

Upgrade Advisor

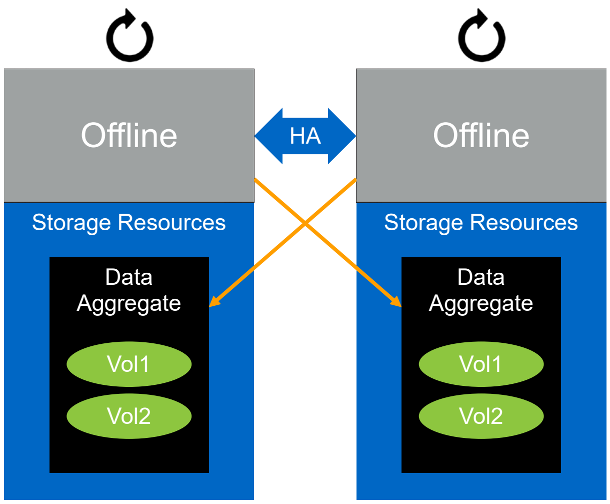


Upgrade Advisor, which is part of NetApp Active IQ, simplifies the process of planning ONTAP upgrades. NetApp strongly recommends that you generate an upgrade plan from Upgrade Advisor before upgrading your cluster.

When you submit your system identification and target release to Upgrade Advisor, the tool compares AutoSupport data about your cluster to known requirements and limitations of the target release. Upgrade Advisor then generates an upgrade plan (and optionally a backout plan) with recommended preparation and execution procedures.

A separate upgrade planning tool exists for customers who disable AutoSupport email for security purposes.

Rolling Upgrade



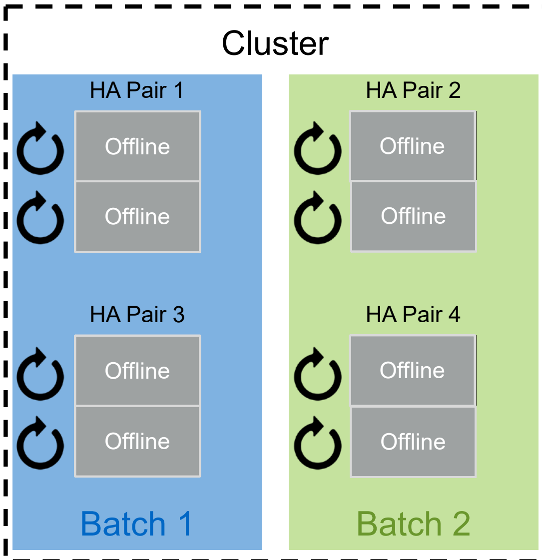
To upgrade software in a cluster of two or more nodes, complete the following steps:

1. Have the high-availability (HA) partner take control of the storage resources.
2. Take the node that is being upgraded offline.
3. Wait as the node reboots and is upgraded.
4. After the upgrade is complete, verify that the failed-over resources are returned home.
5. Repeat the process on the other node of the HA pair.
6. Repeat the process on other HA pairs.

Rolling upgrades can be performed on clusters of two or more nodes, but the upgrade runs on one node of an HA pair at a time. This approach makes it easier to roll back in the unlikely event of an issue during the upgrade.

The cluster does not switch over to the new version of ONTAP software until all nodes have installed the new version.

Batch Upgrade



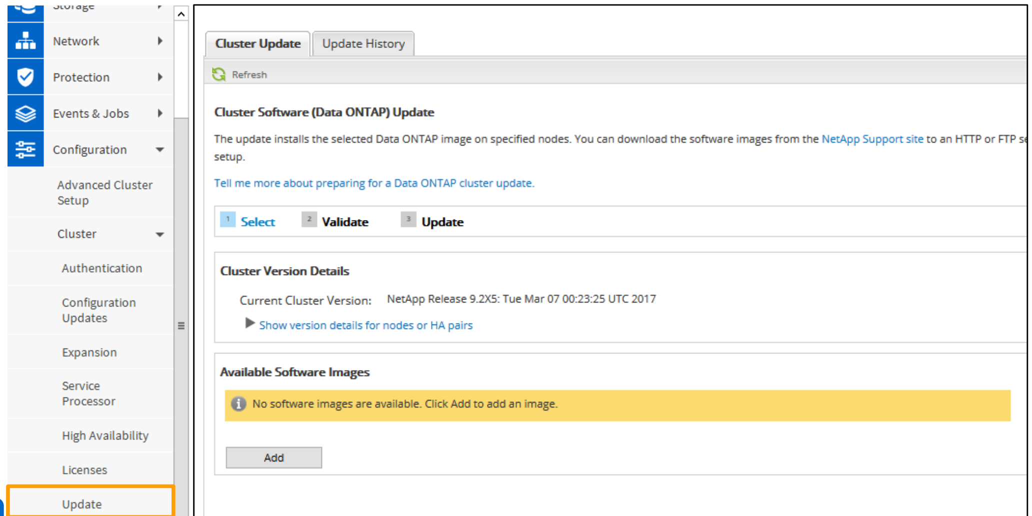
To upgrade software in a cluster of eight or more nodes, complete the following steps:

1. Separate the cluster into two batches, each of which contains multiple HA pairs.
2. In the first batch, take one node in each HA pair offline and upgrade the nodes while the partner nodes take over the storage.
3. After upgrades are completed on the first nodes, upgrade the other nodes of the HA pairs.
4. Repeat the process on the second batch.

You can perform batch upgrades on clusters of eight or more nodes. Unlike rolling upgrades, batch upgrades can run on more than one HA pair at a time.

As in rolling upgrades, in a batch upgrade the cluster does not switch over to the new version of ONTAP software until all nodes have installed the new version.

Automated Nondisruptive Upgrade (ANDU)



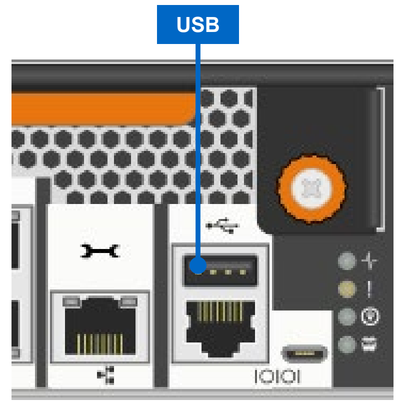
? More info in Addendum

 26

Use CLI commands to perform rolling upgrades and batch upgrades. If your cluster meets all the conditions, you can use System Manager to perform an automated nondisruptive upgrade (ANDU) instead of using the CLI. Read the ONTAP 9 Upgrade Express Guide (https://library.netapp.com/ecm/ecm_download_file/ECMLP2507747) to prepare your cluster, and then follow the simple wizard to get the package, validate, and start the upgrade process.

Install and Upgrade from a USB Drive

- Many FAS and AFF systems support the installation of ONTAP software and firmware from a FAT32 formatted USB device to:
  - Perform boot device recovery from the LOADER prompt.
  - Fetch ONTAP software for installation.
  - Fetch service images for firmware update.
- Use the `system node image` CLI commands.



More info in Addendum

You can also install ONTAP software and firmware from an external USB device on most FAS and AFF systems shipping since late 2016.

ACTION: Try This Task

From the clustershell on cluster1, type:

`system node image show -instance`

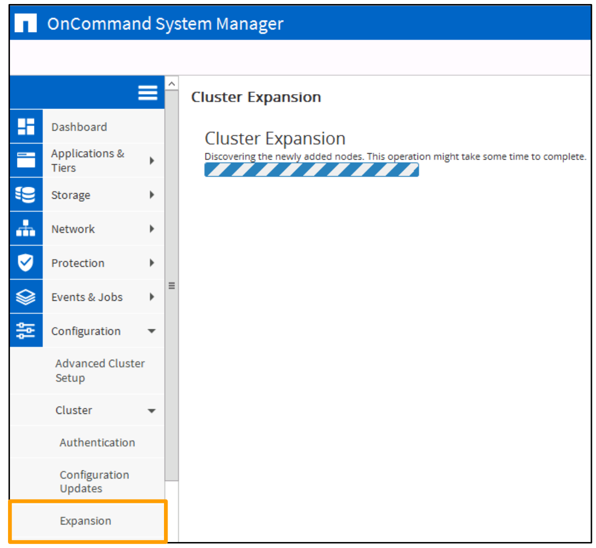
1. How many nodes are in your cluster?
2. Which version of ONTAP software is current on each node?
3. Can you tell which image is booted?

1. There are four nodes in the cluster.
2. Some revision of ONTAP 9.0 software should be installed, but the revision varies.
3. Verify the image in the Image Name field.

System Manager

Cluster expansion

- Automatic switchless cluster detection
- Automatic discovery of new compatible nodes
- Network configuration of new nodes



 29

OnCommand System Manager simplifies the process to join new nodes to a cluster.

Nondisruptive Addition of Nodes to a Cluster

Using the CLI

Complete the following steps in the CLI to add nodes to a multinode switched cluster:

1. Verify that the nodes are configured as HA pairs and are connected to the cluster interconnect.
2. Power on both nodes of the HA pair.
3. Start the Cluster Setup wizard on one of the nodes.
4. Use the **`join`** command and follow the wizard.
5. Repeat Steps 3 and 4 on the partner node.

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question
 clarified,
 "back" - if you want to change previously answered
 questions, and
 "exit" or "quit" - if you want to quit the cluster
 setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing
"cluster setup".
To accept a default or omit a question, do not enter
a value.

Do you want to create a new cluster or join an
existing cluster?
{create, join}join
```


You can expand an existing cluster by using the CLI to nondisruptively add nodes to the cluster.

You must add nodes from HA pairs that are connected to the cluster interconnect. Nodes are joined to the cluster one at a time.

Lesson 4
Performance Recommended Practices

Performance Considerations

- Workloads
- I/O operation types:
  - Random
  - Sequential
- Quality of service (QoS)

 32

Storage system performance calculations vary widely based on the kinds of operations, or workloads, that are being managed.

The storage system sends and receives information in the form of I/O operations. l/O operations can be categorized as either random or sequential. Random operations, such as database operations, are usually small, lack any pattern, and happen quickly. In contrast, sequential operations, such as video files, are large and have multiple parts that must be accessed in a particular order.

Some applications have more than one dataset. For example, a database application's data files and log files might have different requirements. Data requirements might also change over time. For example, data might start with specific requirements that change as the data ages.

If more than one application shares the storage resources, each workload might need to have quality of service (QoS) restrictions imposed. QoS restrictions prevent applications or tenants from being either bullies or victims.

Analyzing I/O

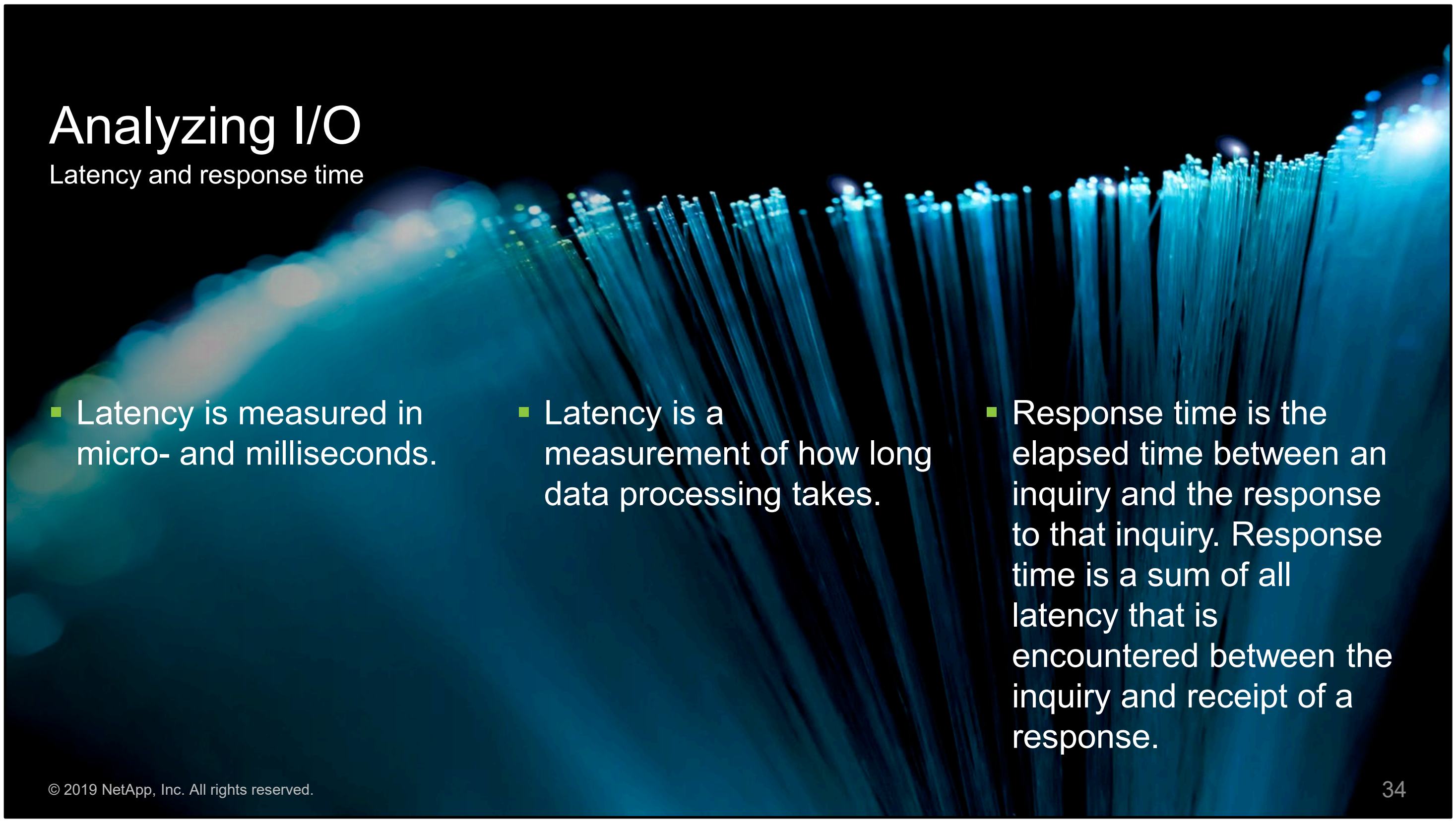
IOPS

- I/O is measured in IOPS.
- IOPS measures how many requests can be managed in one second.
- IOPS data is most useful if I/O has any of the following features:
  - I/O request patterns are random.
  - I/O requests are small.
  - Multiple I/O sources must be managed.

 33

IOPS is a measurement of how many requests can be managed in one second. Factors that affect IOPS include the balance of read and write operations in the system and whether traffic is sequential, random, or mixed. Other factors that affect IOPS include the application type, operating system, background operations, and I/O size.

Applications with a random I/O profile, such as databases and email servers, usually have requirements that are based on an IOPS value.



Latency is the measurement of how long a storage system takes to process an I/O task. Smaller latency values are better.

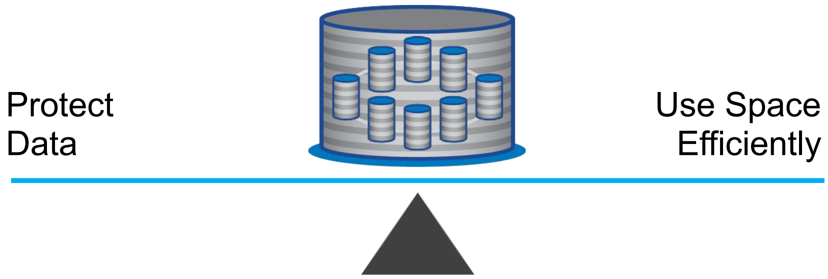
Latency for hard drives is typically measured in milliseconds. Because solid-state media is much faster than hard drives, the latency of the media is measured in submilliseconds or microseconds.

Response time is the elapsed time between an inquiry on a system and the response to that inquiry. Every mechanical and digital component along the way introduces some latency. All the latencies are added together to constitute the response time.

ONTAP Performance

You must balance the need for performance and the need for resilience:

- Performance: More drives per RAID group spread the workload over more drives.
- Resilience: Fewer drives per RAID group mean that parity must protect fewer drives.



Avoid being above the maximum optimal operating point.

 35

ONTAP software performance is measured at the aggregate level. To support the differing security, backup, performance, and data sharing needs of your users, you can group the physical data storage resources on your storage system into one or more aggregates. You can then design and configure the aggregates to provide the appropriate level of performance and redundancy.

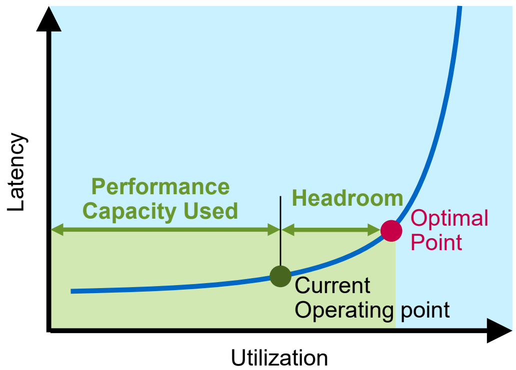
When creating aggregates and the underlying RAID group, you must balance the need for performance and the need for resilience. If you use more drives per RAID group, you increase performance by spreading the workload across more drives, but at the cost of resiliency. In contrast, if you use fewer drives per RAID group, you increase resiliency by reducing the amount of data that the parity has to protect, but at the cost of performance.

By following recommended practices when you add storage to an aggregate, you optimize aggregate performance. You should also choose the right drive type for the workload requirements.

Headroom and Performance Capacity Used

Key for optimal use of a system

Optimally used systems should operate within the "safe zone."



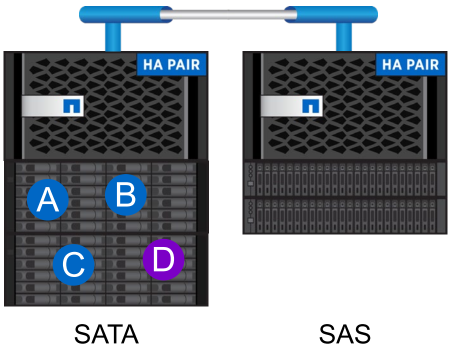
- Optimal point:
  The maximum optimal operating point for a system; a small increase beyond this point results in a bigger increase in latency
- Headroom:
  - A metric that is used in ONTAP 9 software
  - The remaining useful capacity of a resource, when measured from the optimal point
- Performance capacity used:
  - Metric used in Performance Manager
  - Equal to the optimal point minus headroom
  - Performance metric for node and aggregate

QoS is effective in optimally used systems.

If you know the available performance capacity in the cluster, you can better provision to balance workflows. Performance capacity is how much work you can place on a node or an aggregate before latency affects the performance of all workloads. You can use OnCommand Performance Manager to identify available performance capacity.

Maintain Optimal Operating Point

Adding and relocating resources



Relocating resources nondisruptively:

- Moving volumes and LUNs
- Moving an aggregate between the nodes of an HA pair
- Creating a flexible clone of a volume or LUN

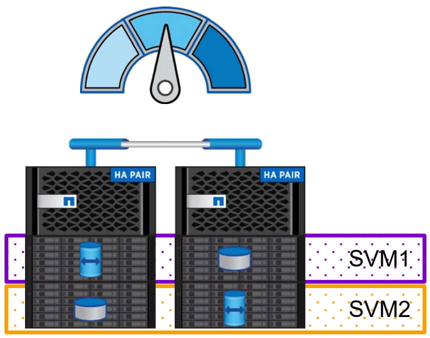
As well as discussing performance at the node level, discussing performance at the cluster level is important.

In the example, an administrator creates volumes on a two-node cluster that is used for file services. The system is configured with SATA disks to meet the workload requirements.

After some time, the administrator needs to add a volume for a database application. The SATA disks do not meet the requirements for the new workload. The administrator decides, for future growth, to nondisruptively add another HA pair with SAS disks. With new nodes with SAS disks active in the cluster, the administrator can nondisruptively move the volume to the faster disks.

Maintain Optimal Operating Point

QoS



- Key capability to manage and control performance
- Effective in optimally used systems
- Increasingly sought by both enterprise and service provider market segments
- Use cases:
  - Contain “runaway” workloads (QoS Max)
  - Experience dedicated workload performance (QoS Min)
  - Enable performance services classes

38

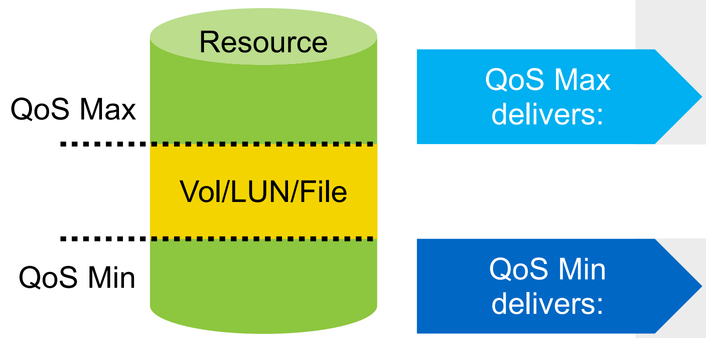
You can use storage QoS to deliver consistent performance by monitoring and managing application workloads.

You can configure the storage QoS feature to prevent user workloads or tenants from affecting one another. The feature can be configured to isolate and throttle resource-intensive workloads. The feature can also enable critical applications to achieve consistent performance expectations.

Essentially, QoS is about managing and controlling performance in heavily used systems. Both enterprise and service provider market segments increasingly seek QoS.

Controlling Performance for Shared Storage

Guaranteeing performance



QoS Max delivers:

- Guarantees performance for IOPS, megabytes per second, or both
- Enables service-level objectives
- Prevents “runaway” applications
- Is applicable to storage virtual machine (SVM), volume, LUN, or file
- Scales up to 12,000 objects per cluster

QoS Min delivers:

- Guarantees IOPS performance
- Enables service classes
- Prevents application timeouts
- Is applicable to volume and LUN
- Scales up to 12,000 objects per cluster

 39

The goal of controlling performance in a shared storage environment is to provide dedicated performance for business-critical workloads against all other workloads. To guarantee performance, you must apply QoS policies on these resources.

QoS Max, which is used to contain runaway workloads, was introduced in the Data ONTAP 8.2 software and has been continually enhanced. QoS Min, which provides a throughput floor, was introduced with ONTAP 9.2 software.

QoS Min (sometimes called a throughput floor or TP Floor) has a similar policy group scaling of up to 12,000 objects per cluster. The major difference is that QoS Max can guarantee IOPS, megabytes per second, or both, but QoS Min only guarantees IOPS performance. Also, QoS Min is applicable to volume, LUN, and file in a cluster. SVMs are not supported.

Maximizing Performance

Ways to minimize performance issues:

- Correctly size and follow recommended practices for the specific workload.
- Verify the supported minimums and maximums.
- Adhere to the ONTAP storage system mixing rules (Hardware Universe).
- Verify the compatibility of components, host operating system, applications, and ONTAP software (NetApp Interoperability Matrix Tool [IMT]).
- Collect statistics during the backup process.

Potential performance issues:

- Controller: Resource overutilization, ONTAP version, offline, or rebooting
- Storage: drive types, aggregate configuration, volume movement, or free space
- Networking: Configuration, LIF location, port saturation, port speeds, or indirect access
- Host or clients: Application, drivers, network adapter, or user knowledge

 40

Start with a properly sized system, and then follow recommended practices for ONTAP software, the host operating system, and the application. Verify and adhere to the supported minimums, maximums, and mixing rules. Use the NetApp Interoperability Matrix Tool (IMT) to check compatibility. Use the backup process to gauge how the system performs at peak usage. Backups consist of large sequential reads of uncached data that can consume all available bandwidth and therefore are not accelerated. Backups also are a good measure of network performance.

Situations can change and issues arise over time. Performance issues can occur for many reasons. Performance analysis can be complex and is beyond the scope of this course.

Create Free Space in an Aggregate

Simple steps

A full aggregate affects performance and might lead to an inability to write new data. Use these no-risk measures to free space:

- Add drives to the aggregate.
- Move some volumes to another aggregate with available space.
- Enable space-saving features, such as deduplication or compression.

Even the most diligently watched storage systems can occasionally have an aggregate that fills up. The situation results in a performance degradation and can result in failed writes. You can take three simple steps to free space in a full aggregate:

- The easiest step is to grow the aggregate by adding disks. Be sure to leave adequate spare disks in the spare pool.
- Moving volumes to a less full aggregate takes some time but safely frees up space.
- If you haven't enabled deduplication or compression, these efficiency features can make more space but require some time to run.

Create Free Space in an Aggregate

Complex steps

Use these measures with caution:

- Shrink the size of volume-guaranteed volumes in the aggregate.
  You can do so manually, or you can use the `autoshrink` option of the automatic resize capability.
- Change volume guarantee type to `none` on volumes that use large amounts of space so that the volumes take up less space in the aggregate.
- Delete unneeded volume Snapshot copies if the volume has a guarantee type of `none`.
  Note: Blocks are returned to free space only when there are no pointers to the block. You might need to delete multiple Snapshot copies before you gain any space.
- Delete unneeded volumes.
  The volume recovery queue holds a deleted volume for 12 hours. Contact NetApp Technical Support if you need to purge the queue sooner.

 42

The following steps can involve some risk of future issues or potential unrecoverable loss of data:

- If space-guaranteed volumes with significant unused space exist, you can resize them to return some of the unused space. The potential risk is that the volume might run out of space and cause failed writes.
- Changing the volume guarantees to none removes space reservations in the aggregate for those volumes.
- Deleting old or unneeded Snapshot copies might free space. Only blocks that no longer have any pointers to them are returned to the free space. If multiple Snapshot copies reference a block, the block is not released until all the Snapshot copies are deleted. After a Snapshot copy is deleted, it can no longer be used to recover data.
- Deleting unneeded volumes carries the biggest risk. If you later discover that the volume is needed, you cannot recover the volume. One exception, which can also cause confusion, is that deleted volumes are held in a recovery queue for 12 hours. The recovery queue provides you time to realize that a volume was deleted by mistake and recover it. If you and your users are certain that the volume is no longer needed and do not want to wait 12 hours, you need to contact NetApp Technical Support for the procedure to purge the queue.

When freeing up space in an aggregate, follow the maxim to “measure twice and cut once”, to avoid making the situation worse by deleting useful data.

Lesson 5
Technical Support

System Logs

- Log messages can be sent to the following:
  - The console
  - The message log
- You can access the message log by using the following:
  - The `debug log` command
  - System Manager
  - OneCollect
  - A web browser:
    https://<*cluster-mgmt-ip*>/spi/<*nodename*>/etc/log/

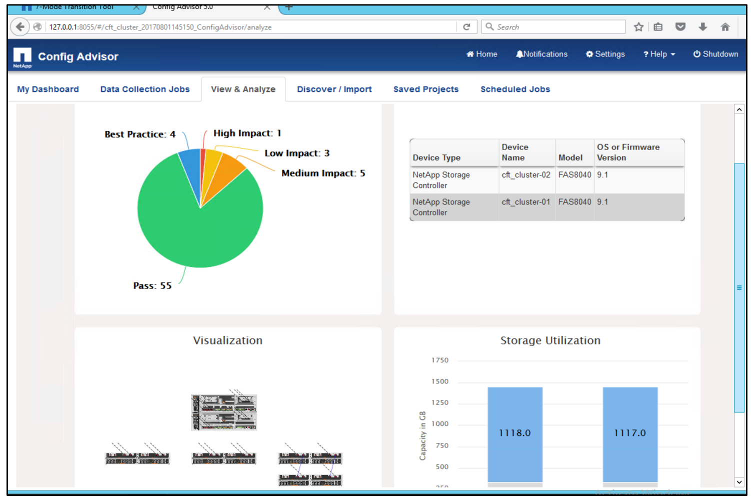
Use the **`debug log`** command to browse the messages.log file.

The system log contains information and error messages that the storage system displays on the console and logs in message files.

Use Config Advisor Before and After Maintenance

What is Config Advisor?

- Use to verify or troubleshoot cabling and configuration of cluster and switches.
- Can be configured to run on a schedule.
- Download from the Support site and run from PC connected to the serial port or over the network.



 45

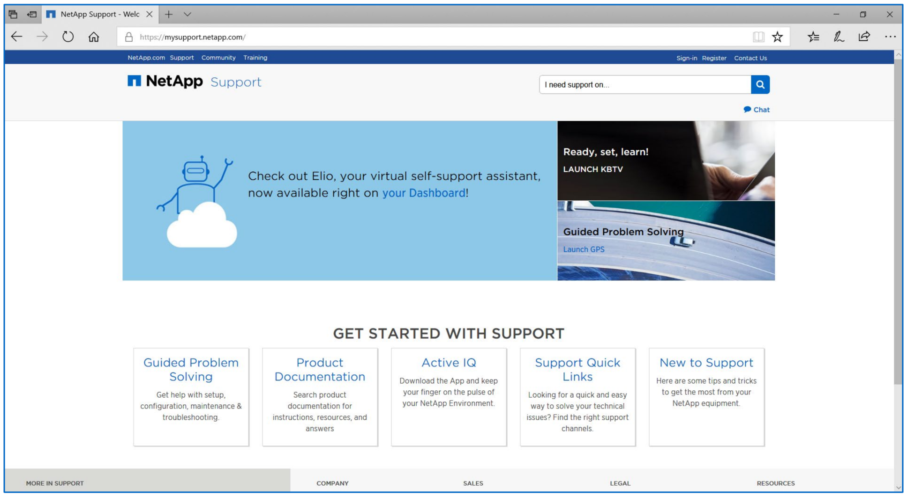
Config Advisor is a configuration validation and health check tool for NetApp systems. It can be deployed at secure sites and nonsecure sites for data collection and analysis. Config Advisor can be used to check a NetApp system or FlexPod solution for the correctness of hardware installation and conformance to NetApp recommended settings. Config Advisor collects data and runs a series of commands on the hardware, then checks for cabling, configuration, availability, and best practice issues.

The time that Config Advisor spends collecting data depends on how large the cluster is, but it usually takes just minutes.

The View and Analyze tab show the results of the data collection. The first panel allows you to drill down into errors messages based on severity. The next panel shows an inventory of all devices queried. The Visualization panel is a visual depiction of how the systems are cabled. The last panel displays total storage available and how it is utilized.

Config Advisor is downloaded from Toolchest on the NetApp Support site.

NetApp Support



- **NetApp Support:** mysupport.netapp.com
- **Hardware Universe:** hwu.netapp.com
- **NetApp IMT:** mysupport.netapp.com/ matrix

For support information, documentation, software downloads, and access to Active IQ, see NetApp Support at mysupport.netapp.com.

For system configuration information, see the NetApp Hardware Universe at hwu.netapp.com.

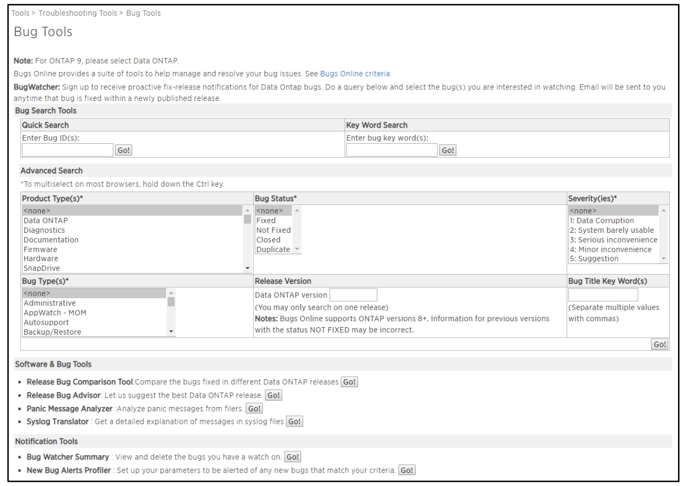
To determine the compatibility between various NetApp and third-party products that are officially supported, see the NetApp IMT at mysupport.netapp.com/matrix.

Bug Tools and Reports

Stay up to date about bugs and bug fixes with the tools on the NetApp Support site.

https://mysupport.netapp.com/NOW/cgi-bin/bol/

- BugWatcher
- Release Bug Comparison Tool
- Release Bug Advisor
- Bug Watcher Summary
- New Bug Alerts Profiler



https://mysupport.netapp.com/NOW/cgi-bin/bol/

Lesson 6
Documentation

Maintenance-Related Documentation

- Checklists
  - Create a plan. Follow the plan. Document the outcome and refine the plan.
  - Submit checklists with change control procedure documentation.
  - Pro tip: Include go/no-go checkpoints.
- Change control procedures
  - Implement a formal approval change control process to track changes to the storage system (and protect yourself when the unexpected happens).
  - Use the NetAppDocs PowerShell Toolkit (available in the ToolChest on the NetApp Support site) to build configuration documentation.

 49

Checklists reduce the probability of errors, especially during unplanned downtime at 2 AM on a Saturday. NetApp provides documentation for all hardware maintenance and ONTAP upgrades and can be used to create checklists. For other hardware and software, you might be required to create your own checklists. Record any revisions and the outcome so that the checklist is better the next time you need to use it.

Place go/no-go checkpoints in your checklists wherever steps might be difficult to roll back if they do not work. Checkpoints also serve as reminders to stop and check how much time remains in the maintenance window. You can easily spend 20 minutes solving a problem you thought would take only a minute or two. Better to request an extension to the maintenance window early and not need it than to wait until after you have exceeded the window.

If your company does not have a change control procedure, you should create one. Change control works to notify upper management of maintenance work and any potential risks. By having someone in management approve the change control, you buy yourself some protection if someone needs to be held responsible. Including a checklist with the change control form shows that you have a plan and general idea of how long the maintenance will take.

Maintenance Related Documentation

Communication and Call logs

- Maintenance downtime communication
  - Become familiar with work of end-users and how downtime will impact them.
  - Provide end-users frequent advance warning.
  - Create and use a short, standardized email template so end-users recognize it and know to read it.
  - Set an established maintenance window. Use it even if there is no maintenance to perform. This will train users to see downtime as mandatory and not negotiable.
- Call logs
  - Track every support call with your vendors – what the problem was, how long it took to get a solution, effectiveness of solution.
  - Ensure you are receiving the level of support your company paid for and you expect.

Even potential downtime is an inconvenience to your end-users. Learn what they do with the storage systems and how downtime will impact them. Just because an end-user is not onsite during maintenance does not always mean there is not some process of theirs that needs access to storage. By providing advance warning of the downtime – often repeatedly – gives them ample time to make other arrangements.

Create a standardized email format to notify end-users of planned and unplanned downtime. Use it regularly so they learn to recognize it and know not to ignore it. Keep it short and simple so they actually read it. Tell them what will be offline, how it will impact them, and when to expect the storage to be available again. Do not forget to provide contact information.

If you can get approval for a regularly scheduled maintenance window, use the downtime window every time. The first time you decide not to use it, end-users will now believe that downtime can be negotiated. If there is no maintenance, use the time to practice restoring data from a backup or performing disaster recovery procedures.

Call logs not only serve as documentation on what issues your equipment experiences, they also serve as a grading card for vendor support. If the equipment you are purchasing is unreliable or the support you are receiving is inadequate, the call log can help you to negotiate a better deal on future purchases and renewals.

Manage Log Files

- Consider setting up log forwarding of systems and servers to a central system log (syslog) server.
  Use the `cluster log-forwarding` command to set up forwarding on ONTAP clusters.
- Establish a schedule to roll forward the log files of applications, like PuTTY, that do not have the capability built in.
- Add the creation of dedicated log files to your maintenance checklists.

In addition to the monitoring and reporting applications that watch over your systems, consider creating a dedicated syslog server. A syslog server acts as a repository for log files and as a failsafe and sanity check to your primary monitoring tools. You can configure your ONTAP clusters to forward their logs to up to 10 destinations by using the `cluster log-forwarding` command.

Log rolling is the process of closing out a log file before it becomes too large and cumbersome and opening a new log file. Many commercials applications that generate large or numerous log files do this automatically and retain three or more old log files. Applications like PuTTY, which are used intermittently, do not have this capability. To keep the log files from becoming unwieldy, create a schedule to manually roll the logs forward every month, quarter, or at least once per year. Archive the old log files so that you maintain a history. This information can be vital in tracking down a long-term issue that might have gone unnoticed.

Every time you perform maintenance, include a copy of the log files with your records. Doing so is easier if you make the creation of a new log file at the start and end of a maintenance cycle part of your process. If you need to send log files to Technical Support, a dedicated log file has less noise for the Technical Support team to read through.

Recommended Preventive Maintenance Checklist

- ✓ Replace failed components as soon as possible.
- ✓ View weekly AutoSupport and health checks in Active IQ on the NetApp Support site.
- ✓ Run Config Advisor once per month to detect cabling issues.
- ✓ Twice per year, read the release notes for new versions of ONTAP software to determine whether you can benefit from new features or bug fixes.
- ✓ Twice per year, verify Return Material Authorization (RMA) contact information and the expiration date of the support contracts.
- ✓ Change the Cluster and SVM Admin passwords at least twice per year.

 52

A properly configured NetApp storage system can be run with a set-it-and-forget-it mentality. But just like an automobile, the system runs better and more reliably with regular maintenance.

Knowledge Check: Questions

1. Where do you find the Upgrade Advisor tool to plan an ONTAP upgrade?
   a. System Manager
   b. in the ToolChest on the NetApp Support site
   c. upgradeontap.netapp.com
   d. in Active IQ on the NetApp Support site

Knowledge Check: Questions

2. Which three intervals does ONTAP follow when creating configuration backup files? (Choose three.)
   a. every hour
   b. every 8 hours
   c. every 12 hours
   d. daily
   e. weekly
   f. monthly

Additional Learning Resources

- OnCommand WFA blog: http://www.wfaguy.com/
- OneCollect 1.6 demonstration: https://www.youtube.com/watch?v=rvN2fI-OLIQ
- Storage Networking Industry Association (SNIA): https://www.snia.org/
- SAN Storage blog: http://www.sanadmin.net/
- Enterprise Storage website: http://www.enterprisestorageforum.com/
- Justin Parisi’s blog: https://whyistheinternetbroken.wordpress.com
- Drunken Data blog: http://www.drunkendata.com/
- Book: The Practice of System and Network Administration

OnCommand WFA blog: http://www.wfaguy.com/

OneCollect 1.6 demonstration: https://www.youtube.com/watch?v=rvN2fI-OLlQ

Storage Networking Industry Association (SNIA): https://www.snia.org/

SAN Storage blog: http://www.sanadmin.net/

Enterprise Storage website: http://www.enterprisestorageforum.com/

Justin Parisi’s blog: https://whyistheinternetbroken.wordpress.com

Drunken Data blog: http://www.drunkendata.com/

Book: The Practice of System and Network Administration

You can find the technical triage templates at https://kb.netapp.com/support/index?page=content&cat=TRIAGE&channel=HOW_TO

NetApp Hardware Universe: http://hwu.netapp.com

ONTAP 9 Documentation Center:

http://docs.netapp.com/ontap-9/index.jsp

System Administration Reference

Upgrade Express Guide

Upgrade and Revert/Downgrade Guide

Performance Monitoring Express Guide

Performance Management Power Guide

Workflow Automation 5.0 Installation and Setup Guide

TR-4211: Storage Performance Primer ONTAP 9.2 https://www.netapp.com/us/media/tr-4211.pdf

How to efficiently search the event log in clustered Data ONTAP

https://www.youtube.com/watch?v=5qu8hJYfKm8

Module Review

This module focused on enabling you to:

- Navigate the Active IQ customer dashboard
- Plan for ONTAP software upgrades
- Follow recommended practices for peak performance
- Configure event notifications and alerts
- Prepare to engage NetApp technical support
- Perform cluster maintenance

ACTION: Complete an Exercise

Module 10: Installing and Configuring Config Advisor

Duration: 30 minutes

Access your exercise equipment.

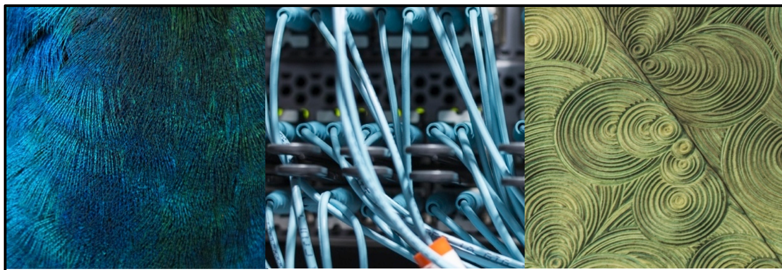
Use the login credentials that your instructor provided to you.

Complete the specified exercises.

- Go to the exercise for the module.
- Start with Exercise 10-1.
- Stop at the end of Exercise 10-1.

Participate in the review session.

- Share your results.
- Report issues.



Addendum
ONTAP Software Upgrades

Stages of an Automated Upgrade

Stage 1
Select

Select the ONTAP software image:

- Display the current cluster version.
- Select a software image:
  - Select an available image.
  - Download an image from the NetApp Support site.

Stage 2
Validate

View and validate the cluster:

- Validate cluster update readiness.
- Display validation errors and warnings with corrective action.
- Update when the validation is completed successfully.
- Enable update with warnings.

Stage 3
Update

Update the cluster:

- Update all the nodes in the cluster or update an HA pair in the cluster.
- Support a rolling update or a batch update. (The default update type depends on the number of nodes in the cluster.)

The automated upgrades that you can perform by using System Manager consist of three stages: select, validate, and update.

In the first stage, you select the ONTAP software image. The current version details are displayed for each node or HA pair.

In the second stage, you view and validate the cluster against the software image version for the update. A pre-update validation helps you determine whether the cluster is ready for an update. If the validation is completed with errors, a table displays the status of the various components and the required corrective actions. You can perform the update only when the validation is completed successfully.

In the third and final stage, you either update all the nodes in the cluster or update an HA pair in the cluster to the selected version of the software image. While the update is in progress, you can pause and then either cancel or resume the update. If an error occurs, the update is paused, and an error message is displayed with the remedial steps. You can resume the update after performing the remedial steps or cancel the update. You can view the table with the node name, uptime, state, and ONTAP software version when the update is successfully completed.

USB Port Use Cases

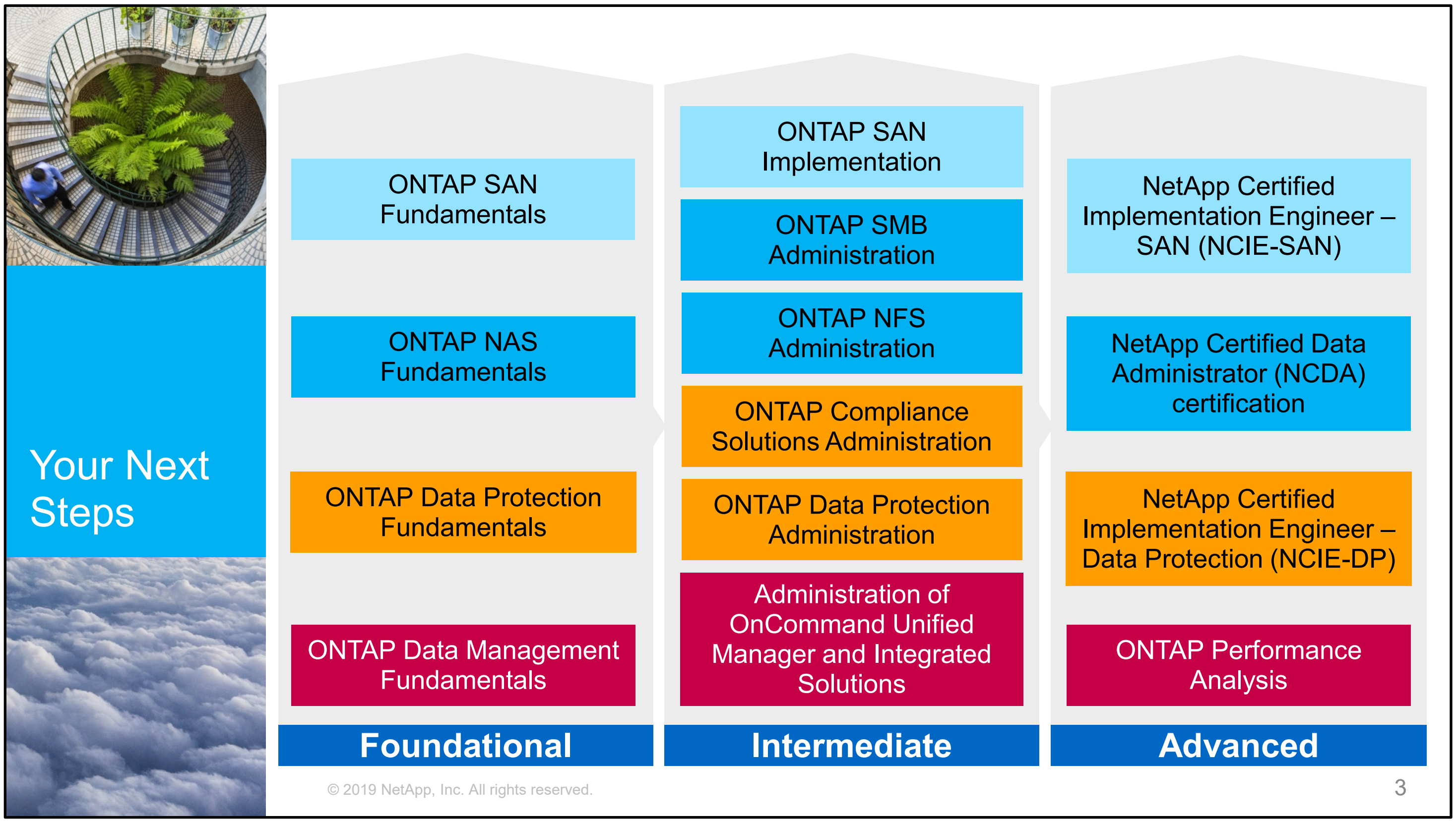
Scenario	Prerequisites	Command
Perform boot device recovery from the LOADER prompt.	▪ The USB 2.0 device is formatted to FAT32 with the correct ONTAP image.tgz file. ▪ The device is not hot-pluggable; after you insert the USB device, you must boot to the LOADER prompt.	▪ At the LOADER prompt, use **`boot_recovery`** by using the netboot image. ▪ At the boot menu, select the appropriate ONTAP image.
Fetch ONTAP software for installation.	The USB 2.0 device is formatted to FAT32 with the correct ONTAP image.	▪ Use the **`system node image update/get`** command. ▪ From the additional options for the command, fetch ONTAP software from the USB device.
Fetch service images for firmware update.	The USB 2.0 device is formatted to FAT32 with the correct service image.	▪ Use the **`system node firmware download`** command. ▪ From the additional options for the command, fetch ONTAP software from the USB device.

The chart shows scenarios in which you can use the USB port. Each scenario has prerequisite considerations. The Command column shows you the commands to use in each scenario.

Module 11
Course Review

Course Review

Day 1	Day 2	Day 3
NetApp ONTAP 9 features Cluster management Networking review	Managing physical and logical storage Data access with NAS and SAN protocols	Data-protection features Storage efficiency Cloning volumes, files, and LUNs Preventive maintenance



Regardless of where your role as a storage administrator takes you, NetApp offers courses and documentation to take you there. Never stop learning and growing.

Read the ONTAP *Storage Administration Reference Guide* cover to cover.

-Your future self

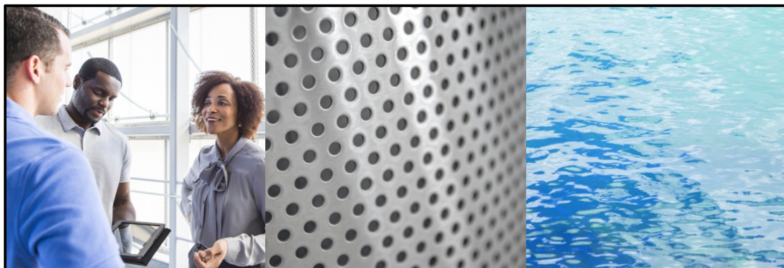
The *Storage Administration Reference Guide* contains information you will need for your day-to-day work.

NetApp also encourages you to cross-train your coworkers and contribute to the larger storage administration community.

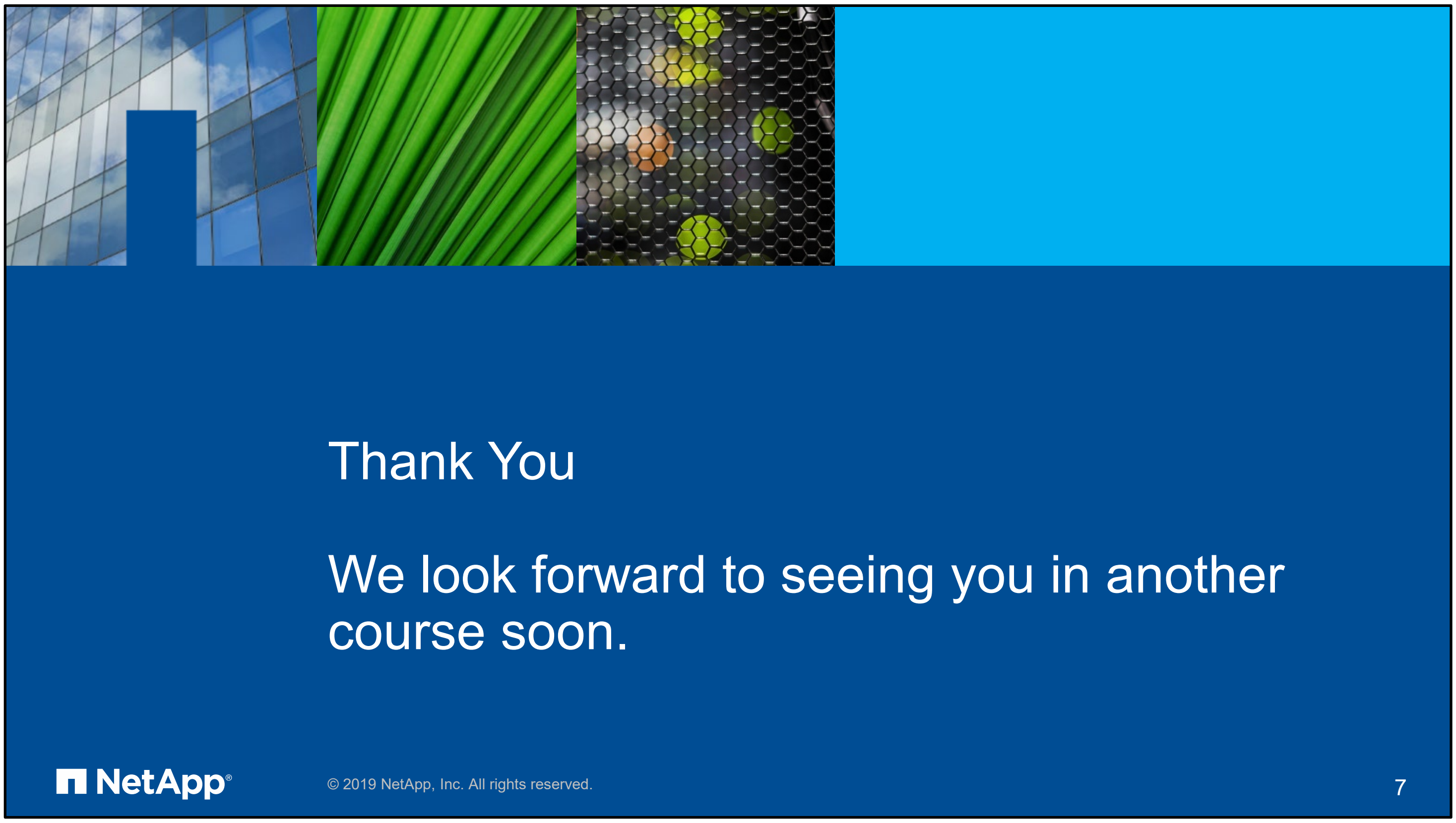
ACTION: Provide Feedback

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 instruct you on how to find the survey for this class and how to use the survey website.



Closing Thoughts



Thank you for attending the course and providing your voice to the conversation. We hope you are staying for the Data Protection course. If not, we hope to see you return for another course soon.