# Contents

- Deciding whether to read this information .................................................. 6
- Data Fabric Solution for Cloud Backup overview ........................................... 7
  - Data Fabric Solution for Cloud Backup components ...................................... 8
  - Data Fabric Solution for Cloud Backup features ........................................... 9
  - What you can do with Data Fabric Solution for Cloud Backup .................... 10
- Installation and configuration workflow with SnapCenter data protection management .......................................................... 11
- Installation and configuration workflow without SnapCenter data protection management .......................................................... 12
- Preparing for the Data Fabric Solution for Cloud Backup deployment ...................... 13
  - ONTAP requirements .................................................................................. 13
  - SnapCenter host requirements .................................................................... 14
  - SnapCenter file catalog requirements ...................................................... 15
  - AltaVault requirements ............................................................................... 16
  - Supported browsers .................................................................................... 16
  - Licensing requirements ............................................................................... 17
  - Connection and port requirements ............................................................ 19
  - Credential requirements ............................................................................ 20
- Installing the Data Fabric Solution for Cloud Backup ......................................... 21
  - Preparing the ONTAP environment ............................................................. 21
    - Installing or upgrading ONTAP ............................................................... 21
    - Adding appropriate ONTAP licenses ...................................................... 22
    - Establishing cluster peering for ONTAP to cloud backups .................... 23
  - Preparing the SnapCenter Linux file catalog server .......................................... 30
    - Installing Linux catalog servers ............................................................ 30
    - Configuring SnapCenter file catalog ports .......................................... 31
    - Adding a non-root user and configuring sudo privileges ....................... 32
    - Verifying the Java runtime environment ............................................... 33
    - Ensuring the Linux server is accessible for NAS file services file catalog ... 33
  - Installing SnapCenter for Data Fabric Solution for Cloud Backup ..................... 34
    - Installing the SnapCenter Server ............................................................ 34
    - Checking the status of NAS File Services components after SnapCenter installation ............................................................................. 36
    - Installing or upgrading AltaVault ............................................................ 38
- Configuring the AltaVault appliance .............................................................. 39
  - Logging in to AltaVault ............................................................................... 40
  - Configuring basics in AltaVault ................................................................. 40
  - Configuring AltaVault using the GUI ....................................................... 40
    - Enabling the SnapMirror service and configuring whitelist IP connections using the AltaVault GUI ......................................................... 40
Enabling SnapMirror long-term retention mode in AltaVault .................. 42
Enabling SnapCenter access to AltaVault ............................................... 43
Adding a SnapCenter role-based user account to enable SnapCenter
storage connections to an AltaVault appliance .................................. 43
Starting the AltaVault Storage Optimization Service ................................ 44
Configuring AltaVault using the AltaVault CLI ........................................ 44
Enabling the SnapMirror service using the AltaVault CLI .................... 44
Configuring a whitelist of IP connections using the AltaVault CLI .......... 45
Enabling SnapMirror long-term retention mode using the AltaVault CLI .. 46
Enabling access to SnapCenter using the AltaVault CLI ....................... 47
Adding a SnapCenter role-based user account to enable storage
connections to an AltaVault appliance .................................................. 47
Starting the AltaVault Optimization Service using the AltaVault CLI ...... 48

Configuring SnapCenter for Data Fabric Solution for Cloud Backup
.................................................................................................................. 49
Logging in to SnapCenter ........................................................................ 49
Configuring the Infrastructure Admin role for AltaVault access .......... 50
Setting up storage system connections ............................................... 51
Setting up your CIFS servers Run As credentials for SnapCenter Plug-in for
NAS File Services .................................................................................... 54
Configuring CIFS servers for Data Fabric Solution for Cloud Backup ..... 54
Protecting the SnapCenter file catalog and the repository ...................... 55
Preparing the PowerShell environment ............................................... 55
Protecting the file catalog and SnapCenter repository with PowerShell
cmdlets .................................................................................................. 56

Backing up NAS file services data to the cloud and restoring data
with SnapCenter management .................................................................. 58
Using policies to protect NAS file services data ..................................... 59
Backing up NAS file services data to the cloud ....................................... 61
    Backing up NAS file services data to the cloud using SnapCenter and
    AltaVault ............................................................................................ 61
    Monitoring data protection progress in the SnapCenter Activity pane ... 62
    Monitoring backup operations from the Jobs page ......................... 63
    Verifying backup to the cloud completion on AltaVault (optional) ....... 64
Restoring NAS file data from the cloud using SnapCenter ..................... 67
    Searching in the file catalog for a specific file to restore using keywords
    and filters ............................................................................................ 68
    Restoring NAS file data from the cloud using SnapCenter .................. 70
    Monitoring restore operations from the Jobs page ......................... 71

Backing up NAS file services data to the cloud and restoring it using
ONTAP commands ................................................................................... 72
    Creating a SnapMirror protection relationship .................................. 72
    Reviewing volume status and contents ............................................. 73
    Creating and initializing a SnapMirror protection relationship .......... 73
    Backing up NAS file services data to the cloud using ONTAP commands .. 75
Performing an incremental backup from ONTAP to the cloud using the ONTAP CLI ........................................ 75
Monitoring backup progress using the ONTAP CLI ....................................... 77
Restoring NAS file services data from the cloud using ONTAP commands ....... 78
Restoring a full backup from the cloud using the ONTAP CLI ...................... 78
Restoring a single file from the cloud to ONTAP using the ONTAP CLI .... 80
Viewing data protection reports for NAS file services .............................. 83
Where to go next ...................................................................................... 84
Copyright information ............................................................................... 85
Trademark information ............................................................................. 86
How to send comments about documentation and receive update notifications ...................................................................................................................... 87
Index ......................................................................................................... 88
Deciding whether to read this information

This information explains how to back up local NAS file services data to the cloud and restore it. This information also explains how to install and configure components of the Data Fabric Solution for Cloud Backup, which includes ONTAP, AltaVault, and SnapCenter.

You should read this information if you want to protect NAS file services data in the following ways:

- Back up NAS file services data to the cloud or restore from the cloud using AltaVault and using SnapCenter protection management
- Back up NAS file services data to the cloud or restore from the cloud without using SnapCenter protection management and instead using ONTAP CLI commands

Before you begin the installation, you should read the following planning information in this guide:

- ONTAP requirements
- SnapCenter Server requirements and SnapCenter Linux file catalog requirements
- AltaVault requirements
- Host requirements, connection and port requirements, supported browsers, and licensing requirements

You can find more information available on the Data Fabric Solution for Cloud Backup Resources page.

NetApp Data Fabric Solution for Cloud Backup Resources
Data Fabric Solution for Cloud Backup overview

With the Data Fabric Solution for Cloud Backup, storage administrators and IT generalists can perform Snapshot copy-based data protection operations for Windows and UNIX file shares to and from public or private cloud object stores. Delivering high service levels with fast Snapshot copies and efficient array-based replication, the solution includes NetApp ONTAP, SnapCenter data management software, and AltaVault cloud-integrated storage software and appliance.

ONTAP provides storage management and initiation and management of protection operations using a command-line interface (CLI). SnapCenter provides support for protection operations initiation and management. AltaVault provides storage-optimized caching in and replication to cloud storage providers for Snapshot copies of file share data from ONTAP.

The Data Fabric Solution for Cloud Backup using SnapMirror technology enables administrators to back up NFS (NFS v4) and SMB (SMB v3) NAS file services and home directories to the cloud using AltaVault appliances.

The ONTAP CLI can be used for additional operations not supported by the SnapCenter graphical interface. For example, using the ONTAP CLI, you can also back up ONTAP LUNs.

Flexible configurations are available for All Flash FAS (AFF) or FAS in these topologies:

- Primary storage (AFF or FAS) to AltaVault
- Primary storage (AFF or FAS) to secondary storage (FAS) to AltaVault
Data Fabric Solution for Cloud Backup components

Data Fabric Solution for Cloud Backup involves multiple products that together provide data protection of NAS file services to public or private cloud providers.

- ONTAP 9.1
- SnapCenter 2.0 and the SnapCenter Plug-in for NAS File Services
- AltaVault 4.3 (physical or virtual)

ONTAP provides the foundation for data protection operations of NAS file services. Using ONTAP CLI, you can initiate, manage, and monitor data protection operations.

SnapCenter provides support for the management of policies and schedules, and the orchestration of backup and restore operations via AltaVault for NAS file services.

AltaVault provides optimized storage for backup and restore operations, backed by both public and private cloud providers, including NetApp StorageGRID Webscale, Amazon Web Services, Microsoft Azure, and IBM BlueMix.

When an administrator creates a SnapMirror relationship in ONTAP with AltaVault, a share is created in AltaVault, however, when you use SnapCenter to initiate backups to AltaVault, the
SnapMirror relationship is automatically created. AltaVault can simultaneously accept workloads from SnapMirror as well as SMB, NFS, and Open Storage (OST).

Each share on AltaVault is associated with one ONTAP FlexVol volume. AltaVault supports up to 500 SnapMirror shares.

**Data Fabric Solution for Cloud Backup features**

Each component in the Data Fabric Solution for Cloud Backup contributes to the completion of cloud-integrated data protection services for NAS file services.

The Data Fabric Solution for Cloud Backup includes the following key features using ONTAP, SnapCenter, and AltaVault in combination:

- Ability to transport NAS file services data on primary or secondary storage systems to private or public cloud service providers
- Data protection of ONTAP FlexVol volumes to the cloud via AltaVault
- Choice of All Flash FAS (AFF) or FAS hybrid storage for primary storage and FAS on optional secondary storage backup to the cloud
- Use of Snapshot copy technology and SnapMirror data protocol, which enables fast and efficient data transfer between ONTAP and AltaVault without having to stream data through a backup server and then to the AltaVault appliance
- Cost-effective tape replacement solution

ONTAP includes these key features:

- Data management across flash and disk
- Data protection of file workloads for this solution
- Ability to leverage the architecture you want: NetApp engineered systems, software-defined storage, and the cloud
- Deployment of NAS workloads for this solution on a unified storage architecture
- Storage footprint and cost reduction with inline data compression and deduplication

When you use the Data Fabric Solution for Cloud Backup, data deduplication occurs in AltaVault.

**Note:** This solution does not support ONTAP Select or ONTAP Cloud.

SnapCenter enables self-service data management with role-based access control. With support for NAS file services, SnapCenter provides these additional features:

- Single management interface to manage NAS file services
- Access governed by role-based access control
- Preconfigured backup policies that simplify management for NAS file services
- Scalable, highly available file catalog for quick location and recovery of single files
- Search or browse option to identify a file for restore quickly
- Visual representation of backup copies that lets you quickly identify backup to restore

AltaVault include these key features:

- Ability to transport data to both public and private cloud providers

**Note:** Data Fabric Solution for Cloud Backup does not currently support AWS Glacier.
• Accelerated data protection with the deduplication and compression of data volumes at ingest
Data transmitted from ONTAP to AltaVault is not deduplicated or compressed. All data stored on AltaVault is deduplicated and compressed upon ingest and is always replicated to the specified cloud storage for efficient transmission.

• Data encryption applied at ingest and securely transmitted to the cloud storage provider, reducing security and compliance risks locally and in the cloud

• Flexible deployment and scale with physical or virtual environments

What you can do with Data Fabric Solution for Cloud Backup

Using ONTAP, SnapMirror technology, SnapCenter, and AltaVault, administrators can protect their NAS file services data on FlexVol volumes in public or private clouds.

With the Data Fabric Solution for Cloud Backup, you can accomplish the following:

• Perform a single baseline Snapshot copy-based backup and then block-level incremental backups forever from ONTAP to AltaVault and then to public or private cloud providers.

• Perform a single file restore of data from AltaVault to ONTAP using SnapCenter or ONTAP CLI. The ONTAP CLI can be used for additional operations not supported by the SnapCenter graphical interface. For example, using the ONTAP CLI, you can also back up ONTAP LUNs. Also, using SnapCenter to perform a single file restore, you must restore the file to the original location while using the ONTAP CLI, you can specify a different path to restore the file. With the ONTAP CLI, you can perform a full volume restore in addition to the single file restore.

Using SnapCenter, you can orchestrate the following:

• Back up NAS file services data (on FlexVol volumes) from flash to disk to AltaVault and to the cloud.

• Apply predefined or custom policies that you have copied for your backup and retention requirements.

• Restore individual files within file shares to the original location on the same volume.

  **Best Practice:** You might want to rename the current file if it exists, so it is not overridden.

• Search for data to restore in one of two ways. Either use a powerful keyword search in the SnapCenter file catalog and apply filters to find specific files quickly among many files or, from a selected backup, find and restore a file.

• Manage backup schedules and policies.

Using AltaVault, a required component of the solution, you can complete the cloud backup protection by performing these tasks:

• Perform efficient and secure backup to more than 30 clouds, public or private.

• Reduce bandwidth traffic to the cloud, saving network usage and in-cloud storage capacity with inline deduplication and compression.

• Accomplish long-term retention in the cloud.

• Protect the data with Always On 256 AES encryption

• Connect multiple FAS systems to a single AltaVault, providing global deduplication across your entire environment.
Installation and configuration workflow with SnapCenter data protection management

Follow this workflow when using SnapCenter as part of the Data Fabric Solution for Cloud Backup.

- Prepare ONTAP environment:
  - Install or upgrade ONTAP.
  - Add appropriate licenses.
  - Establish cluster peering for backups from ONTAP to the cloud and configure intercluster LIFs.

- Prepare SnapCenter Linux file catalog servers:
  - Install catalog server.
  - Configure file catalog ports.
  - Add non-root user and sudo privileges.
  - Verify Java runtime environment.
  - Ensure Linux server is accessible to SnapCenter Server host for the file catalog.

- Install SnapCenter:
  - Enable file catalog indexing and add catalog servers.
  - Check components after SnapCenter installation.

- Install or upgrade AltaVault.

- Configure AltaVault with AltaVault GUI or CLI:
  - Configure basics such as cloud providers and encryption key in Cloud Settings wizard, as usual.
  - Enable the SnapMirror service.
  - Optionally enable SnapMirror long-term retention mode in AltaVault.
  - Enable SnapCenter access to AltaVault.
  - Add a role-based user to enable SnapCenter storage connections to an AltaVault appliance.
  - Start the AltaVault Storage Optimization Service.

- Configure SnapCenter environment:
  - Configure role-based access control (RBAC) with Infrastructure Admin role.
  - Configure a storage connection to each AltaVault appliance and to an ONTAP Cluster.
  - For CIFS shares only (not for NFS), create a Run As account.
  - For CIFS shares only (not for NFS), configure a CIFS server.
  - Protect the file catalog and repository.

- Create backup and restore tests of NAS file services data with SnapCenter GUI or ONTAP CLI:
  - Create a test backup and first indexed file catalog.
  - Monitor backup progress.
  - Verify the file catalog using the Restore option.
  - Restore the test backup.
Installation and configuration workflow without SnapCenter data protection management

The Data Fabric Solution for Cloud Backup can also be implemented with just ONTAP and AltaVault without using SnapCenter. To do so, you use ONTAP commands to install and configure the components of the solution without SnapCenter.

1. **Prepare ONTAP environment:**
   - Install or upgrade ONTAP.
   - Add appropriate licenses.
   - Establish cluster peering for backups from ONTAP to the cloud and configure intercluster LIFs.

2. **Install or upgrade AltaVault.**

3. **Configure AltaVault with AltaVault GUI or CLI:**
   - Configure basics such as cloud providers and encryption key in Cloud Settings wizard, as usual.
   - Enable and configure SnapMirror service, add intercluster LIFs to an IP whitelist.
   - Optionally enable SnapMirror long-term retention mode in AltaVault.
   - Start the AltaVault Storage Optimization Service.

4. **Create backup and restore tests of NAS file services data with ONTAP CLIs:**
   - Create a test backup.
   - Monitor backup progress.
   - Restore the test backup.
Preparing for the Data Fabric Solution for Cloud Backup deployment

Before you install and set up Data Fabric Solution for Cloud Backup, you must prepare your environment and understand the information that you need for installation and setup.

About this task
The single most important key to a successful implementation of the Data Fabric Solution for Cloud Backup is proper preparation. Ensuring that the proper hardware and software is in place and is properly configured is essential prior to beginning installation. Follow the guidance for supported versions, models, and configurations.

ONTAP requirements
Before you begin the Data Fabric Solution for Cloud Backup deployment, you should be familiar with the ONTAP requirements. You should configure one or more clusters using these requirements.

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP version</td>
<td>ONTAP 9.1 or greater</td>
</tr>
<tr>
<td>Models</td>
<td>No restrictions on models.</td>
</tr>
<tr>
<td></td>
<td>For storage system requirements for ONTAP 9.1, see the Hardware Universe.</td>
</tr>
<tr>
<td></td>
<td><em>NetApp Hardware Universe</em></td>
</tr>
<tr>
<td>Storage type</td>
<td>Primary: Any system that runs ONTAP 9.1 or greater. FAS and All Flash FAS (AFF) only.</td>
</tr>
<tr>
<td></td>
<td>Secondary: FAS only.</td>
</tr>
<tr>
<td>Storage amount</td>
<td>No minimum requirements.</td>
</tr>
<tr>
<td>Intercluster LIFs</td>
<td>Required.</td>
</tr>
<tr>
<td>Cluster peering and SVM peering</td>
<td>Cluster peering requirements differ based on the type of backup:</td>
</tr>
<tr>
<td></td>
<td>• For backups from ONTAP to AltaVault, cluster peering is not required.</td>
</tr>
<tr>
<td></td>
<td>• For backups from ONTAP to ONTAP to AltaVault, cluster peering and storage virtual machine (SVM) peering are required.</td>
</tr>
<tr>
<td></td>
<td>The process for configuring cluster and SVM peering differs depending on whether peering has already been configured:</td>
</tr>
<tr>
<td></td>
<td>• If cluster peers are not already configured, you must configure both cluster and SVM peering manually.</td>
</tr>
<tr>
<td></td>
<td>• If cluster peers are already configured, you do not need to configure SVM peering; it is done automatically.</td>
</tr>
</tbody>
</table>

If you want to restore using AltaVault directly to the primary FAS, the primary system requires ONTAP 9.1 or greater.
In a cascade configuration where SnapMirror relationships (such as from ONTAP to ONTAP) exist, the secondary system requires ONTAP 9.1 or greater, but the primary system could use ONTAP 8.3.1 or greater.

The Data Fabric Solution for Cloud Backup supports cascade configurations as well where AltaVault becomes the endpoint. The restore path in this configuration requires two steps: restoring from AltaVault to secondary FAS and then from secondary FAS to primary FAS or AFF.

For the latest information, see the Interoperability Matrix.

**Related information**

*NetApp Interoperability Matrix Tool*

---

**SnapCenter host requirements**

Before you begin the Data Fabric Solution for Cloud Backup deployment, you should be familiar with SnapCenter host requirements.

The SnapCenter Server should meet the following minimum requirements. The SnapCenter Server should have a dedicated resource; it should not be shared.

All supported Windows operating systems are 64-bit only.

The Data Fabric Solution for Cloud Backup requires MySQL Server on new SnapCenter installations only. Upgrades from existing SnapCenter installations are not supported.

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>2.0</td>
</tr>
<tr>
<td>CPU</td>
<td>4 CPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>16 GB</td>
</tr>
<tr>
<td>Operating System</td>
<td>The following are supported:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 DCE, R2, Se, R2 SE</td>
</tr>
<tr>
<td></td>
<td>Microsoft has identified an HTTP security vulnerability in their Windows operating systems that requires the installation of KB3042553-x64.</td>
</tr>
<tr>
<td>SnapCenter storage amount</td>
<td>40 GB for both the software and the repository</td>
</tr>
<tr>
<td>SnapCenter metadata repository</td>
<td>MySQL Server 5.7 or greater</td>
</tr>
<tr>
<td></td>
<td>The installation places the SnapCenter repository on drive C of the host. After installation, you might want to migrate the repository to a different location. See the repository migration information in the <a href="#">Administration Guide</a>.</td>
</tr>
<tr>
<td>Third-party libraries required on the SnapCenter Server</td>
<td>• Java 1.8.0.71 or later (Oracle or OpenJDK), 64-bit version. Must be installed before installing SnapCenter.</td>
</tr>
<tr>
<td></td>
<td>• File archiver utility p7zip-9.20.1-8.1.1.x86_64.rpm or exe. Included in installation.</td>
</tr>
</tbody>
</table>

For the latest information, see the Interoperability Matrix.
SnapCenter file catalog requirements

Before you begin the Data Fabric Solution for Cloud Backup deployment, you should be familiar with SnapCenter file catalog requirements.

File catalog requirements

One or more servers or VMs should be dedicated to the file catalog.

**Best Practice:** We recommend two separate nodes for the SnapCenter file catalog, with each node having enough disk space for indexing, depending on how much data will be indexed per the table below. We also recommend a replica for each partition shard for file catalog high availability and disaster recovery.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 cores</td>
</tr>
<tr>
<td>Memory</td>
<td>24 GB RAM</td>
</tr>
<tr>
<td>Operating system</td>
<td>Red Hat Enterprise Linux (RHEL) 7.0, 7.1, and 7.2</td>
</tr>
<tr>
<td>Dedicated or shared server</td>
<td>Dedicated VM</td>
</tr>
<tr>
<td>Supported Hypervisors</td>
<td>VMware, Hyper-v</td>
</tr>
<tr>
<td>Java requirements</td>
<td>Java 1.8.0.71 or later (Oracle or OpenJDK), 64-bit version. Must be installed before installing SnapCenter.</td>
</tr>
<tr>
<td>Local storage</td>
<td>1 GB minimum space available in /tmp and /opt</td>
</tr>
<tr>
<td>Linux host permissions</td>
<td>Root access is not required.</td>
</tr>
</tbody>
</table>

You must have enabled the password-based SSH connections for the root or non-root user. You must configure the sudo privileges for the non-root user.

File catalog sizing recommendations

We recommend the following file catalog storage depending on the number of files to be indexed:

<table>
<thead>
<tr>
<th>Total number of files</th>
<th>Size</th>
<th>Disk capacity per node</th>
<th>CPU per node</th>
<th>Physical RAM per node</th>
<th>Replica per shard*</th>
<th>Total number of machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 million</td>
<td>50 GB</td>
<td>250 GB</td>
<td>8 cores</td>
<td>12 GB</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>200 million</td>
<td>100 GB</td>
<td>250 GB</td>
<td>8 cores</td>
<td>24 GB</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>400 million</td>
<td>250 GB</td>
<td>250 GB</td>
<td>8 cores</td>
<td>48 GB</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1 billion</td>
<td>500 GB</td>
<td>500 GB</td>
<td>8 cores</td>
<td>120 GB</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

* A shard is a logical piece of a complete logical index. Each shard is made up of one or more replicas. A replica is a copy of a shard. Each replica is a running instance of the catalog.
A LUN must be provisioned for storing the file catalog data. During installation, you can specify the path to the preconfigured, provisioned LUN.

For High Availability, we recommend that there be a minimum of two catalog servers, each with a replica. In the case of two replicas, both must be running when the SnapCenter software is installed.

**AltaVault requirements**

Before you begin the Data Fabric Solution for Cloud Backup deployment, you should be familiar with the AltaVault requirements.

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Models</td>
<td>AltaVault physical models: AVA-400, AVA-800</td>
</tr>
<tr>
<td></td>
<td>AltaVault virtual models: AVA-v2, AVA-v8, AVA-v16, AVA-v32</td>
</tr>
<tr>
<td></td>
<td>AltaVault cloud models (AVA-c) are not supported.</td>
</tr>
<tr>
<td>Version</td>
<td>4.3 or greater</td>
</tr>
<tr>
<td>Storage type</td>
<td><strong>Best Practice:</strong> For virtual appliances, we recommend a minimum of RAID-1 and high performing SATA, NL-SAS, or SSD.</td>
</tr>
<tr>
<td>AltaVault cache storage amount</td>
<td>Workload dependent. Size depends on how much data is to be protected and cached locally.</td>
</tr>
</tbody>
</table>

Each AltaVault instance can be connected to one cloud provider. If you configure multiple AltaVault appliances, then each AltaVault appliance can be configured to a different cloud provider. Each AltaVault appliance can support multiple protocols simultaneously, for example, SnapMirror and NFS.

Each ONTAP volume has a single relationship with one AltaVault system.

**Note:** The Data Fabric Solution for Cloud Backup configuration cannot fan out from a single ONTAP volume to multiple AltaVault destinations. However, multiple different ONTAP volumes can be pointed to the same AltaVault (fan-in) for global deduplication of data.

For the latest information and additional AltaVault requirements, see the AltaVault documentation and Interoperability Matrix.

**Related information**

*NetApp Interoperability Matrix Tool*
*NetApp Documentation: AltaVault*

**Supported browsers**

Data Fabric Solution for Cloud Backup supports the following web browsers.

- Chrome version 53 or later
- Internet Explorer 11.0 or later
  - Only default-level security is supported.
  - Making changes to Internet Explorer security settings results in significant browser display issues.
  - Internet Explorer compatibility view must be disabled.
Connections to AltaVault and SnapCenter require HTTPS.
For the latest information, see the Interoperability Matrix.

**Related information**

*NetApp Interoperability Matrix Tool*

**Licensing requirements**

The Data Fabric Solution for Cloud Backup requires several licenses to enable protection operations.

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
<th>Where required</th>
</tr>
</thead>
</table>
| ONTAP    | ONTAP requires one of the following licenses:  
• SnapMirror license (by itself or with Premium bundle)  
• SnapVault license (by itself or with Premium bundle)  
  Some platforms require the Premium bundle; no separate licenses are available for SnapMirror or SnapVault with these platforms.  
  The Premium bundle can be on a legacy system or on a new platform. |                                                                                                                                                                                                              |
| SnapMirror | A license for mirroring backup sets to a destination storage system. Required for this solution.  
  Existing SnapMirror licenses can be used.                                                                                                                                                                                                                               | On primary storage system only.  
  Typically for FAS-to-FAS replication,  
  SnapMirror is required on both primary and destination systems.  
  With Data Fabric Solution for Cloud Backup, the SnapMirror license is required only on primary storage, not on the destination system because AltaVault is the destination. |
<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
<th>Where required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapVault</td>
<td>An optional license for disk-to-disk backup replication to a destination storage system.</td>
<td>Depends on the type of operation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For primary storage (AFF or FAS) to AltaVault, required on primary storage system only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For primary storage (AFF or FAS) to secondary storage (FAS) to AltaVault, required on both primary and destination.</td>
</tr>
<tr>
<td>SnapRestore</td>
<td>A required license that enables SnapCenter to restore and verify backup sets.</td>
<td>On primary storage systems. Also required on SnapVault destination systems to perform remote verification and to restore from a backup. Also required on SnapMirror destination systems to perform remote verification.</td>
</tr>
</tbody>
</table>
| AltaVault | A capacity-based license required for virtual models to enforce capacity-based storage sizes. Capacities for physical appliances are limited by the amount of cache installed on the system.  
**Note:** A 90 days trial license is available for virtual appliances.     | On AltaVault virtual appliance                                                                                                           |
SnapCenter includes these licenses:

- Standard – Support for backup and recovery of ONTAP storage, Clone Life Cycle management, basic reporting, task automation, host file systems (Windows, Linux, UNIX), support for custom applications or databases, update of Snapshot copies to SnapMirror and SnapVault secondary destinations, virtualization with VMware, and support for enterprise applications (Microsoft SQL Server, Oracle)
  - FAS and All Flash FAS (AFF): Included in Premium Bundle

  **Note:** ONTAP Select and ONTAP Cloud are not supported in the Data Fabric Solution for Cloud Backup.

- Advanced - Optional license. Required to support using AltaVault and the file catalog
  - FAS, All Flash FAS, ONTAP Select, ONTAP Cloud: A la carte license, charged on the used storage capacity that is managed by SnapCenter

  **Note:** ONTAP Select and ONTAP Cloud are not supported in the Data Fabric Solution for Cloud Backup.

**Note:** A 90 days trial license is available for both SnapCenter standard and advanced licenses.

You can use SnapCenter to configure multiple replication relationships with one or more AltaVault appliances without additional licenses.

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
<th>Where required</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapCenter</td>
<td>Require for Data Fabric Solution for Cloud Backup.</td>
<td>On primary storage systems</td>
</tr>
<tr>
<td>FlexClone</td>
<td>Required for Data Fabric Solution for Cloud Backup.</td>
<td>On SnapCenter Server</td>
</tr>
<tr>
<td>Protocols</td>
<td>For SMB shares, the CIFS license</td>
<td>On primary storage systems. Required on SnapMirror destination systems to serve data if a source volume is unavailable.</td>
</tr>
</tbody>
</table>
### Type of port

<table>
<thead>
<tr>
<th>Type of port</th>
<th>Default port</th>
</tr>
</thead>
</table>
| SnapCenter port | 8146 (HTTPS), customizable as in the URL \texttt{https://server:8146}  
Used for communication between the SnapCenter client (the SnapCenter user) and SnapCenter Server. Also used for communication from plug-in hosts to SnapCenter Server. |
| SnapCenter SMCore communication port | 8145 (HTTPS), bidirectional, customizable  
Used for communication between SnapCenter Server and hosts where SnapCenter plug-ins are installed. |
| SnapCenter file catalog ports on Linux server | 8145 customizable  
2181, 2888, 3888, 8983  
Used for communication between SnapCenter Server and the index servers and also between index servers. |
| SnapCenter Service Level Manager port | 58443 (HTTPS)  
Used for communication between SnapCenter Server and SnapCenter Service Level Manager Application Server. |
| ONTAP to AltaVault | 5010 (TCP).  
Used for communication between ONTAP and AltaVault; requires at least one intercluster LIF. The best practice is to connect to a 10Gb Ethernet switch. |
| AltaVault | 5010 (TCP).  
Requires one or more data interfaces. |
| AltaVault GUI | 443 (HTTPS), bidirectional, fixed  
Used for communication between the client and AltaVault GUI. Only HTTPS is supported. |
| AltaVault REST APIs | 8443 (HTTPS), bidirectional, fixed  
Used for communication between SnapCenter and AltaVault. |

Firewalls, proxies, or other network devices should not interfere with connections.

You cannot modify the SnapCenter port number after you install. To change a port number after installation, you must uninstall and install SnapCenter again.

---

### Credential requirements

Using SnapCenter in the Data Fabric Solution for Cloud Backup requires a user with ONTAP cluster administration credentials. These credentials are also required to sign in to the ONTAP CLI, if you prefer to use the CLI.

In addition to ONTAP cluster administration credentials, you must add a role-based account to AltaVault that enables you to add a storage connection in SnapCenter, and in SnapCenter, you must must add a role-based access control user with the Infrastructure Admin role for AltaVault access.

### Related tasks

- [Adding a SnapCenter role-based user account to enable SnapCenter storage connections to an AltaVault appliance](#) on page 43
- [Configuring the Infrastructure Admin role for AltaVault access](#) on page 50

To configure role-based access control for SnapCenter users, you add users or groups to a role and the role's permissions.
Installing the Data Fabric Solution for Cloud Backup

Although you can install the components of the solution in a different order, you should follow the recommended installation order.

- ONTAP 9.1. This can be an existing ONTAP deployment or an upgrade to ONTAP 9.1.
- SnapCenter 2.0. This must be a new installation.
- AltaVault 4.3. This can be an existing AltaVault deployment or an upgrade to AltaVault 4.3 or later.

Steps

1. Preparing the ONTAP environment on page 21
   Preparing the ONTAP environment for using the SnapCenter Plug-in for NAS File Services involves several tasks.

2. Preparing the SnapCenter Linux file catalog server on page 30
   SnapCenter requires one or more Linux file catalog servers in addition to the SnapCenter Server. Before you install the SnapCenter Server, you should prepare the file catalog servers so that they are accessible during the installation.

3. Installing SnapCenter for Data Fabric Solution for Cloud Backup on page 34
   SnapCenter is one of the Data Fabric Solution for Cloud Backup components. Installing SnapCenter involves several tasks.

4. Installing or upgrading AltaVault on page 38
   The Data Fabric Solution for Cloud Backup requires AltaVault to perform data protection to the cloud.

Preparing the ONTAP environment

Preparing the ONTAP environment for using the SnapCenter Plug-in for NAS File Services involves several tasks.

About this task

- Installing or upgrading ONTAP
- Adding appropriate ONTAP licenses
- Establishing cluster peering and intercluster LIFs

Installing or upgrading ONTAP

For the Data Fabric Solution for Cloud Backup, you can install ONTAP 9.1, use an existing ONTAP deployment of ONTAP 9.1 or upgrade to ONTAP 9.1.

Steps

1. Download the ONTAP install or upgrade package from the NetApp Support Site at mysupport.netapp.com.

2. Follow ONTAP install or upgrade instructions.
   http://docs.netapp.com/ontap-9/index.jsp
Adding appropriate ONTAP licenses

Installing license keys, also known as license codes, enables you to use certain features or services on your cluster. Data ONTAP enables you to manage feature licenses and monitor feature usage and license entitlement risk.

About this task

Each cluster requires a cluster base license key, which you can install either during or after the cluster setup. Some features require additional licenses.

Note: If you intend to back up NAS file services data from ONTAP to AltaVault, add a SnapMirror license on the source only. If you intend to back up NAS file services data from ONTAP to ONTAP to AltaVault, add a SnapMirror license on both the source and destination cluster.

You can find license keys for your initial or add-on software orders at the NetApp Support Site under My Support > Software Licenses (login required). If you cannot locate your license keys from the Software Licenses page, contact your sales or support representative.

Steps

1. Identify licensed features on the source cluster:

```
source_cluster::> system license show
```

<table>
<thead>
<tr>
<th>Package</th>
<th>Type</th>
<th>Description</th>
<th>Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base</td>
<td>site</td>
<td>Cluster Base License</td>
<td></td>
</tr>
<tr>
<td>NFS</td>
<td>site</td>
<td>NFS License</td>
<td></td>
</tr>
<tr>
<td>CIFS</td>
<td>site</td>
<td>CIFS License</td>
<td></td>
</tr>
<tr>
<td>iSCSI</td>
<td>site</td>
<td>iSCSI License</td>
<td></td>
</tr>
<tr>
<td>FCP</td>
<td>site</td>
<td>FCP License</td>
<td></td>
</tr>
<tr>
<td>SnapMirror</td>
<td>site</td>
<td>SnapMirror License</td>
<td></td>
</tr>
<tr>
<td>FlexClone</td>
<td>site</td>
<td>FlexClone License</td>
<td></td>
</tr>
</tbody>
</table>

7 entries were displayed.

2. Identify licenses on the destination cluster:

```
destination_cluster::> system license show
```

3. If any required feature or protocol is not licensed on the source or destination cluster, then add a license:

```
destination_cluster::> system license add -license-code xxxxxxxxxxxxxxxx
```

Related information

ONTAP 9 System Administration Reference
Establishing cluster peering for ONTAP to cloud backups

If you intend to back up NAS file services data from ONTAP to ONTAP and to the cloud using AltaVault, a cluster peering relationship must be established between the two clusters to enable replication to occur between them.

About this task

You establish the cluster peering relationship for the ONTAP-to-ONTAP path by completing the following tasks:

- Ensuring that prerequisites are met
- Preparing each cluster
- Creating intercluster logical interfaces (LIFs) on each node
- Setting up each peer relationship

This procedure provides an overview of the process. For full details, see information about cluster peering.

ONTAP 9 Cluster Peering Express Guide

Prerequisites for cluster peering

Before you set up cluster peering, you should confirm that the connectivity, port, IP address, subnet, firewall, and cluster-naming requirements are met.

Connectivity requirements

The subnet used in each cluster for intercluster communication must meet the following requirements:

- The subnet must belong to the broadcast domain that contains the ports that are used for intercluster communication.
- The IP addresses that are used for intercluster LIFs do not need to be in the same subnet, but having them in the same subnet is a simpler configuration.
- You must have decided whether the subnet is dedicated to intercluster communication or is shared with data communication.
- The subnet must have enough IP addresses available to allocate to one intercluster LIF per node.

For example, in a six-node cluster, the subnet used for intercluster communication must have six available IP addresses.

The intercluster network must be configured so that cluster peers have pair-wise full-mesh connectivity within the applicable IPspace, which means that each pair of clusters in a cluster peer relationship has connectivity among all of their intercluster LIFs.

A cluster’s intercluster LIFs have an IPv4 address or an IPv6 address.

Port requirements

The ports that are used for intercluster communication must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace. You can use multiple IPspaces to peer with multiple clusters. Pair-wise full-mesh connectivity is required only within an IPspace.
• The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port.

• Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).

• All ports must be cabled.

• All ports must be in a healthy state.

• The MTU settings of the ports must be consistent.

• You must decide whether the ports that are used for intercluster communication are shared with data communication.

**Firewall requirements**

Firewalls and the intercluster firewall policy must allow the following protocols:

• ICMP service

• TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105

• HTTPS

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

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

**Cluster requirements**

Clusters must meet the following requirements:

• The time on the clusters in a cluster peering relationship must be synchronized within 300 seconds (5 minutes). Cluster peers can be in different time zones.

• A passphrase should be used for each cluster peer relationship. The passphrase must be at least eight characters and cannot contain spaces. You should use a unique passphrase for each relationship.

<table>
<thead>
<tr>
<th>For the relationship between</th>
<th>The passphrase will be:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster A and Cluster B</td>
<td></td>
</tr>
</tbody>
</table>

**Preparing each cluster**

Before setting up cluster peering, you must verify that each cluster's time is synchronized with an external Network Time Protocol (NTP) server and you must plan subnets, ports, and passphrases.

**About this task**

On each cluster, verify that the time is synchronized to an external NTP server to ensure that the time on all of the cluster peers is within five minutes of each other.

**Steps**

1. Open a session to each cluster and enter the following command:
Login: admin
Password:
clusterA::> cluster time-service ntp server show
Server                         Version
------------------------------ -------
192.168.0.253                  auto

2. If the time-service area is blank, add an NTP server:

clusterA::> cluster time-service ntp server create -server <IP address>

Configuring intercluster interfaces on all nodes

Clusters communicate with each other through logical interfaces (LIFs) that are dedicated to intercluster communication. You must create an intercluster LIF on each node in each cluster that will be in a cluster peer relationship.

About this task

**Best Practice:** Configuring intercluster LIFs to use dedicated data ports enables greater bandwidth than using shared data ports on your intercluster networks.

Creating intercluster LIFs that use dedicated ports involves creating a failover group for the dedicated ports and assigning LIFs to those ports. As an example in this procedure, a two-node cluster exists in which each node has two data ports that you have added, e0e and e0f. These ports are ones you will dedicate for intercluster replication and currently are in the default IPspace. These ports will be grouped together as targets for the intercluster LIFs you are configuring.

Typically, you must configure intercluster LIFs on the peer cluster before you can create cluster peer relationships. However, for the Data Fabric Solution for Cloud Backup, you do not need to create cluster peer relationships after you configure intercluster LIFs.

In your own environment, you might replace the ports, networks, IP addresses, subnet masks, and subnets with those specific to your environment.

Steps

1. List the ports in the cluster by using the *network port show* command.

   **Example**

   ```
   cluster01::> network port show
   Node  Port  IPspace  Broadcast Domain  Link  MTU  Speed  Admin/Oper
   ------  ------  -------  ----------------  -----  ----  -------  ---------
   cluster01-01
   e0a     Cluster  Cluster  up  1500  auto/1000
   e0b     Cluster  Cluster  up  1500  auto/1000
   e0c     Default  Default  up  1500  auto/1000
   e0d     Default  Default  up  1500  auto/1000
   e0e     Default  Default  up  1500  auto/1000
   e0f     Default  Default  up  1500  auto/1000
   cluster01-02
   e0a     Cluster  Cluster  up  1500  auto/1000
   e0b     Cluster  Cluster  up  1500  auto/1000
   e0c     Default  Default  up  1500  auto/1000
   e0d     Default  Default  up  1500  auto/1000
   e0e     Default  Default  up  1500  auto/1000
   e0f     Default  Default  up  1500  auto/1000
   ```

2. Determine whether any of the LIFs are using ports that are dedicated for replication by using the *network interface show* command.
Example

Ports e0e and e0f do not appear in the following output; therefore, they do not have any LIFs located on them:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
   cluster_mgmt        e0c       e0c
cluster01
   cluster01-01_mgmt1  e0c       e0c
cluster01
   cluster01-02_mgmt1  e0c       e0c
```

3. If a LIF is using a port that you want dedicated to intercluster connectivity, migrate the LIF to a different port.

   a. Migrate the LIF to another port by using the `network interface migrate` command.

   **Example**

   The following example assumes that the data LIF named `clusterA_data01` uses port e0e and you want only an intercluster LIF to use that port:

   ```
   clusterA::> network interface migrate -vserver clusterA
   -lif clusterA_data01 -dest-node clusterA-01 -dest-port e0d
   ```

   b. You might need to modify the migrated LIF home port to reflect the new port where the LIF should reside by using the `network interface modify` command.

   **Example**

   ```
   clusterA::> network interface modify -vserver clusterA
   -lif clusterA_data01 -home-node clusterA-01 -home-port e0d
   ```

4. Group the ports that you will use for the intercluster LIFs by using the `network interface failover-groups create` command.

   **Example**

   ```
   clusterA::> network interface failover-groups create -vserver clusterA
   -failover-group interclusterA -targets clusterA-01:e0e,clusterA-01:e0f,
   clusterA-02:e0e,clusterA-02:e0f
   ```

5. Display the failover group you created by using the `network interface failover-groups show` command.

   **Example**

   ```
   clusterA::> network interface failover-groups show
   Vserver Group                Failover Targets
   --------------------         --------------------------------------------
Cluster clusterA: Cluster
clusterA: Default          clusterA-01:e0d, clusterA-01:e0f,
clusterA-02:e0c, clusterA-02:e0d,
clusterA-01:e0e, clusterA-01:e0f
```
6. Create an intercluster LIF on the admin SVM clusterA by using the `network interface create` command.

**Example**

This example uses the LIF naming convention `clusterA_icl#` for the intercluster LIF:

```bash
clusterA::> network interface create -vserver clusterA -lif clusterA_icl01 -role intercluster -home-node clusterA-01 -home-port e0e -address 192.0.2.250 -netmask 255.255.255.0 -failover-group interclusterA

clusterA::> network interface create -vserver clusterA -lif clusterA_icl02 -role intercluster -home-node clusterA-02 -home-port e0e -address 192.0.2.251 -netmask 255.255.255.0 -failover-group interclusterA
```

7. Verify that the intercluster LIFs were created properly by using the `network interface show` command.

**Example**

```
clusterA::> network interface show
Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Cluster
clusterA-01_clus_1 up/up    192.0.2.xxx/24   clusterA-01  e0a     true
clusterA-01_clus_2 up/up    192.0.2.xxx/24   clusterA-01  e0b     true
clusterA-02_clus_1 up/up    192.0.2.xxx/24   clusterA-01  e0a     true
clusterA-02_clus_2 up/up    192.0.2.xxx/24   clusterA-01  e0b     true
clusterA-01_mgmt up/up    192.0.0.xxx/24   clusterA-01  e0c     true
clusterA-02_mgmt up/up    192.0.0.xxx/24   clusterA-02  e0c     true
clusterA-01_icl01 up/up    192.0.2.xxx/24   clusterA-01  e0e     true
clusterA-02_icl01 up/up    192.0.2.xxx/24   clusterA-02  e0e     true
clusterA-01_icl02 up/up    192.0.2.xxx/24   clusterA-01  e0f     true
clusterA-02_icl02 up/up    192.0.2.xxx/24   clusterA-02  e0f     true
```

8. Verify that the intercluster LIFs are configured for redundancy by using the `network interface show` command with the `-role intercluster` and `-failover` parameters.

**Example**

```
clusterA::> network interface show -role intercluster –failover
Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
clusterA-01clusterA-01_icl01 clusterA-01:e0e   local-only      intercluster01
      Failover Targets:  clusterA-01:e0e,
                        clusterA-01:e0f
clusterA-01_icl02 clusterA-02:e0e   local-only      intercluster01
      Failover Targets:  clusterA-02:e0e,
                        clusterA-02:e0f
```

9. Display the routes in the cluster by using the `network route show` command to determine whether intercluster routes are available or you must create them.

Creating a route is required only if the intercluster addresses in both clusters are not on the same subnet and a specific route is needed for communication between the clusters.
Example
In this example, no intercluster routes are available:

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>0.0.0.0/0</td>
<td>192.0.2.1</td>
<td>20</td>
</tr>
<tr>
<td>cluster01</td>
<td>0.0.0.0/0</td>
<td>192.0.2.1</td>
<td>10</td>
</tr>
</tbody>
</table>

10. If communication between intercluster LIFs in different clusters requires routing, create an intercluster route by using the `network route create` command.

The gateway of the new route should be on the same subnet as the intercluster LIF.

Example
In this example, 192.168.1.1 is the gateway address for the 192.168.1.0/24 network. If the destination is specified as 0.0.0.0/0, then it becomes a default route for the intercluster network.

```
clusterA::> network route create -vserver clusterA -destination 0.0.0.0/0 -gateway 192.0.2.1 -metric 40
```

11. Verify that you created the routes correctly by using the `network route show` command.

Example

```
cluster01::> network route show
Vserver   Destination     Gateway         Metric
--------- --------------- --------------- ------
Cluster   0.0.0.0/0       192.0.2.1     20
clusterA  0.0.0.0/0       192.0.2.1     10
0.0.0.0/0       192.0.2.2     40
```

12. Repeat these steps to configure intercluster networking in the peer cluster.

Creating peer relationships among clusters

As part of the ONTAP setup for performing data protection operations using AltaVault or the Data Fabric Solution for Cloud Backup, you must create a cluster peer relationship on each cluster. If you created intercluster LIFs in a nondefault IPspace, you need to designate the IPspace when you create the cluster peer.

Before you begin

- Intercluster LIFs should be created in the IP spaces of both clusters you want to peer.
- You should ensure that the intercluster LIFs of the clusters can route to each other.
- If there are different administrators for each cluster, the passphrase used to authenticate the cluster peer relationship should be agreed upon.

Steps

1. Create the cluster peer relationship on each cluster by using the `cluster peer create` command.

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

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

In the following example, cluster01 is peered with a remote cluster named cluster02. Cluster01 is a two-node cluster that has one intercluster LIF per node. The IP addresses of the intercluster LIFs created in cluster01 are 192.168.2.201 and 192.168.2.202. Similarly, cluster02 is a two-node cluster that has one intercluster LIF per node. The IP addresses of the intercluster LIFs created in cluster02 are 192.168.2.203 and 192.168.2.204. These IP addresses are used to create the cluster peer relationship.

```
cluster01::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
Please type the passphrase:
Please type the passphrase again:
```

```
cluster02::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
Please type the passphrase:
Please type the passphrase again:
```

If DNS is configured to resolve host names for the intercluster IP addresses, you can use host names in the `peer-addrs` option. It is not likely that intercluster IP addresses frequently change; however, using host names allows intercluster IP addresses to change without having to modify the cluster peer relationship.

Example

In the following example, an IPspace called IP01A was created on cluster01 for intercluster connectivity. The IP addresses used in the previous example are used in this example to create the cluster peer relationship.

```
cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
-ipspace IP01A
Please type the passphrase:
Please type the passphrase again:
```

```
cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
Please type the passphrase:
Please type the passphrase again:
```

2. Display the cluster peer relationship by using the `cluster peer show` command with the `-instance` parameter.

Displaying the cluster peer relationship verifies that the relationship was established successfully.

Example

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster02
Remote Cluster Name: cluster02
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Active IP Addresses: 192.168.2.203,192.168.2.204
Cluster Serial Number: 1-80-000013
```

3. Preview the health of the nodes in the peer cluster by using the `cluster peer health show` command.

Previewing the health checks the connectivity and status of the nodes on the peer cluster.
Preparing the SnapCenter Linux file catalog server

SnapCenter requires one or more Linux file catalog servers in addition to the SnapCenter Server. Before you install the SnapCenter Server, you should prepare the file catalog servers so that they are accessible during the installation.

About this task

SnapCenter maintains a catalog of backups on a Linux server to facilitate easy search and location of files for restore requests.

Steps

1. Installing Linux catalog servers on page 30
   You must install at least one Linux file catalog server in addition to the SnapCenter Server. You can install Linux catalog servers on physical or virtual machines. The Linux catalog servers are used only for cataloging NAS files and should not be used for any other plug-in operations.

2. Configuring SnapCenter file catalog ports on page 31
   After installing one or more Linux servers for the SnapCenter file catalogs, you configure the ports that SnapCenter uses to communicate with the Linux servers.

3. Adding a non-root user and configuring sudo privileges on page 32
   SnapCenter 2.0 or later enables a non-root user to install the plug-ins and start the plug-in process. However, you must configure sudo privileges for the non-root user to provide access to several paths.

4. Verifying the Java runtime environment on page 33
   Before you install SnapCenter on the Linux server for the file catalog, you should verify that the Linux server is running a Java version that is supported by SnapCenter.

5. Ensuring the Linux server is accessible for NAS file services file catalog on page 33
   Before you install the SnapCenter Server, you must ensure that the Linux server that you will use for the file catalog is available and will be accessible to the SnapCenter Server.

Installing Linux catalog servers

You must install at least one Linux file catalog server in addition to the SnapCenter Server. You can install Linux catalog servers on physical or virtual machines. The Linux catalog servers are used only for cataloging NAS files and should not be used for any other plug-in operations.

Before you begin

You must have read the file catalog requirements.
About this task
Complete file catalog server configuration steps for each Linux server used for the file catalog.

Steps
1. Physically install Linux servers or create them on a virtual machine.
2. Configure storage for the SnapCenter file catalog in the location /opt/NetApp/snapcenter/indexer.

After you finish
After installing a Linux server, you next need to configure the ports.

Configuring SnapCenter file catalog ports
After installing one or more Linux servers for the SnapCenter file catalogs, you configure the ports that SnapCenter uses to communicate with the Linux servers.

Before you begin
You must have installed at least one Linux server and configured storage for it.

About this task
Complete file catalog server configuration steps for each Linux server used for the file catalog.

Steps
1. Open a ssh session to the Linux server and view the ports that are in use.

   Example

   ```
   netstat -anp | grep -E '8145|8983|2181|2888|8145'
   ```

   If no results are returned, then all the required ports are available.
2. Disable the firewalld daemon, by using the following steps:

   a. Check status of firewalld daemon by using the status firewalld command.

      Example

      ```
      [root@rhel72-01 ~]# systemctl status firewalld
      firewalld.service - firewalld - dynamic firewall daemon
      Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled)
      Active: inactive (dead)
      Main PID: 674 (firewalld)
      ```

   b. If the firewalld daemon is running, disable it by stopping the firewalld daemon and verifying that it is stopped, using the stop firewalld and status firewalld commands.

      Example

      ```
      [root@rhel72-01 ~]# systemctl stop firewalld
      [root@rhel72-01 ~]# systemctl status firewalld
      firewalld.service - firewalld - dynamic firewall daemon
      Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled)
      Active: inactive (dead)
      ```
c. Prevent the `firewalld` daemon from restarting by using the `disable firewalld` command.

**Example**

```
[root@rhel72-01 ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
Removed symlink /etc/systemd/system/basic.target.wants/firewalld.service
```

This prevents the `firewalld` daemon from restarting when the server is restarted.

**After you finish**

After configuring the ports for each SnapCenter file catalog server, you need to add a non-root user and configure sudo privileges.

### Adding a non-root user and configuring sudo privileges

SnapCenter 2.0 or later enables a non-root user to install the plug-ins and start the plug-in process. However, you must configure sudo privileges for the non-root user to provide access to several paths.

**Before you begin**

You must have installed at least one Linux server for the SnapCenter file catalog and configured the ports.

**About this task**

This procedure applies to the SnapCenter Plug-in for Oracle Database, SnapCenter Plug-in for NAS File Services, and also if you deploy SnapCenter in the Data Fabric Solution for Cloud Backup, because the file catalog accessed in the solution uses a Linux server.

Complete file catalog server configuration steps for each Linux server used for the file catalog.

You must configure sudo privileges for the non-root user to provide access to the following paths:

- `/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin`
- `/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/custom_location/NetApp/snapcenter/spl/bin/spl`

**Steps**

1. Open an ssh session to the Linux catalog server.

2. Using a text editor, add the non-root user to the `/etc/passwd` file.

**Example**

```
NonRootUser:x:1000:1000:NonRootUser:/home/NonRootUser:/bin/bash
```

3. Using a text editor, add the newly created user to the `/etc/group` file.
4. Add the following lines to the `/etc/sudoer` file by using the `visudo` Linux utility.

```
Cmnd_Alias SCCMD=/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin,/opt/NetApp
    /snapcenter/spl/installation/plugins/uninstall,/opt/NetApp/snapcenter/spl/bin/spl
NonRootUser ALL=(ALL) NOPASSWD:SCCMD
NonRootUser ALL=(ALL) NOPASSWD:ALL
Defaults:NonRootUser !visiblepw
Defaults:NonRootUser !requiretty
```

After you finish

Optional: For environments that do not have DNS, you need to add the SnapCenter server and the file catalog servers to the `/etc/hosts` file.

### Verifying the Java runtime environment

Before you install SnapCenter on the Linux server for the file catalog, you should verify that the Linux server is running a Java version that is supported by SnapCenter.

Before you begin

You must have read the file catalog requirements.

About this task

Complete file catalog server configuration steps for each Linux server used for the file catalog.

Step

1. Verify the Java runtime environment, by using the `java` command.

```
[root@rhe172-01 ~]# java -version
openjdk version "1.8.0_65"
OpenJDK Runtime Environment (build 1.8.0_65-b17)
OpenJDK 64-Bit Server VM (build 25.65-b01, mixed mode)
[root@rhe172-01 ~]# which java
/usr/bin/java
```

### Ensuring the Linux server is accessible for NAS file services file catalog

Before you install the SnapCenter Server, you must ensure that the Linux server that you will use for the file catalog is available and will be accessible to the SnapCenter Server.

About this task

Complete file catalog server configuration steps for each Linux server used for the file catalog.

Steps

1. Before installing the SnapCenter Server, mount the volume for storing the file catalog installation on the following path on the Linux server: `/opt/NetApp/snapcenter/indexer`
This step is optional. It should be completed when you want to allocate dedicated storage for the file catalog, which can take a large amount of space depending on your configuration.

2. On each Linux server you are going to install as a SnapCenter file catalog server, determine whether the server can access the SnapCenter Server:

```
ping snapcenter-server-name@domain-name
```

3. On the SnapCenter Server, determine whether the server can access each of the Linux catalog servers, by using the `ping` command:

```
ping catalog-server-name@domain-name
```

4. On the SnapCenter Server, use a utility such as PuTTY to determine whether you can connect to the Linux catalog servers using the non-root user you created.

**Installing SnapCenter for Data Fabric Solution for Cloud Backup**

SnapCenter is one of the Data Fabric Solution for Cloud Backup components. Installing SnapCenter involves several tasks.

**Steps**

1. **Installing the SnapCenter Server** on page 34
   
   After you have completed the installation prerequisites, you can use the InstallShield wizard to install the SnapCenter Server and configure the SnapCenter file catalog server or servers. Installing the SnapCenter Server also installs the file catalog software on the file catalog servers.

2. **Checking the status of NAS File Services components after SnapCenter installation** on page 36
   
   On each file catalog server, you should check the status of the NAS File Services components, including processes, port statuses, and properties, to ensure that the installation completed successfully.

**Installing the SnapCenter Server**

After you have completed the installation prerequisites, you can use the InstallShield wizard to install the SnapCenter Server and configure the SnapCenter file catalog server or servers. Installing the SnapCenter Server also installs the file catalog software on the file catalog servers.

**Before you begin**

- The SnapCenter catalog server or servers must be installed and accessible from the SnapCenter Server.

- Your SnapCenter host system must be up to date with Windows updates with no pending system restarts.

- You must have enabled Windows installer debugging. See the Microsoft web site for information about enabling and disabling Windows Installer logging.

  

- Your system must meet the SnapCenter prerequisites.

- The SnapCenter Server must be installed on a server that is part of a domain.
Note: SnapCenter Server cannot be installed on a domain controller.

- A two-way trust relationship between the SnapCenter Server domain and the plug-in domain using the Microsoft Active Directory Domains and Trusts snap-in must have been established. While domain trusts, multi-domain forests, and cross-domain trusts are supported, cross-forest domains are not supported. See Microsoft documentation about Active Directory Domains and Trusts. https://technet.microsoft.com/en-us/library/cc770299.aspx

Steps

1. Optionally, gather information in a SnapCenter installation worksheet provided in the installation instructions. 
   *SnapCenter Software 2.0 Installation and Setup Guide*

2. Download the SnapCenter Server installation package from the NetApp Support Site at mysupport.netapp.com.

3. Install the SnapCenter Server by performing one of the following methods:
   - Double-click the downloaded .exe file to launch the SnapCenter Server installer. Proceed through the wizard.
   - From a Windows command prompt on the local host, change to the directory where you downloaded the installer and run the .exe file.

4. In the Application Request Routing screen, select Configure ARR farm for SnapCenter to enable and configure ARR.

5. In the Network Load Balancing screen, if you want to enable and configure NLB select Enable and configure NLB on the host.
   a. Select Create new NLB cluster and enter the details for node 1.
   b. After creating the NLB cluster, when you run the installer on node 2, select Join existing NLB cluster and enter the details.

6. In the Credentials and Certificate screen, enter the credentials that you want to use to log in to SnapCenter as the administrator.
   You need a domain user with local administrator permissions.

7. In the Installation Folder screen, you can browse and provide the path where you want to install SnapCenter Server and SnapCenter repository.
   - The SnapCenter Server web component and SMCore is installed in the corresponding folders at the default location C:\Program Files\NetApp\SnapCenter WebApp.
   - The repository component is installed at the default location C:\ProgramData\NetApp\SnapCenter\MySQL Data.
   - The plug-in packages are available at the default location C:\ProgramData\NetApp\SnapCenter\Package Repository.

8. In the SnapCenter Ports Configuration screen, enter the port details.
   The default ports are auto populated but you can specify a custom port.

9. In the MySQL Database Connection screen, enter the port and password details.
   The default port is auto populated but you can specify the custom port. In a NLB setup, if you have specified a custom port for node 1, while installing on node 2 the same port is used and it is non configurable.
**Note:** MySQL NSM database is not uninstalled when you uninstall SnapCenter. Therefore, when you re-install SnapCenter, you must enter the same custom port specified during the earlier installation.

In a NLB setup, while installing SnapCenter on the node 1, MySQL NSM database is installed. While installing SnapCenter on the node 2, you must join the NLB of the first node and a copy of the NSM database is created on the node 2. Thus, MySQL replication for high availability is configured.

**10.** Enable indexing of NAS file services data by adding one or more file catalog servers according to the following steps.

**Important:** To protect NAS file services data, you must enable NAS file services indexing and configure file catalog servers during the installation. You cannot do this after installation.

a. For NAS file services, enter the IP address or host name for one or more servers that you will use to index file catalog information. For high availability, you should add at least two file catalog servers.

b. For the file catalog server, specify Linux as the server type.

c. For the file catalog server, enter port **8145**

d. For the file catalog server, enter the Linux OS username and password.

e. After entering the details, click **Add index server** to validate whether the installer package is unzipped and SnapCenter Plug-ins Package for Linux is installed. If requirements are not met appropriate error or warning messages are displayed. After fixing the issue, click **Add index server** to proceed.

f. To add more indexing servers, click **Add another index server**.

**After you finish**

If you encounter installation issues, run the installation using a command prompt and generate a log file:

```
SnapCenterversion.exe /debuglog"DirPath\LogFileName"
```

For example,

```
SnapCenter2.0.exe /debug"c:\snapcenterlog.txt"
```

The `debuglog` parameter generates a log file that checks the installation against SnapCenter prerequisites. If necessary, you can find additional troubleshooting information in the log file for the Plug-in for Windows package. Log files for the package are listed (oldest first) in the `%Temp%` folder.

**Related information**

*SnapCenter Software 2.0 Installation and Setup Guide*

### Checking the status of NAS File Services components after SnapCenter installation

On each file catalog server, you should check the status of the NAS File Services components, including processes, port statuses, and properties, to ensure that the installation completed successfully.

**About this task**

Commands are entered from the Linux server where the file catalog is installed.
Steps

1. Open an ssh session to the Linux server.
2. Check the SnapCenter Plug-in Loader (SPL) status:
   \[ \text{/opt/NetApp/snapcenter/spl/bin/spl status} \]

   Example
   
   ```
   [nonroot@rhel72-01 ~]# /opt/NetApp/snapcenter/spl/bin/spl status
   Checking status of SnapCenter Plugin Loader
   SnapCenter Plugin Loader is running as process 13363
   ```

3. Check scAgent status: \[ /opt/NetApp/snapcenter/scc/bin/scAgent status \]

   Example
   
   ```
   [nonroot@rhel72-01 ~]# /opt/NetApp/snapcenter/scc/bin/scAgent status
   Checking Status of scAgent:
   Watchdog: Running
   Agent: Running
   ```

4. Check the Java process for the SPL to verify that it is present: \[ ps -ef | grep spl \]
5. Check the Java process for ZooKeeper to verify that it is present: \[ ps -ef | grep zookeeper \]
6. Check the Java process for Solr to verify that it is present: \[ ps -ef | grep solr \]
7. Check the TCP port for the SPL: \[ netstat -a|grep <port_number> \]. The default port number is 8145.
8. Check that the SPL properties are available: \[ /var/opt/snapcenter/spl/etc/spl.properties \]

   Example
   
   ```
   /var/opt/snapcenter/spl/etc/spl.properties
   SPL_PORT=8145
   SPL_PROTOCOL=https
   SPL_KEYSTORE_PATH=/var/opt/snapcenter/spl/etc/keystore.jks
   SPL_KEYSTORE_PASS=snapcenter
   SNAPCENTER_SERVER_HOST=win2012-005.ava-test.local
   SNAPCENTER_SERVER_PROTOCOL=https
   SNAPCENTER_SERVER_PORT=8146
   LOG_LEVEL=DEBUG
   SPL_LOGS_MAX_COUNT=5000
   ```

9. Check the installation log files for errors: \[ /tmp/netapp/install-yyyymmddhhmmss.log \]

   Example
   
   ```
   sudo: no tty present and no askpass program specified
   ```
   This example message might indicate that there is an issue with the \text{/etc/sudoer} file.

10. From a browser, check that you can connect to Solr catalog server port 8983:
    \[ \text{catalog_server_name/IP_address:8983/solr/#!/} \]
Installing or upgrading AltaVault

The Data Fabric Solution for Cloud Backup requires AltaVault to perform data protection to the cloud.

About this task
You can use the following deployments of AltaVault:

- Physical
- Virtual (.OVF, Hyper-V, and Linux KVM images)

The AltaVault cloud version (AVA-c) is not currently supported.
Refer to the Interoperability Matrix for the latest information about supported configurations.

Steps
1. Download the AltaVault Physical Appliance or Virtual Appliance package from the NetApp Support Site at mysupport.netapp.com.
2. Do one of the following:
   - For the physical appliance, rack and connect the physical AltaVault appliance according to the AltaVault physical installation guide.
   - For the virtual appliance, deploy the virtual AltaVault appliance according to the AltaVault virtual installation guide.

Related information

NetApp Documentation: AltaVault
NetApp Interoperability Matrix Tool
Configuring the AltaVault appliance

Using the Data Fabric Solution for Cloud Backup requires additional AltaVault configuration beyond the basic configuration. You must have one AltaVault instance per cloud provider with the provider associated with one bucket.

About this task

AltaVault configuration for Data Fabric Solution for Cloud Backup includes the following tasks depending on whether you are using SnapCenter in the deployment. These are the tasks that you must perform. For example, if you use SnapCenter in the deployment, you do not need to add approved intercluster LIFs to an IP whitelist in AltaVault. (In this case, SnapCenter creates the whitelist of approved IP connections for you.)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Using SnapCenter in deployment</th>
<th>Not using SnapCenter in deployment and using only ONTAP commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SnapMirror service in AltaVault</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Add approved intercluster LIFs to an IP whitelist in AltaVault</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable SnapCenter access to AltaVault</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Optionally, enable SnapMirror long-term retention mode in AltaVault</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Add a role-based user in AltaVault to enable SnapCenter storage connection to an AltaVault appliance</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Start the AltaVault Storage Optimization Service</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Steps

1. **Logging in to AltaVault** on page 40
   You can log in to AltaVault using either the graphical user interface (GUI) or a command line interface (CLI).

2. **Configuring basics in AltaVault** on page 40
   Using AltaVault requires setting up basic options such as system settings, cloud connections, data interfaces, licenses, and encryption key.

3. **Configuring AltaVault using the GUI** on page 40
   To configure AltaVault, you can use the AltaVault graphical user interface (GUI) or command-line interface (CLI).

4. **Configuring AltaVault using the AltaVault CLI** on page 44
   To configure AltaVault, you can use the AltaVault command-line interface (CLI) rather than the graphical user interface (GUI).
Logging in to AltaVault

You can log in to AltaVault using either the graphical user interface (GUI) or a command line interface (CLI).

Steps
1. Log in to AltaVault using one of the following:
   - From a web browser, log in to the AltaVault Management Console using HTTPS and the IP address or DNS host name of the AltaVault Appliance.
   - To access the CLI, log in from an SSH client using the IP address or DNS of the AltaVault Appliance.
     For example:

```
ssh admin@172.16.4.4
NetApp AltaVault
admin@172.16.4.4's password:
```

2. Enter the administrator credentials.

Configuring basics in AltaVault

Using AltaVault requires setting up basic options such as system settings, cloud connections, data interfaces, licenses, and encryption key.

About this task
Configuring AltaVault includes setting the following options:

- AltaVault system settings
- Cloud providers
- AltaVault data interfaces
- AltaVault licenses
- AltaVault encryption key

See the *AltaVault Cloud Integrated Storage Administration Guide* on the NetApp Support Site at [mysupport.netapp.com](http://mysupport.netapp.com).

Configuring AltaVault using the GUI

To configure AltaVault, you can use the AltaVault graphical user interface (GUI) or command-line interface (CLI).

Enabling the SnapMirror service and configuring whitelist IP connections using the AltaVault GUI

AltaVault supports backup and restore operations for ONTAP FlexVol volumes using the SnapMirror service running on the AltaVault appliance. You must enable the SnapMirror service, which then enables ONTAP to create the SnapMirror relationship in AltaVault and enable backup and restore
operations of NAS file services. You must also create a whitelist of approved intercluster LIF IP addresses from which AltaVault accepts connections for data protection.

**About this task**

When the SnapMirror service is enabled, the shares and Snapshot copies that exist on AltaVault are accessible and available for restoration via ONTAP. If the SnapMirror service is disabled, the shares and Snapshot copies that exist on AltaVault are not deleted; however, Snapshot copies are not accessible by ONTAP.

The list of authorized IP addresses must be populated prior to initiating a connection from the source system or the connection will be rejected.

If you use SnapCenter as part of this solution, SnapCenter creates the whitelist of approved IP connections and enables the SnapMirror long-term retention mode when you initiate the backup from SnapCenter. In this case, there is no need to create the IP whitelist and enable SnapMirror long-term retention mode by using AltaVault.

**Steps**

1. Log in to AltaVault.
2. Select **Configure > SnapMirror**.
3. Under SnapMirror Service, click **Enable**.
4. If the "Service restart required" prompt appears, click the **Restart** button that becomes enabled in the upper right and refresh the browser page after the green healthy checkbox returns in the upper left.
5. Under Whitelist IP, click **Add Whitelist IP**.
6. Enter the IP addresses of the intercluster LIFs from which AltaVault will accept connections for backup and restore operations and click **Add**.

To remove an IP address, select the IP address and click **Remove Selected**.
Note: Removing an IP address from the whitelist disables access to the AltaVault from that IP address.

Enabling SnapMirror long-term retention mode in AltaVault

AltaVault supports up to 500 shares in one of two modes: short-term retention mode (default) or long-term retention mode. For Data Fabric Solution for Cloud Backup, the mode impacts the retention of your Snapshot copies. SnapMirror long-term retention mode is required if you want to retain more than 251 Snapshot copies for a relationship on AltaVault. Long-term retention mode is disabled by default.

About this task

Snapshot copy retention is dependent upon the retention policy set up in either ONTAP or SnapCenter. For example, if a retention policy is set to 100 Snapshot copies, and the maximum is reached, AltaVault, adhering to ONTAP instructions, begins deleting the oldest Snapshot copies to make room for newer ones. If you are using SnapCenter, then SnapCenter controls the retention. Otherwise, ONTAP controls the retention.

- In short-term retention mode, each share supports up to 251 Snapshot copies. The Snapshot copy retention is governed by the SnapMirror policy set in either ONTAP or SnapCenter.
  For example, suppose a share has a two-tier retention policy supporting 50 hourly and 100 daily Snapshot copies. In this case, when the count of hourly Snapshots exceeds 50 or the daily count exceeds 100, the oldest Snapshot copy of the respective tier is deleted.

- In long-term retention mode, each share supports up to 3700 Snapshot copies, which is the equivalent to 10 years of daily Snapshot copies.
  Retention of Snapshot copies in archival mode can be managed by AltaVault or SnapCenter:
    - Snapshot copies managed by AltaVault: AltaVault continues accumulating Snapshot copies with a maximum of 3700 before deleting the oldest Snapshot copy in the share. The oldest is deleted irrespective of the label (hourly/daily/monthly).
    - Snapshot copies managed by SnapCenter: SnapCenter manages any number of Snapshot copies with a maximum of 3700.

Long-term retention mode is enabled automatically when SnapCenter transfers data to AltaVault. When long-term retention mode is disabled, AltaVault reverts to using the retention policy set up in ONTAP or SnapCenter. If there are large numbers of Snapshot copies (more than 251) when long-term retention mode is disabled, the number of Snapshot copies will be reduced to match the count set in the retention policy.

Warning: When you use SnapCenter to manage backups, you should not disable long-term retention mode in AltaVault.

The mode used for long-term retention applies to all SnapMirror shares created on AltaVault.

If you use SnapCenter as part of this solution, SnapCenter creates the whitelist of approved IP connections and enables the SnapMirror long-term retention mode when you initiate the backup from SnapCenter. In this case, there is no need to create the IP whitelist and enable SnapMirror long-term retention mode by using AltaVault.

Steps

1. Log in to AltaVault.
2. Under SnapMirror Long-term Retention Mode, click Enable.
Enabling SnapCenter access to AltaVault

AltaVault supports using SnapCenter to back up, delete, and restore Snapshot copies, including individual file restores. If you are using SnapCenter to manage backups to AltaVault, you must enable SnapCenter access on AltaVault.

**Steps**

1. Log in to AltaVault.
2. Select **Configure > SnapMirror**.
3. If you are using SnapCenter to initiate and manage data protection operations, under SnapCenter Access, click **Enable**.
4. If the Service restart required prompt appears, click **Restart** in the upper right of the console.

Adding a SnapCenter role-based user account to enable SnapCenter storage connections to an AltaVault appliance

If you are using SnapCenter for data protection management, you must add a SnapCenter role-based account to AltaVault. You will later add a storage connection in SnapCenter and will need this account's credential information.

**About this task**

You can add a user using the AltaVault graphical user interface (GUI) or by using the AltaVault CLI.

**Steps**

1. Log in to AltaVault.
2. Select **Configure > User Permissions**.

3. In the Role-Based Accounts section, click **Add a New User** to add a user account that will be used by SnapCenter.
4. Enter an account name and password and check **Enable Account**.
5. Click **Read/Write** permissions for the following roles: General Settings, Replication Settings, and Storage Settings.

6. Click **Add**.

### Starting the AltaVault Storage Optimization Service

After you configure other AltaVault settings, you must start the Storage Optimization Service, which provides compression, deduplication, and encryption of data upon ingest into AltaVault.

**Steps**

1. From the AltaVault menu, select **Maintenance > Service**.
2. Click **Start** or **Restart**.
3. To verify that the service is running again, select **Home > Optimization Service**.
   
   The display indicates that the service is running and that the status is "Ready."

### Configuring AltaVault using the AltaVault CLI

To configure AltaVault, you can use the AltaVault command-line interface (CLI) rather than the graphical user interface (GUI).

### Enabling the SnapMirror service using the AltaVault CLI

AltaVault supports backup and restore operations for ONTAP FlexVol volumes using the SnapMirror service running on an AltaVault appliance. You must enable the SnapMirror service, which then enables ONTAP to create the SnapMirror relationship in AltaVault and enable backup and restore operations of NAS file services data.

**About this task**

Instead of using a graphical user interface, you can use the AltaVault command-line interface (CLI) to configure SnapMirror. If you already configured SnapMirror using the AltaVault graphical user interface, you do not need to perform this procedure using the CLI.

When the SnapMirror service is enabled, the shares and Snapshot copies that exist on AltaVault are accessible and can be restored. If the SnapMirror service is disabled, the shares and Snapshot copies that exist on AltaVault are not deleted; however, Snapshot copies are not accessible.

**Steps**

1. From an SSH client, log in to the AltaVault appliance command line interface (CLI) using administrator credentials. Use the IP address or DNS of the AltaVault appliance:
   
   Example:
   ```
   ssh admin@172.16.4.4
   NetApp AltaVault
   admin@172.16.4.4's password:
   ```

2. Use SSH to log in to the AltaVault CLI and enter configuration mode:
   
   ```
   <hostname> > enable
   <hostname> # configure terminal
   <hostname> (config) #
   ```

3. Enable SnapMirror service:
To disable the SnapMirror service, use the `no snapmirror enable` command.

4. At the prompt, restart the Storage Optimization Service:

```
<hostname> (config)# service restart
```

5. Verify that the SnapMirror service is ready:

```
<hostname> (config)# show snapmirror state
SnapMirror Server: Ready
```

### Configuring a whitelist of IP connections using the AltaVault CLI

You must configure a whitelist of approved IP addresses from which AltaVault accepts SnapMirror connections.

**About this task**

If you use SnapCenter as part of this solution, SnapCenter creates the whitelist of approved IP addresses and enables the SnapMirror long-term retention mode when you initiate the backup from SnapCenter. In this case, there is no need to create the IP whitelist and enable SnapMirror long-term retention mode by using AltaVault.

**Steps**

1. If you are not already logged into the AltaVault appliance, from an SSH client, log in to the AltaVault appliance command line interface (CLI) using administrator credentials. Use the IP address or DNS of the AltaVault appliance:

   Example:

   ```
   ssh admin@172.16.4.4
   NetApp AltaVault
   admin@172.16.4.4's password:
   ```

2. Use SSH to log in to the AltaVault CLI and enter configuration mode:

   ```
   <hostname> > enable
   <hostname> # configure terminal
   <hostname> (config) #
   ```

3. Verify that the SnapMirror service is ready:

   ```
   <hostname> configure terminal
   <hostname> (config)# enable
   <hostname> show snapmirror state
   SnapMirror Server: Ready
   ```

4. If you are not using SnapCenter to manage NAS file services data protection, configure the whitelist of IP addresses from which AltaVault accepts SnapMirror data:

   You can enter only one IP address at a time.

   ```
   <hostname> (config)# snapmirror whitelist add ip <IP address>
   ```

5. Display a list of IP addresses:

   ```
   show snapmirror whitelist
   Entry: 192.0.2.253
   Entry: 192.0.2.254
   ```
To delete an IP address from the list, enter the `snapmirror whitelist delete ip <IP address>` command.

6. Restart the Storage Optimization Service:

   `<hostname> (config)# service restart`

7. Verify that the Storage Optimization Service is running:

   `<hostname> (config)# show service
   Storage Optimization Service: ready`

---

Enabling SnapMirror long-term retention mode using the AltaVault CLI

AltaVault supports up to 500 shares in one of two modes: short-term retention mode (default) or long-term retention mode. For Data Fabric Solution for Cloud Backup, the mode impacts the retention of your Snapshot copies. SnapMirror long-term retention mode is required if you want to retain more than 251 Snapshot copies for a relationship on AltaVault. Long-term retention mode is disabled by default.

About this task

If you already enabled SnapMirror long-term retention mode using the AltaVault graphical user interface, you do not need to perform this procedure using the CLI.

Snapshot copy retention is dependent upon the retention policy set up in either ONTAP or SnapCenter. For example, if the retention policy is set to 100 Snapshot copies, and the maximum is reached, AltaVault begins deleting the oldest Snapshot copies to make room for newer ones.

- In short-term retention mode, each share supports up to 251 Snapshot copies. The Snapshot copy retention is governed by the SnapMirror policy set in either ONTAP or SnapCenter.
  For example, suppose a share has a two-tier retention policy supporting 50 hourly and 100 daily Snapshot copies. In this case, when the count of hourly Snapshots exceeds 50 or the daily count exceeds 100, the oldest Snapshot copy of the respective tier is deleted.

- In long-term retention mode, each share supports up to 3700 Snapshot copies, which is the equivalent to 10 years of daily Snapshot copies.

Retention of Snapshot copies in archival mode can be managed by AltaVault or SnapCenter:

- Snapshot copies managed by AltaVault: AltaVault continues accumulating Snapshot copies with a maximum of 3700 before deleting the oldest Snapshot copy in the share. The oldest is deleted irrespective of the label (hourly/daily/monthly).

- Snapshot copies managed by SnapCenter: SnapCenter manages any number of Snapshot copies with a maximum of 3700.

Long-term retention mode is enabled automatically when SnapCenter transfers data to AltaVault.

Step

1. Using the AltaVault CLI, if you are not using SnapCenter to manage NAS file services data protection, optionally display and enable long-term retention mode to increase the number of Snapshot copies that can be retained in AltaVault:

   `<hostname> (config)# show snapmirror long-retention
   SnapMirror Archival mode: disabled
   <hostname> (config)# snapmirror long-retention enable`

   To disable long-term retention mode, enter the `no snapmirror long-retention` command.
Enabling access to SnapCenter using the AltaVault CLI

AltaVault supports using SnapCenter to back up, delete, and restore Snapshot copies, including individual file restores. If you are using SnapCenter to manage backups to AltaVault, you must enable SnapCenter access on AltaVault.

Steps
1. Using the AltaVault CLI, enable SnapCenter access to AltaVault:

   ```
   <hostname> (config)# rest enable
   ```

   To disable SnapCenter access, enter the `no rest enable` command.

2. Verify that SnapCenter access is enabled in AltaVault:

   ```
   <hostname> (config)# show rest status
   REST Service: running
   ```

   The status is either running (enabled) or stopped (disabled).

Adding a SnapCenter role-based user account to enable storage connections to an AltaVault appliance

If you are using SnapCenter for data protection management, you must add a SnapCenter role-based account to AltaVault. You will later add a storage connection in SnapCenter and will need this account's credential information.

Steps
1. Using the AltaVault CLI, create a role-based user account for SnapCenter in AltaVault:

   a. Create the account:

   ```
   <hostname> (config)# username <username> password <password>
   ```

   b. Set the role-based permissions on the account:

   ```
   <hostname> (config)# rbm user <username>
   role cb_general_settings permission read-write
   role cb_replication_settings permission read-write
   role cb_storage_settings permission read-write
   ```

2. Verify the account:

   ```
   <hostname> (config)# show rbm users
   User: storadmin
   role: cb_general_settings   permissions: read-write
   role: cb_replication_settings permissions: read-write
   role: cb_storage_settings permissions: read-write
   ```
Starting the AltaVault Optimization Service using the AltaVault CLI

After you configure AltaVault settings, you must start the Storage Optimization Service, which provides compression, deduplication, and encryption of data upon ingest into AltaVault.

Steps

1. If you are not already logged into the AltaVault appliance, from an SSH client, log in to the AltaVault appliance command line interface (CLI) using administrator credentials. Use the IP address or DNS of the AltaVault appliance:

   Example:
   ```
   ssh admin@172.16.4.4
   NetApp AltaVault
   admin@172.16.4.4's password:
   ```

2. Use SSH to log in to the AltaVault CLI and enter configuration mode:

   ```
   <hostname> > enable
   <hostname> # configure terminal
   <hostname> (config) #
   ```

3. Restart the Storage Optimization Service:

   ```
   <hostname> (config)# service restart
   ```

4. Verify that the Storage Optimization Service is running:

   ```
   <hostname> (config)# show service
   Storage Optimization Service: ready
   ```
Configuring SnapCenter for Data Fabric Solution for Cloud Backup

If you are using SnapCenter for data protection management and for file searches using the SnapCenter file catalog, you must configure SnapCenter.

Steps

1. **Logging in to SnapCenter** on page 49
   Through SnapCenter role-based access control, users or groups are assigned roles and resources. When you log in to the SnapCenter graphical user interface, you log in with an Active Directory account.

2. **Configuring the Infrastructure Admin role for AltaVault access** on page 50
   To configure role-based access control for SnapCenter users, you add users or groups to a role and the role's permissions.

3. **Setting up storage system connections** on page 51
   Before you can perform backup and restore operations with SnapCenter, you must set up the storage system connections to each AltaVault system and to each ONTAP Cluster.

4. **Setting up your CIFS servers Run As credentials for SnapCenter Plug-in for NAS File Services** on page 54
   SnapCenter uses Run As credentials to authenticate users for Plug-in for NAS File Services operations. For SMB (CIFS) shares only (not for NFS), you must create Run As credentials for mounting CIFS shares and configure a CIFS server for the ONTAP cluster.

5. **Configuring CIFS servers for Data Fabric Solution for Cloud Backup** on page 54
   For Data Fabric Solution for Cloud Backup for SMB (CIFS) shares only (not for NFS), you must create configure a CIFS server for the ONTAP cluster. This configuration associates the Run As credentials with the CIFS server for authentication.

6. **Protecting the SnapCenter file catalog and the repository** on page 55
   SnapCenter includes a NAS file services file catalog, which you should protect on a regular basis. You should also protect the SnapCenter repository. You can protect both using a PowerShell `protect-SmRepository` cmdlet.

Logging in to SnapCenter

Through SnapCenter role-based access control, users or groups are assigned roles and resources. When you log in to the SnapCenter graphical user interface, you log in with an Active Directory account.

**About this task**

During the installation, the SnapCenter Server Installation wizard creates a shortcut and places it on the desktop where SnapCenter is installed. Additionally, at the end of the installation, the Install wizard displays the SnapCenter URL, based on information you supplied during the installation, which you can copy if you want to log in from a remote system.

**Attention:** Closing just the SnapCenter browser tab does not log you off of SnapCenter if you have multiple tabs open in your web browser. If you need to comply with security requirements, you must log off of SnapCenter either by clicking the **Sign out** button or shutting down the entire web browser.

**Attention:** Do not allow your browser to save your SnapCenter password.
The default GUI URL is a secure connection to port 8146 on the server where the SnapCenter Server is installed (https://server:8146). If you provided a different server port during the SnapCenter installation, that port is used instead.

For Network Load Balance (NLB) deployment, you must access SnapCenter using the NLB cluster IP (https://NLB_Cluster_IP:8146).

In addition to using the SnapCenter GUI, you can use the following interfaces depending on the SnapCenter plug-in:

- PowerShell cmdlets on Windows hosts to perform data protection operations.
- SnapCenter command-line interface (CLI), such as sccli for Oracle databases on Linux machines to script configuration and data protection operations.

Note: Some cmdlets have changed in SnapCenter 2.0. If you use cmdlets in older versions of SnapCenter scripts, you might need to update your scripts.

For details, see the SnapCenter cmdlet or SnapCenter CLI documentation.

Steps

1. Launch SnapCenter from the shortcut located on your local host desktop, from the URL provided at the end of the installation, or from the URL provided to you by your SnapCenter administrator.

2. Enter your user credentials:

   Domain\UserName

3. If you are assigned more than one role, from the Role box, select the role you want to use for this login session.

   Your current user and associated role are shown in the upper right of SnapCenter.

Configuring the Infrastructure Admin role for AltaVault access

To configure role-based access control for SnapCenter users, you add users or groups to a role and the role’s permissions.

Before you begin

You must have logged in with the SnapCenterAdmin role.

About this task

The Data Fabric Solution for Cloud Backup requires that you add users to the predefined Infrastructure Admin role or create a role using the same permissions. When you assign users to this role, you should assign the AltaVault administration account for authorization and authentication. The Infrastructure Admin role enables users assigned to this role access to the SnapCenter file catalog.

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Settings.

2. In the Settings page, click Roles.

3. In the Roles page, select the Infrastructure Admin role to which you want to add the user.
4. Click Modify.
5. Click Next until you reach the Users/Groups page of the wizard.
6. In the Users/Groups page, specify the domain to which the user belongs.
7. In the user or group name field, enter a user or group name and click Add.
   Repeat to add additional users or groups to the selected role.
8. Click Next to view the summary, and then click Finish.

### Setting up storage system connections

Before you can perform backup and restore operations with SnapCenter, you must set up the storage system connections to each AltaVault system and to each ONTAP Cluster.

**Before you begin**

You must have permissions in the Infrastructure Admin role to create storage connections.

**About this task**

If you are planning to replicate Snapshot copies to a SnapMirror destination, make sure to set up storage system connections for the destination volume as well as the source volume.

Complete this procedure for each ONTAP connection and once for the AltaVault connection.

**Steps**

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Storage Systems.
2. In the Storage Systems page, click New.
3. In the **New Storage Connection** wizard, provide the following information for each ONTAP and AltaVault connection:

<table>
<thead>
<tr>
<th>For this field...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name/Password</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• ONTAP: Enter the credentials used (usually VSAdmin) to access the storage system.</td>
</tr>
<tr>
<td></td>
<td>• ONTAP SVM: Typically, enter the vsadmin credentials.</td>
</tr>
<tr>
<td></td>
<td>• AltaVault: Enter the role-based access control credentials you entered in AltaVault.</td>
</tr>
<tr>
<td>Site</td>
<td>Applicable only if you choose ONTAP Cluster or AltaVault as your storage type. Enter the physical site name, for example, the data center city. The site you enter is displayed in the SnapCenter interface.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol used for connection to the SVM that was configured during SVM setup, typically HTTPS.</td>
</tr>
</tbody>
</table>

If you have questions about these values, consult your storage administrator.

4. In the **New Storage Connection** wizard, provide the following information for the ONTAP connection:

<table>
<thead>
<tr>
<th>For this field...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage System</td>
<td>Enter the storage system name or IP address of the ONTAP cluster management interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Storage system names, not including the domain name, must be 15 characters or fewer. To create storage system connections with names with more than 15 characters, you can use the <code>Add-SmStorageConnection</code> PowerShell cmdlet. SnapCenter does not support multiple SVMs with the same name on different clusters. Each SVM supported by SnapCenter must have a unique name.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Select <strong>ONTAP Cluster</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you add a new ONTAP SVM connection and you have already added an ONTAP Cluster for the Data Fabric Solution for Cloud Backup, after you add the SVM, you must run the <strong>Modify Storage Connection</strong> wizard on the ONTAP Cluster that you already added to ensure the following updates are made:</td>
</tr>
<tr>
<td></td>
<td>• The SVM is in the NSM database</td>
</tr>
<tr>
<td></td>
<td>• CIFS server discovery is enabled on the SVM</td>
</tr>
<tr>
<td></td>
<td>• The SnapCenter cache is updated with information about the new SVM</td>
</tr>
</tbody>
</table>
For this field… | Do this…
---|---
Timeout | Applicable only if you choose ONTAP Cluster or ONTAP SVM as the storage type. Enter the time in seconds that should elapse before communication attempts are halted. The default value is 60 seconds.
Event Management System (EMS) | Applicable only if you choose ONTAP Cluster or ONTAP SVM as the storage type. If you want to have Event Management System (EMS) messages sent to the storage system syslog or have AutoSupport messages sent to the storage system for failed operations, select the appropriate check box. When you select the AutoSupport check box, the EMS messages check box is also selected because EMS messaging is required to enable AutoSupport notifications.

If you have questions about these values, consult your storage administrator.

5. In the **New Storage Connection** wizard, provide the following information for the AltaVault connection:

<table>
<thead>
<tr>
<th>For this field…</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage System</td>
<td>Enter the storage system name or IP address of the AltaVault primary interface that was configured during the AltaVault installation and configuration. <strong>Note:</strong> Storage system names, not including the domain name, must be 15 characters or fewer. To create storage system connections with names with more than 15 characters, you can use the <code>Add-SmStorageConnection</code> PowerShell cmdlet.</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Select AltaVault. For each AltaVault system, choose AltaVault as the storage type, and choose ONTAP Cluster as the second storage type.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port that the storage system accepts. If you are configuring the AltaVault connection, enter the AltaVault port.</td>
</tr>
</tbody>
</table>

If you have questions about these values, consult your storage administrator.

6. Optional: If the SVM has multiple management interfaces, select the **Preferred IP address** check box, and then enter the preferred IP address for SVM connections.

**Note:** If you have more than one iSCSI or FC session configured per SVM connected to the host, then use the host device for multipathing rather than using the native device. While performing a restore, clone, mount, or backup verification operation, if the storage system and the host have iSCSI and FC configured together, then FC is preferred.

**ONTAP 9 Cluster Management Using OnCommand System Manager**

7. Click **OK**.
Setting up your CIFS servers Run As credentials for SnapCenter Plug-in for NAS File Services

SnapCenter uses Run As credentials to authenticate users for Plug-in for NAS File Services operations. For SMB (CIFS) shares only (not for NFS), you must create Run As credentials for mounting CIFS shares and configure a CIFS server for the ONTAP cluster.

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Settings.

2. In the Settings page, click Run As Credentials.

3. Click New.

4. In the Run As Credentials page, do the following:

<table>
<thead>
<tr>
<th>For this field…</th>
<th>Do this…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run As name</td>
<td>Enter a descriptive label for the Run As credentials.</td>
</tr>
<tr>
<td>User name/Password</td>
<td>Enter the credentials used for authentication. You must add the domain name as the prefix to the username (for example, domainname\administrator).</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>For Data Fabric Solution for Cloud Backup for CIFS shares only, select Windows as the mode.</td>
</tr>
</tbody>
</table>

5. Click OK.

After you finish

After you finish setting up Run As credentials, you might want to assign Run As credential maintenance to a user or group of users on the My SnapCenter Assets page.

Configuring CIFS servers for Data Fabric Solution for Cloud Backup

For Data Fabric Solution for Cloud Backup for SMB (CIFS) shares only (not for NFS), you must create configure a CIFS server for the ONTAP cluster. This configuration associates the Run As credentials with the CIFS server for authentication.

Before you begin

You must have already fulfilled these prerequisites:

- You must have already created Windows Run As credentials for CIFS.
- The CIFS server domain must already be in a trust relationship with the SnapCenter Server domain.
- The CIFS server name should be available from the SnapCenter Server host and file catalog host.
Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Storage Systems.
2. In the Storage Systems page, click on an ONTAP cluster.
3. Click Configure CIFS Servers.
4. For each CIFS server, select the associated Run As credential.
5. Click OK.

Protecting the SnapCenter file catalog and the repository
SnapCenter includes a NAS file services file catalog, which you should protect on a regular basis. You should also protect the SnapCenter repository. You can protect both using a PowerShell protect-SmRepository cmdlet.

Before you begin
If you have not done so previously for SnapCenter use, you should prepare the PowerShell environment.

About this task
During the SnapCenter installation, the SnapCenter repository is placed on the C drive of the Windows host. However, you might want to move it to a NetApp volume. To do so, you can use the SnapCenter Protect-SmRepository cmdlet.

Best Practice: You should back up the file catalog and repository daily or at least once a week.

Preparing the PowerShell environment
Preparing the PowerShell environment includes verifying that the modules that contain the cmdlets are loaded, and if not, importing the necessary modules.

About this task
For information about PowerShell cmdlets, use the SnapCenter cmdlet help or see the cmdlet reference information.

SnapCenter Software 2.0 Windows Cmdlet Reference Guide

Steps
1. On either the SnapCenter Server or the application host where a SnapCenter plug-in is installed, open a PowerShell session window and verify that the proper modules are loaded by using the get-module cmdlet.

Example

```
PS C:\> get-module
ModuleType Version Name ExportedCommands
---------- ------- ---- ----------------
```
2. If the cmdlets that reside on the SnapDrive module are not displayed, import that module:

import-module

**Note:** import-module imports a module only into the current session. To import a module into all sessions, add an `import-module` cmdlet to your Windows PowerShell profile.

**Example**

```
PS C:\> get-module -listavailable snap* | import-module
PS C:\> get-module
Directory: C:\Windows\system32\WindowsPowerShell\v1.0\Modules

ModuleType Version Name          ExportedCommands
---------- ------- ----          ----------------
Manifest   1.0    SnapCenter    {Add-SmPolicy, Add-SmRunAs, Add-SmVeri...
Manifest   1.0.0  SnapDrive     {Add-SdIgroupInitiator, Add-SdPortSetPort, C...
```

**Protecting the file catalog and SnapCenter repository with PowerShell cmdlets**

For the Data Fabric Solution for Cloud Backup solution, SnapCenter includes a file catalog, which you should protect. You should also protect the SnapCenter metadata repository. You can accomplish both using a PowerShell cmdlet.

**About this task**

**Steps**

1. Launch PowerShell.

2. From the SnapCenter Server command prompt, enter the following and enter your credentials:

```
Open-SMConnection -RoleName <role>
```

If you use multiple SnapCenter roles, you should add the `<role>` parameter.

**Example**

```
Open-SMConnection -RoleName SnapCenterAdmin
```
3. Protect the file catalog by using the `Protect-SmRepository` command:

```
```

**HostName**

Specifies the SnapCenter database host name. If the SnapCenter database is hosted by a failover cluster instance (FCI), then specify the FCI owner host name.

**Path**

Specifies the NetApp destination disk path.

**Schedule**

Specifies the backup schedule type.

Options are as follows:

**ScheduleType**

Specifies the backup schedule type.

**StartTime**

Specifies the scheduled backup start time. The default is the current time.

**EndTime**

Specifies the scheduled end time.

**RetentionCount**

Specifies the number of backups to retain. By default, seven backups are retained.

**CatalogBackupPath**

Specifies an NFS mount point on ONTAP storage. The NFS mount point must be accessible to all backup catalog servers.

This parameter is used only when you have NAS file services installed.

**Example**

```
Protect-SmRepository -HostName Dan-NGVM2.sme711ad.net -Path F:\ -Schedule @("ScheduleType"="hourly","StartTime"="11/30/2016 5:55 AM","RepeatTask_Every_Hour"="00:15") -CatalogBackupPath /mnt/catalog_backup -RetentionCount 4
```

4. Protect the SnapCenter metadata repository:

```
```

**Example**

```
Protect-SmRepository -HostName NB-MVA-DEV057.nbsdsm.mycompany.netapp.in -Path E:\DBs -InstanceCredential sa -SQLServerAuthenticationMode SQL -Schedule @("ScheduleType"="hourly","StartTime"="10/21/2016 5:18 PM")
```
You can back up NAS file services data to the cloud and restore it from the cloud using SnapCenter and AltaVault. Using SnapCenter, you can orchestrate a baseline backup from ONTAP to AltaVault. Subsequently, all backups of that volume from ONTAP are incremental backups and are initiated by the SnapCenter policy-driven schedule.

**About this task**

For information about initiating backups using the ONTAP command line interface (CLI) instead, see information about backing up NAS file services data using the CLI.

*Back up NAS file services data to the cloud and restore it using ONTAP commands* on page 72

You can back up all shares on a FlexVol volume from primary or secondary storage to AltaVault, which then replicates data to the cloud, as specified in AltaVault configurations.

Each volume is linked with one share in AltaVault.

You can define policies that govern the timing and retention of backups.

Later, if needed, you can perform a single file restore of data from AltaVault to ONTAP using SnapCenter or ONTAP CLI.

**Note:** With the ONTAP CLI, you can perform a full volume restore in addition to a single file restore.

SnapCenter supports up to 100 concurrent transfers to a single AltaVault node, including both backup and restore operations. This means that if 100 concurrent backups are running against a single node, you cannot initiate any restore operations from that node. Concurrent restore operations can be done only if you restore to different volumes; concurrent restore operations cannot occur with the same source and destination volume.

**Best Practice:** As a best practice, we recommend that you initiate no more than 10 concurrent restore operations. Otherwise, transfers might time out and slower restore throughput might occur.

You can add up to 80 volumes in a single policy-governed backup operation.
Steps

1. **Using policies to protect NAS file services data** on page 59
   A backup policy is a set of rules that governs how you manage and retain backups, and how frequently the resource is backed up. Additionally, you can specify replication options. Specifying options in a policy saves time when you want to reuse the policy for another resource.

2. **Backing up NAS file services data to the cloud** on page 61
   Backing up NAS file services data to the cloud involves starting the backup process, monitoring the process, and verifying that the backup was completed.

3. **Restoring NAS file data from the cloud using SnapCenter** on page 67
   You can restore a single file from the cloud to ONTAP. Restoring NAS file data from the cloud includes several short tasks.

**Using policies to protect NAS file services data**

A backup policy is a set of rules that governs how you manage and retain backups, and how frequently the resource is backed up. Additionally, you can specify replication options. Specifying options in a policy saves time when you want to reuse the policy for another resource.

**About this task**

SnapCenter includes the following predefined policies that govern the protection of NAS file services:

- **Backup to the Cloud**: Backs up ONTAP FlexVol volumes on primary storage to AltaVault.
- **Backup to Vault to Cloud**: Backs up ONTAP FlexVol volumes on primary storage to secondary storage and then to AltaVault.

To back up NAS file services data, you must first copy and modify predefined policies to suit your needs.

**Note**: You cannot use the predefined policies for NAS file services without first copying them and you cannot create your own policies for NAS file services.

You can copy and modify policies before or during the setup of the backup process. This procedure describes how to copy a policy before starting the backup process.

**Steps**

1. In the SnapCenter left navigation pane, click **Settings**.
2. On the Settings page, click **Policies**.
3. To review the details of any predefined policies, click one of the predefined policies and click **Details**.
4. Click the policy, click **Copy**, enter a new policy name, which must be unique, and then click **OK**.
5. Click the copy and click **Modify**.
6. In the **Policy** wizard, enter an optional description and click **Next**.
7. In the Protection page, click on one of the protection schedule boxes at the top to configure the options for that schedule.

**Note:** You can modify Storage Cluster and Storage VM information only until the policy is attached to a volume and protected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site or Vault Site</td>
<td>Enter the data center site name.</td>
</tr>
<tr>
<td>Cloud Bucket</td>
<td>Applicable only if you select the cloud copies location. Enter the name of the bucket associated with the cloud provider.</td>
</tr>
<tr>
<td>Choose Storage Cluster</td>
<td>Applicable only if you select the vault copies location. Select the ONTAP Cluster as the backup destination.</td>
</tr>
<tr>
<td>Choose Storage VM</td>
<td>Applicable only if you select the vault copies location. Select the Storage Virtual Machine (SVM) as the backup destination.</td>
</tr>
<tr>
<td>Backup Transfer Start Time</td>
<td>Enter the time when the initial baseline backup should begin. This is based on the ONTAP source storage time zone.</td>
</tr>
<tr>
<td>Transfer Window</td>
<td>Select the number of hours during which the backup transfer should occur. After that time plus the lag time elapses, if the backup is not available in ONTAP SnapVault or AltaVault, the backup will be in a warning state.</td>
</tr>
<tr>
<td>Lag Time</td>
<td>Select the number of additional hours that the backup transfer can take after the transfer window elapses. The minimum lag time is 1 hour. After the transfer window plus the lag time elapses and if the backup is not available in ONTAP SnapVault or AltaVault, the backup will be in a warning state.</td>
</tr>
<tr>
<td>Daily, Weekly, Monthly options</td>
<td>Enter the time when the daily, weekly, or monthly backup should start, enter how frequently the backup should occur, and enter how many backups to retain. Note: This is based on the SnapCenter Server time zone.</td>
</tr>
</tbody>
</table>
Example
Consider this example:

- Backup Transfer Start Time: 5 PM
- Transfer Window: 3 hours
- Lag Time: 2 hours

In this example, the Snapshot copy transfer will start at 5 PM and will have 3 hours for a transfer window. However, if the backup does not complete in the 3 hours of transfer window, then it has lag time of another 2 hours. By 10 PM, the data should have been transferred.

8. Review the summary and click Finish.

Backing up NAS file services data to the cloud

Backing up NAS file services data to the cloud involves starting the backup process, monitoring the process, and verifying that the backup was completed.

About this task
- Back up files to the cloud using SnapCenter and AltaVault
- Monitor data protection progress in the SnapCenter backup Activity pane
- Monitor backup operations progress in the SnapCenter Jobs page
- Verify backup to the cloud completion in AltaVault

Backing up NAS file services data to the cloud using SnapCenter and AltaVault

You can back up all shares on a NFS or CIFS protocol-supported volume to the cloud.

About this task
When you apply a policy to a volume, you can indicate when the initial baseline backup should be performed. After this baseline backup completes, all subsequent backups, which are incremental backups, occur according to the schedule in the policy.

Steps
1. From the SnapCenter left navigation pane, click Resources.
2. From the Resources page, search for the volume you want to back up by entering criteria in the Search box and pressing Enter.
3. Optionally, filter the list of results by clicking on the Filter icon.
   A list of volumes appears.
The green shield on a volume indicates that the volume has been protected already and you cannot set up protection again. The red shield indicates that the volume is unavailable for protection (for example, if it is offline).

4. To view details about the volume, click the down arrow on the volume.

5. Select a policy among in the policy boxes on the right.

   If you do not select a policy, the first policy is selected by default.

   **Note:** Predefined policies do not appear among the policy boxes on the right. You must first copy a predefined policy and modify it before you can use it to govern data protection.

6. To back up the volume to the cloud and index the files within it, either click the + on the volume or drag the volume to the policy box on the right.

   You can back up multiple volumes in one job by dragging each volume to the policy or clicking the + sign on each volume.

   When a volume is placed on the policy, the Policy card shows a blue outline and displays a number in the upper left indicating the number of volumes placed on this policy.

7. To view details of the policy, click the down arrow on the policy box.

   You might want to add tags, for example, “finance,” to the backup so that you can later find it by searching for all backups with the tag. Or you might want to add an email notification.

8. To initiate a backup immediately, click the down arrow on the policy box and check **Run initial backup immediately**.

   You can also schedule a backup for a specific date and time.

9. To finish the backup, in the policy box, click **Create Backup**.

**After you finish**

Monitor the progress of the data transfer to AltaVault in the Activity pane at the bottom.

**Monitoring data protection progress in the SnapCenter Activity pane**

After you initiate an ONTAP backup in SnapCenter, you can immediately review the progress of the data transfer from ONTAP to AltaVault using the Activity pane that appears on the bottom of the backup page in SnapCenter. You can also track progress for restore operations.

**About this task**

The Activity pane shows information for the following data protection processes:
• Backup operations to AltaVault

  **Note:** Scheduled backup job activity does not appear on the Activity pane.

• Restore operations from AltaVault if you used the file catalog from the Dashboard or from the Resources option.

**Step**

1. After you initiate an ONTAP backup or restore operation in SnapCenter, review the SnapCenter Activity pane on the bottom of the page.

   ![Activity pane screenshot](image)

The Activity pane shows the following information:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active, Failed, Completed information in the top bar</td>
<td>Displays a status for all volumes. For example, if two volumes are being backed up at the same time and one failed instantly, the status shows Active = 1 and Failed = 1.</td>
</tr>
<tr>
<td>1st column: &lt;number of minutes&gt;</td>
<td>Displays when the activity began.</td>
</tr>
<tr>
<td>2nd column: &lt;status&gt;</td>
<td>Displays the activity, such as applying protection on volume, replicating Snapshot, or restoring data.</td>
</tr>
</tbody>
</table>
| 3rd column: progress bars and icons | The first bar shows the backup progress from ONTAP to AltaVault. The second bar shows the backup progress from ONTAP to ONTAP to AltaVault. During the restore process, the restore activity appears.  
  - **Snapshot icon:** Displays the progress of the backup of primary storage data.  
  - **Vault icon:** Displays the progress of the backup from ONTAP to ONTAP to AltaVault.  
  - **Cloud icon:** Displays the progress of the transfer of data from SnapCenter to AltaVault. |
| 4th column: percentage | Shows the percentage complete for the entire data transfer process to AltaVault. |

**Monitoring backup operations from the Jobs page**

You can monitor the progress of different backup operations by using the SnapCenter Jobs page. You might want to check the progress of an operation to determine when it is complete or if there is an issue.

**About this task**

The following icons appear on the Jobs page and indicate the state of the operation:

- ![In progress icon] In progress
Steps
1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Monitor.
2. In the Monitor page, click Jobs.
3. Optional: In the Jobs page, perform the following steps:
   a. Click to filter the list so that only backup operations are listed.
   b. Specify the start and end dates.
   c. From the Type drop-down list, select Backup.
   d. From the Status drop-down, select the backup status.
   e. Click Apply to view the operations completed successfully.
4. Select the backup job, and then click Details to view the job details.
   Note: Though the backup job status displays ✔, when you click on job details you might see that some of the child tasks of the backup operation are still in progress.
5. Optional: In the Job Details page, click View logs.
   The View logs button displays the detailed logs for the selected operation.

Verifying backup to the cloud completion on AltaVault (optional)

Based on SnapMirror policies created using ONTAP CLI or SnapCenter, Snapshot copies of ONTAP volumes are backed up to the associated AltaVault share. If the backup job is successful, you do not need to verify the backup. However, you still might want to verify that the share was transmitted to AltaVault and then replicated to the cloud.

About this task

Snapshot copies backed up to AltaVault shares are read-only copies and can be restored back to ONTAP using only ONTAP CLI commands or SnapCenter. (A SnapMirror share is created automatically when the SnapMirror relationship with the AltaVault is created in ONTAP.)

During the lifetime of a volume, there is only one baseline Snapshot copy. Any Snapshot copy after the baseline is always incremental. Baseline transfer can take a long time to complete depending on the size of the Snapshot copy.

During incremental backups, only the changed blocks between two Snapshot copies are transferred. Backups can be triggered in ONTAP either through SnapMirror policies in SnapCenter or by using the ONTAP snapmirror update command.

AltaVault provides compression, global deduplication, and encryption of all Snapshot copy backup streams prior to replication to the cloud.
## Steps

1. Log in to AltaVault.
2. Select **Configure > SnapMirror**.
3. Under SnapMirror Shares, review the information associated with share.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>&lt;Share&gt; Name</strong></td>
<td>Specifies the name of the share. When the ONTAP administrator creates a SnapMirror relationship with AltaVault or when a NAS file services backup is completed in SnapCenter, a share is automatically created in AltaVault. Each share is associated with one ONTAP FlexVol volume.</td>
</tr>
<tr>
<td><strong>Peer Path</strong></td>
<td>Identifies the path to the vServer and source volume in ONTAP (vServer:ONTAP volume) that is being backed up in AltaVault.</td>
</tr>
<tr>
<td><strong>UUID</strong></td>
<td>Lists the unique identifier associated each SnapMirror share. The Snapshot copy UUID value is generated by ONTAP. The Share UUID value is generated by AltaVault.</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>Specifies the size of the SnapMirror share. The size can grow or shrink as Snapshot copies are backed up or deleted from the share. Shares on AltaVault have no size limitation but are bound by the AltaVault appliance cache capacity. The size of source volume, change rate, and number of Snapshot copies impact the number and size of SnapMirror shares on AltaVault.</td>
</tr>
</tbody>
</table>

4. Optionally, select a share and view the Snapshot copy information.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Snapshot copy&gt; Name</td>
<td>Lists the label of the Snapshot copy. When the ONTAP administrator creates a SnapMirror relationship with AltaVault or when a NAS file services backup is completed in SnapCenter, a share is automatically created in AltaVault. Each share is associated with one ONTAP FlexVol volume. During the lifetime of a share, there is only one baseline Snapshot copy. Any Snapshot copy after the baseline is always incremental. Baseline transfer can take a long time to complete depending on the size of the Snapshot copy. During incremental Snapshot backups, only the changed blocks between two Snapshot copies are transferred.</td>
</tr>
<tr>
<td>UUID</td>
<td>Specifies the unique identifier associated each Snapshot copy. The UUID value is generated by ONTAP.</td>
</tr>
<tr>
<td>Created</td>
<td>Indicates the date and time when the Snapshot copy was created in ONTAP.</td>
</tr>
<tr>
<td>Size</td>
<td>Specifies the size of the Snapshot copy.</td>
</tr>
</tbody>
</table>
| Status               | Indication of progression of the Snapshot copy backup to the cloud:  
  • Pending: Snapshot copy replication to the cloud is in progress.  
  • Completed: Snapshot copy replication to the cloud was successful.  
  Snapshots appear only after they have been ingested into AltaVault. |

5. Optionally, to remove a share or Snapshot copy, select the item from the list and click **Remove Selected**.

Snapshot copies can be deleted on AltaVault through ONTAP or SnapCenter policies, or by manual deletion on AltaVault. Upon Snapshot copy deletion, the data belonging to a Snapshot copy is not deleted immediately from AltaVault. When long-term retention is enabled, AltaVault has an asynchronous reclamation process, meaning the data is reclaimed only when a certain number of Snapshot copies have been deleted.

When a share is deleted, Snapshot copies in that share are also deleted. Snapshot copies cannot be restored once deleted even though the Snapshot copy data may not have been deleted.

**Verifying backup to the cloud completion using AltaVault CLI (optional)**

Based on SnapMirror policies created in ONTAP or SnapCenter, Snapshot copies of ONTAP volumes are backed up to the associated AltaVault share. If the backup job is successful, you do not need to verify the backup. However, you might want to verify that the share was transmitted to AltaVault and then replicated to the cloud. You can perform this using the AltaVault command-line interface (CLI).

**Steps**

1. Use SSH to log in to the AltaVault CLI and enter configuration mode:

```
<hostname> > enable
<hostname> # configuration terminal
<hostname> (config) #
```
2. After the backup has occurred, look at the SnapMirror shares on AltaVault:

```
<hostname> (config)# show snapmirror shares
Total Snapmirror shares - 2
Share: dst1
  Peer path: vs1:src1
  UUID: a7f871fb-b757-cb42-86fc-1b3cf8746346
  Size: 20.0 KB
Share: dst2
  Peer path: vs1:src2
  UUID: 6aa603ba-0084-1248-a71c-6de5dbdac92
  Size: 20.0 KB
```

3. After the backup has occurred, look at the Snapshot copies on those shares on AltaVault:

```
<hostname> (config)# show snapmirror snapshots share-name dst1
Total snapshots - 2
Name:         UUID:                                  Create Time:       Size:      Replication Status
snap1         82c5671a-746b-4358-86a7-50744a0bea33   11-11-2016 13:11   10.0 KB     Complete
snap2         2d825301-33bc-4ae-a8fa-c75230a57dddb  11-11-2016 13:11   10.0 KB     Pending
```

Restoring NAS file data from the cloud using SnapCenter

You can restore a single file from the cloud to ONTAP. Restoring NAS file data from the cloud includes several short tasks.

**About this task**

- Locate the file to be restored.
- Restore the file from the cloud using SnapCenter
- Monitor restore progress in the SnapCenter backup Activity pane
- Monitor restore progress in the SnapCenter Jobs page

SnapCenter supports up to 100 concurrent transfers to a single AltaVault node, including both backup and restore operations. This means that if 100 concurrent backups are running against a single node, you cannot initiate any restore operations from that node. Concurrent restore operations can be done only if you restore to different volumes; concurrent restore operations cannot occur with the same source and destination volume.

**Best Practice:** As a best practice, we recommend that you initiate no more than 10 concurrent restore operations. Otherwise, transfers might time out and slower restore throughput might occur.

You can locate the file in different ways:

- Search the file catalog if you do not know the exact file name.
- Browse through the backups to locate the copy you want to restore
Searching in the file catalog for a specific file to restore using keywords and filters

Using the SnapCenter file catalog, you can search for a specific file to restore possibly among thousands of files across volumes. You can narrow down the list of results quickly and easily.

About this task

You can search for NAS file services file that you want to restore in the following ways:

- From the SnapCenter Dashboard: If you know the specific file, keywords in that file name, type of file, or date of the file, but do not know the volume that stores the file, you should use the file catalog.
  
  For example, you can find a specific file from years ago that you want to restore. You can filter by volume or share name, tag names assigned to backups, file types, file size, owner, and data range.

- From the SnapCenter Resources page: If you know the volume name, you should search for volumes using the Resource page. Then, you can filter by volume, storage virtual machine (SVM), share, or path.
  
  For details, see information about searching for volumes.

Cataloging of files is performed only in the primary storage system. The file catalog is updated with information on where the backup exists (primary, secondary, or AltaVault) after the data transfer is complete. Indexing of files for the catalog is done only at the file level, not on the contents inside files.

If there is at least one share in a volume, the SnapCenter file catalog includes only the shares. Otherwise, the catalog includes the entire volume.

Steps

1. From the SnapCenter Dashboard, click **Restore Backups**.
2. Search for the file you want to restore using the following search tips:
   - Search for single terms.
   - To search by multiple words, surround the phrase with double quotes.
   - To combine multiple phrases, use Boolean operators in all capital letters: AND, OR, NOT.

   **SnapMirror AND "archival mode"**

   - To search for any single character, enter "?" for that character, even in the middle of a term, for example:

     **te?t**

   - To search for multiple characters, enter "*" at the end or even in the middle of the term. For example, "test*" yields the results of "test," "testing," and "tester."

     **Note:** You cannot use a * or ? as the first character of a search.

   - To search for similar "fuzzy" terms, enter the tilde "~" at the end of the term. For example, "backup~" could yield terms like "rack" and "backed."

     **backup~**
• To search for words that are within a specific number of words away from each other, use the tilde "~" at the end of a phrase. For example, to search for "licensing" and "SnapMirror" within 10 words of each other in the document, enter the following phrase that is surround by double quotes:

"licensing SnapMirror"~10

• To include a special character such as the following in your query, use the \ character before the special character:

+ - && || ! ( ) { } [ ] ^ " ~ ? : \

A list of files appears, which could include possibly thousands of files that match your search criteria.

3. To find the specific file you want to restore, filter the results by volume or share name, tag names assigned to backups, file types, file size, owner, or data range.

4. Click **Apply**.

5. From the list of filtered results, click on the file you want to restore.

6. From the topology view showing the backups, click the Backups box.

7. From the list of backups at the selected location, click the backup and drag it over to the Restore tile.

8. At the bottom of the Restore tile, click **Restore**.
Restoring NAS file data from the cloud using SnapCenter

When you want to restore a NAS file that has been damaged, accidentally changed or deleted, you can use SnapCenter to request that AltaVault restore the file from a cloud backup to its original location.

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Resources.
2. In the Resources page, locate and select the volume in the Backup Object Selection view from which you want to restore a file, and then click Actions.
3. In the Manage Copies view, select the backup you want to use to restore a file, and then click the Browse (eye) icon.
4. Expand the folders as needed to locate the file you want to restore, and then select the file.
5. In the Restore Files view, select to restore it to its original location.
6. Click Restore.

Caution: If you continue, all data in the restore location will be overwritten. If you want to preserve the file, you should rename the file that you are trying to restore, not the backup file itself, and restart the process.

7. In the confirmation message that all data written to the file will be overwritten with the backup data, click Yes to continue.
8. Monitor the progress of the operation by viewing the Activity pane at the bottom of the page.
   The Activity pane shows information for the following data protection processes:
   • Backup operations to AltaVault
   • Restore operations from AltaVault if you used the file catalog from the Dashboard or if you used the Resources option.
9. Monitor the progress of the operation using the Jobs page.
Related tasks

- Monitoring restore operations from the Jobs page on page 71
- Monitoring data protection progress in the SnapCenter Activity pane on page 62

Monitoring restore operations from the Jobs page

You can monitor the progress of different SnapCenter restore operations by using the Jobs page. You might want to check the progress of an operation to determine when it is complete or if there is an issue.

About this task

Post-restore states describe the conditions of the resource after a restore operation and any further restore actions that you can take.

The following icons appear on the Jobs page, and indicate the state of the operation:

- In progress
- Completed successfully
- Failed
- Completed with warnings or could not start due to warnings
- Queued
- Cancelled

Steps

1. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Monitor.
2. In the Monitor page, click Jobs.
3. Optional: In the Jobs page, perform the following steps:
   a. Click to filter the list so that only restore operations are listed.
   b. Optional: Specify the start and end dates.
   c. From the Type drop-down list, select Restore.
   d. From the Status drop-down list, select the restore status.
   e. Click Apply to view the operations that are completed successfully.
4. Select the restore job, and then click Details to view the job details.
5. Optional: In the Job Details page, click View logs.

The View logs button displays the detailed logs for the selected operation.
Backing up NAS file services data to the cloud and restoring it using ONTAP commands

You can perform protection operations of NAS file services data using the ONTAP command-line interface (CLI) instead of the SnapCenter graphical user interface (GUI). Using the CLI, you can back up NAS file services data to AltaVault for replication to the cloud and restore it from the cloud back to an ONTAP volume.

About this task

For information about initiating backups using the SnapCenter GUI instead, see information about backing up NAS file services data using SnapCenter.

An ONTAP volume, which can include multiple directories and files, can be backed up to one share in AltaVault. First, you back up a full baseline to AltaVault and then you can perform incremental backups forever.

You can later restore a full backup including all Snapshot copies from AltaVault to a new destination ONTAP volume or you can restore a single file in a Snapshot copy from AltaVault to a new or existing ONTAP volume.

Steps

1. Creating a SnapMirror protection relationship on page 72
   Before performing a backup operation from ONTAP to AltaVault, you create and initialize a SnapMirror relationship. This involves viewing the volume's status and verifying the relationship.

2. Backing up NAS file services data to the cloud using ONTAP commands on page 75
   Backing up NAS file services data to the cloud using ONTAP command-line interface (CLI) involves performing an incremental backup followed by monitoring backup progress. ONTAP FlexVols are backed up to AltaVault as NAS file shares on volumes.

3. Restoring NAS file services data from the cloud using ONTAP commands on page 78
   You can restore a full backup or a single file from a Snapshot copy from AltaVault cache or cloud storage back to ONTAP.

Related tasks

Backing up NAS file services data to the cloud and restoring data with SnapCenter management on page 58

Creating a SnapMirror protection relationship

Before performing a backup operation from ONTAP to AltaVault, you create and initialize a SnapMirror relationship. This involves viewing the volume's status and verifying the relationship.

About this task

When you create and initialize a SnapMirror protection relationship, you perform the following tasks:

• Optionally review the volume's status and contents.
• Create and initialize a SnapMirror relationship.
• Verify that the relationship was created in AltaVault.
• Show the transfer of contents in AltaVault.

**Reviewing volume status and contents**

Prior to backing up a volume from ONTAP to AltaVault, you might want to review the volume status and the volume’s contents.

**Steps**

1. Log in to the ONTAP CLI.

2. List the status of volumes by entering: `volume show`

   The volume you want to back up should have a status of `online`.

   **Example**

   ```
   cluster1::*> volume show
   Vserver   Volume       Aggregate    State      Type       Size  Available Used%
   -------- ------------ ------------ ---------- ---- ---------- ---------- -----  
   cluster1-01 vol0         aggr0_01     online     RW       7.17GB     1.70GB   76%
   cluster1-02 vol0         aggr0_02     online     RW       7.17GB     1.72GB   76%
   svm1      Finance      aggr1_01     online     RW         10GB     9.03GB    9%
   svm1      svm1_root    aggr1_01     online     RW         20MB    18.67MB    6%
   svm1      vol1         aggr1_01     online     RW         20GB    18.53GB    7%
   5 entries were displayed.
   ```

3. Optionally, verify the contents of the volume.

   **Example**

   ```
   cluster1::> set diag
   cluster1::> run local ls -lr /vol/Finance
   ```

**Creating and initializing a SnapMirror protection relationship**

Prior to backing up a volume from ONTAP to AltaVault, you must create and initialize a SnapMirror relationship between ONTAP and AltaVault. This creates a share on AltaVault.

**About this task**

For a backup of an ONTAP FlexVol to an ONTAP FlexVol, both the source and destinations use the format `<Vserver>:<volume>`. However for the AltaVault endpoint, you use the format `<IP_address>:/share/<share_name>`

**Steps**

1. Log in to the ONTAP CLI.

2. Create and initialize a SnapMirror relationship, which creates a share in AltaVault.

   The protection type must be "XDP" for Extended Data Protection, which is used for SnapVault protection.

   **Example**

   ```
   snapmirror initialize -destination-path 192.168.0.75:/share/Finance -source-path svm1:Finance -type XDP
   ```

3. Show the status of the baseline backup of the volume:
Example

```
cluster1::*> snapmirror show

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Type</th>
<th>Destination Path</th>
<th>State</th>
<th>Relationship</th>
<th>Total Progress</th>
<th>Healthy</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>svm1:Finance</td>
<td>XDP</td>
<td>192.168.0.75:/share/Finance</td>
<td>-</td>
<td>Idle</td>
<td>-</td>
<td>true</td>
<td>-</td>
</tr>
</tbody>
</table>
```

The Idle state indicates the transfer is complete.

4. Show the Snapshot copy creation for the baseline transfer.

Example

```
cluster1::*> snapshot show Finance

---Blocks---
Vserver Volume Snapshot                                  Size Total% Used%
-------- -------- ------------------------------------- -------- ------ -----
svm1     Finance snapmirror.e200c372-bb7e-11e4-a4b7-005056011d47_1101668560875.2017-05-02_170619 76KB 0% 0%
```

5. Using the AltaVault CLI, look for the baseline backup of shares on the destination volume in AltaVault.

a. From an SSH client, log into the AltaVault appliance command line interface (CLI) using administrator credentials. Use the IP address or DNS of the AltaVault Appliance:

```
ssh admin@192.168.0.75
NetApp AltaVault
admin@192.168.0.75's password:
```

b. View the SnapMirror share created for the volume:

```
<hostname> > enable
onk-sm# show snapmirror shares
Total Snapmirror shares - 1
Share: Finance
Peer path: svm1:Finance
UUID: 95ce78be-08da-704b-a463-fbe0f72c2a29
Size: 477.73 MB
altavault # show snapmirror snapshots share-name Finance
Total snapshots - 1
Name: UUID: Create Time: Size:
Replication Status
snapmirror.e200c372-bb7e-11e4-a4b7-005056011d47_1101668560875.2017-05-02_170619 0bfb9ddf-19d2-451f-b7e6-2ea0df59c4a 05-02-2017 13:06 477.73 MB
Completed
```

The Replication Status changes from Pending to Completed, indicating that the replication to AltaVault has completed.

After you finish

If you configured the SnapMirror relationship with a policy containing update schedules, then no further action is necessary. Backups to the cloud will occur on the schedules specified in the policy. If you want to view the backups that have occurred, see information about monitoring backups. If you want to perform an on-demand backup, see information about performing on-demand backups to the cloud.

Monitoring backup progress using the ONTAP CLI on page 77
Back up NAS file services data to the cloud using ONTAP commands

Back up NAS file services data to the cloud using ONTAP command-line interface (CLI) involves performing an incremental backup followed by monitoring backup progress. ONTAP FlexVol volumes are backed up to AltaVault as NAS file shares on volumes.

Performing an incremental backup from ONTAP to the cloud using the ONTAP CLI

Performing incremental backups capture additional Snapshot copy data since the SnapMirror protection relationship was established. After you create and initialize a SnapMirror protection relationship, which creates a baseline backup, backups occur according to the schedules set in the selected ONTAP SnapMirror policies. In addition to scheduled backups, you can perform an on-demand backup of a LUN.

Before you begin

A protection relationship must exist between the ONTAP volume and the AltaVault share, which creates a baseline backup from ONTAP to AltaVault.

About this task

When you perform an incremental backup from ONTAP to AltaVault and to the cloud, you review the volume’s contents, create a Snapshot copy, update the SnapMirror relationship using the Snapshot copy, transfer the data to AltaVault, and finally show the transfer of the contents in AltaVault.

Steps

1. Log in to the ONTAP CLI.
2. Create a Snapshot copy:

   Example

   ```bash
   cluster1::> snapshot create -vserver vs2
   -volume ontap_source
   -snapshot base_snapshot
   ```

   Alternatively, you can schedule a backup by using the command: `snapmirror policy create` or schedule the update by using the command: `snapmirror modify -destination-path <dest-path> -schedule <schedule>

3. Verify successful Snapshot copy creation in AltaVault:
4. Create an incremental backup using the Snapshot copy just created:

Example

```
cluster1::> snapmirror update
    -source-path vs2:ontap_source
    -destination-path 192.0.2.150:/share/ava_dest_1
    -source-snapshot incremental_snapshot
```

Do not use the `--enable-storage-efficiency` option with the `snapmirror update` command for Data Fabric Solution for Cloud Backup operations.

5. Show the transfer of the contents:

Example

```
cluster1::> snapmirror show
```

The Relationship Status changes from `Transferring` to `Idle`, indicating that the transfer is complete.

6. Show the transfer of the contents to verify completion:

Example

```
cluster1::> snapmirror show
```

7. Additionally, using the AltaVault CLI, look for baseline and incremental backup of shares on the destination volume in AltaVault.

Example

```
onk-sm# show snapmirror snapshots share-name ava_dest_1
```

Total Snapshots - 2
The Replication Status changes from *Pending* to *Completed*, indicating that the replication to AltaVault has completed. After cloud provider settings are configured in AltaVault as instructed in the configuration information, the backup of data that was transferred to AltaVault is automatically replicated to the cloud.

**Monitoring backup progress using the ONTAP CLI**

After you initiate a backup, you can monitor the progress of that backup to the cloud using the ONTAP command-line interface (CLIL).

**Steps**

1. Log in to the ONTAP CLI.
2. Show the progress of the Snapshot copy transfer:

   ```bash
   cluster1::> snapmirror show
   ``

   **Example**

   ```bash
   cluster1::>* snapmirror show
   Source Path: vs34:src
   Source Cluster: -
   Source Vserver: vs34
   Source Volume: src
   Destination Path: 192.0.2.22:/share/dst
   Destination Cluster: -
   Destination Vserver: vs34
   Destination Volume: -
   Relationship Type: XDP
   Relationship Group Type: none
   Managing Vserver: vs34
   SnapMirror Schedule: -
   SnapMirror Policy Type: vault
   SnapMirror Policy: XDPDefault
   Tries Limit: -
   Throttle (KB/sec): unlimited
   Current Transfer Throttle (KB/sec): 0
   Mirror State: Uninitialized
   Relationship Status: Transferring
   File Restore File Count: -
   File Restore File List: -
   Transfer Snapshot: snapmirror.b8f64f8f-94cb-11e6-8193-0050568576ed_1101672341869.2016-10-24_123309
   Snapshot Progress: 12.86MB
   Total Progress: 12.86MB
   Network Compression Ratio: 1:1
   Snapshot Checkpoint: 0B
   ...
   ``

3. Show the progress of the Snapshot copy transfer again until you see that the Mirror State shows "Snapmirrored" and the Relationship status shows "Idle" as in the following example:

   ```bash
   cluster1::> snapmirror show
   ```
### Example

```bash
cluster1:/> snapmirror show
```

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Type</th>
<th>Destination Path</th>
<th>State</th>
<th>Relationship</th>
<th>Total Progress</th>
<th>Healthy</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs34:src</td>
<td>XDP</td>
<td>192.0.2.22:/share/dst</td>
<td>Snapmirrored</td>
<td>Idle</td>
<td>true</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

### Restoring NAS file services data from the cloud using ONTAP commands

You can restore a full backup or a single file from a Snapshot copy from AltaVault cache or cloud storage back to ONTAP.

**About this task**

You can restore data in the following ways:

- Restore a full backup from the AltaVault cloud to a new destination volume in ONTAP
- Restore a single file from a Snapshot copy in AltaVault to a new or existing volume in ONTAP

SnapCenter supports up to 100 concurrent transfers to a single AltaVault node, including both backup and restore operations. This means that if 100 concurrent backups are running against a single node, you cannot initiate any restore operations from that node. Concurrent restore operations can be done only if you restore to different volumes; concurrent restore operations cannot occur with the same source and destination volume.

**Best Practice:** As a best practice, we recommend that you initiate no more than 10 concurrent restore operations. Otherwise, transfers might time out and slower restore throughput might occur.

### Restoring a full backup from the cloud using the ONTAP CLI

Restoring a full baseline backup from the cloud storage to ONTAP includes creating a new destination volume in ONTAP for the restored data, restoring cloud data back to the new destination volume in ONTAP, reviewing the transfer of data, and ensuring that the ONTAP volume reverts to a read/write volume.

**Before you begin**

You must have already backed up data from ONTAP to AltaVault.

**About this task**

You can only perform a baseline full volume restore of any Snapshot copy backed up to AltaVault. If you have say, for example, 365 incremental restore operations, you would restore 365 volumes separately.

Alternatively, you can restore a single file to ONTAP rather than the entire baseline backup.

**Steps**

1. Log into the AltaVault CLI.
2. Using the AltaVault CLI, identify the share:

```bash
<hostname> (config) # show snapmirror shares
```
3. Using the AltaVault CLI, identify the Snapshot copies for a share:

   
   ```
   <hostname> (config) # show snapmirror snapshots share-name <share_name>
   ```

4. Log in to the ONTAP CLI.

5. Using the ONTAP CLI, create a destination volume where you will restore the Snapshot data using a relationship type of DP:

   ```
   cluster1::> volume create -volume <volume> -type DP
   ```

   **Example**

   The following command creates a 2 GB volume of type DP:

   ```
   cluster1::> volume create -volume ontap_dest
     -aggregate agg1 -type DP -size 2GB
   ```

   For a full volume restore, the transfer of a share from AltaVault back to ONTAP converts the volume automatically to a read/write volume. Note that this is different from a single file restore, where the destination volume must be read/write.

6. Look at the list of volumes to see the volume you created:

   **Example**

   ```
   cluster1::> volume show
   ```

7. Restore AltaVault share data back to the ONTAP volume:

   ```
   cluster1::> Snapmirror restore
     -source-path <IP_address>:/share/<share_name>
     -destination-path <Vserver_name>:<volume_name>
     -source-snapshot <Snapshot_name>
   ```

   Do not use the `snapmirror restore -use-network-compression` option for Data Fabric Solution for Cloud Backup.

   **Example**

   ```
   cluster1::> Snapmirror restore
     -source-path 192.0.2.150:/share/ava_dest_1
     -destination-path vs2:ontap_dest
     -source-snapshot base_snapshot
   ```

8. Look at the data transferred from AltaVault back to ONTAP:

   **Example**

   ```
   cluster1::> Snapmirror show
   ```

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Destination Path</th>
<th>Mirror State</th>
<th>Relationship Status</th>
<th>Total Progress</th>
<th>Healthy</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.150:/share/ava_dest_1</td>
<td>RST vs2:ontap_dest</td>
<td>Snapmirrored Idle</td>
<td>Transferring</td>
<td>0B</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>vs2:ontap_source XDF 192.0.2.150:/share/ava_dest_1</td>
<td>Snapmirrored Idle</td>
<td>true</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   2 entries were displayed.

   The Mirror State of RST indicates that restore relationships exist while the transfer is occurring. After the transfer completes, the RST relationship is removed.

9. Again, look at the data transferred from AltaVault back to ONTAP:
### Example

```
cluster1::> Snapmirror show
```

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Type</th>
<th>Destination Path</th>
<th>Type</th>
<th>Mirror</th>
<th>State</th>
<th>Status</th>
<th>Relationship Status</th>
<th>Total Progress</th>
<th>Healthy</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.150:/share/ava_dest_1</td>
<td>RST</td>
<td>vs2:ontap_dest</td>
<td>XDP</td>
<td></td>
<td></td>
<td></td>
<td>Snapmirrored</td>
<td>true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vs2:ontap_source</td>
<td>XDP</td>
<td>192.0.2.150:/share/ava_dest</td>
<td>XDP</td>
<td></td>
<td></td>
<td></td>
<td>Snapmirrored</td>
<td>true</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 entries were displayed.

The Relationship Status changes from **Uninitialized Transferring** to **Snapmirrored**.

10. Again, look at the data transferred from AltaVault back to ONTAP:

```
cluster1::> Snapmirror show
```

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Type</th>
<th>Destination Path</th>
<th>Type</th>
<th>Mirror</th>
<th>State</th>
<th>Status</th>
<th>Relationship Status</th>
<th>Total Progress</th>
<th>Healthy</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.150:/share/ava_dest_1</td>
<td>RST</td>
<td>vs2:ontap_dest</td>
<td>XDP</td>
<td></td>
<td></td>
<td></td>
<td>Broken-off</td>
<td>true</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vs2:ontap_source</td>
<td>XDP</td>
<td>192.0.2.150:/share/ava_dest</td>
<td>XDP</td>
<td></td>
<td></td>
<td></td>
<td>Snapmirrored</td>
<td>true</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2 entries were displayed.

The Relationship Status changes from **Snapmirrored** to **Broken-off** indicating that the relationship has been removed.

11. Look at the volume on ONTAP and verify that the destination relationship changes from DP to R/W:

```
cluster1::> volume show
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Aggregate</th>
<th>State</th>
<th>Type</th>
<th>Size</th>
<th>Available</th>
<th>Used%</th>
</tr>
</thead>
<tbody>
<tr>
<td>onk-vsim1</td>
<td>vol0</td>
<td>aggr0</td>
<td>online</td>
<td>RW</td>
<td>2.85GB</td>
<td>705.4MB</td>
<td>76%</td>
</tr>
<tr>
<td>vs2</td>
<td>ontap_dest</td>
<td>aggr1</td>
<td>online</td>
<td>RW</td>
<td>1GB</td>
<td>1021MB</td>
<td>5%</td>
</tr>
<tr>
<td>vs2</td>
<td>ontap_source</td>
<td>aggr1</td>
<td>online</td>
<td>RW</td>
<td>1GB</td>
<td>966.4MB</td>
<td>5%</td>
</tr>
<tr>
<td>vs2</td>
<td>vs_root1</td>
<td>aggr1</td>
<td>online</td>
<td>RW</td>
<td>20MB</td>
<td>10MB</td>
<td>9%</td>
</tr>
</tbody>
</table>

4 entries were displayed.

12. Verify that the Snapshot copy was restored on ONTAP:

```
cluster1::> snapshot show ontap_dest
```

<table>
<thead>
<tr>
<th>Vserver</th>
<th>Volume</th>
<th>Snapshot</th>
<th>Size</th>
<th>Total%</th>
<th>Used%</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs2</td>
<td>ontap_dest</td>
<td>base_snapshot</td>
<td>112KB</td>
<td>0%</td>
<td>5%</td>
</tr>
</tbody>
</table>

### Related tasks

* Monitoring backup progress using the ONTAP CLI on page 77

### Restoring a single file from the cloud to ONTAP using the ONTAP CLI

Instead of restoring an entire volume, you can restore individual files from the Snapshot copy back to an existing or new ONTAP volume. Restoring a single file from cloud storage to ONTAP includes creating a new destination volume if needed in ONTAP into which you will restore the file, restoring
AltaVault data back to the destination volume in ONTAP, reviewing the transfer of data, and ensuring that the ONTAP volume reverts to a read/write volume.

**Before you begin**

You must have already backed up data from ONTAP to AltaVault. 

You must already know the volume name, the Snapshot copy name, and the file name that you want to restore.

**Steps**

1. Log into the AltaVault CLI.
2. Using the AltaVault CLI, identify the share:
   ```
   <hostname> (config) # show snapmirror shares
   ```
3. Using the AltaVault CLI, identify the Snapshot copies for a share:
   ```
   <hostname> (config) # show snapmirror snapshots share-name <share_name>
   ```
4. Log in to the ONTAP CLI.
5. Using the ONTAP CLI, optionally create a destination volume where you will restore the Snapshot data using a relationship type of DP:
   ```
   cluster1::> volume create –volume <volume> -type RW -size <volume_size>
   ```

   **Example**

   The following command creates a 1 GB volume named "sfr_dest" of type Read/Write:
   ```
   cluster1::> volume create –volume sfr_dest
   -aggregate aggl -type RW -size 1GB -state online
   ```

   You can restore a single file back to a new or existing volume in ONTAP. If the file that you are restoring exists in the existing volume, the existing file will be overwritten. 

   For a single file restore, the destination volume must be read/write. Note that this is different for a full volume restore, where the transfer of a share from AltaVault back to ONTAP converts the volume automatically to a read/write volume.

6. Look at the list of volumes to see the volume you created:
   ```
   cluster1::> volume show
   ```

   **Example**

   ```
   cluster1::> volume show
   ```

7. Restore the single file from AltaVault to the ONTAP volume:
   ```
   cluster1::> Snapmirror restore
   -source-path <IP_address>:/share/<share_name>
   -destination-path <Vserver_name>:/<volume_name>
   -source-snapshot <snapshot_name>
   -file-list /<filename>
   ```

   Do not use the `snapmirror restore -use-network-compression` option for Data Fabric Solution for Cloud Backup.
Example

This example restores a single file "file3" from the Snapshot copy in AltaVault named "incremental_snapshot" to an ONTAP destination volume named "sfr_dest":

```bash
cluster1::> Snapmirror restore
   -source-path 192.0.2.150:/share/ava_dest_1
   -destination-path vs2:sfr_dest
   -source-snapshot incremental_snapshot
   -file-list /file3
```

8. Look at the data transferred from AltaVault back to ONTAP:

Example

```bash
cluster1::> snapmirror show
```

<table>
<thead>
<tr>
<th>Source Path</th>
<th>Destination Path</th>
<th>Mirror</th>
<th>Relationship</th>
<th>Total Progress</th>
<th>Progress Last</th>
<th>Healthy</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.2.150:/share/ava_dest_1</td>
<td>RST vs2:sfr_dest</td>
<td>Idle</td>
<td>Snapmirrored</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>vs2:ontap_source</td>
<td>XDP 192.0.2.150:/share/ava_dest_1</td>
<td>Idle</td>
<td></td>
<td>true</td>
<td>true</td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>

2 entries were displayed.

The Mirror State of RST indicates restore.

9. List the contents of the volume to verify that file was restored:

Example

```bash
cluster1::> set diag
ccluster1::> run local ls -lr /vol/sfr_dest
10644 96 i 2097152 Fri Oct 21 12:02:59 EST 2016 file3
```

Related tasks

*Monitoring backup progress using the ONTAP CLI* on page 77
Viewing data protection reports for NAS file services

Using the SnapCenter Dashboard page, you can view reports about backup and restore operations for NAS file services that have a particular status. This is useful if you want to identify the total number of successful or failed operations in your SnapCenter environment.

About this task

<table>
<thead>
<tr>
<th>Report type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Report</td>
<td>The Backup Report provides overall data about backup trends for NAS file services, the backup success rate, and some information about each backup performed during the specified time. If a backup is deleted, the report does not display any status information for the deleted backup. The Backup Detail Report provides detailed information about a specified backup job and lists the resources successfully backed up and any that have failed.</td>
</tr>
<tr>
<td>Restore Report</td>
<td>The Restore Report provides overall information about restore operations. The Restore Detail Report provides details about a specified restore operation, including host name, backup name, job start and duration, and the status of individual job tasks. If a task fails, the Restore Detail Report displays information about the failure.</td>
</tr>
<tr>
<td>Data Protection Report</td>
<td>This report provides protection details for NAS file services. You can see how many volumes are or are not protected.</td>
</tr>
</tbody>
</table>

Steps

1. Log in to SnapCenter.

2. In the left navigation pane, select the appropriate plug-in from the drop-down list, and then click Dashboard.

3. Locate the data protection pie chart.

4. Click the pie slice representing the status for which you want a report.

   You are directed to the Reports page. The report displays only operations with the status you selected.

5. Review the report, download it to your local system, print it, export it, or have it emailed.

   To email the report, select the Settings > Global Settings option and configure the SMTP server.
Where to go next

You can find more information about different features and release-specific information for Data Fabric Solution for Cloud Backup in the documentation available on the NetApp Support Site at mysupport.netapp.com.

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

• NetApp AltaVault Cloud Integrated Storage Administration Guide
  NetApp Documentation: AltaVault

• Release Notes
  Provides important information about this release of SnapCenter Server and the SnapCenter plug-in packages, including fixed issues, known issues, cautions, limitations, and any documentation updates or corrections.
  SnapCenter Software 2.0 Release Notes

• Installation and Setup Guide
  Describes the steps required to prepare for installation and to install SnapCenter and the SnapCenter plug-in packages. Setup processes are described for both current SnapManager users who are importing data to SnapCenter and users who are implementing a new SnapCenter environment.
  SnapCenter Software 2.0 Installation and Setup Guide

• Administration Guide
  Provides information about how to administer SnapCenter, provision Windows hosts with storage, configure and maintain role-based access control (RBAC), and use the centralized reporting options.
  SnapCenter Software 2.0 Administration Guide

• Windows Cmdlet Reference Guide
  Provides reference information about the Windows PowerShell cmdlets available in SnapCenter, including a description of each cmdlet, its syntax, and examples for its use. This content is also available through the SnapCenter PowerShell cmdlet help.
  SnapCenter Software 2.0 Windows Cmdlet Reference Guide

• Linux Command Reference Guide
  Provides reference information about the Linux commands available for Linux plug-ins, including a description of each command, its syntax, and examples for its use. This content is also available through the SnapCenter command-line interface help.
  SnapCenter Software 2.0 Linux Command Reference Guide

• SnapCenter Software Resources
  Provides a collection of videos, technical reports, and SnapCenter documentation.
  NetApp SnapCenter Software Resources
Copyright information

Copyright © 1994–2017 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).
Trademark information

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANscreen, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, Tech OnTap, Unbound Cloud, and WAF and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277
Index

A

about this guide
   deciding whether to use 6
access
   enabling SnapCenter in AltaVault 43, 47
   logging in to AltaVault 40
   logging in to SnapCenter 49
administrator
   logging in to SnapCenter as 49
administrator role
   adding in AltaVault 43, 47
AltaVault
   adding a SnapCenter user 43, 47
   configuring 39, 40
   configuring SnapMirror service using AltaVault CLI 44
   configuring using the CLI 44
   configuring using the GUI 40
   configuring whitelist of approved IP addresses 40
   configuring whitelist of approved IP addresses in AltaVault CLI 45
   enabling access to SnapCenter 43, 47
   enabling SnapMirror long-term retention mode 42, 46
installation 38
logging in 40
managing SnapMirror shares 64
managing SnapMirror shares using CLI 66
starting Storage Optimization Service 44
starting Storage Optimization Service using the CLI 48
supported versions 16
architecture
   components 8
   prerequisites 13
audience
   for this guide 6
authentication
   setting up your Run As account 54
AutoSupport notifications
   enabling for storage system connections 51

B

backing up
   monitoring NAS file services backup using ONTAP CLI 77
   monitoring progress 62
   monitoring progress in SnapCenter 63
   NAS file services using SnapCenter GUI 61
   performing an incremental backup of NAS file services using ONTAP CLI 75
   using ONTAP CLI, overview 75
   using or creating policies 59
backing up NAS file services
   with ONTAP CLI, overview 72
backing up volumes
   creating a SnapMirror protection relationship 72
creating SnapMirror relationship 73
viewing volume status and contents 73
best practices
   AltaVault requirements 16
   concurrent operations 58
   concurrent restore operations 58, 67, 78
   configuring intercluster LIFs 25
   protecting file catalog and repository 55
   renaming file 10
   setting up your Run As account 54
   SnapCenter file catalog 15
   SnapCenter file catalog requirements 15
browsers
   supported versions 16

C

catalog
   Linux server availability 33
   protecting 55, 56
   requirements 15
   searching for files to restore 68
CIFS
   configuring server 54
   required licenses for SnapCenter 17
cloud backup
   components 8
   overview 7
cluster peering
   preparing 24
   prerequisites 23
clusters
   configuring peer relationships for Data Fabric Solution for Cloud Backup 28
   creating cluster peering relationship 23
   credential requirements 20
comments
   how to send feedback about documentation 87
configuring
   AltaVault 40
   AltaVault overview 39
   CIFS server 54
   intercluster LIFs 25
   SMB server 54
   SnapCenter file catalog server ports 31
   SnapCenter overview 49
   workflow diagram with SnapCenter implementation 11
   workflow diagram without SnapCenter implementation 12
connections
   required before installing 19
   setting up for storage systems 51
credentials
   requirements 20
   setting up your Run As account 54
Data Fabric Solution for Cloud Backup
  configuring AltaVault 40
  connection and port requirements for installation 19
  documentation resources 84
  features 9
  installation order 21
  installing AltaVault 38
  installing ONTAP 21
  overview 7
  preparing for deployment 13
  what you can do 10
data transfer
  monitoring cloud backup completion in AltaVault 64
to AltaVault 62
databases
  preparing the PowerShell environment 55
documentation
  additional resources 84
  how to receive automatic notification of changes to 87
  how to send feedback about 87
documentation resources 84

how to send feedback about improving
  documentation 87
  installation log files
    checking for errors 36
  installing
    AltaVault 38
    connection and port requirements 19
    ONTAP 21
    operating systems supported 14
    order of components 21
    prerequisites 13
    SnapCenter 34
   SnapCenter file catalog server 30
    space and sizing requirements for packages 14
    space requirements for packages 14
    workflow diagram with SnapCenter implementation
    11
    workflow diagram without SnapCenter implementation
    12
  installing
    ONTAP 21
  intercluster LIFs
    configuring 25
    enabling for storage systems connections 51
feedback
  how to send comments about documentation 87
file catalog
  Linux server availability 33
  protecting 56
  requirements 15
  searching for files to restore 68
file catalog server
  configuring ports 31
  installing 30
  verifying Java version 33
FlexClone licenses
  required for SnapCenter 17
hosts
  licenses for SnapCenter plug-ins 17
  operating systems supported 14
  space and sizing requirements for installing Data
  Fabric Solution for Cloud Backup 14
  supported systems 13
  system requirements for installing Data Fabric
  Solution for Cloud Backup 14
HTTP
  port requirements 19
I
  information
  backing up to the cloud 61
  backing up to the cloud overview 58, 61

Index | 89
cloud backup overview 7
configuring AltaVault 39
configuring SnapCenter 49
protecting file catalog 56
protecting indexing catalog 55
reporting from the Dashboard 83
restoring from the cloud 70
restoring from the cloud overview 58, 67
searching in catalog for a file to restore 68
NAS File Services components
checking the status of 36
NFS
required licenses for SnapCenter 17
non-root user
installing plug-in for Oracle databases 32

**O**

ONTAP
adding a license 22
configuring for Data Fabric Solution for Cloud Backup 28
installation 21
preparing the environment overview 21
supported versions 13
ONTAP CLI
backing up and restoring NAS file services overview 72
backing up NAS file services to the cloud, overview 75
monitoring progress of cloud backup 77
performing an incremental backup of NAS file services 75
restoring a single file from the cloud to ONTAP 80
restoring NAS file services from the cloud to ONTAP, overview 78
restoring NAS file services from the cloud to ONTAP, overview 78
operating systems
supported 14
operations
monitoring backup progress from the Jobs page 63
monitoring restore progress from the Jobs page 71

**P**

permissions
setting for applications 54
plug-ins
space and sizing requirements for Data Fabric Solution for Cloud Backup installation 14
policies
using or creating 59
port requirements
before installing 19
port status
checking for Solr 36
checking for Solr server 36
ports
configuring SnapCenter file catalog server 31
PowerShell
preparing the environment 55
prerequisites
cluster peering 23
protecting
NAS file services file catalog 56
SnapCenter metadata repository 56

**R**

reports
data protection 83
repository
protecting 55, 56
requirements
connection and port, before installing Data Fabric Solution for Cloud Backup 19
credentials 20
restore operations
monitoring progress from the Jobs page 71
restoring
full baseline restore using ONTAP CLI 78
searching in catalog for a file 68
single file from the cloud 70
single file from the cloud, overview 67
single file restore using ONTAP CLI 80
restoring NAS file services with ONTAP CLI, overview 72
restoring NAS file services data using ONTAP CLI 78
role-based access control
adding account in AltaVault 43, 47
adding users to a role in SnapCenter 50
Run As account
setting up 54

**S**

services
Storage Optimization 44, 48
shares
managing in AltaVault 64
managing in AltaVault CLI 66
SMB
configuring server 54
SnapCenter
configuring 49
configuring file catalog server ports 31
enabling access to in AltaVault 43, 47
finding the URL 49
installing 34
installing file catalog server 30
installing overview 34
SnapCenter file catalog
installing file catalog server 34
SnapCenter Plug-in Loader
checking the status of 36
SnapMirror
configuring using AltaVault CLI 44
configuring with the AltaVault CLI 45
creating protection relationship 72, 73
enabling long-term retention mode in AltaVault 42, 46
licenses required for SnapCenter 17
SnapMirror shares
  managing in AltaVault 64
  managing using AltaVault CLI 66

SnapRestore
  licenses required for SnapCenter 17

Snapshot copies
  enabling AltaVault access to SnapCenter 43, 47
  impact on retention by SnapMirror long-term retention mode 42, 46

SnapVault
  licenses required for SnapCenter 17

storage system connections
  enabling AutoSupport notifications for 51
  enabling EMS messaging for 51

storage systems
  licenses for SnapCenter plug-ins 17
  setting up connections to 51

sudo privileges
  configuring for non-root user 32, 54

suggesting
  how to send feedback about documentation 87

systems
  requirements for Data Fabric Solution for Cloud Backup installation 14
  space and sizing requirements for SnapCenter installation 14

SnapVault
  licenses required for SnapCenter 17

status
  checking for SnapCenter Plug-in Loader 36
  checking NAS file components 36

support for Data Fabric Solution for Cloud Backup 14

T

Twitter
  how to receive automatic notification of documentation changes 87

U

users
  adding a SnapCenter user in AltaVault GUI 43, 47
  adding to a role in SnapCenter 50
  using roles at login 49

V

volumes
  viewing status and contents 73

W

web address
  for SnapCenter 49

whitelist of approved IP addresses
  configuring in AltaVault CLI 45
  configuring in AltaVault GUI 40

Windows Server
  operating systems supported 14

workflows
  preparing the PowerShell environment 55