Data Fabric Solutions

Data Fabric Solution for Cloud Backup Workflow Guide

Using ONTAP®, SnapCenter®, and AltaVault®

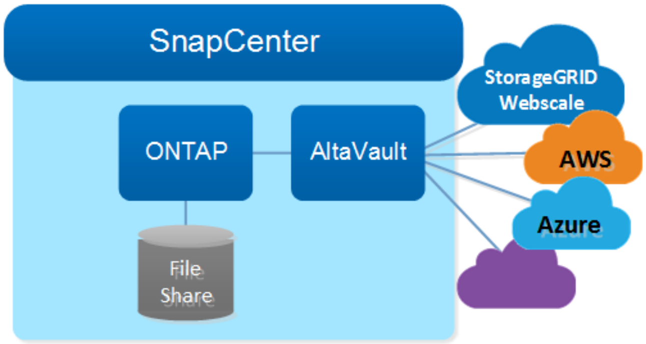
January 2017 | 215-11811_A0
doccomments@netapp.com

Contents

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.

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 space in cloud storage providers for Snapshot copies of file share data from ONTAP.

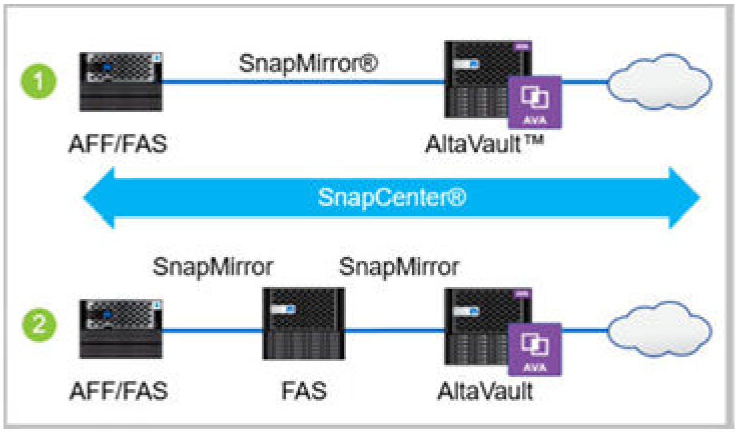


The Data Fabric Solution for Cloud Backup using SnapMirror technology enables administrators to back up NFS and SMB NAS file services (NFS v4, SMB3) and home directories to the cloud using an AltaVault cloud provider connection.

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:

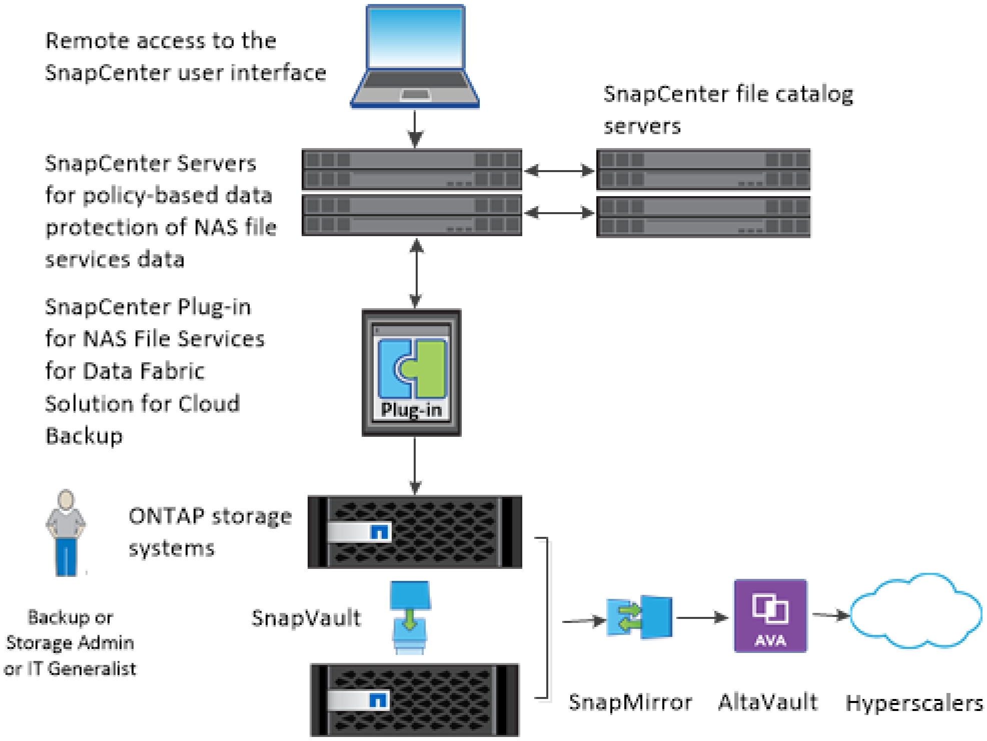
- Primary storage (AFF or FAS) to AltaVault
- Primary storage (AFF or FAS) to secondary storage (FAS) to AltaVault



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 with either a SnapMirror or SnapVault license
- SnapCenter 2.0 and the SnapCenter Plug-in for NAS File Services
- AltaVault 4.3 (physical or virtual)


Remote access to the SnapCenter user interface
SnapCenter file catalog servers
SnapCenter Servers for policy-based data protection of NAS file services data
SnapCenter Plug-in for NAS File Services for Data Fabric Solution for Cloud Backup
Plug-in
ONTAP storage systems
Backup or Storage Admin or IT Generalist
SnapVault
AVA
SnapMirror
AltaVault
Hyperscalers

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, schedules, and backup and restore operations 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, Google Cloud Storage, and IBM SoftLayer. When an administrator creates a SnapMirror relationship in ONTAP with AltaVault, a share is automatically created in AltaVault. When you use SnapCenter to initiate backups to AltaVault, the relationship is automatically created.

Each share 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
- 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 reduction

  When you use the Data Fabric Solution for Cloud Backup, data reduction 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 along with other applications and databases in the enterprise
- Access governed by role-based access control
- Preconfigured backup policies that simplify management for NAS file services
- End-to-end protection automation with policy-based management and secondary and tertiary relationship configuration
- 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 replicated over the Internet to cloud storage for efficient WAN 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 on FlexVol volumes in public or private clouds.

With the Data Fabric Solution for Cloud Backup and ONTAP, 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. With the ONTAP CLI, you can perform a full volume restore or a single file restore.

  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.

Using SnapCenter, you can accomplish the following:

- Back up NAS file services (on FlexVol volumes) from flash to disk to AltaVault and to the cloud.
- Apply predefined or custom policies for your backup and retention requirements.
- Restore individual files within file shares to the original location on the same volume.

  Note: 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 millions of files or, from a selected backup, find and restore a file
- Manage backup schedules and policies.

Using AltaVault, you can complete the cloud backup protection by performing these tasks:

- Perform efficient and secure backup to most clouds, public or private.
- Reduce I/O traffic to the cloud, saving ingest costs and in-cloud storage capacity with inline deduplication and compression.
- Accomplish long-term retention in the cloud.
- Connect multiple FAS systems to a single AltaVault. Using ONTAP CLI, you can manage this fan-in configuration relationship.

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.

ONTAP requirements

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

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

Primary FAS or All Flash FAS (AFF) systems directly connected to AltaVault require ONTAP 9.1 or greater. If you want to recover using AltaVault directly to the primary FAS or AFF, the primary system requires ONTAP 9.1 or greater.

In a cascade configuration where SnapMirror relationships exist such as from ONTAP to ONTAP, 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 and file catalog requirements

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

SnapCenter Server 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.

Item	Minimum
Version	2.0
CPU	4 CPUs
Memory	16 GB
Operating System	The following are supported: • Windows Server 2016 • Windows Server 2012 DCE, R2, Se, R2 SE Microsoft has identified an HTTP security vulnerability in their Windows operating systems that requires the installation of KB3042553-x64. *https://support.microsoft.com/en-us/kb/3042553*
SnapCenter storage amount	40 GB for both the software and the repository
SnapCenter metadata repository	MySQL Server 5.7 or greater The installation installs the SnapCenter repository on drive C of the host. After installation, you might want to move the repository using the `protect-SMRepository` PowerShell cmdlet.
Third-party libraries required on the SnapCenter Server	• Java 1.8.0.71 or later (Oracle or OpenJDK), 64-bit version. Must be installed before installing SnapCenter. • File archiver utility p7zip-9.20.1-8.1.1.x86_64.rpm or exe. Included in installation.

For the latest information, see the Interoperability Matrix.

SnapCenter file catalog requirements

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

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. We also recommend a replica for each partition shard for file catalog high availability and disaster recovery.

Item	Description
CPU	8 cores
Memory	24 GB RAM
Operating system	Red Hat Enterprise Linux (RHEL) 7.0, 7.1, and 7.2
Dedicated or shared server	Dedicated VM
Supported Hypervisors	VMware, Hyper-v
Java requirements	JRE 1.8
Linux host permissions	Root access is not required. 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.

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

Total number of files	Size	Disk capacity per node	CPU per node	Physical RAM per node	Shards	Replica per shard	Total number of machines
100 million	50 GB	250 GB	8 cores	12 GB	1	1	2
200 million	100 GB	250 GB	8 cores	24 GB	1	1	2
400 million	250 GB	250 GB	8 cores	48 GB	1	1	2
1 billion	500 GB	500 GB	8 cores	120 GB	1	1	2

A LUN must be provisioned for storing the file catalog data. During installation, you can specify the path to the preconfigured, provisioned LUN.

AltaVault requirements

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

Item	Minimum
Models	AltaVault physical models: AVA-400, AVA-800 AltaVault virtual models: AVA-v2, AVA-v8, AVA-v16, AVA-v32 AltaVault cloud models (AVA-c) are not supported.
Version	4.3
Storage type	Not applicable
Storage amount	Model dependent. Size depends on requirements of your ONTAP Snapshot copy policies to AltaVault

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, for example, SnapMirror and SMB.

Each volume in SnapCenter has a 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.

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.
- Microsoft Edge 2016

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.

License	Description	Where required
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.	

License	Description	Where required
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.
SnapVault	An optional license for disk-to-disk backup replication to a destination storage system.	Depends on the type of operation: • For primary storage (AFF or FAS) to AltaVault, required on primary storage system only. • For primary storage (AFF or FAS) to secondary storage (FAS) to AltaVault, required on both primary and destination.
SnapRestore	A required license that enables SnapCenter to restore and verify backup sets.	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.
AltaVault	A capacity-based license required for virtual models to enforce capacity-based storage sizes. Physical appliances do not require a license.	On AltaVault virtual appliance

License	Description	Where required
SnapCenter	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 enterprise applications (Microsoft SQL Server, Oracle) ◦ FAS and All Flash FAS (AFF): Included in Premium Bundle ◦ ONTAP Select and ONTAP Cloud: A la carte license, charged by capacity on the primary storage that is managed by SnapCenter **Note:** ONTAP Select and ONTAP Cloud are not supported in the Data Fabric Solution for Cloud Backup. • Advanced - Optional license. Required to support for NAS shares backup to the cloud using AltaVault and the file catalog ◦ FAS, AFF, ONTAP Select, ONTAP Cloud: A la carte license for unlimited hosts, charged by capacity on the primary storage managed by SnapCenter **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.	On SnapCenter Server
FlexClone	Required for Data Fabric Solution for Cloud Backup.	On primary storage systems
Protocols	For SMB shares, the CIFS license	On primary storage systems. Required on SnapMirror destination systems to serve data if a source volume is unavailable.

Connection and port requirements

Connections and ports must meet minimum requirements before you can install Data Fabric Solution for Cloud Backup.

Data Fabric Solution for Cloud Backup uses the following default ports. You can configure these ports during the installation process.

Type of port	Default port
SnapCenter port	8146 (HTTPS), customizable as in the URL `https://server:8146`
SnapCenter SMCore communication port	8145 (HTTPS), bidirectional, customizable
SnapCenter file catalog ports on Linux server	8145 customizable 2181, 2888, 3888, 8983
ONTAP to AltaVault	5010. Requires one or more intercluster LIFs. Recommend connection to 10 Gigabit Ethernet switch.
AltaVault	5010. Requires one or more data interfaces. Only HTTPS is supported for graphical user interface.

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

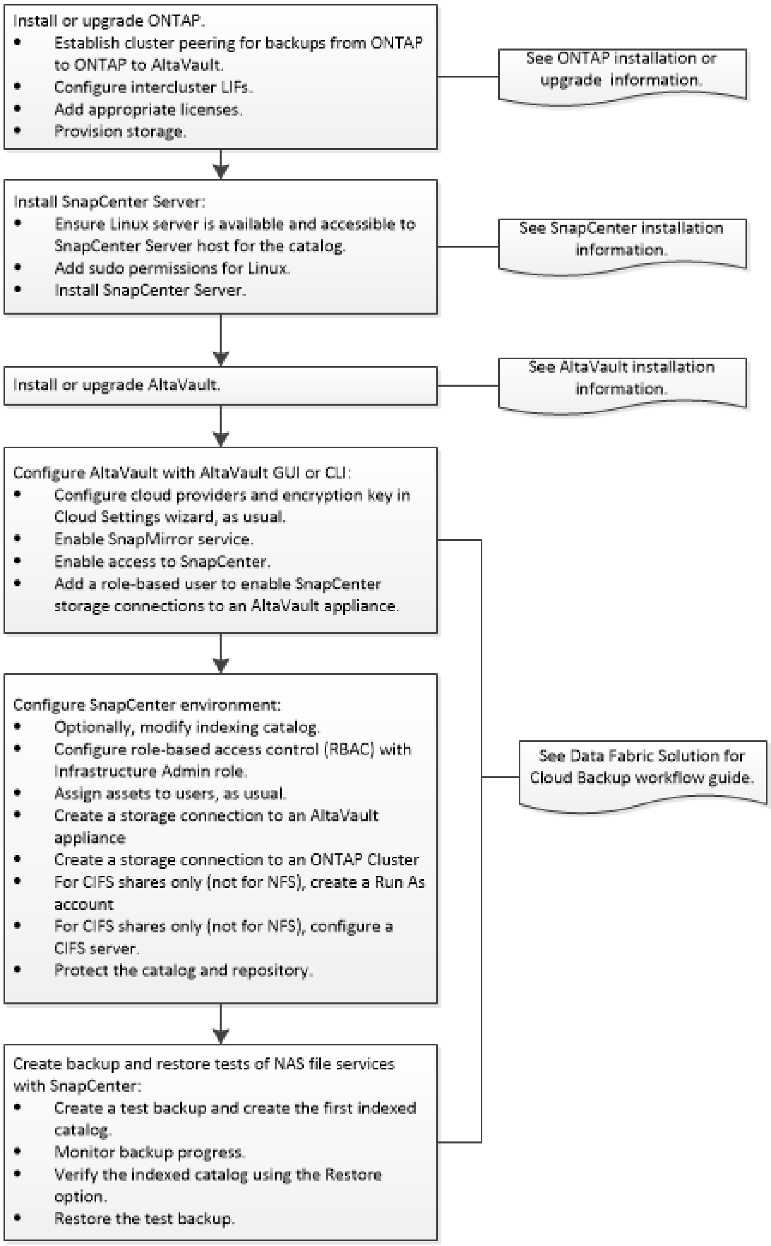
You cannot modify the port number after you install. To change a port number after installation, you must uninstall and install SnapCenter again.

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.

Installation and configuration workflow with SnapCenter data protection management

The Data Fabric Solution for Cloud Backup can be implemented with or without SnapCenter. Follow this workflow when using SnapCenter.



Install or upgrade ONTAP.

- Establish cluster peering for backups from ONTAP to ONTAP to AltaVault.
- Configure intercluster LIFs.
- Add appropriate licenses.
- Provision storage.

See ONTAP installation or upgrade information.

Install SnapCenter Server:

- Ensure Linux server is available and accessible to SnapCenter Server host for the catalog.
- Add sudo permissions for Linux.
- Install SnapCenter Server.

See SnapCenter installation information.

Install or upgrade AltaVault.

See AltaVault installation information.

Configure AltaVault with AltaVault GUI or CLI:

- Configure cloud providers and encryption key in Cloud Settings wizard, as usual.
- Enable SnapMirror service.
- Enable access to SnapCenter.
- Add a role-based user to enable SnapCenter storage connections to an AltaVault appliance.

Configure SnapCenter environment:

- Optionally, modify indexing catalog.
- Configure role-based access control (RBAC) with Infrastructure Admin role.
- Assign assets to users, as usual.
- Create a storage connection to an AltaVault appliance
- Create a storage connection 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 catalog and repository.

See Data Fabric Solution for Cloud Backup workflow guide.

Create backup and restore tests of NAS file services with SnapCenter:

- Create a test backup and create the first indexed catalog.
- Monitor backup progress.
- Verify the indexed catalog using the Restore option.
- Restore the test backup.

Related information

SnapCenter Software 2.0 Installation and Setup Guide

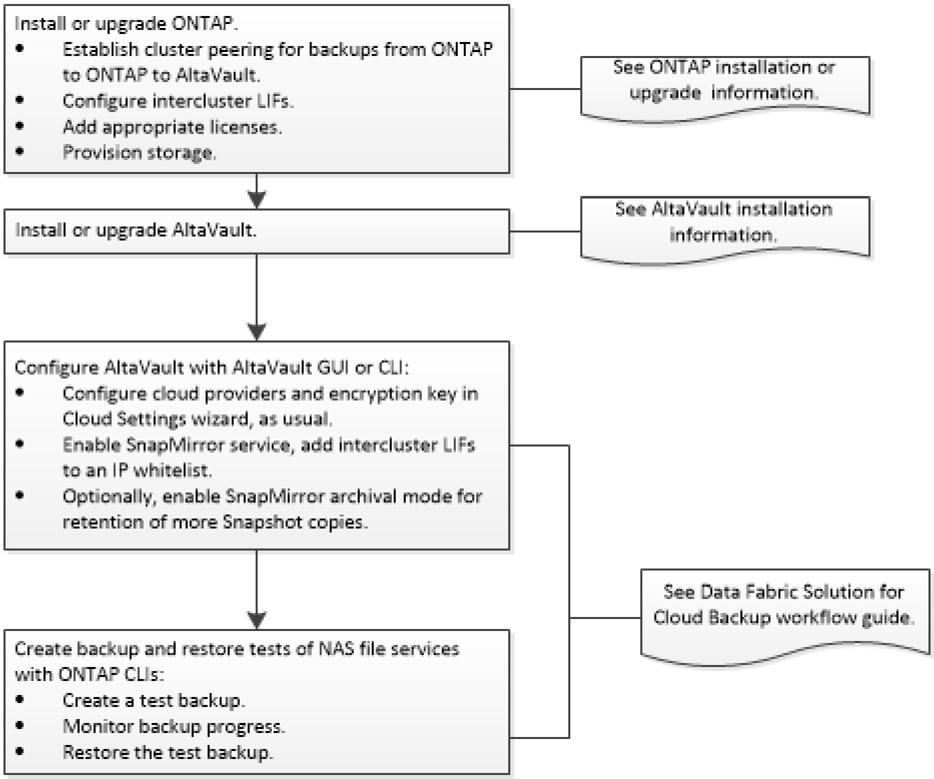
NetApp Documentation: AltaVault

ONTAP 9 Cluster Peering Express Guide

ONTAP 9 Upgrade Express Guide

Installation and configuration workflow without SnapCenter data protection management

The Data Fabric Solution for Cloud Backup can be implemented using ONTAP, AltaVault, and SnapCenter or the solution can be implemented with just ONTAP and AltaVault without SnapCenter data protection management. To install and configure the components of the solution without SnapCenter, you will need to follow the recommended workflow sequence.


Install or upgrade ONTAP.
• Establish cluster peering for backups from ONTAP to ONTAP to AltaVault.
• Configure intercluster LIFs.
• Add appropriate licenses.
• Provision storage.
See ONTAP installation or upgrade information.
Install or upgrade AltaVault.
See AltaVault installation information.
Configure AltaVault with AltaVault GUI or CLI:
• Configure cloud providers and encryption key in Cloud Settings wizard, as usual.
• Enable SnapMirror service, add intercluster LIFs to an IP whitelist.
• Optionally, enable SnapMirror archival mode for retention of more Snapshot copies.
See Data Fabric Solution for Cloud Backup workflow guide.
Create backup and restore tests of NAS file services with ONTAP CLIs:
• Create a test backup.
• Monitor backup progress.
• Restore the test backup.

Related information

NetApp Documentation: AltaVault
ONTAP 9 Cluster Peering Express Guide
ONTAP 9 Upgrade Express Guide

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. Typically, you do not use SMB/NFS and SnapMirror deployments on the same AltaVault instance, so we recommend a new AltaVault installation.

Upgrading ONTAP

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

Steps

1. Download the ONTAP upgrade package from the NetApp Support Site at *mysupport.netapp.com*.
2. Follow ONTAP upgrade instructions.

   ONTAP 9 Upgrade Express Guide

   http://docs.netapp.com/ontap-9/index.jsp
3. If you intend to back up NAS file services data from ONTAP to AltaVault, add a SnapMirror relationship 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.

   a. Identify licensed features on the source cluster:

   ```
   source_cluster::>system license show
   Serial Number: 1-80-000011
   Owner: source_cluster
   Package           Type    Description           Expiration
   ----------------- ------- --------------------- -----------
   Base              site    Cluster Base License   -
   NFS               site    NFS License            -
   CIFS              site    CIFS License           -
   iSCSI             site    iSCSI License          -
   FCP               site    FCP License            -
   SnapMirror        site    SnapMirror License     -
   FlexClone         site    FlexClone License      -
   7 entries were displayed.
   ```

   b. Identify licenses on the destination cluster:

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

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

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

Establishing cluster peering for Data Fabric Solution for Cloud Backup

If you intend to back up NAS file services from ONTAP to ONTAP to AltaVault, Data Fabric Solution for Cloud Backup requires a cluster peering relationship, a one-time operation that connects typically at least three clusters together to enable replication to occur among them.

About this task

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

- Preparing each cluster
- Creating intercluster logical interfaces (LIFs) on each node
- Setting up each peer relationship

Step

1. Establish the cluster peering relationship by following the cluster peering instructions.

   ONTAP 9 Cluster Peering Express Guide

Configuring intercluster LIFs to use dedicated intercluster ports

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

About this task

Creating intercluster LIFs that use dedicated ports involves creating a failover group for the dedicated ports and assigning LIFs to those ports. 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
                                                             Speed (Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    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 `cluster01_data01` uses port e0e and you want only an intercluster LIF to use that port:

```
cluster01::> network interface migrate -vserver cluster01
-lif cluster01_data01 -dest-node cluster01-01 -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

```
cluster01::> network interface modify -vserver cluster01
-lif cluster01_data01 -home-node cluster01-01 -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

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group intercluster01 -targets cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

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

   Example

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ---------------- --------------------------------------------
Cluster
```

```
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

6. Create an intercluster LIF on the admin SVM cluster01 by using the `network interface create` command.

Example

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

```
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl01
  -role intercluster -home-node cluster01-01 -home-port e0e
  -address 192.0.2.250 -netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif cluster01_icl02
  -role intercluster -home-node cluster01-02 -home-port e0e
  -address 192.0.2.251 -netmask 255.255.255.0 -failover-group intercluster01
```

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

Example

```
cluster01::> network interface show
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Cluster
            cluster01-01_clus_1
                         up/up    192.0.2.xxx/24   cluster01-01  e0a     true
            cluster01-01_clus_2
                         up/up    192.0.2.xxx/24   cluster01-01  e0b     true
            cluster01-02_clus_1
                         up/up    192.0.2.xxx/24   cluster01-01  e0a     true
            cluster01-02_clus_2
                         up/up    192.0.2.xxx/24   cluster01-01  e0b     true
cluster01
            cluster_mgmt up/up    192.0.0.xxx/24   cluster01-01  e0c     true
            cluster01_icl01
                         up/up    192.0.1.201/24   cluster01-01  e0e     true
            cluster01_icl02
                         up/up    192.0.1.202/24   cluster01-02  e0e     true
            cluster01-01_mgmt1
                         up/up    192.0.0.xxx/24   cluster01-01  e0c     true
            cluster01-02_mgmt1
                         up/up    192.0.0.xxx/24   cluster01-02  e0c     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

The LIFs in this example are assigned the e0e home port on each node. If the e0e port fails, the LIF can fail over to the e0f port.

```
cluster01::> network interface show -role intercluster –failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01-01
         cluster01-01_icl01 cluster01-01:e0e   local-only      intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01-01_icl02 cluster01-02:e0e   local-only      intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02: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:

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

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.

    ```
    cluster01::> network route create -vserver cluster01
    -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
    cluster01
              0.0.0.0/0       192.0.2.1     10
              0.0.0.0/0       192.0.2.2     40
    ```

12. If using peer clusters, repeat these steps to configure intercluster networking in the peer cluster.

13. Verify that the ports have access to the proper subnets, VLANs, and so on.

    Dedicating ports for replication in one cluster does not require dedicating ports in all clusters; one cluster might use dedicated ports, while the other cluster shares data ports for intercluster replication.

Adding an ONTAP license

A license is a record of one or more software entitlements. 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.

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.

Step

1. Add a license:

   ```
   system license add -license-code code
   ```

Related information

ONTAP 9 System Administration Reference

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.

About this task

Installing SnapCenter for Data Fabric Solution for Cloud Backup involves the following tasks:

- Ensuring that the Linux server is available and accessible to the SnapCenter Server host for the NAS file services catalog
- Adding sudo permissions for Linux
- Installing the SnapCenter Server

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 indexed file catalog is available and will be accessible to the SnapCenter Server.

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. Determine whether the Linux server is accessible. Choose one of the following methods:

   ```
   ping <hostname@domainname>
   ```

   ```
   ping <xxx.xxx.xxx.xxx>
   ```

3. Use a utility such as PuTTY to determine whether you can connect as the same user that SnapCenter will use to communicate with the catalog.

Configuring sudo privileges for non-root user

SnapCenter 2.0 enables a non-root user to install the Plug-in for Oracle Database and start the plug-in process. However, you must configure sudo privileges for the non-root user to provide access to several paths. You can configure sudo privileges for the non-root user also if you deploy SnapCenter in the Data Fabric Solution for Cloud Backup, since the file catalog uses a Linux server.

About this task

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`
- `/opt/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/opt/NetApp/snapcenter/spl/bin/spl`

Steps

1. Create a key by running the following command:

   ```
   dgst -binary -sha224 /tmp/sc-plugin-installer/
   snapcenter_linux_host_plugin.bin | openssl base64
   ```

2. Open the `/etc/sudoers` file by running the `visudo` command.

   You must use Sudo 1.8.7 or later.

3. Edit the file to include the non-root user name:

   a. `Cmnd_Alias` SCCMD = sha224:*`generated_key`* `/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin` , `/opt/NetApp/snapcenter/spl/installation/plugins/uninstall`, `/opt/NetApp/snapcenter/spl/bin/spl`

   b. Defaults:*`username/groupname`* !requiretty

   c. *`username/groupname`* ALL=(ALL) NOPASSWD:SETENV: SCCMD

   #### Example

   For example, if the non-root user name is ‘oracle’, modify the lines as:

   - Defaults:oracle !requiretty
   - oracle ALL=(ALL) NOPASSWD:SETENV: SCCMD

   While creating Run As credentials for a non-root user, you must select the **Use sudo privileges** checkbox.

   Note: The **Use sudo privileges** checkbox is selected by default for non-root users.

Installing the SnapCenter Server for Data Fabric Solution for Cloud Backup

After you have completed the installation prerequisites, you can use the InstallShield wizard to install the SnapCenter Server.

Before you begin

- 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.
  https://support.microsoft.com/en-us/kb/223300
- Your system must meet the 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.
     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.

4. If you use the wizard, complete the following steps:

   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 more file catalog servers.

      File catalog servers can be configured only during SnapCenter installation.

   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 OS username and password.

Related information

SnapCenter Software 2.0 Installation and Setup Guide

Installing AltaVault

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.
3. Configure AltaVault, including the following options:
   - Cloud providers
   - AltaVault system settings
   - AltaVault interfaces
   - AltaVault licenses
   - AltaVault encryption key

   See the *AltaVault Cloud Integrated Storage Administration Guide* on the NetApp Support Site at *mysupport.netapp.com*.

Related information

NetApp Documentation: AltaVault
NetApp Interoperability Matrix Tool

Configuring AltaVault for Data Fabric Solution for Cloud Backup

Using the Data Fabric Solution for Cloud Backup requires configuring AltaVault. 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:

Tasks	Using SnapCenter in deployment	Not using SnapCenter in deployment
Enable SnapMirror service in AltaVault	Yes	Yes
Add approved intercluster LIFs to an IP whitelist in AltaVault	No	Yes
Optionally, enable SnapMirror long-term retention mode in AltaVault	Yes	Yes
Enable SnapCenter access to AltaVault	Yes	No
Add a role-based user in AltaVault to enable SnapCenter storage connection to an AltaVault appliance	Yes	No
Start the AltaVault Storage Optimization Service	Yes	Yes

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 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.

Enabling the SnapMirror service and 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

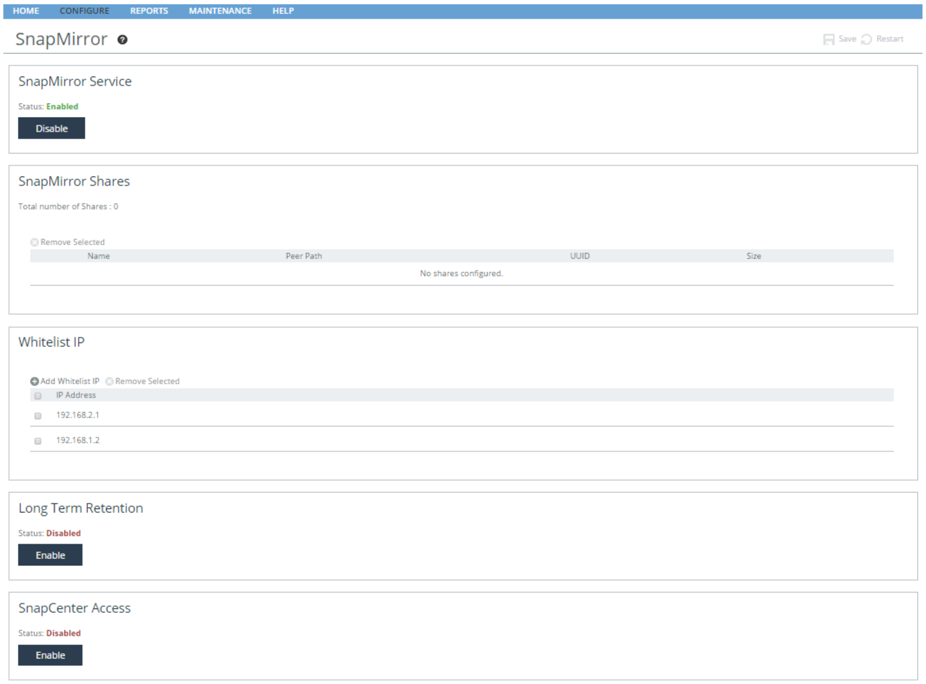
When the SnapMirror service is enabled, the shares and Snapshot copies that exist on AltaVault are accessible and can be restored. If the SnapMirror service is disabled, the shares and Snapshot copies that exist on AltaVault are not deleted; however, Snapshot copies are not accessible.

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**.



SnapMirror

SnapMirror Service

Status: Enabled

SnapMirror Shares

Total number of Shares : 0

Name	Peer Path	UUID	Size
No shares configured.			

Whitelist IP

□	IP Address
□	192.168.2.1
□	192.168.1.2

Long Term Retention

Status: Disabled

SnapCenter Access

Status: Disabled

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.

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.

7. If you are using SnapCenter to initiate and manage data protection operations, under SnapCenter Access, click **Enable**.

   This enables communication between AltaVault and SnapCenter.

8. If the Service restart required prompt appears, click **Restart** in the upper right of the console.

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 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. In this mode, AltaVault continues to store Snapshot copies until it reaches the maximum. If a share exceeds 3700 Snapshot copies, AltaVault begins deleting the oldest Snapshot copies to make room for newer ones.
  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, which supports a maximum of 251 Snapshot copies per share. 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**.

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

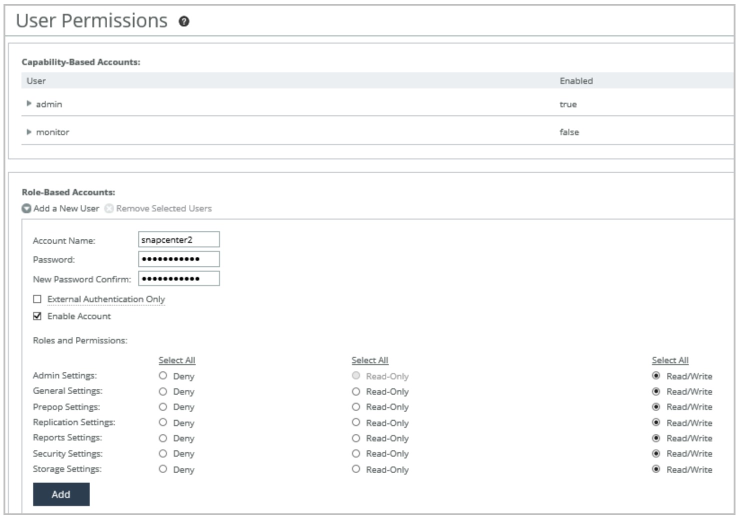
To perform data protection operations using the Data Fabric Solution for Cloud Backup, you must add a SnapCenter role-based account to AltaVault. You will later add a storage connection in SnapCenter and will need this account's credential information.

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**.



User Permissions

Capability-Based Accounts:

User	Enabled
▸ admin	true
▸ monitor	false

Role-Based Accounts:

Add a New User   Remove Selected Users

Account Name: snapcenter2

Password: ••••••••••••

New Password Confirm: ••••••••••••

☐ External Authentication Only

☑ Enable Account

Roles and Permissions:

	Select All	Select All	Select All
Admin Settings:	○ Deny	○ Read-Only	● Read/Write
General Settings:	○ Deny	○ Read-Only	● Read/Write
Prepop Settings:	○ Deny	○ Read-Only	● Read/Write
Replication Settings:	○ Deny	○ Read-Only	● Read/Write
Reports Settings:	○ Deny	○ Read-Only	● Read/Write
Security Settings:	○ Deny	○ Read-Only	● Read/Write
Storage Settings:	○ Deny	○ Read-Only	● Read/Write

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. 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 SnapMirror and enabling SnapCenter access using the AltaVault CLI

In addition to using a graphical user interface, you can use the AltaVault command-line interface (CLI) for configuring SnapMirror. SnapMirror configuration includes enabling the SnapMirror service, restarting the Storage Optimization Service, configuring a whitelist of approved IP addresses from which AltaVault accepts SnapMirror connections, enabling SnapMirror long-term retention mode, and enabling SnapCenter access.

About this task

If you already configured SnapMirror using the AltaVault graphical user interface, you do not need to perform this procedure.

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

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

2. Enable SnapMirror service:

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

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

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

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

4. Verify that the SnapMirror service is ready:

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

5. If you are not using SnapCenter to manage NAS file services data protection, configure the list 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>
   ```

6. 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.

7. 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 archival
      SnapMirror Archival mode: disabled
   <hostname> (config)# snapmirror archival enable
   ```

   To disable long-term retention mode, enter the `no snapmirror archival` command.

8. Enable SnapCenter access to AltaVault:

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

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

9. 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).

10. 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
<hostname> (config # rbm user <username>
   role cb_replication_settings permission read-write
<hostname> (config # rbm user <username>
   role cb_storage_settings permission read-write
```

c. 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
```

11. Restart the Storage Optimization Service:

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

12. 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

Using the Data Fabric Solution for Cloud Backup requires configuring SnapCenter.

About this task

To configure SnapCenter for Data Fabric Solution for Cloud Backup, you should complete the following:

- Configure the predefined SnapCenter Infrastructure Admin role for AltaVault access and setting up role-based access control
- Configure a storage connection to an AltaVault appliance
- Configure a storage connection to an ONTAP cluster
- For CIFS shares only (not for NFS), create a Run As account
- For CIFS shares only (not for NFS), configure CIFS server credentials
- Protect the SnapCenter file catalog and SnapCenter repository

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

The SnapCenter graphical user interface (GUI) URL is configured based on information that you provide during installation. It is useful to know where to find it after you complete the SnapCenter installation.

During the installation, the SnapCenter Server Install wizard creates a shortcut and places it on your local host desktop. Additionally, at the end of the installation, the Install wizard provides the SnapCenter URL, 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. Saving your password creates a high security risk.

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:

- PowerShell cmdlets for Microsoft SQL databases and Windows file systems

You can use PowerShell cmdlets on SQL databases to script configuration, backup, restore, verification, and clone operations. You can use PowerShell cmdlets on Windows file systems to script backup, restore, and clone operations.

- SnapCenter command-line interface (CLI), *sccli* for Oracle databases on Linux machines.

  You can use the CLI to script configuration, backup, catalog, uncatalog, restore, verification, mount, unmount, and clone operations.

Note: Some cmdlets have changed in SnapCenter 2.0. If you use cmdlets in 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. Choose which user you want to log in as:

If you want to ...	Do the following …
Log in as the SnapCenter administrator	Enter the domain user with local administrator credentials provided during the SnapCenter installation.
Log in as a SnapCenter user	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 complete a two-step process: you add users or groups to a role and then add assets to that user. The first step of adding users or groups to a role determines the options that SnapCenter users can access.

Before you begin

You must have logged in as 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, 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**.

After you finish

To continue with role-based access control, assign assets to users next.

Assigning users access to assets

Setting up role-based access control (RBAC) for users is a two-step process. After you add a user or group to a role that contains the appropriate permissions, you must assign the user access to SnapCenter assets, such as hosts and storage connections. This enables users to perform the actions for which they have permissions on the assets that are assigned to them.

About this task

You can assign access to users even if the user is not part of a role. This helps you add users; however, you must add the user to a role at some point to take advantage of role-based access control efficiencies.

You can also assign Run As credential maintenance to a user.

If you are planning to replicate Snapshot copies to a mirror or vault, you must assign the storage connection for both the source and destination volume to the user performing the operation.

You should add assets before assigning access to the users.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **SnapCenter Assets**.
3. In the **My SnapCenter Assets** page, select the type of asset you want to assign from the **SnapCenter Asset Type** drop-down list.
4. In the **SnapCenter Asset Name** table, highlight the asset you want to assign and click **Assign**.
5. Provide the domain name to which the asset belongs.
6. Choose whether you want to assign access to a user or a group.
7. Enter the user or group name and click **Add**.

   If you are not sure about the name, use a more advanced search by clicking the **Search users or group** heading, typing a partial name, and clicking **Search**.
8. Repeat this procedure until each user or group has all the required assets.
9. Click **OK** to save your changes.

Setting up storage system connections

Before you can perform backup, restore, clone, and provisioning operations with SnapCenter, you must set up the storage system connections that give SnapCenter access to ONTAP storage. If you are configuring connections for the Data Fabric Solution for Cloud Backup, you must create connections to each AltaVault system and one to an ONTAP Cluster.

Before you begin

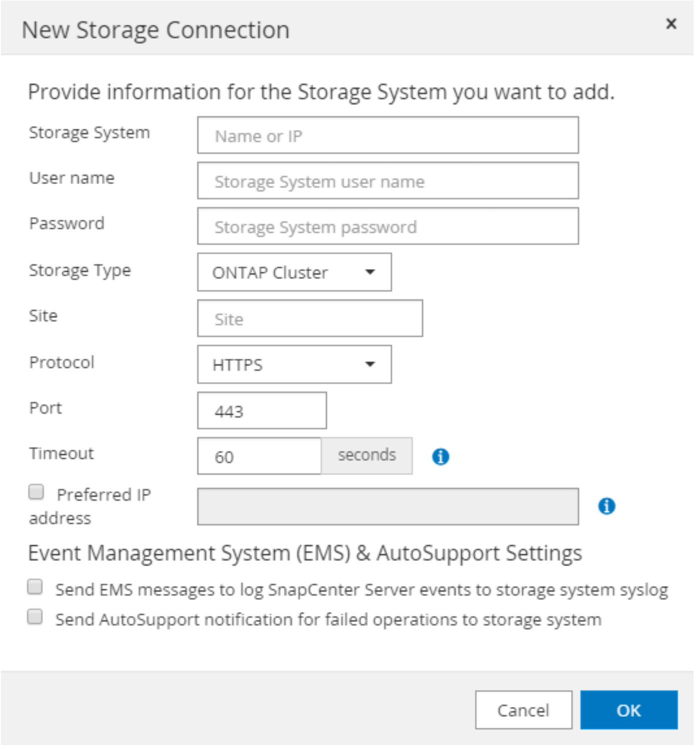
You must have permissions in the Infrastructure Admin role to create storage connections.

About this task

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

Steps

1. In the left navigation pane, click **Storage Systems**.
2. In the **Storage Systems** page, click **New**.



New Storage Connection ×

Provide information for the Storage System you want to add.

Storage System	Name or IP
User name	Storage System user name
Password	Storage System password
Storage Type	ONTAP Cluster ▾
Site	Site
Protocol	HTTPS ▾
Port	443
Timeout	60 seconds ⓘ
□ Preferred IP address	ⓘ

Event Management System (EMS) & AutoSupport Settings

□ Send EMS messages to log SnapCenter Server events to storage system syslog

□ Send AutoSupport notification for failed operations to storage system

3. In the **New Storage Connection** wizard, provide the following information:

For this field…	Do this…
Storage System	Enter the storage system name or IP address. **Note:** 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 `Add-SmStorageConnection` 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.
User name/Password	Do one of the following: • ONTAP: Enter the credentials used (usually VSAdmin) to access the storage system. • AltaVault: Enter the role-based access control credentials you entered in AltaVault.
Storage Type	Select ONTAP SVM, ONTAP Cluster, or AltaVault. If you are configuring connections for SnapCenter application plug-ins, choose ONTAP SVM as the storage type. If you are configuring connections for the Data Fabric Solution for Cloud Backup, you must add connections to each AltaVault system and to an ONTAP Cluster. For each AltaVault system, choose AltaVault as the storage type, and choose ONTAP Cluster as the second storage type. **Note:** 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 **Modify Storage Connection** wizard on the ONTAP Cluster that you already added to ensure the following updates are made: • The SVM is in the NSM database • CIFS server discovery is enabled on the SVM • The SnapCenter cache is updated with information about the new SVM
Site	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.
Protocol	Select the protocol used for connection to the SVM that was configured during SVM setup, typically HTTPS.
Port	Enter the port that the storage system accepts. The defaults typically work. If you are configuring the AltaVault connection, enter the AltaVault port.

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.

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

4. 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

5. 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.

6. Click **OK**.

Setting up your Run As credentials

SnapCenter uses Run As credentials to authenticate users for SnapCenter operations. You should create Run As credentials for installing SnapCenter plug-ins and additional Run As credentials for performing data protection operations on databases or Windows file systems.

About this task

- Linux hosts
  You must set up Run As credentials for scheduling on Linux hosts.
  Although you are allowed to create Run As credentials for Linux after deploying hosts and installing plug-ins, the best practice is to create Run As credentials after you add SVMs, before you deploy hosts and install plug-ins. You must set up the Run As credentials for the root user or a non root user who has sudo privileges to install and start the plug-in process.

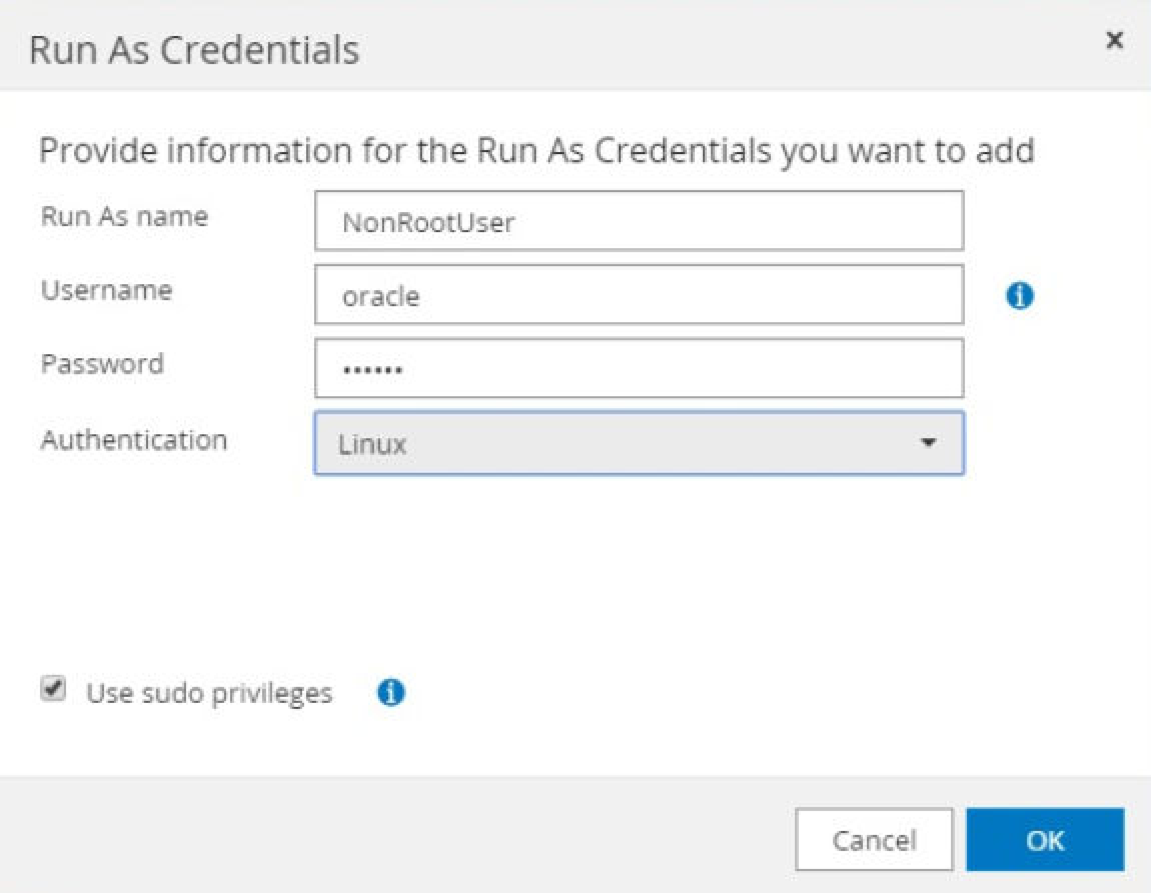
- Windows hosts
  You must set up Windows Run As credentials before installing plug-ins.
  Set up the Run As credentials with administrator privileges, including administrator rights on the remote host.

- SQL authentication on Windows hosts
  You must set up SQL Run As credentials after installing plug-ins.
  If you are deploying SnapCenter Plug-in for Microsoft SQL Server, you must set up SQL Run As credentials after installing plug-ins. Set up a Run As credential for a user with SQL Server sysadmin permissions.
  The SQL authentication method authenticates against a SQL Server instance. This means that a SQL Server instance must be discovered in SnapCenter. Therefore, before adding a SQL Run As credential, you must add a host, install plug-in packages, and refresh resources. You need SQL Server authentication for performing operations such as scheduling or discovering resources.

- Custom Plug-ins applications
  The plug-in uses the Run As credentials selected or created when adding a resource. If a resource does not require a Run As credentials during data protection operations, you can set the Run As credentials as **None**.
- For Data Fabric Solution for Cloud Backup for CIFS shares only (not for NFS), you must create Run As credentials and configure a CIFS server for the ONTAP cluster.

Steps

1. In the left navigation pane, click **Settings**.
2. In the **Settings** page, click **Run As Credentials**.
3. Click **New**.



Run As Credentials

Provide information for the Run As Credentials you want to add

Run As name: NonRootUser

Username: oracle

Password: ••••••

Authentication: Linux

☑ Use sudo privileges

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

For this field…	Do this…
Run As name	Enter a name for the Run As credentials.
User name/Password	Enter the user name and password used for authentication. You must add the domain name as the prefix to the username.

For this field…	Do this…
Authentication Mode	Select the authentication mode that you want to use. If you select the SQL authentication mode, you must also specify the SQL server instance and the host where the SQL instance is located. For Data Fabric Solution for Cloud Backup for CIFS shares only, select Windows as the mode.
Use sudo privileges	Applicable to Linux users only. Select the **Use sudo privileges** check box if you are creating run as credentials for a non-root user.

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 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, 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

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

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, open a PowerShell session window and verify that the proper modules are loaded by using the `get-module` cmdlet.

   If you execute the cmdlet on the SnapCenter server, only the SnapCenter module is displayed. The cmdlets that have “Sd” in the suffix, which are the cmdlets that reside in the SnapDrive module, are available only on the application host.

   #### Example

   ```
   PS C:\> get-module

   ModuleType Version  Name                   ExportedCommands
   ---------- -------  ----                   ----------------
   Manifest   3.1.0.0  Microsoft.PowerShell   {Add-Computer,
                       .Management            Add-Content,
                                              Checkpoint-Computer,
                                              Clear-Con...}

   Manifest   3.1.0.0  Microsoft.PowerShell   {Add-Member, Add-Type,
                       .Utility               Clear-Variable,
                                              Compare-Object...}

   Manifest   1.0      SnapCenter             {Add-SmResourceGroup,

                                              Add-SmGroupToRol...

   Manifest   1.0.0    SnapDrive              {Add-SdIgroupInitiator,
                                              Add-SdLunMap,
                                              Add-SdPortSetPort, C...
   ```

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,
                                   Connect-SdIscsi...
```

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
```

3. Protect the file catalog by using the `Protect-SmRepository` command:

```
Protect-SmRepository [-HostName] string[-Path] Hashtable [-
InstanceCredential][[-SQLServerAuthenticationMode]SQLServerAuthMode][[-
RetentionCount] Int32] CommonParameters [-CatalogBackupPath] string
```

```
Protect-SmRepository [-HostName] string[-Path] Hashtable [[-
RetentionCount] Int32] CommonParameters [-CatalogBackupPath] string
```

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:

   Protect-SmRepository [-HostName] ***string*****[-Path]** ***Hashtable*** **[[-RetentionCount]** ***Int32*****]** ***CommonParameters*** **[-CatalogBackupPath]** ***string***

Example

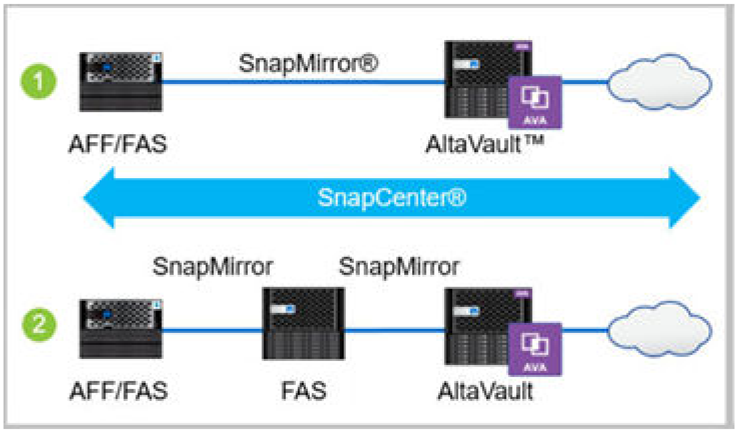
```
Protect-SmRepository -HostName NB-MVA-
DEV057.nbsdsm.mycompany.netapp.in
-Path E:\DBs  -InstanceCredential sa -SQLServerAuthenticationMode SQL
-Schedule @{"ScheduleType"="hourly";"StartTime"="10/21/2016 5:18 PM"}
```

Backing up NAS file services to the cloud and restoring them with SnapCenter management

You can back up NAS file services to the cloud and restore them from the cloud using SnapCenter and AltaVault. You can perform a baseline backup from SnapCenter. Subsequently, all backups of that volume from SnapCenter are incremental backups and are initiated by the policy-driven schedule.

About this task

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 and SnapCenter 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.

Note: With the ONTAP CLI, you can perform a full volume restore or a single file restore.

As a best practice, we recommend that you initiate no more than 10 concurrent restore operations. Otherwise, transfer time outs and slower restore throughput may occur. 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.

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

Using policies to govern backing up NAS file services

A backup policy is a set of rules that governs how you manage and retain backups, and how frequently the resource or resource group is backed up. Additionally, you can specify replication and script settings. Specifying options in a policy saves time when you want to reuse the policy for another resource group. To use a predefined policies, you must first copy and modify it to meet your needs before you can use it to govern data protection.

About this task

SnapCenter includes the following predefined policies that govern the backup 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.

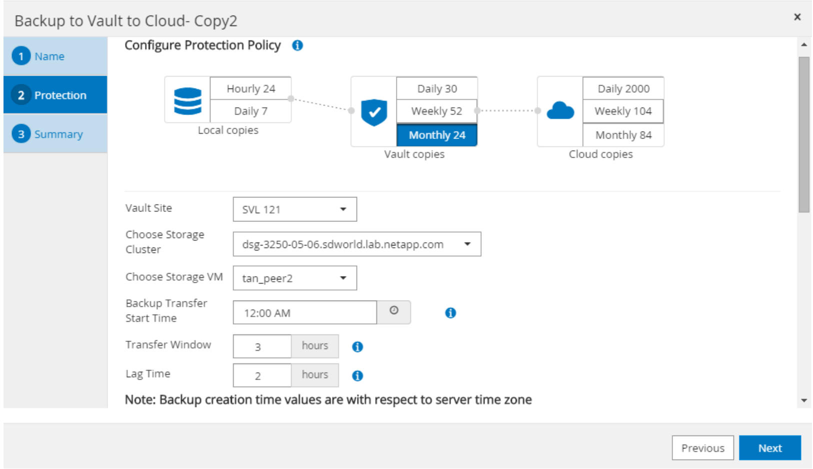
To back up NAS file services, you must first copy and modify predefined policies to suit your needs.

> **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 setting up 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 the predefined policy and click **Details**.
4. Click the policy, click **Copy**, and enter a new policy name.
5. Click the copy and click **Modify**.
6. In the **Policy** wizard, enter the new policy name, which must be unique, and an optional description and click **Next**.


Backup to Vault to Cloud- Copy2

Configure Protection Policy

Hourly 24
Daily 7
Local copies

Daily 30
Weekly 52
Monthly 24
Vault copies

Daily 2000
Weekly 104
Monthly 84
Cloud copies

Vault Site: SVL 121
Choose Storage Cluster: dsg-3250-05-06.sdworld.lab.netapp.com
Choose Storage VM: tan_peer2
Backup Transfer Start Time: 12:00 AM
Transfer Window: 3 hours
Lag Time: 2 hours

Note: Backup creation time values are with respect to server time zone

7. In the **Protection** page, click on one of the protection boxes at the top to configure the policy.

Option	Description
Site or Vault Site	Enter the data center site name.
Cloud Bucket	Applicable only if you select the cloud copy. Enter the name of the bucket associated with the cloud provider.

Option	Description
Choose Storage Cluster	Applicable only if you select the vault copy. Select the ONTAP Cluster as the backup destination.
Choose Storage VM	Applicable only if you select the vault copy. Select the Storage Virtual Machine (SVM) as the backup destination.
Backup Transfer Start Time	Enter the time when the initial baseline backup should begin. This is based on the ONTAP source storage time zone.
Transfer Window	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.
Lag Time	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.
Daily, Weekly, Monthly options	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.

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. Enter any script information that should be applied either before or after the backup and click Next.
9. Review the summary and click **Finish**.

Backing up NAS file services to the cloud

Backing up NAS file data to the cloud includes several short tasks.

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 to the cloud using SnapCenter and AltaVault

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

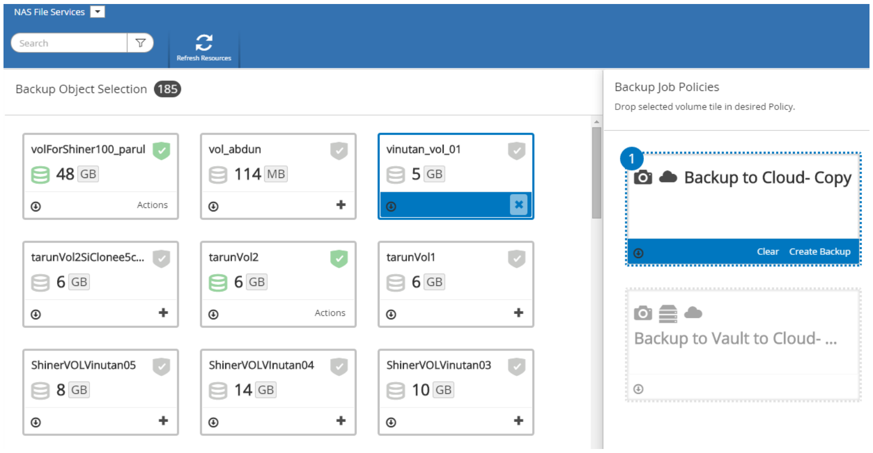
About this task

When you apply a policy to a volume, you can indicate when the initial baseline backup should be performed (either immediately or at a time you specify). 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.

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, drag the volume to the policy box on the right.
7. To view details of the policy and optionally change them, 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.

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

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 a backup in SnapCenter, you can immediately review the progress of the data transfer from SnapCenter 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:

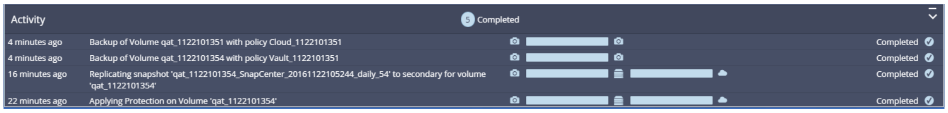
- Backup operations to AltaVault

  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 a backup or restore operation in SnapCenter, review the SnapCenter Activity pane on the bottom of the page.



Activity 5 Completed

4 minutes ago	Backup of Volume qat_1122101351 with policy Cloud_1122101351	Completed
4 minutes ago	Backup of Volume qat_1122101354 with policy Vault_1122101351	Completed
16 minutes ago	Replicating snapshot 'qat_1122101354_SnapCenter_20161122105244_daily_54' to secondary for volume 'qat_1122101354'	Completed
22 minutes ago	Applying Protection on Volume 'qat_1122101354'	Completed

The Activity pane shows the following information:

Item	Description
Active, Failed, Completed information in the top bar	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.
1st column: <number of minutes>	Displays when the activity began.
2nd column: <status>	Displays the activity, such as applying protection on volume, replicating Snapshot, or restoring data.
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.

Item	Description
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 SnapCenter backup 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

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, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. 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. In the **Job Details** page, click **View logs**.

Verifying backup to the cloud completion on AltaVault

A SnapMirror share is created automatically when the SnapMirror relationship with the AltaVault is created in ONTAP. Based on SnapMirror policies created in ONTAP or SnapCenter, Snapshot copies of ONTAP volumes are backed up to the associated AltaVault share. You should 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 commands or SnapCenter.

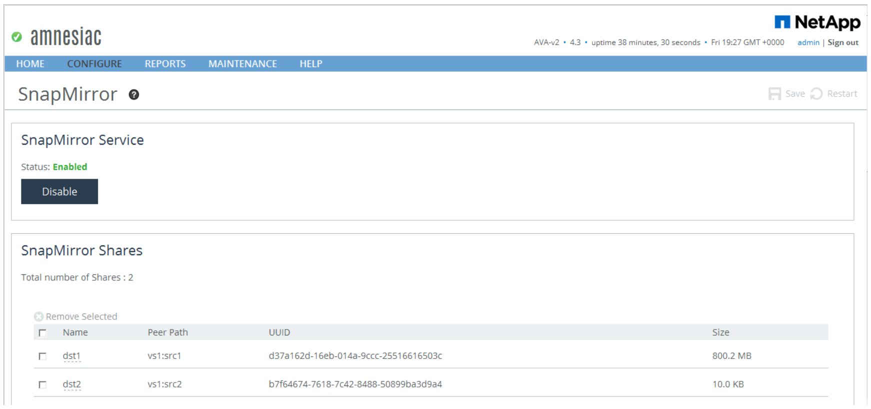
During the lifetime of a share, there is only one baseline Snapshot copy. Any Snapshot copy after the baseline is always incremental. Baseline transfer can take a long time to complete depending on the size of the Snapshot copy.

During incremental 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 explicitly running the ONTAP `snapmirror update` command.

AltaVault provides global deduplication on 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.



SnapMirror Service

Status: Enabled

SnapMirror Shares

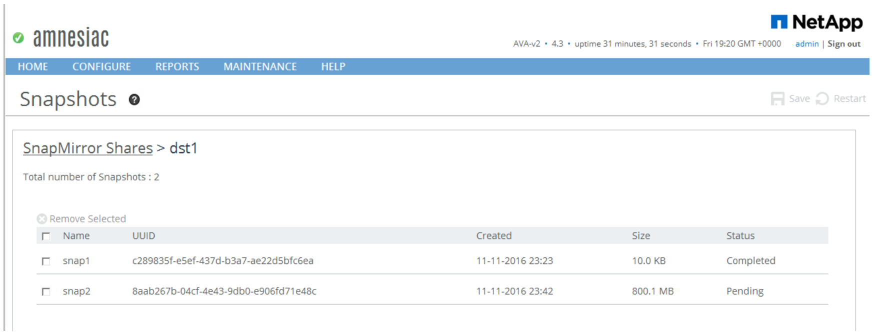
Total number of Shares : 2

	Name	Peer Path	UUID	Size
□	dst1	vs1:src1	d37a162d-16eb-014a-9ccc-25516616503c	800.2 MB
□	dst2	vs1:src2	b7f64674-7618-7c42-8488-50899ba3d9a4	10.0 KB

Field	Description
<Share> Name	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.
Peer Path	Identifies the path to the vServer and source volume in ONTAP (vServer:ONTAP volume) that is being backed up in AltaVault.
UUID	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.

Field	Description
Size	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 capacity. The size of source volume, change rate, and number of Snapshot copies impact the number and size of SnapMirror shares on AltaVault.

4. Optionally, select a share and view the Snapshot copy information.



SnapMirror Shares > dst1

Total number of Snapshots : 2

Remove Selected

□	Name	UUID	Created	Size	Status
□	snap1	c289835f-e5ef-437d-b3a7-ae22d5bfc6ea	11-11-2016 23:23	10.0 KB	Completed
□	snap2	8aab267b-04cf-4e43-9db0-e906fd71e48c	11-11-2016 23:42	800.1 MB	Pending

Field	Description
<Snapshot copy> Name	Lists the name 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.
UUID	Specifies the unique identifier associated each Snapshot copy. The UUID value is generated by ONTAP.
Created	Indicates the date and time when the Snapshot copy was created in ONTAP.
Size	Specifies the size of the Snapshot copy.
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. 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

Based on SnapMirror policies created in ONTAP or SnapCenter, Snapshot copies of ONTAP volumes are backed up to the associated AltaVault share. 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-6de5dbbdac92
         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-4aee-a8fa-c75230a57ddb   11-11-2016 13:11   10.0 KB             Pending
```

Restoring NAS file data from the cloud

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

About this task

- Restore files from the cloud using SnapCenter and AltaVault
- Monitor data protection progress in the SnapCenter backup Activity pane

- Monitor restore operations progress in the SnapCenter Jobs page

As a best practice, we recommend that you initiate no more than 10 concurrent restore operations. Otherwise, transfer time outs and slower restore throughput may occur. 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.

Searching in the file catalog for a specific file to restore using keywords and filters

Using the powerful SnapCenter file catalog, you can search for a specific file to restore 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 restoring 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:

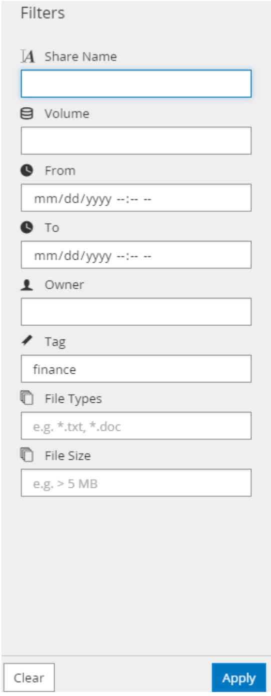
  ```
  "licensing SnapMirror"~10
  ```

- 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.



Tag: finance

4. Click **Apply**.

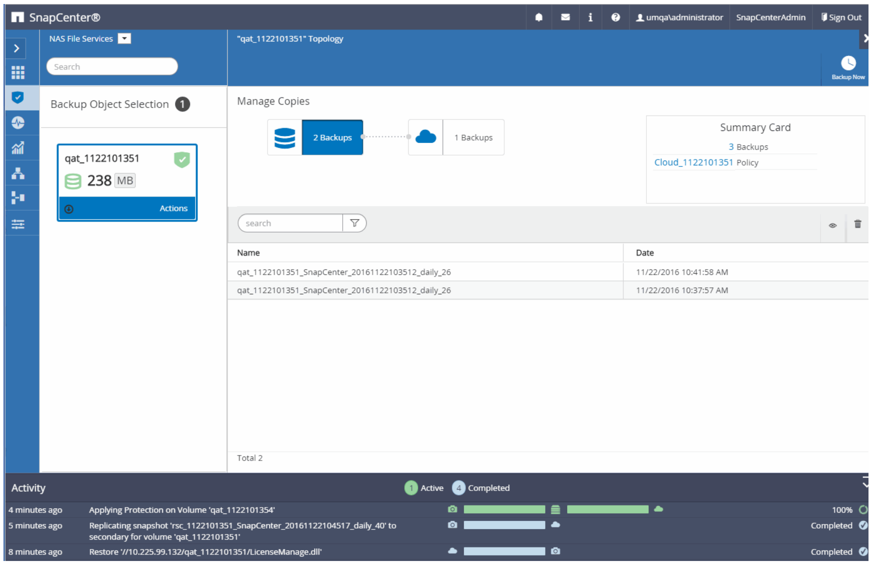
5. From the list of filtered results, click on the file you want to restore.

Restoring NAS file data from the cloud using SnapCenter and AltaVault

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

Steps

1. In the left navigation pane, 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**.



Name	Date
qat_1122101351_SnapCenter_20161122103512_daily_26	11/22/2016 10:41:58 AM
qat_1122101351_SnapCenter_20161122103512_daily_26	11/22/2016 10:37:57 AM

Total 2

```
4 minutes ago   Applying Protection on Volume 'qat_1122101354'                                        100%
5 minutes ago   Replicating snapshot 'rsc_1122101351_SnapCenter_20161122104517_daily_40' to           Completed
                secondary for volume 'qat_1122101351'
8 minutes ago   Restore '//10.225.99.132/qat_1122101351/LicenseManage.dll'                             Completed
```

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 57
Monitoring data protection progress in the SnapCenter Activity pane on page 49

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, click **Monitor**.
2. In the **Monitor** page, click **Jobs**.
3. 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. In the **Job Details** page, click **View logs**.

Managing SnapMirror shares using the AltaVault CLI

Rather than use the AltaVault graphical user interface, you can use the AltaVault command-line interface (CLI) for managing SnapMirror shares.

About this task

If you use the AltaVault graphical user interface, you do not need to perform this procedure.

SnapMirror shares are created automatically after a SnapMirror relationship to the AltaVault is created either in ONTAP or in SnapCenter.

Steps

1. Use SSH to log in to the AltaVault CLI:

   ```
   <hostname> > enable
   ```

2. Display the list of shares created on the AltaVault:

   ```
   <hostname> (config) # show snapmirror shares
   ```

   To delete a share from the AltaVault, use the `snapmirror share delete sharename <share-name>` command.

3. Display the list of all Snapshot copies for a share:

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

   AltaVault displays the Snapshot copy name, UUID, size, and replication status to the cloud. Replication status can be Completed or Pending.

   To delete a Snapshot copy from a share, use the `snapmirror snapshots delete share-name <share-name> snapshot-name name <snapshot name>` command

Backing up NAS file services to the cloud and restoring them using ONTAP commands

Using the ONTAP command-line interface (CLI), you can back up NAS file services to the cloud and restore them from the cloud back to an ONTAP volume.

About this task

Instead of using ONTAP commands, you can initiate backups using the SnapCenter graphical user interface (GUI). See information about backing up NAS file services using SnapCenter.

One 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.

Backing up NAS file services to the cloud using ONTAP commands

Backing up NAS file services to the cloud using ONTAP command-line interface (CLI) involves performing a baseline backup first followed by incremental backups. ONTAP FlexVols are backed up to AltaVault as NAS file shares on volumes.

Related tasks

Backing up NAS file services to the cloud and restoring them with SnapCenter management on page 45

Performing a baseline backup from ONTAP to the cloud using the ONTAP CLI

When you perform a baseline backup, you review the volume's contents, create a SnapMirror relationship, create a Snapshot copy, initialize the SnapMirror relationship, transfer the data to AltaVault, and finally show the transfer of the contents in AltaVault.

About this task

A baseline backup creates a SnapMirror relationship with an AltaVault endpoint.

Steps

1. Log in to the ONTAP CLI.
2. Look at the contents of the primary volume:

Example

```
cluster1::> volume show
Vserver Volume       Aggregate State  Type    Size  Available Used%
------- ------------ --------- ------ ---- ------- ---------- -----
                                vol0         aggr0     online RW    2.85GB   690.4MB   76%
vs2     ontap_source aggr1     online RW       1GB   966.4MB    5%
vs2     vs_root1     aggr1     online RW      20MB   18.01MB    9%
3 entries were displayed.
```

3. Look at the files on the volume:

Example

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

4. Create a SnapMirror relationship, which creates the share on AltaVault:

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`*`>`

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

```
cluster1::> snapmirror create
  -source-path <Vserver><volume>:
  -destination-path <IP_address>:/share/<share_name> -type XDP
```

Example

```
cluster1::> snapmirror create
  -source-path vs2:ontap_source
  -destination-path 192.0.2.150:/share/ava_dest_1 -type XDP
```

5. Verify that the SnapMirror relationship is established and is in the `Unitialized` state:

To view the detailed status of the relationship, use the `-instance` option.

Example

```
cluster1::> destination_cluster::>snapmirror show
                                                                    Progress
Source      Destination Mirror        Relationship Total            Last
Path   Type Path        State         Status       Progress Healthy Updated
------ ---  ----------- -------       ------------ -------- ------- --------
vs34:src    XDP  192.0.2.22:/share/dst Uninitialized Idle -  true    -
1 entries were displayed.

destination_cluster::> snapmirror show -instance

                       Source Path: vs34:src
                       Destination Path: 172.19.201.22:/share/dst
                      Relationship Type: XDP
                Relationship Group Type: none
                    SnapMirror Schedule: -
                 SnapMirror Policy Type: vault
                      SnapMirror Policy: XDPDefault
```

6. Create a Snapshot copy:

Example

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

7. Initialize the SnapMirror relationship and transfer the data to AltaVault:

```
cluster1::> snapmirror initialize
  -source-path <Vserver>:<volume_name>
  -destination-path <IP_address>:/share/<share_name>
  -source-snapshot <Snapshot_name>
```

Example

```
cluster1::> snapmirror initialize -s
  -source-path vs2:ontap_source
  -destination-path 192.0.2.150:/share/ava_dest1
  -source-snapshot base_snapshot
```

If you use `Snapmirror initialize` without the `–s` (explicit snapshot), the Snapshot copy is deleted in the next update.

You can initialize the relationship only once during the lifetime of the relationship.

8. Show the transfer of the contents:

Example

```
cluster1::> snapmirror show
                                                              Progress
Source      Destination Mirror Relationship Total             Last
Path   Type Path        State  Status       Progress  Healthy Updated
------ ---- ----------- ------ ------------ --------  ------- --------
vs34:src    XDP  192.0.2.150:/share/dst Snapmirrored Idle -  true
-
```

The `Idle` state indicates the transfer is complete.

9. Show the transfer of the contents:

Example

```
cluster1::> snapshot show ontap_source
                                                 ---Blocks---
Vserver    Volume  Snapshot                Size   Total% Used%
--------   ------- -------------           -----  -----  -----
vs2        ontap_source
                                     base_snapshot           108KB   0%      2%
                   incremental_snapshot     92KB   0%     1%
                   hourly.2016-10-22_0905  252KB   0%     4%
                   hourly.2016-10-22_1005   92KB   0%     1%
                   hourly.2016-10-22_1105  100KB   0%     2%
```

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

Example

```
onk-sm# show snapmirror shares

onk-sm# show snapmirror snapshots share-name ava_dest_1
Name:
UUID               Create Time:       Replication Status
base_snapshot
   8477ad3d-95bb-4398-9da8-358b5d79cf45
                   10-22-2016 15:46   Completed
Total Snapshots - 1
```

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

After you finish

Perform an incremental backup from ONTAP to AltaVault.

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

After completing a baseline backup, you should perform incremental backups that capture additional Snapshot copy data since the baseline backup occurred.

Before you begin

You must have already completed 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 SnapMirror relationship, create a Snapshot copy, update the SnapMirror relationship, 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 another Snapshot copy:

Example

```
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. Create an incremental backup:

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.

4. Show the transfer of the contents:

Example

```
cluster1::> snapmirror show
                                                             Progress
Source      Destination Mirror Relationship Total            Last
Path   Type Path        State  Status       Progress Healthy Updated
------ ---- ----------- ------ ------------ -------- ------- --------
vs2:ontap_source
       XDP  192.0.2.150:/share/ava_dest_1
                     snapmirrored  Transferring 0B     true    10/22
11:28:00
```

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

5. Show the transfer of the contents:

Example

```
cluster1::> snapmirror show
                                                              Progress
Source      Destination Mirror Relationship Total             Last
Path   Type Path        State  Status       Progress  Healthy Updated
------ ---- ----------- ------ ------------ --------  ------- --------
vs2:ontap_source    XDP  192.0.2.150:/share/dst Snapmirrored Idle -  true
-
```

6. 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
Name:
UUID                   Create Time:       Replication Status
base_snapshot
   8477ad3d-95bb-4398-9da8-358b5d79cf45
                       10-22-2016 15:46   Completed
incremental_snapshot
   41a9268a-67c9-40bb-8c2c-76c5c02fc597
                       10-22-2016 15:58   Completed
Total Snapshots - 2
```

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

After you finish

Using AltaVault, configure the cloud provider settings. After these are set up, the backup of data that was transferred to AltaVault is automatically replicated to the cloud. See AltaVault documentation.

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:

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

Example

```
cluster1::*> snapmirror show
                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
vs34:src    XDP  192.0.2.22:/share/dst Uninitialized Transferring 12.86MB true 10/24
12:33:35

cluster1::*> snapmirror show -instance 192.0.2.22:/share/dst

                                 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:

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

   Example

   ```
   cluster1::> snapmirror show
                                                                           Progress
   Source            Destination Mirror  Relationship   Total              Last
   Path        Type  Path        State   Status         Progress  Healthy Updated
   ----------- ---- ------------ ------- -------------- --------- ------- --------
   vs34:src    XDP  192.0.2.22:/share/dst Snapmirrored Idle -  true    -
   ```

Restoring NAS file services from the cloud using ONTAP commands

You can restore a full backup from the cloud to ONTAP or you can restore a single file from a Snapshot copy in AltaVault 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

As a best practice, we recommend that you initiate no more than 10 concurrent restore operations. Otherwise, transfer time outs and slower restore throughput may occur. 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.

Restoring a full backup from the cloud using the ONTAP CLI

Restoring a full baseline backup from the cloud to ONTAP includes creating a new destination volume in ONTAP into which you will restore the shares, restoring AltaVault 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:

   ```
   <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 single file restore, the destination volume must be read/write. For a full volume restore, 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:

   #### 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
                                                                  Progress
Source       Destination  Mirror    Relationship Total            Last
Path    Type Path         State     Status       Progress Healthy Updated
------- ---- -----------   -----     ------------ -------- ------- --------
192.0.2.150:/share/ava_dest_1 RST vs2:ontap_dest   Unitialized Transferring  0B
                      Snapmirrored  Idle                 true
vs2:ontap_source XDP 192.0.2.150:/share/ava_dest_1
                      Snapmirrored  Idle                 true
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
                                                                     Progress
Source       Destination   Mirror    Relationship  Total             Last
Path    Type Path          State     Status        Progress  Healthy Updated
------- ---- -----------   -----     ------------  --------  ------- --------
192.0.2.150:/share/ava_dest_1 RST  vs2:ontap_dest
                       Snapmirrored  Idle                    true
vs2:ontap_source XDP 192.0.2.150:/share/ava_dest
                       Snapmirrored  Idle                    true
2 entries were displayed.
```

The Relationship Status changes from `Unitialized Transferring` to `Snapmirrored`.

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

Example

```
cluster1::> Snapmirror show
                                                                     Progress
Source       Destination   Mirror    Relationship  Total             Last
Path    Type Path          State     Status        Progress  Healthy Updated
------- ---- -----------   -----     ------------  --------  ------- --------
192.0.2.150:/share/ava_dest_1 RST  vs2:ontap_dest
                        Broken-off   Idle                    true
vs2:ontap_source XDP 192.0.2.150:/share/ava_dest
                       Snapmirrored  Idle                    true
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:

Example

```
cluster1::> volume show
Vserver   Volume       Aggregate State  Type   Size  Available Used%
--------- ------------ --------- ------ ---- ------- --------- -----
onk-vsim1 vol0         aggr0     online  RW   2.85GB  705.4MB   76%
vs2       ontap_dest   aggr1     online  RW      1GB   1021MB    0%
vs2       ontap_source aggr1     online  RW      1GB  966.4MB    5%
vs2       vs_root1     aggr1     online  RW     20MB     10MB    9%
4 entries were displayed.
```

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

Example

```
cluster1::> snapshot show ontap_dest
                                              ---Blocks---
Vserver   Volume    Snapshot            Size  Total% Used%
--------- --------- ------------------  ----- ------ ------
vs2       ontap_dest
                    base_snapshot       112KB  0%     5%
```

Related tasks

Monitoring backup progress using the ONTAP CLI on page 63

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 the cloud 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.

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 agg1 -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. For a full volume restore, 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:

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" :

```
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

```
cluster1::> snapmirror show
                                                                   Progress
Source      Destination  Mirror     Relationship Total             Last
Path   Type Path         State      Status       Progress  Healthy Updated
------ ---- ----------- -----      ------------ --------  ------- --------
192.0.2.150:/share/ava_dest_1 RST vs2:sfr_dest
                                    Idle                   true
vs2:ontap_source XDP 192.0.2.150:/share/ava_dest_1
                      Snapmirrored  Idle                   true
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

```
cluster1::> set diag
cluster1::> run local ls -lr /vol/sfr_dest
10644   96   1    2097152   Fri Oct 21 12:02:59 EST 2016 file3
```

Related tasks

Monitoring backup progress using the ONTAP CLI on page 63

Viewing data protection reports for NAS file services

Using the 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

Report type	Description
Backup Report	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.
Restore Report	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.
Data Protection Report	This report provides protection details for NAS file services. You can see how many volumes are or are not protected.

Steps

1. In the left navigation pane, click **Dashboard**.
2. Locate the data protection pie chart.
3. 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.
4. 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
- *SnapCenter Software 2.0 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 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 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 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 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.

Copyright information

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 WAFL 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.

http://www.netapp.com/us/legal/netapptmlist.aspx

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