NetApp Verified Architecture

NetApp AltaVault and Veritas NetBackup Solution with FlexPod Datacenter

NVA Deployment

Aaron Kirk, NetApp
May 2016 | NVA-0024-DEPLOY | Version 1.0

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Program Summary

The NetApp® Verified Architecture (NVA) program provides you with a verified architecture for NetApp solutions. An NVA offers you a NetApp solution architecture that:

- Is thoroughly tested
- Is prescriptive in nature
- Minimizes customer deployment risks
- Accelerates customer time to market

This NVA deployment guide describes the deployment steps required for NetApp AltaVault™ cloud-integrated storage with the NetApp All Flash FAS (AFF) FlexPod® Datacenter and the VMware vSphere solution. AltaVault appliances readily integrate with preexisting backup software and support 95% of the cloud storage solutions on the market today, including those of all leading cloud storage providers.

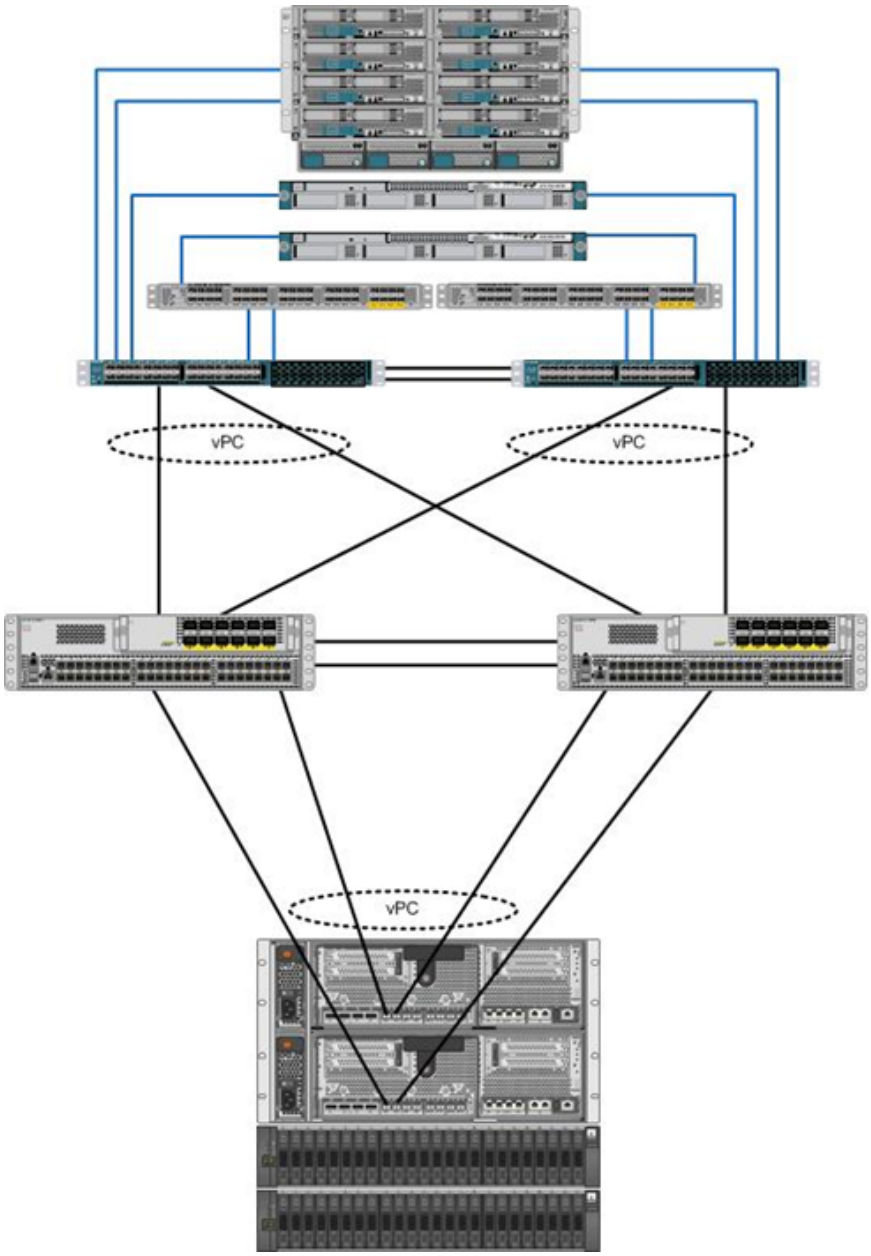
2 Solution Overview

A cloud-based backup architecture can significantly reduce costs, increase business agility, and simplify disaster recovery (DR). However, developing a backup strategy for both on-premises and off-premises data centers while also incorporating a DR solution often creates a complex infrastructure that is difficult to manage and scale.

FlexPod Datacenter with NetApp AFF and the NetApp AltaVault cloud-integrated storage appliance is a shared, verified, and proven solution spanning private and public clouds. This solution is built on the previously validated FlexPod Datacenter with AFF design with the following additional components:

- **The AltaVault AVA-v8 virtual appliance.** For a DR case study.
- **Amazon Simple Storage Service (S3) cloud storage.** The cloud service used by AltaVault.
- **The Veritas NetBackup Catalog.** Provides awareness of NetApp Snapshot® copies and allows point-in-time restores from AltaVault.
- **Veritas NetBackup Replication Director.** Cascades backups from primary storage to secondary storage to the AltaVault virtual appliance.

Figure 1) FlexPod infrastructure with virtualized AltaVault.



2.1 Target Audiences

The target audiences for this deployment guide are customer system administrators, contractors, professional services engineers, and other professionals who might install and configure AltaVault with FlexPod environments.

2.2 Solution Technology

AltaVault is easy to deploy and, when coupled with FlexPod Datacenter with AFF, provides an architecture that is seamless, industry proven, and validated to industry best practices.

This section briefly presents the products included in the AltaVault with FlexPod solution. For detailed information about these components, see the NetApp AltaVault and Veritas NetBackup Solution with FlexPod Datacenter NVA Design Guide.

NetApp AltaVault Appliance

With NetApp AltaVault storage, you can securely back up data to the cloud at costs that are up to 90% less than the costs for on-premises solutions. With AltaVault, you have the power to tap into cloud economics, preserve your investments in backup infrastructure, and meet backup and recovery SLAs.

The AltaVault appliance is a disk-to-disk data storage optimization system that can be integrated with a variety of class-leading cloud storage providers. AltaVault can also be integrated with backup and archive applications to protect critical production data off site. Integration can be achieved without the complexity of tape management solutions or the cost of in-house DR sites and services. When administrators add an AltaVault appliance as a target for their backup or archive infrastructure, the backup server connects to the AltaVault appliance by using the CIFS or NFS protocol.

AltaVault appliances are available in a variety of sizes that scale with business requirements and growth. They are also available in virtual format editions for environments that use hypervisors such as VMware vSphere and Microsoft Hyper-V or the Amazon EC2 Marketplace for cloud-to-cloud backups. This flexibility provides alternative methods for performing data recovery in a disaster when infrastructure and resources might not be available in the same manner as in the lost primary data center.

FlexPod Datacenter with NetApp All Flash FAS and VMware vSphere

FlexPod is a best practice data center architecture that includes the following components:

- The Cisco Unified Computing System (Cisco UCS)
- Cisco Nexus switches
- The NetApp FAS system

These components are connected and configured according to Cisco and NetApp best practices, and they provide an excellent platform for running a variety of enterprise workloads with confidence. FlexPod can scale up for greater performance and capacity, or it can scale out for environments that require multiple consistent deployments. The reference architecture covered in this document uses the Cisco Nexus 9000 for the switching element.

Cisco Unified Computing System

The Cisco UCS is a next-generation solution for blade and rack server computing. The system integrates a low-latency, lossless 10GbE unified network fabric with enterprise-class x86-architecture servers. The system is an integrated, scalable, multichassis platform in which all resources participate in a unified management domain. Cisco UCS accelerates the delivery of new services simply, reliably, and securely through end-to-end provisioning and migration support for virtualized and nonvirtualized environments.

Cisco Nexus 9000 Series Switch

The Cisco Nexus 9000 Series includes both modular and fixed-port switches that are designed to deliver a flexible and agile network fabric. The Cisco Nexus 9300 platform consists of fixed-port switches designed for top-of-rack and middle-of-row deployment in data centers that support enterprise applications, service provider hosting, and cloud computing environments. They are layer 2 and layer 3 nonblocking 10 and 40 Gigabit Ethernet switches with up to 2.56 terabits per second of internal bandwidth.

NetApp All Flash FAS and NetApp Data ONTAP

NetApp solutions offer increased availability while consuming fewer IT resources. A NetApp storage solution includes hardware in the form of FAS controllers and disk storage and the NetApp Data ONTAP® operating system that runs on the controllers. Disk storage is offered in two configurations: FAS systems with SAS disks, SATA disks, or solid-state disks (SSDs) and All Flash FAS systems with only SSDs.

All Flash FAS

NetApp All Flash FAS addresses enterprise storage requirements with high performance, superior flexibility, and best-in-class data management. Built on the clustered Data ONTAP storage operating system, All Flash FAS speeds up businesses without compromising on efficiency, reliability, or the flexibility of IT operations. As true enterprise-class, all-flash arrays, All Flash FAS systems accelerate, manage, and protect business-critical data, now and in the future.

For more information about All Flash FAS systems, see the document NetApp All Flash FAS.

Data ONTAP

With clustered Data ONTAP, NetApp provides enterprise-ready, unified scale-out storage. Developed on a solid foundation of proven Data ONTAP technology and innovation, clustered Data ONTAP is the basis for large, virtualized shared-storage infrastructures that are architected for nondisruptive operations over a system's lifetime. Controller nodes are deployed in HA pairs in a single storage domain or cluster.

Data ONTAP scale-out is a way to respond to growth in a storage environment. As the storage environment grows, additional controllers are added seamlessly to the resource pool that resides on the shared storage infrastructure. Host and client connections as well as datastores can move seamlessly and nondisruptively anywhere in the resource pool. Existing workloads can be easily balanced over the available resources, and new workloads can be easily deployed.

Technology refreshes (such as replacing disk shelves and adding or replacing storage controllers) are accomplished while the environment remains online and continues to serve data. Data ONTAP is the first product to offer a complete scale-out solution, and it provides an adaptable, always-available storage infrastructure for today's highly virtualized environments.

For more information about Data ONTAP, see the document NetApp Data ONTAP 8.3 Operating System.

Note: The design discussed in this document focuses on clustered Data ONTAP and IP-based storage.

VMware vSphere

VMware vSphere is a virtualization platform for holistically managing large collections of infrastructure resources—CPUs, storage, and networking—as a seamless, versatile, and dynamic operating environment. Traditional operating systems manage an individual machine. VMware vSphere, in contrast, aggregates the infrastructure of an entire data center to create a single powerhouse with resources that can be allocated quickly and dynamically to any application.

For more information, see the VMware vSphere product page.

Veritas NetBackup Replication Director

Veritas NetBackup has a three-tiered architecture. The first tier is a master server that provides functions such as configuration services, policy creation, scheduling, reporting, and logging. The master server is the communications mechanism of the backup application and allocates resources to the media servers.

The second tier is the media server, the mainstay of the NetBackup environment. The media server must be a high-rate-of-data I/O importer and exporter. The connections to disks, tape drives, the SAN, and the LAN depend on the backup and storage requirements. The AltaVault appliance is used by the media server to send backups to a public cloud.

The final tier is the clients tier. The clients are the systems in which the data resides and that must be protected. However, certain aspects obscure the line between clients and media servers. From the NetBackup standpoint, when a media server sends its own data to a device for backup, it is considered a client.

With the Replication Director functionality of NetBackup, you can implement end-to-end protection management by performing unified policy management and Snapshot copy monitoring and management. The NetBackup media server also manages client backups by replication Snapshot copies between storage systems.

3 Solution Use Cases

Combining the flexibility of AltaVault with FlexPod infrastructure, the NetApp AltaVault and Veritas NetBackup solution with FlexPod Datacenter accommodates various business and technical needs. These needs include validated use cases that use AltaVault virtual appliances to recover data after on-premises storage has been lost. Tests for the use cases focused on the functionality and seamless integration between AltaVault and FlexPod Datacenter:

- Cascading replication of Snapshot copies from primary storage to secondary storage to NetApp AltaVault
- Recovery of data from an AltaVault virtual appliance to the primary site
- On-premises hardware appliance failure: replacing the appliance, restoring the previous backup configuration, and verifying the data restored from the cloud (Amazon S3)
- Off-premises DR: restoring the failed appliance configuration on a remote AVA-v8 virtual appliance with a new IP address and completing the data restore from the cloud

These validation tests focused exclusively on functionality and excluded performance measurements. However, we did note time savings in these tests for incremental backups to the cloud due to Veritas NetBackup Replication Director Snapshot integration with NetApp FAS.

4 Technology Requirements

You must consult the following interoperability matrixes to determine whether your implementation of the NetApp AltaVault and Veritas NetBackup solution with FlexPod Datacenter is supported:

- The NetApp Interoperability Matrix Tool
- The Cisco UCS Hardware and Software Interoperability Tool
- The VMware Compatibility Guide
- The Veritas NetBackup Master Compatibility List

Although there are no dependencies between FlexPod with AFF, AltaVault (physical and virtual), and NetBackup, NetApp recommends consulting the interoperability matrixes as a best practice.

4.1 Hardware Requirements

Table 1 lists the hardware components used to validate and implement the solution. The components used in specific implementations might vary based on customer requirements. The FlexPod components listed in Table 1 correspond to the minimum hardware required to validate the solution in the lab.

Note: For a list of minimum requirements for a production environment, see the NetApp AltaVault and Veritas NetBackup Solution with FlexPod Datacenter NVA Design Guide.

Table 1) Hardware requirements.

Layer	Hardware	Quantity
Compute	Cisco UCS 6248UP fabric interconnects	2
	Cisco UCS B-200 M4	2
Network	Cisco Nexus 9372	2
Storage	NetApp All Flash FAS8060	1 (HA pair)
	NetApp AltaVault AVA-v8	1

4.2 Software Requirements

Table 2 lists the software components required to implement this solution. The components used in specific implementations might vary based on customer requirements.

Table 2) Software requirements.

Layer	Software	Version
Compute	Cisco UCS Manager infrastructure software bundle	2.2(5b)
	Cisco UCS Manager B-Series software bundle	2.2(5b)
Network	Cisco Nexus 9000 iNX-OS	7.0(3)I1(3)
Storage	NetApp AVA-v8	4.1.0.1
	NetApp Data ONTAP	8.3.1
Software	NetApp OnCommand® Unified Manager for clustered Data ONTAP	6.3
	OnCommand Performance Manager for clustered Data ONTAP	2.0
	NetApp Virtual Storage Console	6.1
	Amazon S3 storage	N/A
	SUSE Linux Enterprise Server	12
	VMware vSphere ESXi	6
	VMware vCenter	6
	Veritas NetBackup	7.7
	NetApp Plug-in for Veritas NetBackup	2.0

5 Deployment Procedures

The procedures in this guide must be completed in a sequential manner to deploy AltaVault and NetBackup with FlexPod Datacenter. These procedures assume that the FlexPod infrastructure has already been deployed. If this is not the case, see the FlexPod Datacenter with VMware vSphere 6.0 Deployment Guide for instructions on how to deploy FlexPod.

To deploy the AltaVault with FlexPod solution, you must complete the following tasks in addition to deploying the FlexPod infrastructure:

- Configure Amazon S3 for AltaVault
- Configure the AltaVault AVA-v8 virtual appliance
- Configure the NetBackup software for AltaVault

Note: In the lab environment, we deployed the virtual AltaVault appliance (AVA-v8) on the FlexPod Cisco UCS server for the validation of local recovery and DR cases. In a production environment, the remote DR location should use FlexPod for consistency and for the rapid recovery of the AltaVault virtual appliance and data.

5.1 Deployment Prerequisites

Before you deploy AltaVault to a backup environment, you must complete the following prerequisites:

- Obtain server systems and related software media supported by NetBackup and the AltaVault appliance.
- Perform physical stacking and racking of equipment at each site. All cabling and power supplies must be operational.
- Verify that all LAN and WAN connections to and from the Internet and cloud storage providers are functioning.
- If applicable, you must have a Windows directory service (Active Directory) or a UNIX Kerberos server available.
- Verify that an AltaVault physical appliance or an AltaVault virtual appliance is online and connected to the physical network infrastructure. A minimum of two IP addresses must be available for AltaVault.
- Procure and install all necessary software licenses from each vendor by using vendor-specific guidelines and obtain cloud storage credentials from your designated cloud storage provider.
- Set up at least one server as a master server and one server as a media server in a single-computer system. NetApp recommends that you separate the master and media servers so that the system is not overloaded. These servers, along with clients, require the minimum hardware features required by the backup application. For more information, visit the Veritas Support site and consult the NetBackup Master Compatibility List.

5.2 Configure Amazon Web Services for AltaVault

AltaVault requires access to the Amazon Simple Storage Service (Amazon S3) before the storage service is enabled. This failsafe feature allows data to be archived at all times. To configure Amazon Web Services (AWS) for AltaVault, you must create an AWS account and an access key for Amazon S3. You must also attach policy permission for access to only Amazon S3. This policy can be granular to a specific S3 bucket. In our validation, the account had full access to Amazon S3.

Create Dedicated Amazon S3 Account for AltaVault

To create a dedicated Amazon S3 account for AltaVault, complete the following steps:

1. Access the AWS Identity and Access Management (IAM) console.
2. In the navigation pane, click Users.
3. Click Create New Users.
4. Type a user name (for example, AltaVault) and keep Generate an Access Key for Each User selected. Click Create.
5. Click Show User Security Credentials or click Download Credentials to obtain the access key ID and the secret access key for your user.

   The key pair should look similar to the following examples:

   - Access key ID: `AKIAIOSFODNN7EXAMPLE`
   - Secret access key: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`

Attach Amazon S3 Policy to AltaVault User

After you create the user, you must assign a policy that allows access to a particular AWS service (in this case, Amazon S3). To attach an Amazon S3 policy to the AltaVault user, complete the following steps:

1. Return to the IAM console and click Users.
2. Double-click the user that you created for AltaVault.
3. Click Permissions to expand the Permissions section.
4. Click Attach Policy.
5. Select AmazonS3FullAccess and click Attach Policy.

   The following example shows a policy applied to a user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
```

Create Amazon S3 Bucket

You can create an Amazon S3 bucket for AltaVault from the Amazon S3 console or from the AltaVault appliance. In our validation, AltaVault created the bucket during the initial configuration.

5.3 Configure AltaVault

AltaVault physical appliances and virtual appliances are configured in the same way. For our validation, we completed the configuration steps on the virtual appliance.

Note: For detailed instructions about how to deploy the AltaVault virtual appliance on VMware vSphere, see the NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliances.

AltaVault requires a minimum of two interfaces: primary and data. The primary interface is used for management, Internet traffic, and cloud archiving. The data interface is used for local backup and restore. You can, however, direct Internet-bound traffic to the data interface if the network segment for the data interface can access the Internet.

Perform Basic AltaVault Configuration

The first time you access an AltaVault appliance, it runs a setup program that prompts you to change the password and supply the basic networking information required for the appliance to communicate over the primary interface. You must enter the following information to configure and manage the appliance:

- The appliance host name
- No Dynamic Host Configuration Protocol (DHCP) use on the primary interface
- The primary IP address
- The network mask
- The default gateway
- The IP address of the primary DNS server
- The domain name

Figure 2 shows a sample startup configuration for an AltaVault appliance. After the initial configuration is completed, the remaining steps can be finalized from the web interface. The default login for AltaVault appliances is admin/password.

Figure 2) AltaVault startup configuration.

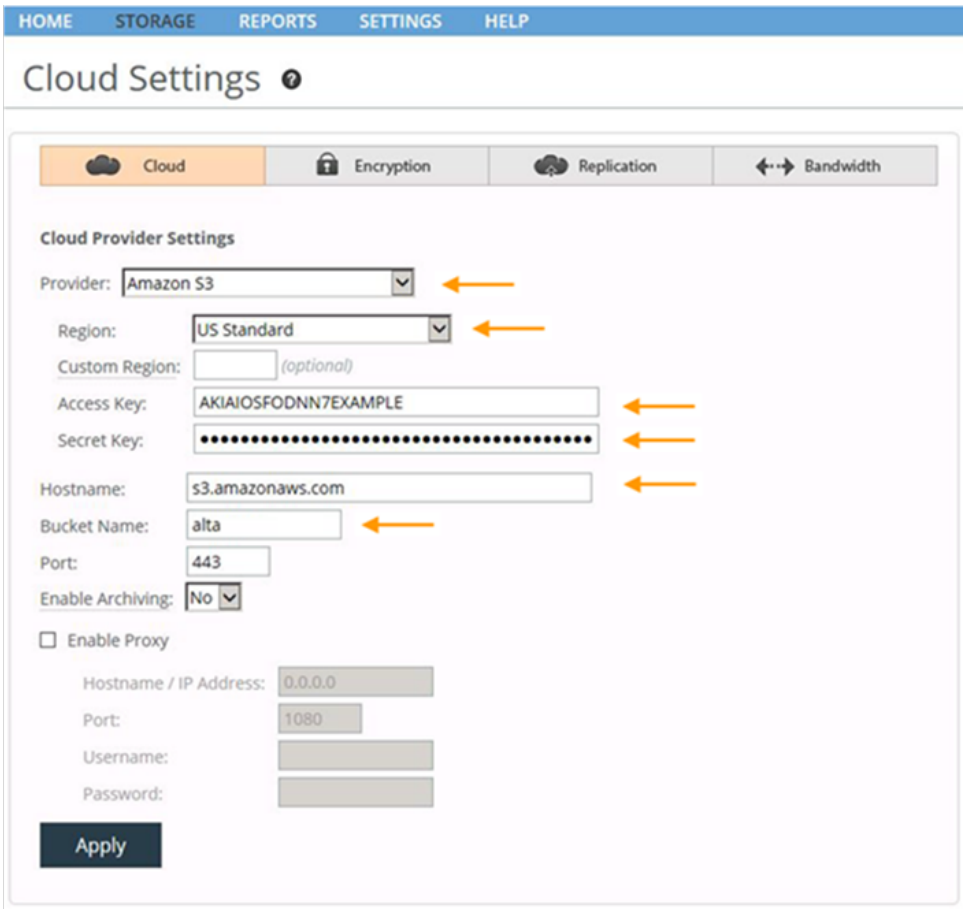
```
Step 1: Admin password?
Step 1: Retype password?
Step 2: Hostname? [amnesiac] altavault
Step 3: Use DHCP on primary interface? [yes] n
Step 4: Primary IP address? 172.20.71.230
Step 5: Netmask? [0.0.0.0] 255.255.255.0
Step 6: Default gateway? 172.20.71.1
Step 7: Primary DNS server? 10.61.185.58
Step 8: Domain name? fvl.rtp.netapp.com

You have entered the following information:

Admin password:
Hostname: altavault
Use DHCP on primary interface: no
Primary IP address: 172.20.71.230
Netmask: 255.255.255.0
Default gateway: 172.20.71.1
Primary DNS server: 10.61.185.58
Domain name: fvl.rtp.netapp.com

To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.

Choice:
```

Configure AltaVault Cloud Settings

Before you configure any storage features on an AltaVault appliance, you must set the cloud configuration and the data encryption key. As noted earlier, cloud configuration is mandatory for running the storage service.

To configure AltaVault cloud settings, complete the following steps:

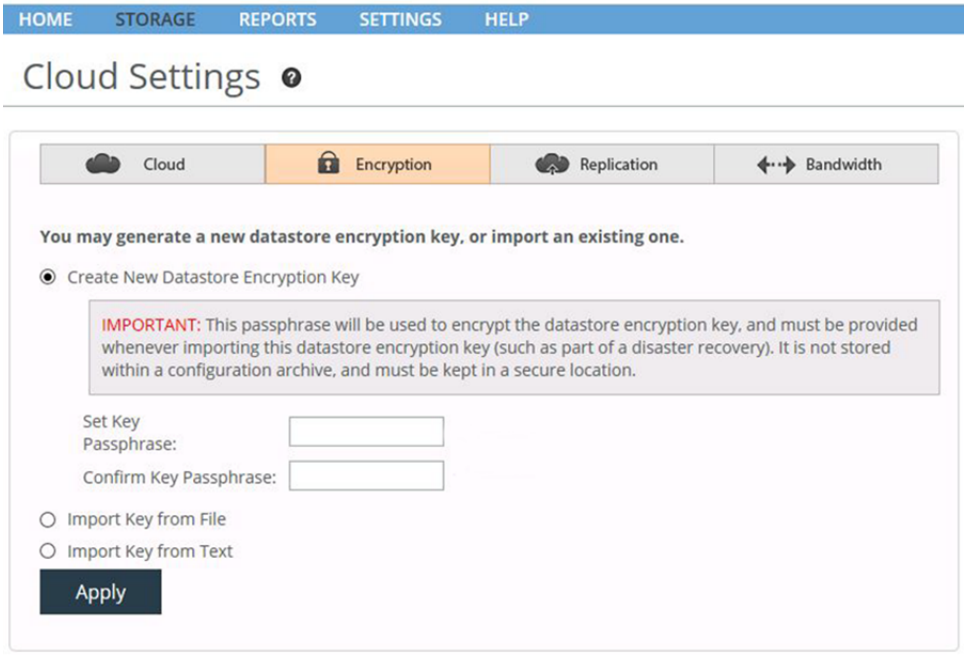
1. From the AltaVault main webpage, select Storage and click Cloud Settings.
2. In the Cloud tab, select Amazon S3 as the cloud provider.
3. Select a region.
4. Type the access key ID and the secret access key that you obtained previously from the Amazon IAM console.
5. Type the host name.
6. Type the bucket name. If the bucket already exists on the Amazon S3 console, make sure that the name you enter matches the existing bucket name. Otherwise, AltaVault creates another bucket on S3 automatically.
7. Click Apply to commit the configuration.



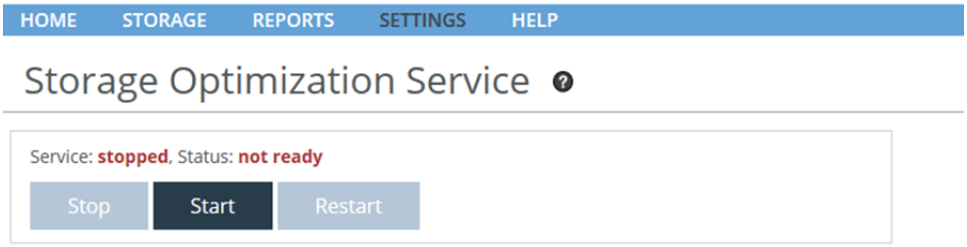
Note: The items flagged with arrows in this screenshot are mandatory for the Amazon S3 cloud configuration. For a list of all supported cloud vendors and the minimum information required to complete the cloud settings for each provider, see the NetApp AltaVault Cloud Integrated Storage Deployment Guide.

8. Click the Encryption tab.
9. Type and confirm a new passphrase and click Apply.

Note: This passphrase is used to encrypt the datastore encryption key and must be provided whenever you import that datastore encryption key (for example, as a part of DR). The passphrase is not stored in a configuration file and must be kept in a secure location.



10. Click Save at the top right corner of the page.
11. To restart the optimization service, select Settings > Service and click Restart.



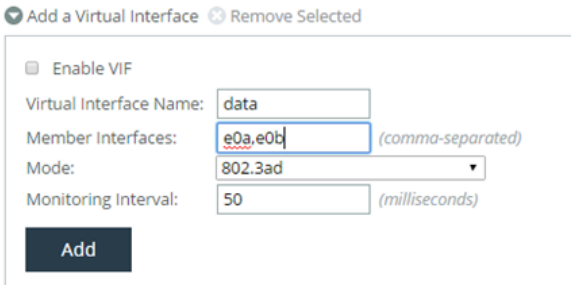
Configure AltaVault Data Interface Settings

The AltaVault appliance supports the Link Aggregation Control Protocol (LACP) on the data interfaces for added network redundancy and additional capacity. To use LACP, you must create a virtual interface (VIF) and assign an IP address to the new VIF.

Create Virtual Interface

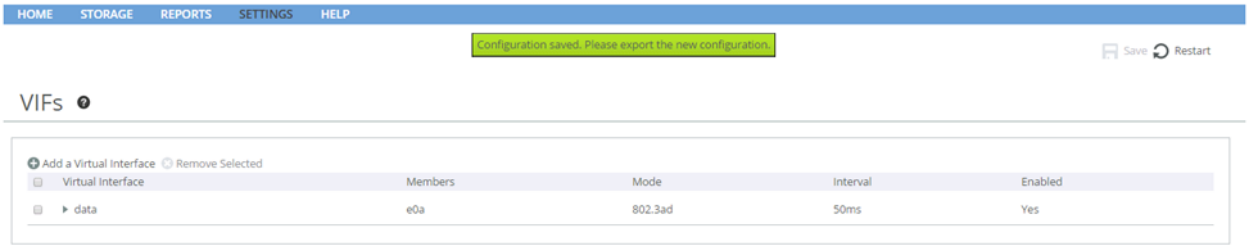
To create a VIF, complete the following steps:

1. From the AltaVault main webpage, select Settings and click VIFs.
2. Click Add a Virtual Interface.
3. Select Enable VIF.
4. Type a name for the VIF.
5. Add the member interfaces separated by a comma. Verify that these interfaces are connected to the network.
6. Select 802.3ad from the Mode list.
7. Click Add.



8. Click Save. The new VIF is added to the VIFs list.

Note: The Save button should appear light gray if the configuration has been saved.



9. Select Settings > Reboot/Shutdown and click Reboot.

Assign IP Address to New VIF

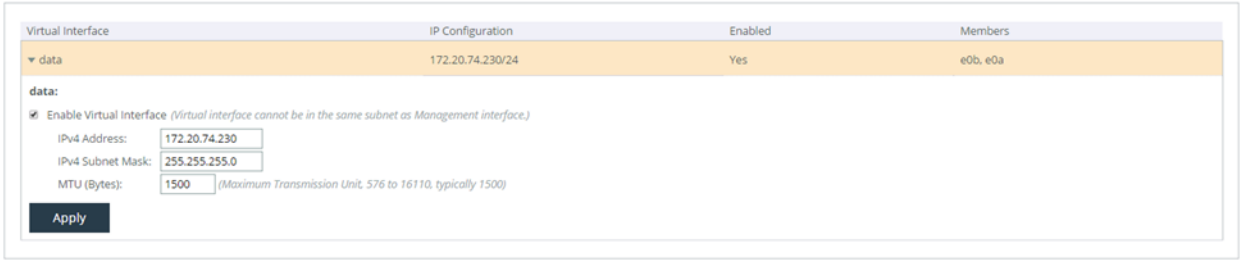
After the appliance reboots, assign an IP address to the new VIF, save the configuration, and restart the service.

To assign an IP address to the VIF, complete the following steps:

1. From the AltaVault main webpage, select Settings and click Data Interfaces.
2. Expand the new VIF by clicking the arrow next to it.
3. Assign an IP address and a subnet mask. The subnet mask is the data subnet reachable by clients.
4. Keep the MTU size at the default value of 1,500.

   Note: You can change the MTU size if your network switches support a different size.

5. Click Apply.



6. Click Save and then click Restart at the top right corner of the page.

Configure NFS for AltaVault

Depending on your requirements, both CIFS and NFS are available for data archiving on AltaVault. This guide focuses on NFS with NetBackup.

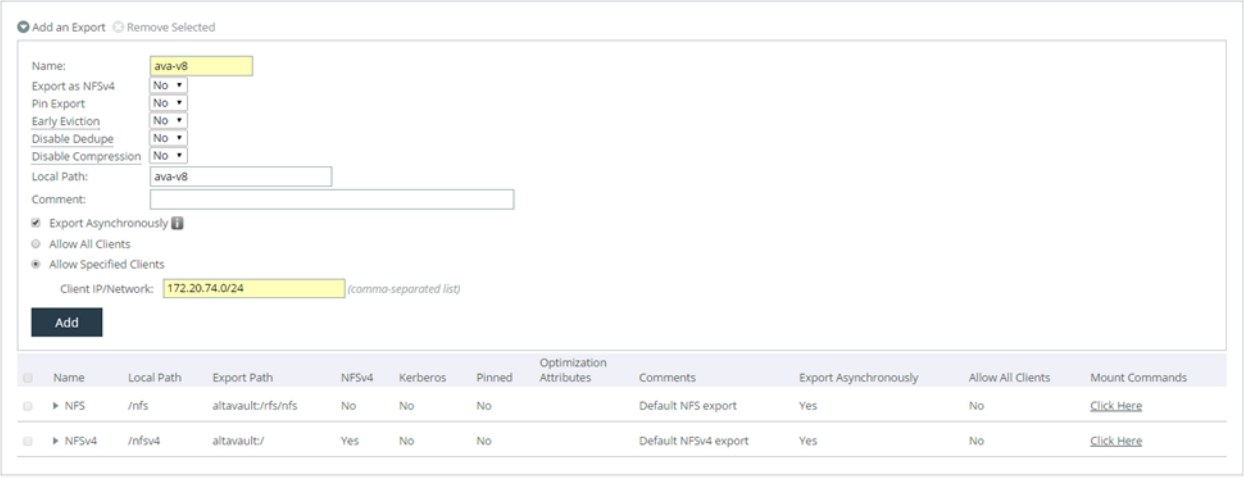
Note: For more information about the CIFS configuration, see the NetApp AltaVault Cloud Integrated Storage User's Guide.

NFS configuration on AltaVault is completed in a few steps. The appliance provisions an NFS share when you perform the initial network and cloud configuration for the appliance. This procedure explains the basic NFS; further configuration might be required to accommodate your environmental requirements.

Note: If the cloud services are not configured, you cannot provision CIFS or NFS shares. The appliance must be running the optimization service for CIFS and NFS to run.

To configure NFS for AltaVault, complete the following steps:

1. From the AltaVault main webpage, select Storage and click NFS.
2. Click Add an Export.
3. Type a name.
4. Type a path (for example, `/appliance_name/export_name`).
5. Identify the client IPs that require access to the export.
6. Keep the default selections for the other options and click Add.



5.4 Configure Veritas NetBackup Replication Director

Replication Director can replicate NetApp Snapshot copies between storage virtual machines by using NetApp SnapMirror® data replication or NetApp SnapVault® backup technologies. Replication Director consists of a media server that accesses storage systems through the OnCommand Unified Manager server. The OnCommand Unified Manager server hosts the NetApp Plug-in for Symantec NetBackup and creates and replicates Snapshot copies between storage systems. This procedure presents the best practice configuration for NetBackup Replication Director with AltaVault virtual appliances.

Note: Instructions for deploying NetBackup and configuring scalability options are beyond the scope of this guide. Because deployment details are specific to each environment, NetApp recommends that you refer to Veritas best practices to complete NetBackup deployment tasks.

Before configuring a backup policy to back up your environment, several entities must be created and configured in Veritas NetBackup:

- **Storage server.** A storage server is a NetBackup object that has exclusive access to manage Snapshot copies in an OnCommand configured resource pool.
- **Disk pool.** A disk pool represents disk storage that is exposed to NetBackup.
- **Storage unit.** A storage unit is a label that NetBackup associates with physical storage. The label can identify a robot, a path to a volume, or a disk pool.
- **Storage lifecycle policy.** A storage lifecycle policy defines where and in what order data is replicated.

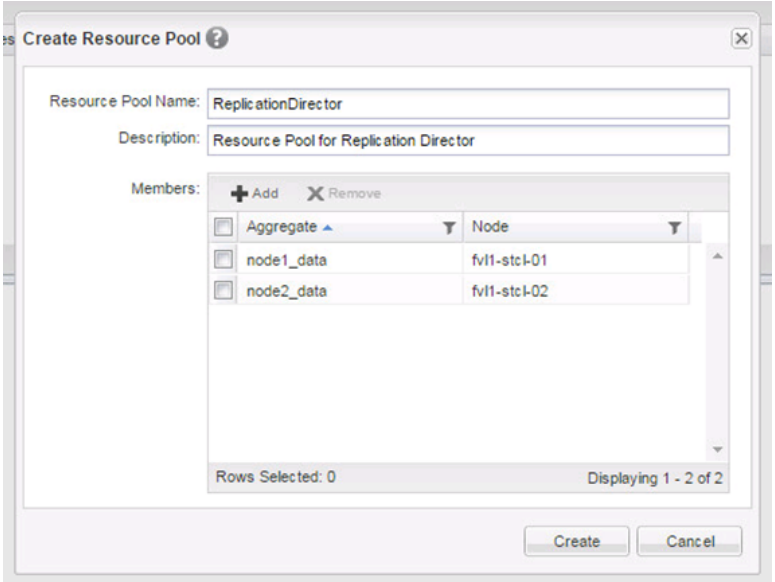
Configure Resource Pool in OnCommand Unified Manager

Note: For installation and configuration of the NetApp Plug-in for Symantec NetBackup, see the Installation and Administration Guide. For the purposes of this solution testing, OnCommand Unified Manager and the NetApp plug-in were both installed on a Windows 2012 virtual machine (VM).

Before adding the OnCommand server as a disk pool in Veritas NetBackup, resource pools must be added in the OnCommand server.

Follow the OnCommand Unified Manager Installation and Setup Guide to add clusters to OnCommand.

1. Navigate to Storage > Resource Pools.
2. Click Create to create a new storage pool.

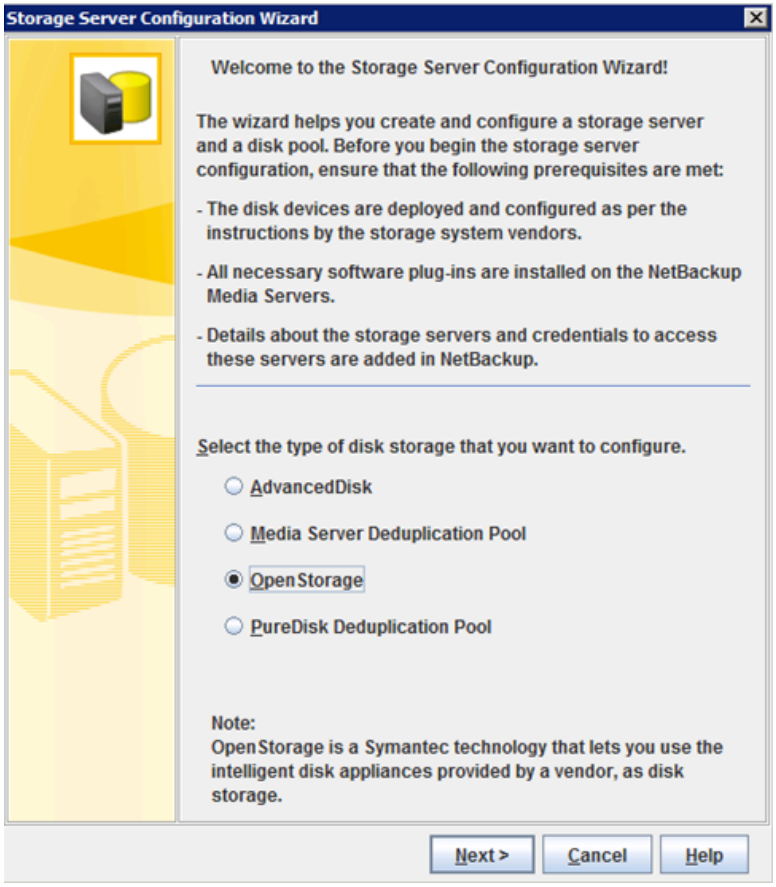


3. Fill in the Resource Pool Name field.
4. Click Add to add aggregates as members.
5. Create a resource pool for the aggregates to configure as the SnapMirror or SnapVault source or destination.

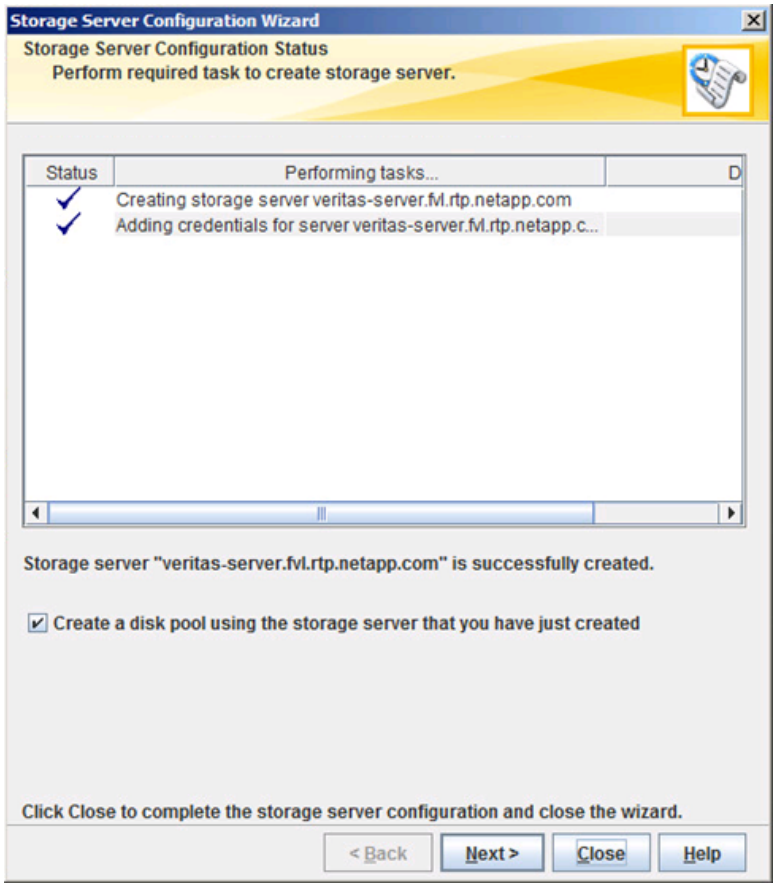
Configure NetBackup to Replicate Snapshot Copies

NetBackup uses an OpenStorage storage server to communicate with the NBUPlugin 2.0. To add the storage pools defined in OnCommand to NetBackup, add the server on which NBUPlugin 2.0 was installed.

1. Open the Storage Server Configuration wizard.
2. Choose OpenStorage as the type of disk storage.



3. Choose the media server to use for backups.
4. Select the storage server type. This was a NetApp OnCommand server (cluster-mode) for our testing.
5. Provide the OnCommand login details.
6. Click Next to review the configuration and Next again to create the storage server.
7. Uncheck Create a Disk Pool to create one more storage server before creating disk pools.



Create AdvancedDisk Storage Server

To add AltaVault to the storage lifecycle policy, an AdvancedDisk storage server must be created.

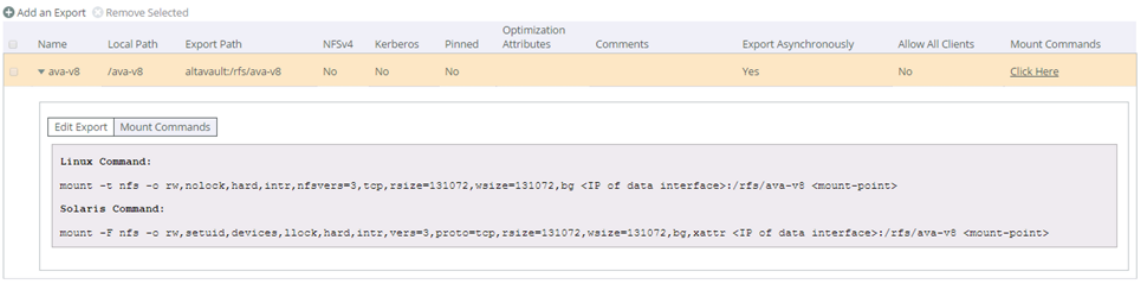
Note: AdvancedDisk was chosen instead of BasicDisk for this solution. BasicDisk cannot be used in a storage pool, and storage pools are required for a Replication Director storage lifecycle policy.

1. Open the Storage Server Configuration wizard.
2. Select AdvancedDisk and click Next.
3. Leave Create a Disk Pool Using the Storage Server That You Have Just Created selected to begin disk pool creation.

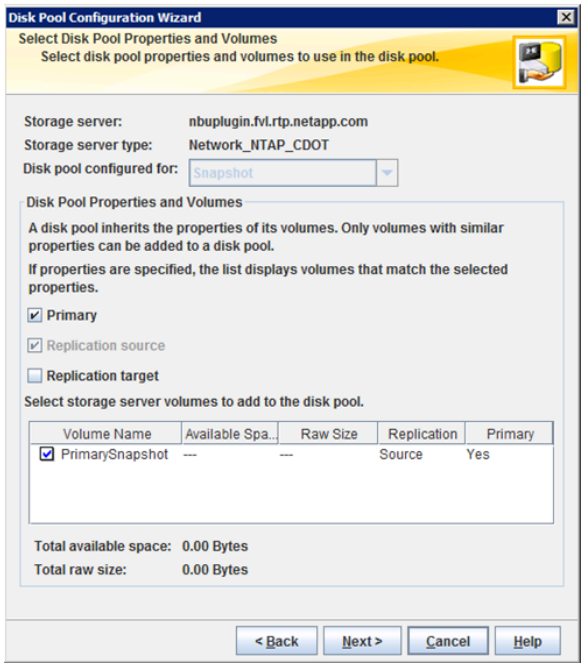
Add Disk Pools to NetBackup

Before creating the storage pool for AltaVault, the NFS export must be mounted on the media server.

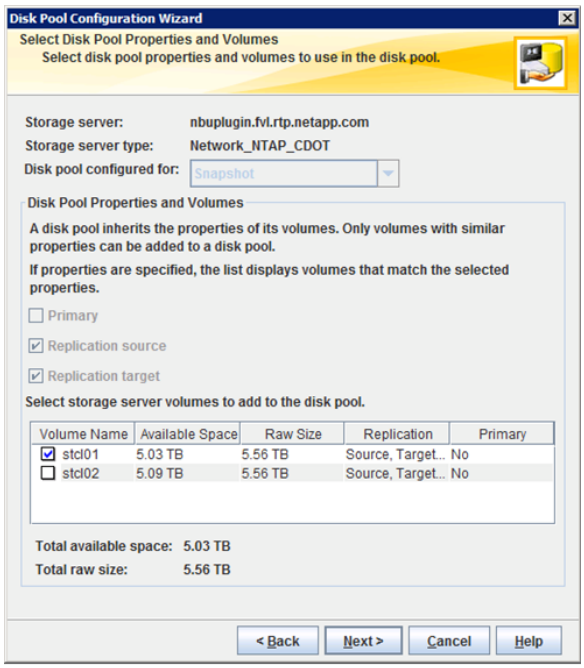
1. To view the command to mount the AltaVault export, navigate to Storage > NFS in the AltaVault GUI and click Mount Commands next to the mount that was created.



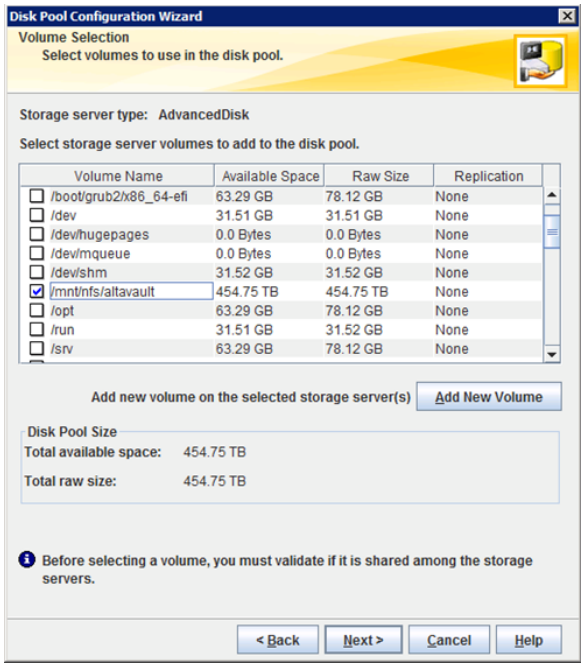
2. Use the Configure Disk Pool wizard to create disk pools for the storage lifecycle policy. This solution requires the creation of at least three disk pools:
   a. **Primary Snapshot disk pool.** This pool is used to create Snapshot copies on primary storage.



   b. **OnCommand resource pool.** This pool is used as the replication target for Snapshot copies.



c. **AltaVault backup target.** This pool is the mounted AltaVault volume. Check the box for the mount point where AltaVault was mounted.

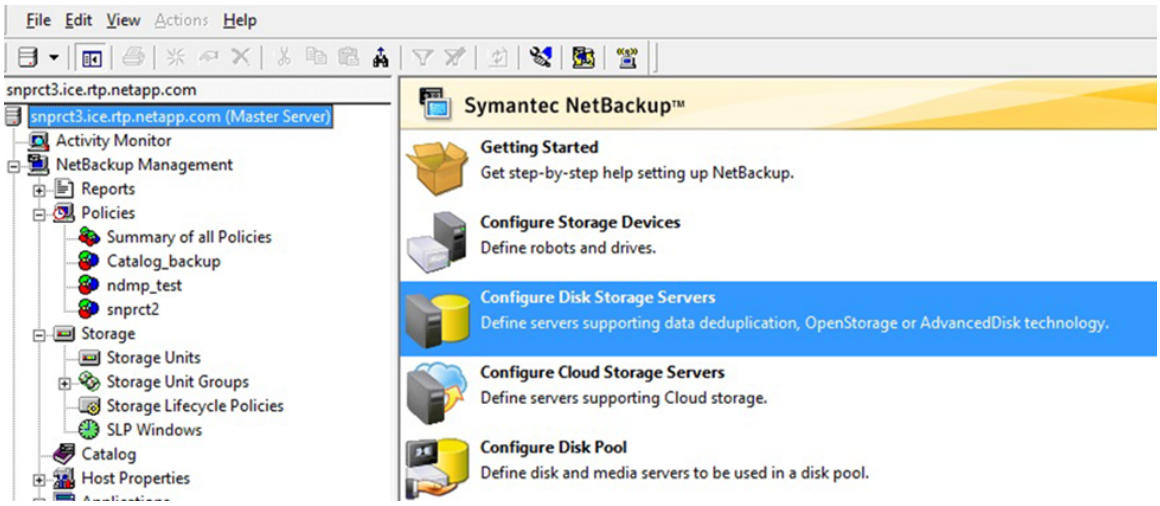


Create Storage Units

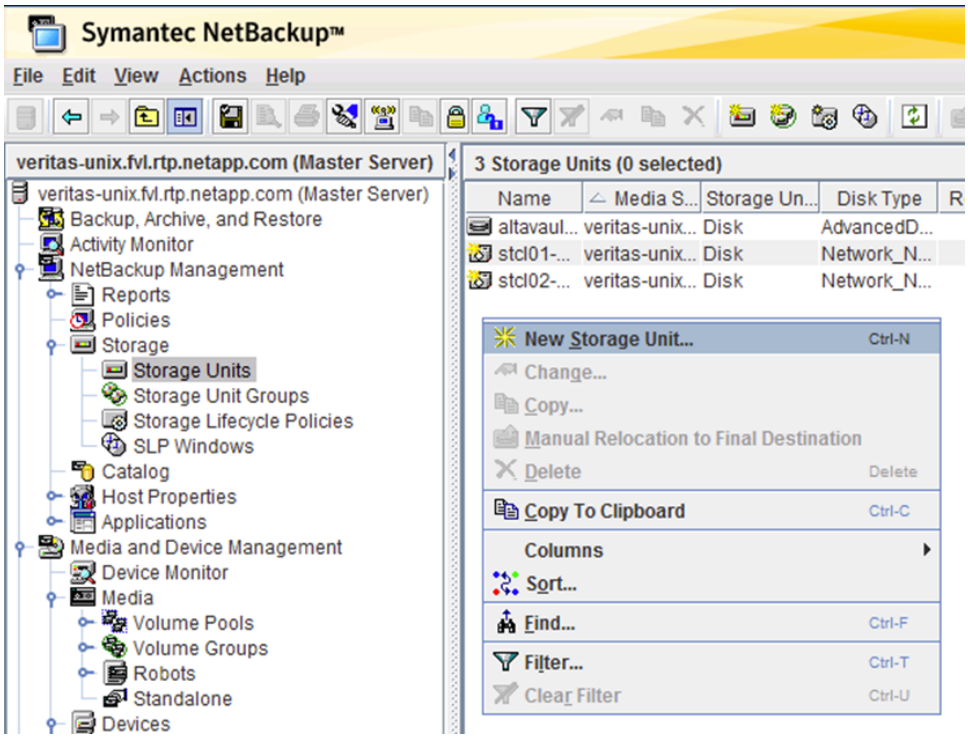
A storage unit is a label that NetBackup associates with physical storage. The label can identify a robot, a path to a volume, or a disk pool.

To create a storage unit and associate it with the AltaVault appliance, complete the following steps:

1. Open the NetBackup management console and point to the master server.

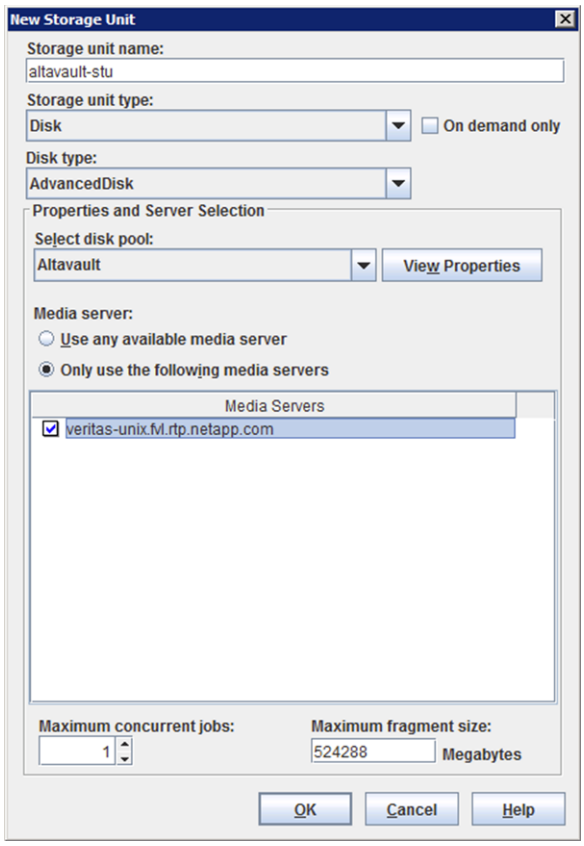


2. Select NetBackup Management > Storage, right-click Storage Units, and select New Storage Unit.



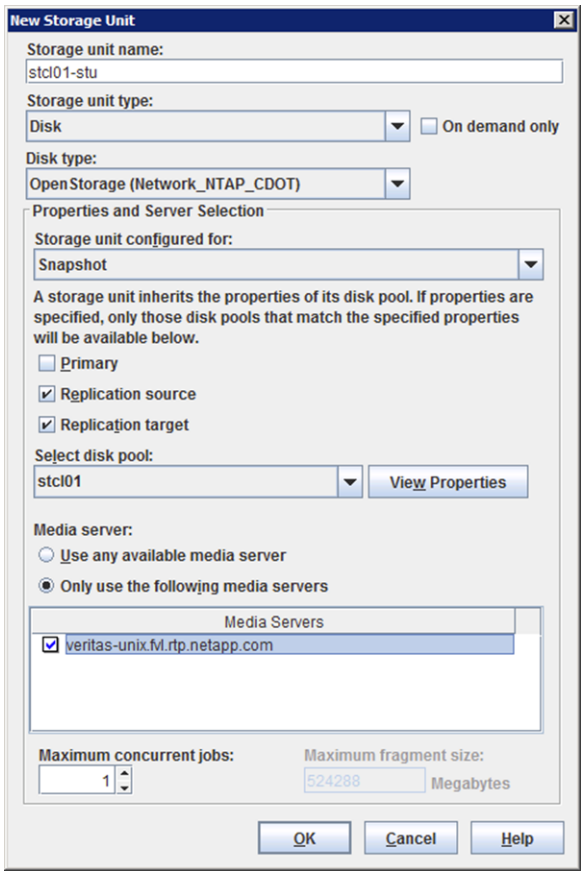
3. Create the storage unit for AltaVault with the following settings:
   a. Type a name for the storage unit.
   b. Set the storage unit type as Disk.
   c. Set the disk type as AdvancedDisk.
   d. Select a media server.
   e. Select Reduce Fragment Size To and set the value to 20480MB (20GB).

Note: For lab validation, we kept the remaining settings at their default values.

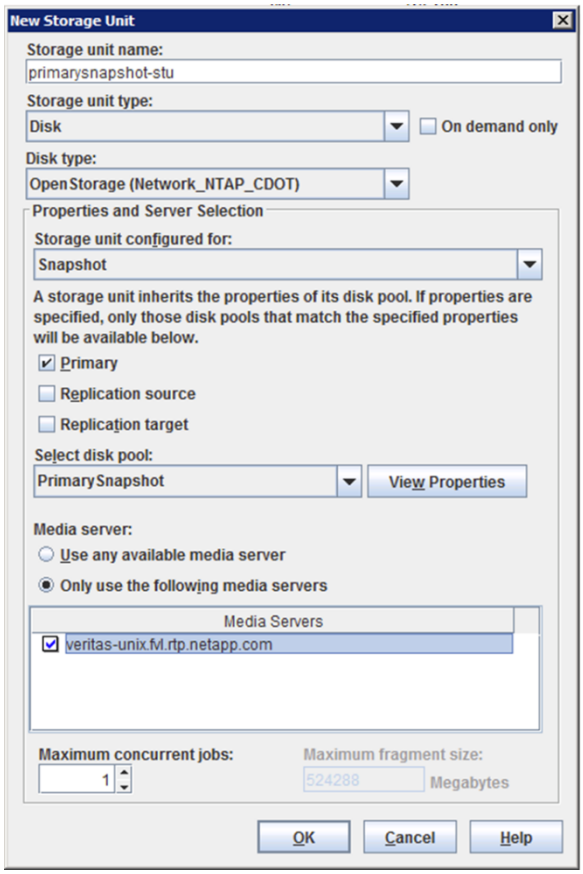


4. To create the storage units for OnCommand resource pools, configure the following settings:
   a. Type a name for the storage unit.
   b. Set the storage unit type as Disk.
   c. Set the disk type as OpenStorage (`Network_NTAP_CDOT`).
   d. Configure the storage unit for Snapshot.
   e. Check Replication Source and Replication Target.
   f. Select the disk pool.
   g. Select the media server.

Note: For the lab validation, we kept the remaining settings at their default values.



5. Create the storage units for primary Snapshot copies with the following settings:
   a. Type a name for the storage unit.
   b. Set the storage unit type as Disk.
   c. Set the disk type as OpenStorage (`Network_NTAP_CDOT`).
   d. Configure the storage unit for Snapshot.
   e. Check Primary.
   f. Select the disk pool.
   g. Select the media server.

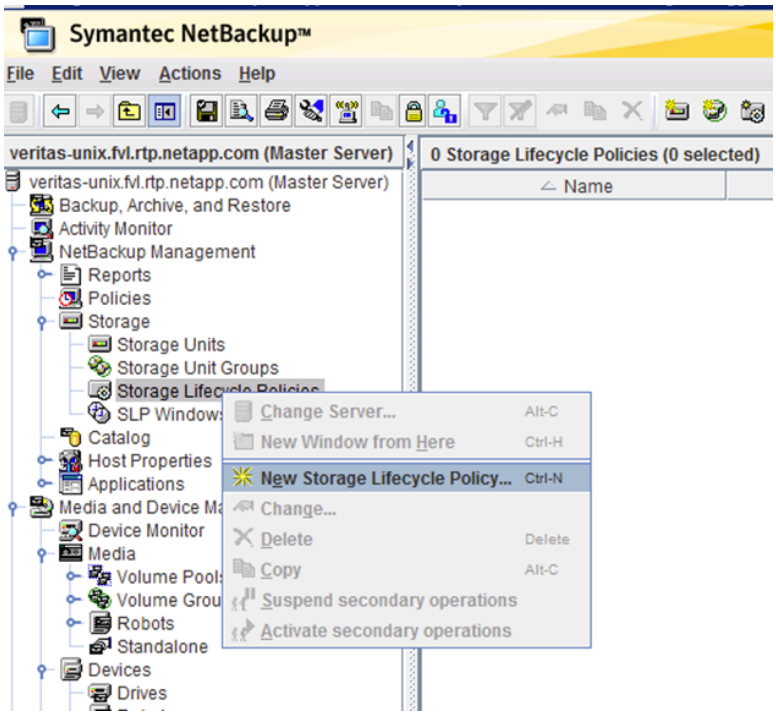


Before you can use NetBackup with AltaVault, you must associate a NetBackup policy with a storage unit that is based on the AltaVault appliance. After you configure the policy, you can create a test backup and restore your data from the backup to verify that NetBackup works with AltaVault.

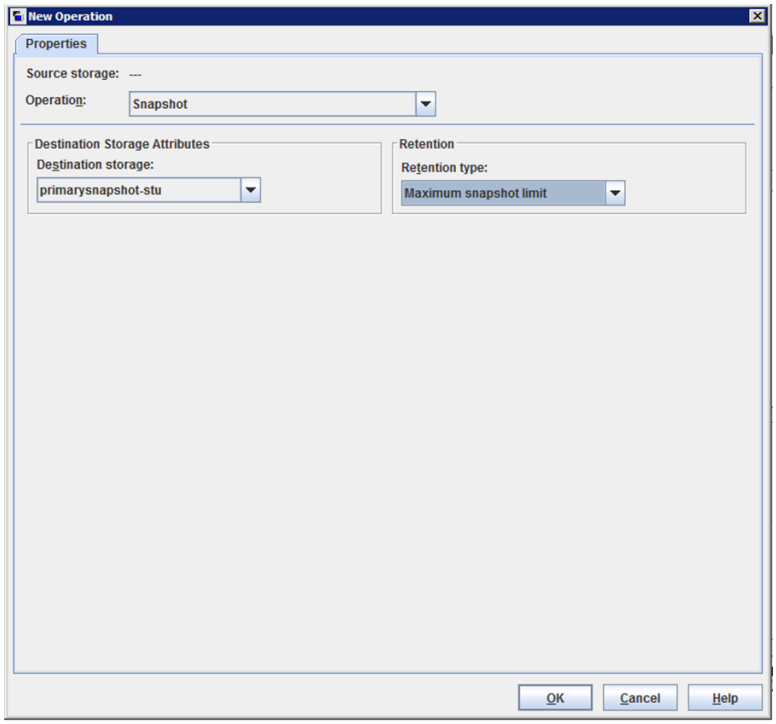
Create Storage Lifecycle Policy

A storage lifecycle policy takes control of disk pools to dictate when Snapshot copies are made and where they are replicated. To create a storage lifecycle policy that makes Snapshot copies, replicates them to a secondary destination, and moves them to AltaVault, complete the following steps:

1. Right-click Storage Lifecycle Policies and click New Storage Lifecycle Policy.

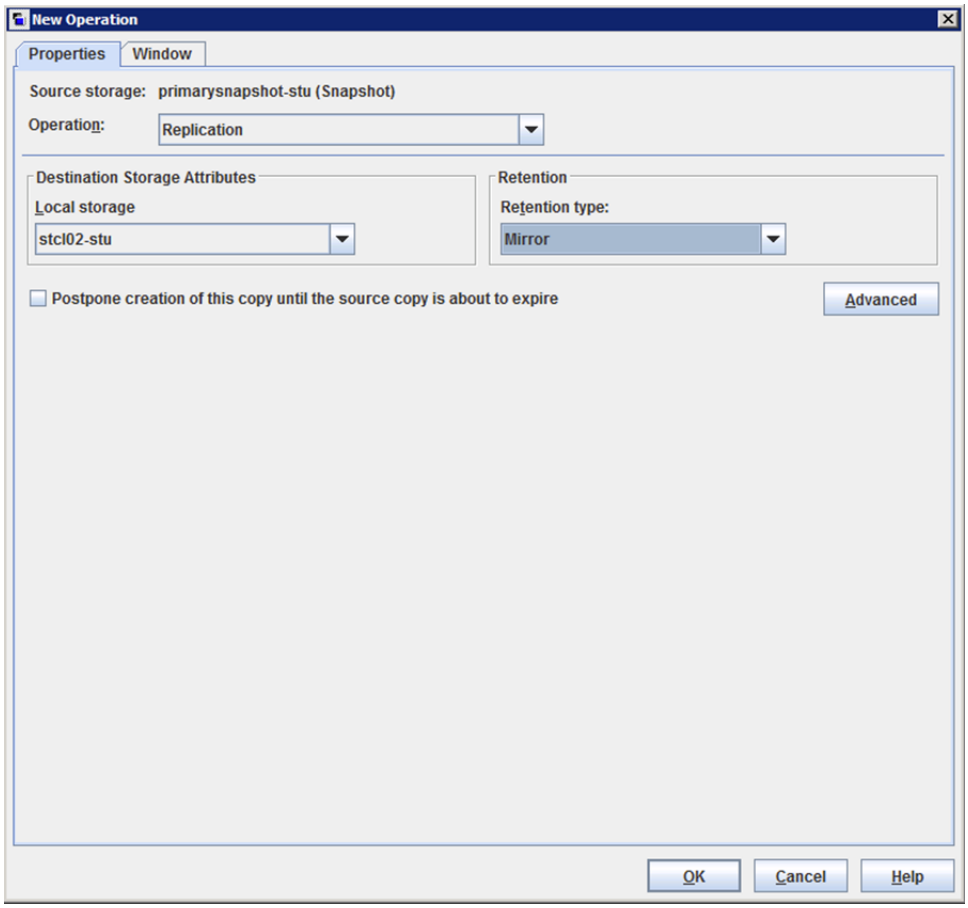


2. Give the storage lifecycle policy a name and click Add to add a new operation.
   a. Select Snapshot in the Operation field.
   b. Select the primary Snapshot storage unit as the destination storage.
   c. Select a retention type.
   d. Click OK.

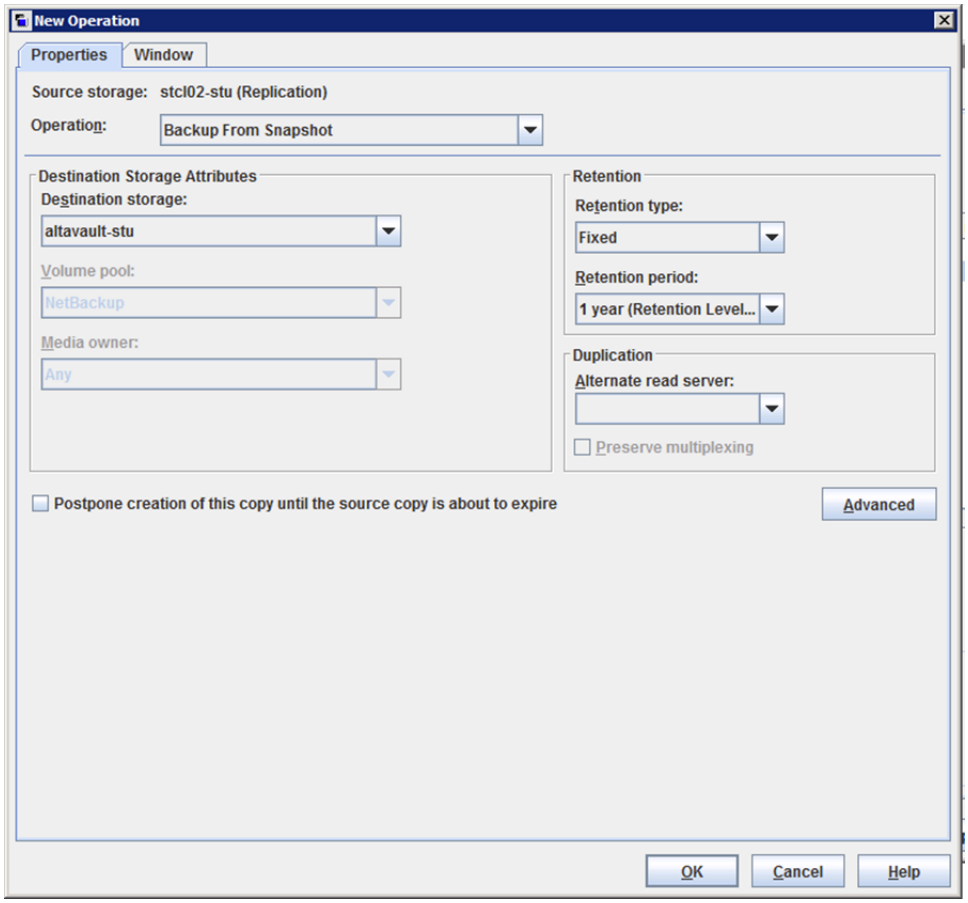


3. Select the Snapshot operation that was just added and click Add.
   a. Choose Replication in the Operation field.
   b. Choose the OnCommand resource pool where the Snapshot copies should be replicated as the destination storage.
   c. Choose the desired retention type and retention period.
   d. Click OK to add the Backup from Snapshot operation.

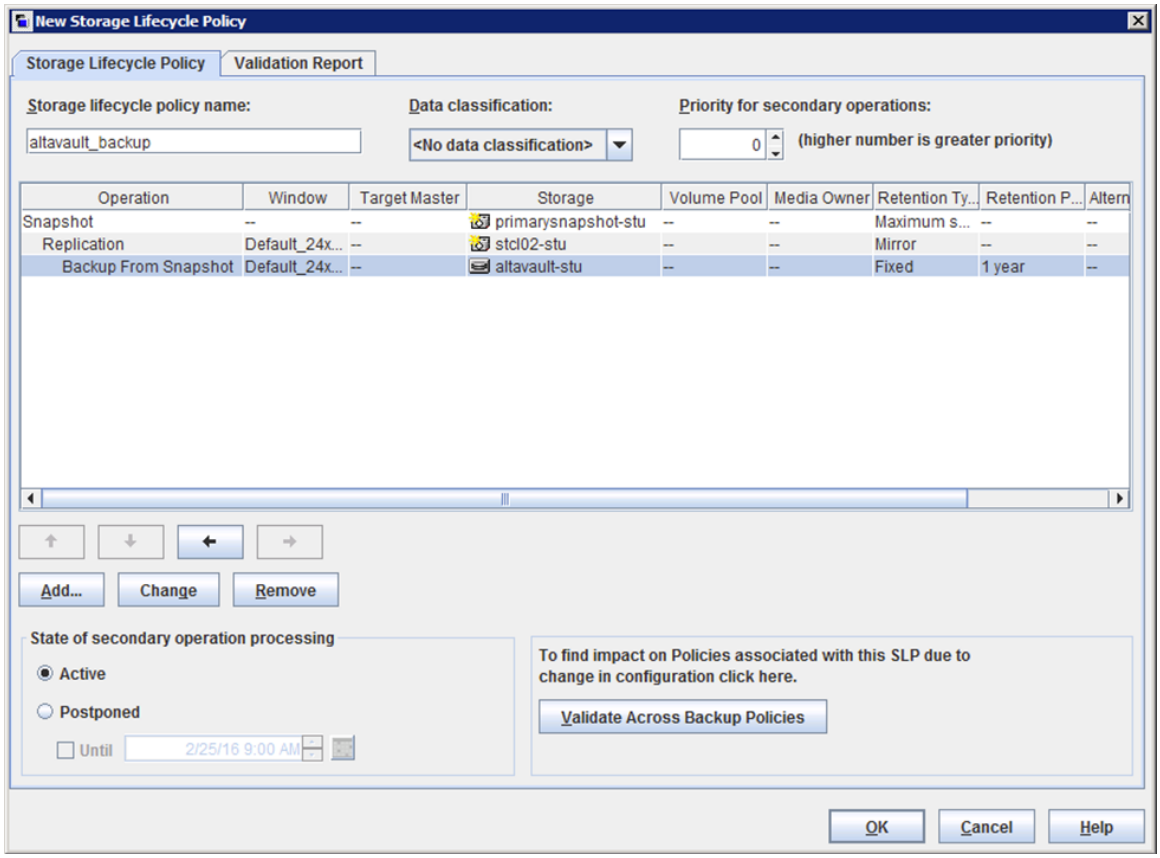
   Note: For the solution validation, the mirror retention type was used. This creates a SnapMirror relationship between the primary and secondary storage. To create a SnapVault policy, set the retention type to Fixed.



4. Select the replication operation that was just added and click Add.
   a. Choose the operation Backup from Snapshot.
   b. Choose the AltaVault storage unit as the destination storage.
   c. Choose Fixed in the Retention Type field and select the desired retention period.



After you make these three changes to the storage lifecycle policy, the policy should look like this:

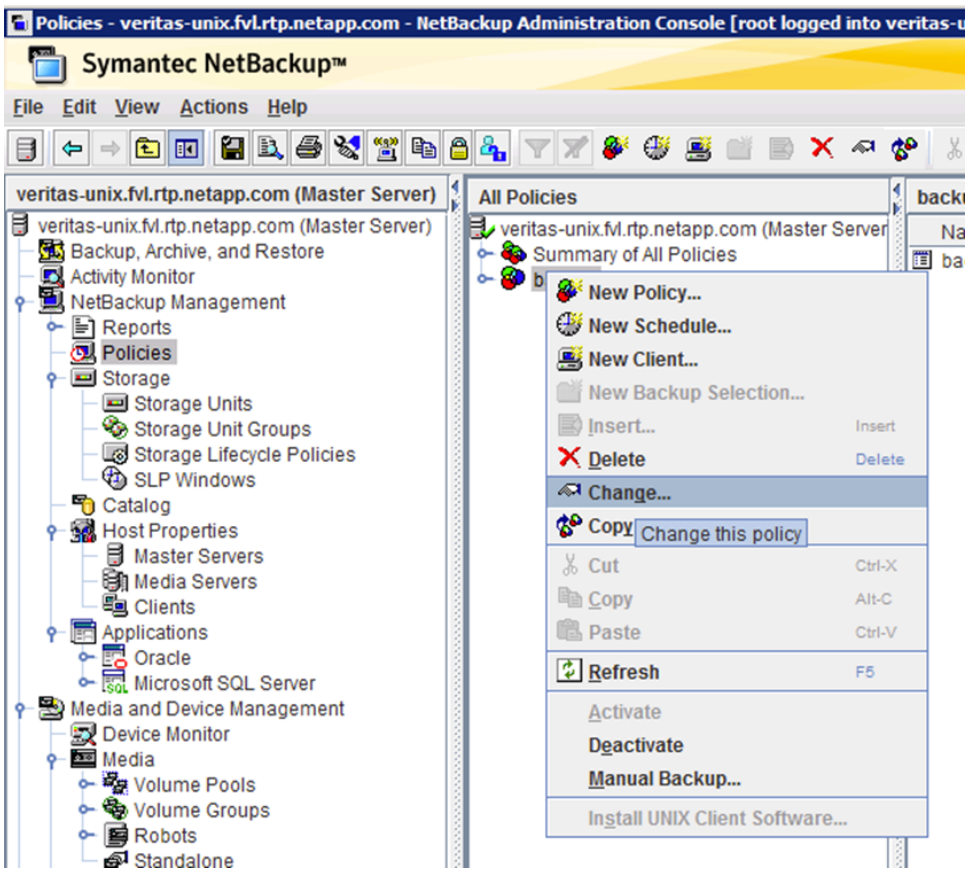


Modify Backup Policy

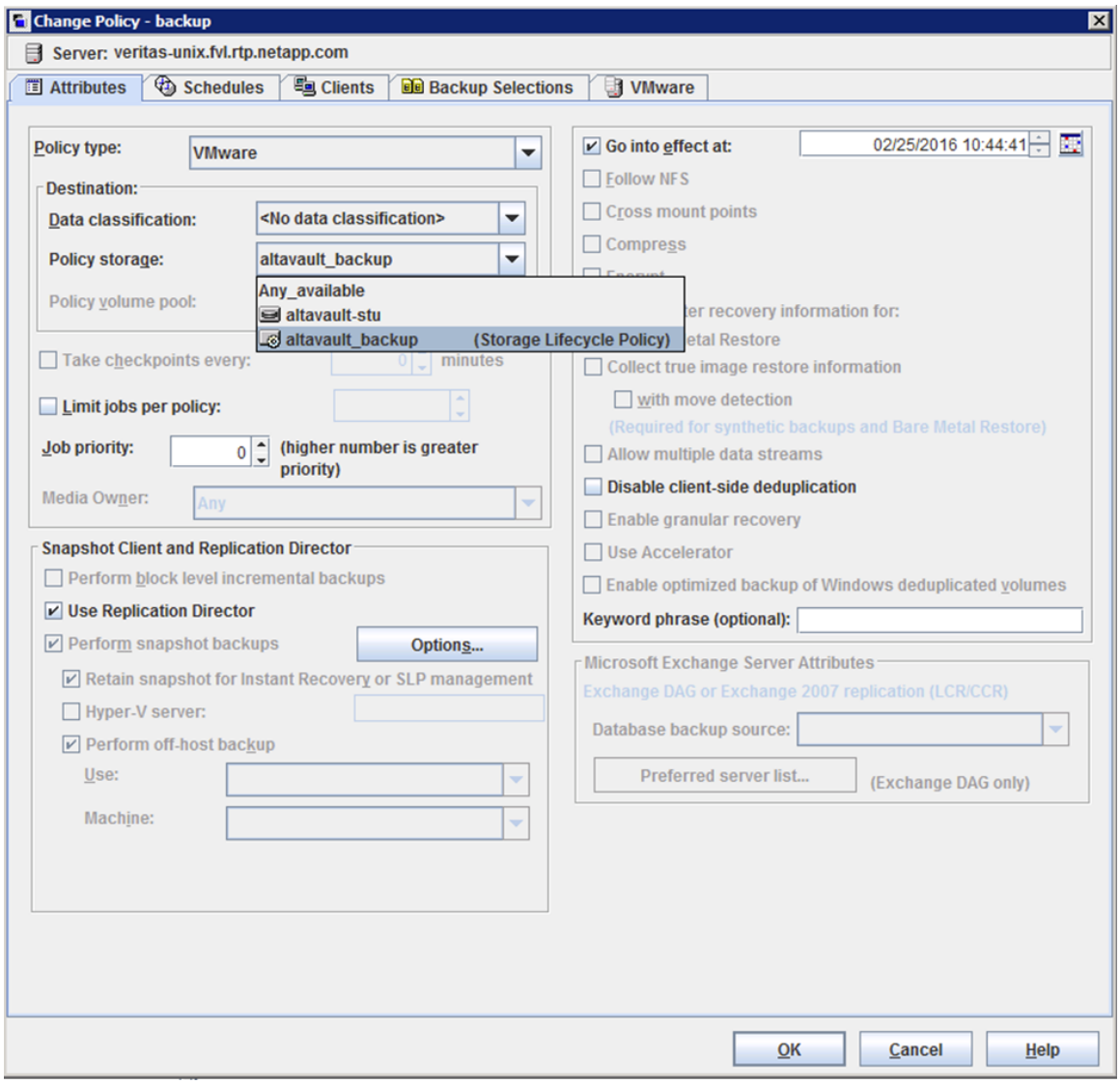
NetBackup policies determine when backups occur, to which backup targets the data is written, which storage lifecycle policies are used, and how long backup versions are maintained. Policies include automatic calendar-based schedules for performing unattended backups for clients. You can also run policies manually as needed. You must associate a policy with a storage unit or a storage lifecycle policy to write the backup jobs.

To associate a NetBackup policy with a storage unit or storage unit group that is based on an AltaVault appliance, complete the following steps:

1. Select NetBackup Management > Policies, right-click an existing policy, and select Change.



2. Modify the existing policy properties to point backups to the storage lifecycle policy that was created previously.

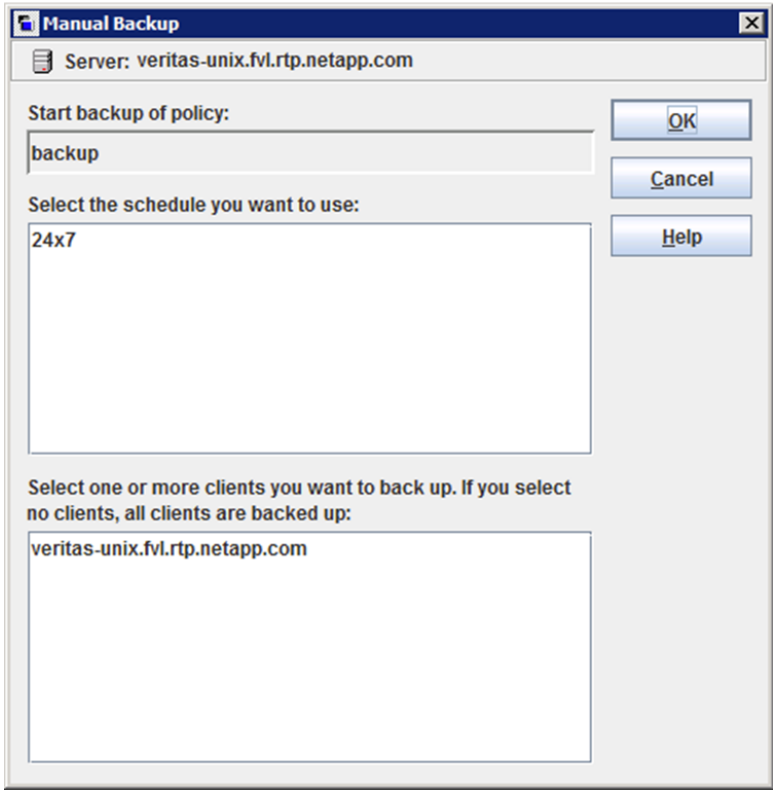


3. Check Use Replication Director.
4. Click OK to save the policy.

Create Test Backup

To test NetBackup with an AltaVault appliance, you can run a manual backup with the policy that you modified in the previous procedure. To run a manual backup, complete the following steps:

1. Under NetBackup Management > Policies, right-click the modified policy and select Manual Backup.
2. Select the schedule and clients to back up and click OK.

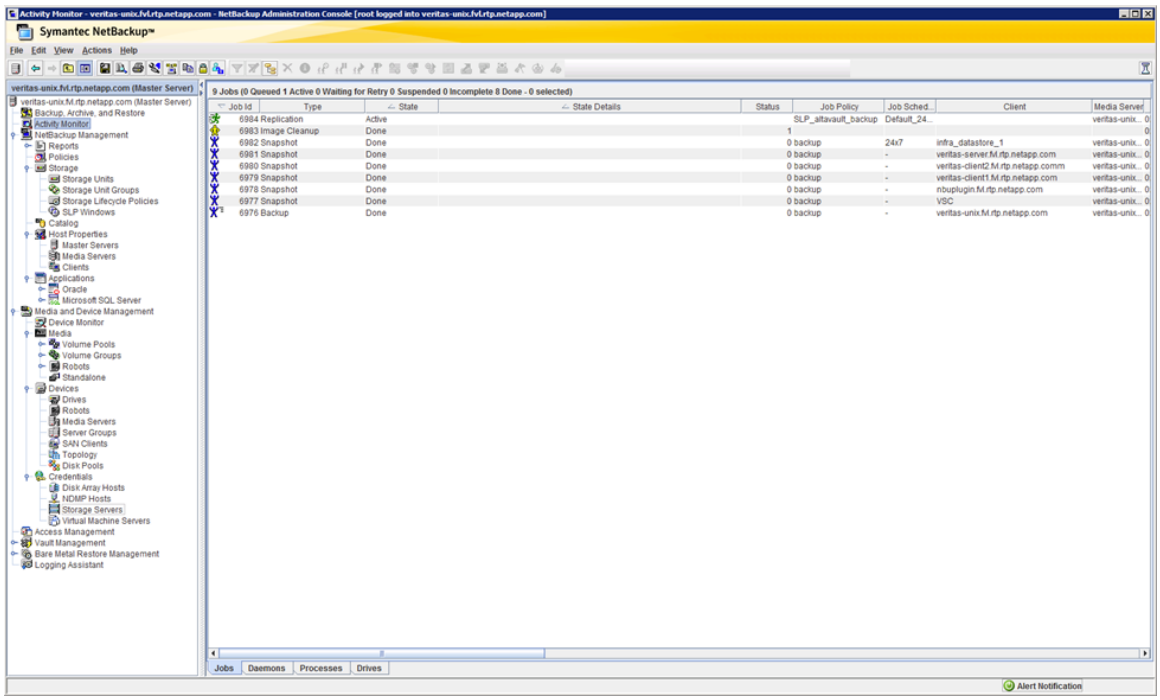


To back up Snapshot copies from secondary storage to AltaVault, the NetBackup media server must mount the SnapMirror destination volume and read from it. If the media server is unable to mount the destination volume, `Error 1542` appears in the NetBackup Activity Monitor.

View Manual Backup Status

To view details of a specific backup job, complete the following steps:

1. In the navigation bar, click Activity Monitor to display the list of backup jobs.
2. Double-click your backup job in the job list.



3. In the Job Details dialog box, review the job details on two tabs: the Job Overview tab and the Detailed Status tab. Information about the elapsed time, transfer rate (in KBps), and current object being processed is also available.

Restore Backup

When the backup is complete, perform a restore operation to verify that the AltaVault appliance can restore the backed-up data.

NetBackup tracks the different Snapshot copies in the NetBackup catalog. The default copy that is used for restore is called the primary copy.

- Snapshot copies on the primary storage are referred to as copy 1. These are always the primary copy unless they expire or are deleted.
- Snapshot copies on the SnapMirror destination are referred to as copy 2.
- Snapshot copies on the AltaVault appliance are referred to as copy 3.

If data is lost on copy 1 or copy 2, the AltaVault copy 3 is automatically made the primary copy. To manually set the AltaVault copy to the primary copy and restore from it, complete the following steps:

1. From the NetBackup catalog, set Copies to Copy 3, choose the appropriate date range, and click Search Now.
2. Right-click the Snapshot copy for the VM that you want to restore and select Set Primary Copy. Write down the Snapshot name for later.
3. From the NetBackup Backup, Archive, and Restore window, click Restore Files and the hand icon in the upper right corner. Choose VMware for the policy type and click Search VM Clients.
4. Click Browse Virtual Machines and vSphere View and click Next.
5. Select the VM you would like to restore and click Select.
6. Set the date range and choose the Snapshot copy from the backup history.
7. Change the entry to Browse Directory field to /.
8. Navigate to the directory that you would like to restore and click Restore.

6 Solution Verification

We tested the use cases listed in Table 3 after FlexPod Datacenter with AFF was deployed. In addition, the AltaVault physical and logical appliances were configured and brought online, and all software was provisioned on the VMware infrastructure, including Windows Server and NetBackup software.

Table 3) Tested use cases.

Test Case	Details
Cascading replication of Snapshot copies from primary storage to secondary storage to NetApp AltaVault	This verification process consisted of the following tasks: • Backing up an ESX cluster's VMs and datastores • Verifying that the backup completed successfully to the AltaVault virtual appliance • Verifying the copied data on both AltaVault appliances by reviewing reports and network utilization logs • Verifying deduplication reports and the cloud operation status • Verifying Amazon S3 buckets and confirming that data slabs were populated
Recovery of data from an AVA-v8 virtual appliance to the primary site	This verification process consisted of the following tasks: • Deleting data from the VMs • Using the NetBackup restore utility to restore data from the AVA-v8 appliance • Verifying data integrity after the restore operation has finished **Note:** This test restored data from the AltaVault local cache rather than from Amazon S3 buckets. AltaVault keeps up to 90% of the appliance's storage capacity hot before a rotational schedule kicks in.
On-premises hardware appliance failure: replacing the appliance, restoring the previous backup configuration, and verifying the data restored from the cloud (Amazon S3)	This verification process consisted of the following tasks: • Backing up the AVA-v8 configuration to a safe location • Simulating hardware failure by destroying the configuration, the data stored on the appliance, and any encryption keys • Deleting data from clients to verify restore from Amazon S3 storage • Reapplying the previously saved configuration to the AVA-v8 appliance • Restoring the archived data from Amazon S3 storage by executing the prepopulation task from the AltaVault storage menu • Performing a restore from the NetBackup client and verifying data integrity
Off-premises DR: restoring the failed appliance configuration on a remote AVA-v8 virtual appliance with a new IP address and completing the data restore from the cloud	This verification process consisted of the following tasks: • Backing up the AVA-v8 configuration to a safe location • Shutting down the AVA-v8 appliance to simulate site failure and deletion of all VMs on the cluster • Configuring an AVA-v8 appliance with an IP address different from the IP address of the failed appliance to simulate a remote DR location • Importing only shared data and not the full configuration; for this step, the encryption key passphrase was required • Restoring the archived data from S3 storage by executing the prepopulation task from the AltaVault storage menu • Performing a restore of all VMs from the NetBackup administration client and verifying data integrity

7 Conclusion

AltaVault coupled with FlexPod Datacenter with NetApp All Flash FAS is a shared infrastructure that scales beyond the boundaries of the private cloud into the public cloud. An infrastructure containing these components provides an ease of use and a low cost of ownership not typically seen with traditional tape backup methods. With Veritas Replication Director, Snapshot copies can be seamlessly replicated to secondary storage and backed up to the cloud. With AltaVault, DR strategies are no longer limited to specific locations, and you no longer need to tolerate the excessive costs, ongoing maintenance, and limited capacity of tape libraries.

The proven and validated design of this architecture can support multiple use cases and applications. With this solution, you can use multiple cloud service providers, which provides you with complete data sovereignty and control. The efficiency of AltaVault deduplication accelerates data archiving and lowers the cost of remote storage.

References

NetApp References

- NetApp All Flash FAS
  http://www.netapp.com/us/products/storage-systems/all-flash-fas/
- NetApp AltaVault Cloud Integrated Storage Deployment Guide
  https://library.netapp.com/ecm/ecm_download_file/ECMP12434738
- NetApp AltaVault Cloud Integrated Storage Installation and Service Guide for Virtual Appliances
  https://library.netapp.com/ecm/ecm_download_file/ECMP12455064
- NetApp AltaVault Cloud Integrated Storage User's Guide
  https://library.netapp.com/ecm/ecm_download_file/ECMP12510035
- NetApp Data ONTAP 8.3 Operating System
  http://www.netapp.com/us/products/platform-os/data-ontap-8/index.aspx
- NVA-0019-DESIGN: NetApp AltaVault and Veritas NetBackup Solution with FlexPod Datacenter and ACI
  http://www.netapp.com/us/media/nva-0019-design.pdf
- NVA-0024-DESIGN: NetApp AltaVault and Veritas NetBackup Solution with FlexPod Datacenter NVA Design
  http://www.netapp.com/us/media/nva-0024-design.pdf
- TR-4405: NetApp AltaVault Cloud-Integrated Storage Appliance: Security Overview
  http://www.netapp.com/us/media/tr-4405.pdf
- TR-4414: NetApp AltaVault Cloud-Integrated Storage Appliance: Best Practices Guide for Backup Applications
  http://www.netapp.com/us/media/tr-4414.pdf
- TR-4420: NetApp AltaVault Cloud-Integrated Storage Appliance: Best Practices for Disaster Recovery
  http://www.netapp.com/us/media/tr-4420.pdf
- TR-4427: NetApp AltaVault Cloud-Integrated Storage Appliance: Technology Overview
  http://www.netapp.com/us/media/tr-4427.pdf

For more information about NetApp technologies, consult the NetApp public document library at http://www.netapp.com/us/library/.

Cisco References

- FlexPod Datacenter with NetApp All Flash FAS, Cisco Application Centric Infrastructure, and VMware vSphere Design Guide

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi55u2_n9k_aci_aff8040_design.html#_Toc425435684

- FlexPod Datacenter with NetApp All Flash FAS, Cisco Application Centric Infrastructure, and VMware vSphere Deployment Guide
  http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi55u2_n9k_aci_aff8040.html

Veritas References

- Veritas NetBackup
  https://www.veritas.com/product/backup-and-recovery/netbackup/
- Veritas NetBackup Administrator's Guide
  https://www.veritas.com/support/en_US/article.DOC8623

Version History

Version	Date	Document Version History
Version 1.0	November 2015	Initial release
Version 2.0	April 2016	Cisco and tech writing edits incorporated

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