AltaVault Backup to Cloud Setup and Administration

November 2017 | SL10337 Version 1.5.3
1 Introduction

This lab uses the virtual appliance version of AltaVault (formerly SteelStore). The AltaVault virtual appliance (AVA-v) is available for lab and proof of concept testing, and can be downloaded from the NetApp support site. AVA-v is available for both VMware vSphere ESXi and Microsoft Hyper-V. The AVA-v used in this lab is the same software that is used in production environments.

A complete set of documentation that describes how the appliance operates is available on the NetApp support site. It includes installation, administration, and command-line guides. The AltaVault OST Plugin is a separate section on the support site for both the documentation and the software downloads. The OST plug-in must match the AltaVault software version.

Supported backup applications, cloud storage

Note: Whenever you deploy the virtual appliance, before powering the VM on, create a second VMDK for use as the data (cache) disk.

AltaVault Appliance

The AltaVault appliance is an instance of the virtual AltaVault cloud integrated storage appliance. The virtual appliance offers the full functionality of a typical system used in production including a web based GUI that is accessed using the Firefox browser on the Jumphost. It is also possible to access the command line interface (CLI) of the AltaVault appliance through SSH with the PuTTY application on the Jumphost. The model used in this lab is the AVA-v8.

NetBackup Server

A NetBackup 7.7.3 Server is accessed using remote desktop from the Jumphost. NetBackup is running on a Windows 2008R2 VM, and supports connectivity through Open Storage Technology (OST) APIs.

CommVault IntelliSnap for NetApp (NetApp SnapProtect)

A CommVault IntelliSnap for NetApp (CI4N) v11sp7 is installed as part of this lab, and is accessed using remote desktop from the Jumphost. The CommCell server enables backup software, that provides snapshot management of NetApp Storage. Integrating with AltaVault is seamless.

OpenStack Swift

OpenStack Swift is configured on an Ubuntu 14.04 LTS virtual machine. The OpenStack identity service, Keystone, is also installed on this VM. The OpenStack dashboard, Horizon, is not installed because it has dependency on other OpenStack components. Horizon requires image service (Glance), compute (Nova), and networking (Neutron) which are not installed.

NetApp StorageGRID Webscale

A suite of StorageGRID Webscale 10.3.0 is included in this lab as a private target for AltaVault. StorageGRID Webscale provides a software-defined object storage solution for large archives and media repositories to help organizations apply intelligent policy-driven data management for a hybrid cloud. Combined with AltaVault, this solution enables customers to efficiently store, manage, and retrieve their data in a secure and encrypted solution for a hybrid cloud environment.

1 AltaVault Overview

AltaVault is a cloud integrated backup appliance that interfaces with backup applications through a NAS (CIFS/NFS) interface on the front end. Data written to the appliance through SMB/NFS/OST and SnapMirror is highly optimized using variable segment size deduplication and compression. After optimization, the data is encrypted and stored in the cache (local disk). As soon as the data is stored in the cache, an asynchronous process replicates the data to a cloud storage service.

Benefits of AltaVault

Here are some key benefits that AltaVault provides:

- Optimized for managing data in cloud storage services.
• Supports a wide range of cloud storage.
• Supports public and private cloud storage (object storage).
• One appliance replicates to one object storage location (bucket/container).
• Provides a NAS (CIFS/NFS) interface for backup applications.
  • Configure multiple shares and OST with varying permissions and optimization.
• Optimizes data and replicates a complete copy to the cloud.
  • Maintains most recent backups in local cache for quick restores.
  • Appliance-wide (global) deduplication.
• Provides disaster recovery to physical or virtual appliances.

Figure 1-1:

AltaVault is designed to ingest data from a wide-range of applications. A key feature to deduplication is the ability to automatically detect file formats of the most common backup applications. Backup applications collect files from clients, and package them together in larger files, often referred to as backup images. These files contain meta data and markers inserted by the backup application. The data inserted by the backup application often inhibits the ability to deduplicate the data. Since AltaVault understands the file formats, it is able handle the data inserted into a backup image and provide a high-level of deduplication for them.

The following illustration identifies the typical components of an AltaVault network configuration.
AltaVault Ecosystem

Primary Storage
- NetApp SnapMirror®
- Acronis Backup
- Amanda Network Backup
- Arconserve
- BridgeHead MEDITECH
- CA Cloud Storage for System z
- CommVault DPX
- Commvault (formerly Simpana)
- Commvault IntelliSnap for NetApp
- Dell NetVault & vRanger
- EMC NetWorker
- HP Data Protector
- IBM Spectrum Protect
- Microsoft SQL Server
- NEC NIAS
- OpenStack Cinder NFS Backup Driver
- Oracle RMAN
- Veeam
- Veritas Backup Exec, Enterprise Vault & NetBackup

NetApp® AltaVault™ Cloud-Integrated Storage

Seamlessly integrates into existing infrastructure
Deduplicates, compresses, and encrypts
Caches recent backups locally, vaults everything to the cloud
Stores data in the public or private cloud of choice

Public Cloud
- Amazon Glacier, S3, S3-IA & GovCloud
- AT&T Synaptic Storage as a Service
- Box Cloud Storage
- Google Cloud Storage
- IBM SoftLayer Object Storage
- Internet Initiative Japan
- Microsoft Azure, Cool Blob & GovCloud
- Oracle Storage Cloud Service
- Orange Cloud for Business
- Outscale
- Rackspace
- Swisscom
- Telefonica
- TELUS
- Verizon

Private Cloud
- NetApp StorageGRID® Webscale
- Cloudian HyperStore
- EMC Atmos
- Engage HealthCloud ObjectStore
- IBM Cleversafe
- OpenStack Swift
- Scality RING

Figure 1-2:
2 Lab Environment

The following illustration identifies the typical components of an AltaVault network configuration.

Figure 2-1:

Table 1: Table of Systems

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Operating System</th>
<th>Role/Function</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster1</td>
<td>clustered Data ONTAP 9.1</td>
<td>cluster</td>
<td>192.168.0.101</td>
</tr>
<tr>
<td>cluster1-01</td>
<td>clustered Data ONTAP 9.1</td>
<td>cluster 1 node 1</td>
<td>192.168.0.111</td>
</tr>
<tr>
<td>svm1</td>
<td>Storage Virtual Machine for VMware datastore on NFS</td>
<td>SVM mgmt lif</td>
<td>192.168.0.130</td>
</tr>
<tr>
<td>jumphost</td>
<td>Windows Server 2012 R2</td>
<td>primary desktop entry point for lab</td>
<td>192.168.0.5</td>
</tr>
<tr>
<td>dc1</td>
<td>Windows Server 2008 R2</td>
<td>Active Directory / DNS</td>
<td>192.168.0.253</td>
</tr>
<tr>
<td>netbackup1</td>
<td>Windows Server 2008 R2</td>
<td>Veritas NetBackup for Windows 7.7.3</td>
<td>192.168.0.42</td>
</tr>
<tr>
<td>ocum</td>
<td>Linux appliance</td>
<td>NetApp OnCommand Unified Manager 6.4P2</td>
<td>192.168.0.71</td>
</tr>
<tr>
<td>spcomm</td>
<td>Windows Server 2012 R2</td>
<td>CommVault IntelliSnap for NetApp v11 sp7 CommCell</td>
<td>192.168.0.76</td>
</tr>
<tr>
<td>openstack1</td>
<td>Ubuntu 14.04.2 LTS Linux</td>
<td>OpenStack Swift 2.2.0 Object Storage server</td>
<td>192.168.0.41</td>
</tr>
<tr>
<td>Host Name</td>
<td>Operating System</td>
<td>Role/Function</td>
<td>IP Address</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>altavault</td>
<td>AVA-V virtual appliance</td>
<td>NetApp AltaVault 4.3.1</td>
<td>192.168.0.75</td>
</tr>
<tr>
<td>sgnkp</td>
<td>SUSE Linux Enterprise 10 SP3</td>
<td>Network Time Protocol server for SGWS</td>
<td>192.168.0.9</td>
</tr>
<tr>
<td>sgdc1s3</td>
<td>SUSE Linux Enterprise 11</td>
<td>StorageGRID Webscale 10.3 Storage Node 3</td>
<td>192.168.0.8</td>
</tr>
<tr>
<td>sgdc1s2</td>
<td>SUSE Linux Enterprise 11</td>
<td>StorageGRID Webscale 10.3 Storage Node 2</td>
<td>192.168.0.7</td>
</tr>
<tr>
<td>sgdc1s1</td>
<td>SUSE Linux Enterprise 11</td>
<td>StorageGRID Webscale 10.3 Storage Node 1</td>
<td>192.168.0.6</td>
</tr>
<tr>
<td>sgdc1g1</td>
<td>SUSE Linux Enterprise 11</td>
<td>StorageGRID Webscale 10.3 Gateway Node</td>
<td>192.168.0.11</td>
</tr>
<tr>
<td>sgdc1arc1</td>
<td>SUSE Linux Enterprise 11</td>
<td>StorageGRID Webscale 10.3 Archive Node</td>
<td>192.168.0.12</td>
</tr>
<tr>
<td>sgdc1adm1</td>
<td>SUSE Linux Enterprise 11</td>
<td>StorageGRID Webscale 10.3 Admin Node</td>
<td>192.168.0.10</td>
</tr>
<tr>
<td>sgdc1nas</td>
<td>SUSE Linux Enterprise 11</td>
<td>StorageGRID Webscale 10.3 NAS node</td>
<td>192.168.0.14</td>
</tr>
</tbody>
</table>

Table 2: User IDs and Passwords

<table>
<thead>
<tr>
<th>Host Name</th>
<th>User ID</th>
<th>Password</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>jumphost</td>
<td>DEMO\Administrator</td>
<td>Netapp1!</td>
<td>Domain Administrator</td>
</tr>
<tr>
<td>cluster1</td>
<td>admin</td>
<td>Netapp1!</td>
<td>Same for individual cluster nodes</td>
</tr>
<tr>
<td>svm1</td>
<td>vsadmin</td>
<td>Netapp1!</td>
<td>svm administrator</td>
</tr>
<tr>
<td>openstack1</td>
<td>stack</td>
<td>Netapp1!</td>
<td>openstack root administrator</td>
</tr>
<tr>
<td>openstack1</td>
<td>SSaccount</td>
<td>Netapp1!</td>
<td>swift user account</td>
</tr>
<tr>
<td>ocum</td>
<td>admin or Administrator</td>
<td>Netapp1!</td>
<td>OnCommand Unified Manager Administrator</td>
</tr>
<tr>
<td>sgws</td>
<td>Vendor</td>
<td>Netapp1!</td>
<td>StorageGRID Webscale Vendor Maintenance Admin</td>
</tr>
<tr>
<td>altavault</td>
<td>admin</td>
<td>Netapp1!</td>
<td>AltaVault Administrator</td>
</tr>
<tr>
<td>spcomm</td>
<td>admin</td>
<td>Netapp1!</td>
<td>CommCell Admin Console Local Administrator</td>
</tr>
</tbody>
</table>
3 Lab Activities

This lab contains the following activities and tasks:

- **Navigating and Configuring the AltaVault User Interface** on page 7
- **Select and Configure a Cloud Target** on page 11 Pick one
  - Configure Cloud Settings to OpenStack Swift on page 11
  - Configure Cloud Settings to StorageGRID Webscale on page 23
  - Configure Cloud Settings using S3 on page 36
- **Configure Backup Sources** on page 44 Pick at least one
  - Configure Veritas NetBackup OST to Backup to AltaVault on page 44
  - Configure CommVault IntelliSnap for NetApp to Backup to AltaVault on page 98
  - Configure NetApp ONTAP for SnapMirror Backup to AltaVault on page 134
- **Restore Data from AltaVault** on page 148
  - Restore data using NetBackup on page 148
  - Restore data using IntelliSnap on page 158
  - Restore data from ONTAP SnapShots created by SnapMirror destination of AltaVault on page 169
  - AltaVault Disaster Recovery on page 171
- **Administer the AltaVault Appliance** on page 183
  - Review AltaVault Reports on page 184
  - AltaVault Operations Tasks on page 186
  - Using the AltaVault Command Line Interface on page 191
- **Review Cloud Target Configurations** on page 193 Optional
  - Review OpenStack Swift Configuration on page 194
  - Review the NetApp StorageGRID WebScale Configuration on page 198

3.1 Navigating and Configuring the AltaVault User Interface

In this lab, a basic configuration of the AltaVault appliance has already been performed. User configuration begins where you access the appliance from the web GUI.

A typical initial configuration includes the following steps:

3.1 Login and Initial Configuration

Login to the AltaVault GUI setup wizard to configure the items necessary to get the AltaVault “Healthy” – cloud settings, and encryption key.

1. Launch the IE web browser from the AltaVault Login shortcut on the desktop of the Jumphost.

![Altavault Login](image)

Figure 3-1:

2. Enter the credentials: username **admin**, and password **Netapp1!**.
Figure 3-2:

3. The Home page of the Management Console serves as the main display for critical appliance parameters and status. When it is ready the red test and icons will turn to green to signify the appliance is ready for backup. After configuring a cloud target, the optimization service will need to be set to running in order for the status to change to ready.
4. Navigating the Management Console is done by the use of the cascading menus. Begin to explore the options available by clicking on the options in the menu bar. When complete, click on **CONFIGURE > TOOLS > Setup Wizard**. This will launch the Wizard Dashboard.
Figure 3-4:

5. The Wizard Dashboard appears after you log into the appliance for the first time. The settings available in the wizards are all available from the menu bar, however the Wizards allow for a more simplified configuration experience. For the purposes of lab, the networking and timezone settings configured from the System Settings wizard have been pre-configured. The lab demonstration will continue with the Cloud Settings Wizard.
3.2 Select and Configure a Cloud Target

3.2 Select a cloud target

The AltaVault appliance may have only one cloud target configured at a time. The following sections include three options. You must configure a cloud target in order to continue using AltaVault. Decide on which target to use: OpenStack, SGWS, or AWS S3 and complete the corresponding section. Then skip to the Configure Backup Sources section.

3.2.1 Configure Cloud Settings to OpenStack Swift

Note: You can only configure one cloud target. If you would like to fast forward the OpenStack section, and skip to the section about using StorageGRID Webscale.

NetApp AltaVault provides a simple, efficient and secure way to deliver a cloud-integrated storage solution to an enterprise. The open integration features allow AltaVault to integrate with an existing backup architecture and point to a preferred cloud provider. These steps will demonstrate how easy it is to integrate AltaVault with an OpenStack based Cloud Provider.

About OpenStack Swift in this Lab

In this section the cloud storage service is configured for the appliance. This lab uses OpenStack Swift for (cloud) object storage. A virtual machine (VM) is configured that provides the necessary OpenStack services. Swift is an
object storage service in OpenStack. Keystone, the OpenStack authentication service, is also configured. The other OpenStack services are not required to provide object storage, and are not installed.

Horizon, the web GUI for administration in OpenStack is not installed as it requires additional components. Configuration and administration of OpenStack is, therefore, done using the CLI. For this lab, the basic configuration for a AltaVault account and tenant is already done, so there are no changes required for Swift. For more information on configuring Swift and Keystone see the sections at the end of this guide.

Note: Horizon could be installed; however, it requires other OpenStack services to be running on the system that are not installed. For more information refer to the OpenStack web site.

Each cloud storage vendor or service has unique settings that allow access and inform the AltaVault appliance how to communicate with the storage service. For OpenStack Swift, there are 3 options for the type of information that can be entered. It is required to choose one of the 3 options, and which one depends on which type of credentials were supplied by the administrator of the storage service.

The options for OpenStack are:

• Access Key ID / Secret Key.
• Username / Password.
• Username / API Access Key.

This lab uses Username / Password credentials.

• The deployment guides for AltaVault located on the Field Portal, as well as the deployment guide in the user documentation, describe each of the supported cloud storage services and the options for configuring them.
• It should be possible to copy and paste values from the lab guide into the lab session. If you experience a problem with the copy and paste function, there is a text file located in the administrator’s documents folder on the Jumphost that you can use to cut and paste inside the lab environment.

OpenStack Swift Configuration Details: Cloud Settings

Note: You can copy and paste the settings from a text file that has a shortcut on the Jumphost desktop.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider</td>
<td>OpenStack Object Storage (Swift)</td>
</tr>
<tr>
<td>Authentication</td>
<td>Username / Password</td>
</tr>
<tr>
<td>Username</td>
<td>SSaccount</td>
</tr>
<tr>
<td>Password</td>
<td>Netapp1</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>3eabe7b1bb614e75895703417b62f640</td>
</tr>
<tr>
<td>Authentication URL Path</td>
<td>/v2.0/tokens</td>
</tr>
<tr>
<td>Web Protocol</td>
<td>http</td>
</tr>
<tr>
<td>Hostname</td>
<td>openstack1.demo.netapp.com</td>
</tr>
<tr>
<td>Bucketname</td>
<td>ssstest1</td>
</tr>
<tr>
<td>Port</td>
<td>5000</td>
</tr>
<tr>
<td>Enable Archiving?</td>
<td>No</td>
</tr>
<tr>
<td>Enable Cloud Deduplication?</td>
<td>leave checked (default)</td>
</tr>
<tr>
<td>Enable Cloud CA Certificate?</td>
<td>leave unchecked (default)</td>
</tr>
</tbody>
</table>

1. Click CONFIGURE > TOOLS > Setup Wizard.
2. Click **Cloud Settings**.
3. Click the drop down arrow for **Provider** to reveal the list, and select **OpenStack Object Storage (Swift)**.
4. Temporarily minimize the browser, and click on the text file shortcut on the desktop.

5. Highlight and copy the Tenant ID.
Figure 3-10:

6. Enter the settings from the table above in the “Cloud Settings” form (using OpenStack Swift as example). Remember to use `Netapp1` as the password.
### Cloud Settings Wizard

**Cloud Settings**

- Encryption Settings
- Confirmation
- Finish

<table>
<thead>
<tr>
<th>Cloud Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider:</td>
<td>OpenStack Object Storage (Swift)</td>
</tr>
<tr>
<td>Use Keys from KMIP Server:</td>
<td>No</td>
</tr>
<tr>
<td>Authentication:</td>
<td>Username / Password</td>
</tr>
<tr>
<td>Username:</td>
<td>SSaccount</td>
</tr>
<tr>
<td>Password:</td>
<td>*********</td>
</tr>
<tr>
<td>Tenant ID:</td>
<td>3eabe7b1bb614e75895703417b62f540</td>
</tr>
<tr>
<td>Authentication URL Path:</td>
<td>/v2.0/tokens</td>
</tr>
<tr>
<td>URL Path:</td>
<td>(Only the part of the URL following the hostname.)</td>
</tr>
<tr>
<td>Web Protocol:</td>
<td>HTTP</td>
</tr>
<tr>
<td>Hostname:</td>
<td>openstack1.demo.netapp.com</td>
</tr>
<tr>
<td>Bucket Name:</td>
<td>sstest1</td>
</tr>
<tr>
<td>Part:</td>
<td>(443 is recommended)</td>
</tr>
</tbody>
</table>

---

**Figure 3-11:**

7. Scroll down to confirm that all the field match the table above, then click **Next**.
8. Set the encryption used for backup data stored both locally on the appliance, and in cloud storage. Enter the following passphrase in the “Set Key Passphrase” field: Netapp1.
9. Enter the following passphrase in the “Confirm Key Passphrase” field: Netapp1.
10. Click Next.
The confirmation dialog is shown with a summary. The optimization service must start afterwards, so leave the check box selected to automatically start it. Review the values in the table and if correct, click Save and Apply.
12. Click Exit.
13. Click Exit Wizard.
14. The “Home” page appears with an overall status of the appliance. The Optimization Service will connect to the OpenStack cloud bucket and perform initial test and claim the bucket. This process takes a minute or two to complete, and is a normal operation.

This completes the configuration of OpenStack Swift as a cloud endpoint for Altavault.
3.2.1 Review AltaVault System Logs to view details of configuring cloud target

It is possible to see the communication with the cloud storage service by reviewing the system log. The log shows details of the operation of the appliance. It also shows any reasons for failure if the optimization service is unable to start (such as incorrect credentials), or the inability to connect to the service due to name resolution problems.

1. Review the system log using the main menu, MAINTENANCE > LOGS > System Logs.

   ![Figure 3-18](image1)

2. Click Last on the right side to skip to the most recent log entries. Browse and review the entries to get an idea of the type of messages that are typically logged on a system.

3. Return to the main view by clicking Home in the upper left part of the window.

   ![Figure 3-19](image2)

The main view shows a high level of the operational status of the appliance. It is possible to go to the management options for each section by clicking on the > arrow beside the title.

This is the end of the Cloud Settings portion of this lab. The next lab activity is the Configure the Backup Sources section.

3.2.2 Configure Cloud Settings to StorageGRID Webscale

**Note:** You can only configure one cloud target. If you have successfully configured OpenStack Swift as a cloud target, you can skip to the Configure Backup Sources section.
NetApp AltaVault provides a simple, efficient and secure way to deliver a cloud-integrated storage solution to an enterprise. The open integration features allow AltaVault to integrate with an existing backup architecture and point to a preferred cloud provider. Combined with NetApp StorageGRID Webscale, AltaVault brings software-defined object storage and intelligent policy-driven data management to unstructured data for a better managed and secure hybrid cloud environment. The following steps demonstrate how easy it is to integrate AltaVault with StorageGRID Webscale.

**NetApp StorageGRID Webscale Configuration Details: Cloud Settings**

*Note:* You can copy and paste the settings from a text file from the shortcut on the Jumphost desktop.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Access Key</td>
<td>Q7420K4UI58EBFDH89X3</td>
</tr>
<tr>
<td>Account Secret Access Key</td>
<td>03U5a3lytaPkdCA14A0/QjHcH+k7dcQSbxD4xx8e</td>
</tr>
<tr>
<td>Web Protocol</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Hostname</td>
<td>sgws.demo.netapp.com</td>
</tr>
<tr>
<td>Bucket Name</td>
<td>altavault-backup</td>
</tr>
<tr>
<td>Port</td>
<td>8082</td>
</tr>
</tbody>
</table>

1. Click **CONFIGURE > TOOLS > Setup Wizard**.

2. Click **Cloud Settings**.

![Figure 3-20:](image)

![Altavault Setup Wizard](image)
3. Click the drop down arrow for **Provider** to reveal the list, and select **NetApp StorageGRID Webscale**.
4. Temporarily minimize the browser, and click on the text file shortcut on the desktop.

5. Highlight and copy the **ACCOUNT ACCESS KEY IDENTIFIER**.
6. Enter the settings from the table above in the “Cloud Settings” form (using NetApp StorageGRID Webscale as example).

   **Note:** This lab uses HTTPS for the Web Protocol, as a production environment would use. However, to overcome some in-lab CA certificate limitations, the AltaVault has a setting that will not verify certificates. As a workaround you have to manually start the Optimization Service.
7. After scrolling down to confirm that all the fields match the table above, click Next.
8. Set the encryption used for backup data stored both locally on the appliance, and in cloud storage. Enter the following passphrase in the “Set Key Passphrase” field: Netapp1.

9. Enter the following passphrase in the “Confirm Key Passphrase” field: Netapp1.

10. Click Next.
11. The confirmation dialog is shown with a summary. The optimization service must start afterwards. Normally you would leave the check box selected to automatically start it, however in this lab you must uncheck this option to manually start it because of an in-lab certificate issue. **Uncheck** the restart option.

12. Review the values in the table, and if correct click **Save and Apply**.
Figure 3-28:

13. Click Exit.
Note: If you see an error you may have left the “Restart” option checked, and because of the certificate issue mentioned previously the Service could not start. Continue with the lab.

14. Click Exit Wizard.
Figure 3-30:

15. The “Home” page appears with an overall status of the appliance. The Optimization Service will show that the service is stopped and the status is not ready. In addition you will see critical alarms set. To correct the alarms, go to MAINTENANCE > APPLIANCE > Service.

Figure 3-31:

Figure 3-32:

17. Click Home.

Figure 3-33:

18. Because this is a lab environment, it might take a short period of time to refresh.
This completes the configuration of NetApp StorageGRID Webscale as a cloud endpoint for Altavault.

3.2.2 Review AltaVault System Logs to view details of configuring cloud target

It is possible to see the communication with the cloud storage service by reviewing the system log. The log shows details of the operation of the appliance. It will also show a reason for failure if the optimization service is unable to start because of incorrect credentials, or the inability to connect to the service due to name resolution problems.

1. Review the system log using the main menu, MAINTENANCE > LOGS > System Logs.
2. Click **Last** on the right side to skip to the most recent log entries. Browse and review the entries to get an idea of the type of messages that are typically logged on a system.

3. Return to the main view by clicking **Home** in the upper left part of the window.

Figure 3-36:

The main view shows a high level of the operational status of the appliance. It is possible to go to the management options for each section by clicking on the > arrow beside the title.

The Cloud Settings section of this lab is complete. Now move to the **Configure the Backup Sources** section.

### 3.2.3 Configure Cloud Settings using S3

This section offers an alternate way to configure cloud settings using Amazon Web Services S3 free tier account. Amazon offers a “free tier” for several low utilization services to help users become more familiar with the service at little, or no cost. Free services are offered through the first year for a new account. See the AWS web site for more information about accounts and free tier access.

**Note:** To use this section you must not have configured Swift, or SGWS in the previous sections. If you completed using another cloud target, request a new lab and skip to this section.

Free tier accounts require a credit card and a phone call-back before an account is enabled. You should follow the recommendations of the legal team for your company for using external services.
Use these basic steps for testing access. Do not use these procedures to set up a product environment. Consult with your organizations expert for AWS services, review AWS documentation and determine the best solution for creating and maintain a secure cloud account with policies that follow company legal requirements.

**Overall steps**

1. Create a new account to get free tier.
2. Create a bucket to store data.
3. Create an account for the appliance.
4. Save access credentials.
5. Assign access permissions to allow user full access to bucket.

1. To begin log into your AWS account and click on S3 under Storage & Content Delivery.

**Figure 3-37:**

2. Press Create Bucket.
3. Create a bucket.
4. When you create a bucket, the bucket name must be unique. The simplest solution is to use your company or some other unique information as part of the bucket name.

5. Your bucket should look similar to this.
6. From the Dashboard under Users, create a user account for access to the bucket.

Figure 3-40:

Figure 3-41:
7. Enter a unique User Name.
8. Press Create.

9. When the account is created, the access information that is required by the AltaVault to connect to the bucket is displayed. Copy the access information.
10. Click Download Credentials to have a backup copy.
11. Assign access permissions to the bucket for the account you created. Under Policies you will begin the process of attaching the policy to the account.

   **Note:** This example gives full access for all buckets in the account to the user in order to simplify the steps. Full access is not required. Review any access policies with your organization's security specialists.
12. After adding a check to the checkbox, press Attach Policy.

**Figure 3-45:**

13. In the AltaVault GUI, from the main menu, choose **CONFIGURE > TOOLS > Setup Wizard**.
14. On the “Wizard Dashboard” choose **Cloud Settings**, and follow the prompts to configure AWS S3, set the encryption, and start the service.

    **Note:** For the AWS S3 public cloud target you will follow the identical steps in the Cloud Settings wizard as in the section on setting up an S3 target to the StorageGRID Webscale private cloud target.
3.3 Configure Backup Sources

3.3 Configuring Backup Sources
In order to backup to a cloud target, the AltaVault Appliance must have a backup source with data to backup configured. You may choose to do one, or all of the following three options, but you must pick at least one option from NetBackup with OST, CI4N, or SnapMirror from ONTAP.

3.3.1 Configure Veritas NetBackup OST to Backup to AltaVault

Veritas OpenStorage Technology (OST) is an plugin capability for NetBackup that allows integration with storage appliances. The AltaVault OST plug-in allows the NetBackup server to communicate with and offload operations to the AltaVault appliance. The OST protocol provides control features, as well as a data transfer mechanism. The data transfer portion of OST allows for a high speed data transfer without the requirement for tuning NetBackup media server settings. The control features provide the ability for NetBackup to have catalog awareness when a backup has fully replicated to cloud storage using the NetBackup Storage Lifecycle Policy (SLP) and optimized duplication.

The AVA OST plug-in is installed on a media server and currently supports Windows, Red Hat Linux and newer versions of the NetBackup appliance. See the IMT for the most recent supportability matrix.

For more information on AltaVault and OST refer to the product documentation on the support site and the field portal.
3.3.1 Configure Altavault for OST

OST support in Altavault is new for version 4.2, and enables OST share creation from the UI.

1. From the Altavault interface, select **Configure > Storage > OST**.

---

**Figure 3-48: NetBackup OST Optimized Duplication of Backup Images**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Backup</td>
<td>Backup job runs to Altavault Regular OST share, data is written to cache and replication to cloud starts, backup job completes</td>
</tr>
<tr>
<td>2 – SLP Duplication Request</td>
<td>SLP request to Altavault to duplicate the image(s) written in the previous backup job</td>
</tr>
<tr>
<td>3 – SLP Duplication Response</td>
<td>Altavault duplicates the meta data only, then waits until the replication of the backup image to cloud storage is complete. When the new optimized backup image data is stored in cloud, Altavault tells NetBackup the duplication of the image is complete</td>
</tr>
</tbody>
</table>
2. Click Add OST share.
3. Enter: ostshare1regular.
4. Leave “Type” as Regular.
5. Click Add.
6. Click **Add OST User**.
7. Enter “User Name:” **ostuser**.
8. Enter “Password:” **netapp1**.
9. Enter “Password Confirm:” **netapp1**.
10. Click **Add User**.
11. Now repeat the process for a second share, click **Add OST Share**.
12. Enter “Share Name:” `ostshare1cloud`.
13. Choose “Type” as **Cloud**.
   
   **Note:** “Cloud” types cannot be pinned, only regular OST shares can be pinned (held) in local cache.

14. Click **Add**.

---

15. Click **Add OST User**.
16. Enter “User Name:” `ostuser`.
17. Enter “Password:” `netapp1`. 
18. Enter “Password Confirm:" netapp1.
19. Click Add User.

20. Click HOME.
3.3.1 Login to the NetBackup Server

Use the Remote Desktop application on the Jumphost to login to the NetBackup server. When the remote desktop session is established, you may have to arrange the window of the remote desktop session to show the scroll bars in the browser window.

Start a remote desktop session to the NetBackup server.

After connecting to the NetBackup server, launch the Administration console to perform the steps in this section.

1. Open the Remote Desktop Console Manager application using the icon on the taskbar.

2. Double-click on the netbackup server listed in the left pane to open that session.

3. When you log in, you will see the desktop of the NetBackup server. The desktop may show the Server Manager tool window. If so, it is okay to close or minimize that window to show the desktop. Depending on your screen size you may need to move and resize the remote desktop window to be able to access the scroll bars. For smaller windows, use the scroll bar to move the NetBackup server window to fully access the taskbar and buttons in the configuration dialogs. HINT:
Tip: To maximize, make sure you are in full screen on the Remote Desktop Connection Manager before you connect to the server. If you are already connected, log off, then maximize RDCMAN and reconnect for full resolution.

4. Click the **Administration Console** icon on the desktop to launch the console.

![Administration Console Icon](image)

**Figure 3-58:**

5. Enter the Password **Netapp1**!

6. Click **Login**.
Figure 3-59:

7. You are presented with the NetBackup Administration Console.
3.3.1 Configure NetBackup OST

1. Click on Configure Disk Storage Servers.

2. Select OpenStorage.

3. Click Next.
4. For the “Media Server” field, choose the netbackup1.demo.netapp.com server.
5. For “Storage server type” field, enter NetAppAltaVault (this needs to be exact, as it is case sensitive).
   The “Storage server name” field is a combination of the share that was created on the AltaVault and the AltaVault host name, separated by an underscore “_”. The host name can be either the short hostname, the fully qualified hostname, or the IP address. We recommend that you use the host name, if it is not configured in DNS, then add it to the hosts file rather than using the IP address as IP addresses can change over time.
6. Enter the following for the regular OST share you previously created: ostshare1regular_altavault.
7. Enter the “User name”: ostuser.
8. Enter the “Password”: netapp1.
10. Click Next.
Figure 3-63:

11. The storage server will be configured in netbackup. Click Next.
12. The status will be shown, and the dialog will continue with setting up the disk pool. Click **Next**.
13. The default type will be **Backup**, which is correct.
14. Click the checkbox for **Replication source**.
15. Click the checkbox for **Isu** to select the disk for the pool.
   
   **Note:** A regular OST share can only be a replication source. A cloud OST share can only be a replication target.

16. Click **Next**.
Figure 3-66:

17. Enter a name for the disk pool – ostshare1regular_altavault.
   We recommend that you name them so that it is easy to distinguish a regular share from a cloud share. Since many shares are supported, the name should also match the share so it is easy to map them at a later point.

18. Leave all other settings as default, click Next.
19. Click **Next**.
20. Click **Next** to create a storage unit. A storage unit is how NetBackup maps the storage to the backup policy/SLP.
21. Use the default name for the storage unit.
22. Leave the default, or choose Only use the selected media servers: netbackup1.demo.netapp.com server. Since there is only one media server it will use the one.
23. Change the “Max concurrent jobs” to 5.
24. Keep the default fragment size of 524288 MB.
25. Click Next.

**Note:** The maximum concurrent jobs can be adjusted to match the specific environment. A single AVA can support 256 concurrent streams (in 4.2). When setting up multiple shares and multiple media servers, the maximum concurrent jobs settings can be used to limit the streams. For example, if you are using 2 media servers with equal number of jobs, you can divide 256 by the number of STUs (and shares) created, then by the number of media servers (2) to get the max concurrent streams. We recommend that you stay below this value, and possibly leave a
small margin. After testing the environment you can adjust the numbers to best fit the actual jobs and schedules running.

For the Maximum fragment size, 20 GB is the recommended starting point. You can adjust this to fit the specific environment. See the NetBackup Tuning Guide for recommendations. A smaller value will result in a larger number of fragments the catalog must track. A larger number may impact restore operations. For example, by requiring larger files to be prepopulated on the AltaVault when not located in cache.

---

**Figure 3-70:**

26. Click **Finish**.
You have successfully completed the NetBackup Disk Pool Configuration Wizard.

You may view or change the current configuration settings within Device Management or Storage Unit Management.

**Figure 3-71:**

27. Repeat the previous steps to configure the cloud share as a replication target. Click on **Configure Disk Storage Servers**.
28. Select **OpenStorage**.
29. Click **Next**.
30. For “Media server”, choose the netbackup1.demo.netapp.com server.
31. For “Storage server type”, enter NetAppAltaVault (this needs to be exact, as it is case sensitive).
32. Enter the following for the regular OST share that was previously created:
   ostshare1cloud_altavault.
33. Enter the “User name:” ostuser.
34. Enter the “Password:” netappl.
35. Confirm the Password: netappl.
36. Click Next.
Figure 3-74:

37. The storage server will be configured in netbackup. Click Next.
The status is displayed, and the dialog continues setting up the disk pool. Click **Next**.
39. The “Disk Pool” default type will be “Backup”, which is correct
40. Select Replication target.
41. Click the checkbox for Isu to select the disk for the pool.
42. Click Next.
Enter the “Disk Pool name” as ostshare1cloudDP.
Leave all other settings as default, and click Next.
45. Click **Next**.
Figure 3-79:

46. Click **Next**.
Use the default name for the “Storage unit name”.

48. Leave the default, or select **Only use the selected media servers**, and select the **netbackup1.demo.netapp.com** server. Since there is only one media server it will pick that server.

49. Change the “Maximum concurrent jobs” to **5**.

50. Leave fragment size at the default.

51. Click **Next**.
52. Click Finish.
3.3.1 Create a Storage Lifecycle Policy (SLP)

1. In the left pane, expand **Storage**.
2. Right click on **Storage Lifecycle Policies**, and choose **New Storage Lifecycle Policy**.
3. Enter a name for the “Storage Lifecycle policy” \textit{s1p1}.
4. Click \textit{Add} to add an operation.
5. Leave the default of **Backup** for the operation.
6. Select the storage unit that represents the regular OST share.
7. It is possible to choose a retention to represent how long you want to keep the local cache copy of the backup. The cache needs to be sized appropriately for a given environment, and the Altavault sizing tool can help with the design and model selection. Click **OK**.
8. Leave the backup operation you just selected in the dialog, and click \textbf{Add} again. Clicking “Add” with backup selected will create a second operation that occurs after the first operation completes. You can also use the arrow buttons to chain together operations.
9. Since this is the second operation, and it defaults to duplicate, leave the default selected. Choose the storage unit that represents the cloud OST share.
10. Again, it is possible to set a different retention for the cloud copy. In most instances this will be the longer term retention, for example 1 month, 1 year, or longer. Click OK.
11. The SLP is now configured correctly to perform a backup to the regular OST share, then a duplication to the cloud share. Click OK.
12. Now create a backup policy and associate it with the SLP. Click on **Policies** to show the policies information.
13. Right click on the **netbackup1.demo.netapp.com** server in the Policy section.
14. Choose **New Policy**...
15. Enter a “Policy name:” – `nbulpolicy`.
16. Click OK (optionally you can use the wizard).

---

17. On the first tab, for “Policy storage:”, choose the SLP you created, `slp1`.
18. Click the Schedules tab.
Figure 3-91:

19. Click New.
20. For “Name:” enter `weekly_full`.
21. Leave the rest of the attribute values as default, and click OK (typically you would define backup windows, but you are just doing a manual backup).
22. Click the Clients tab.
23. Click **New**.
24. In the “Client name:” field enter netbackup1.demo.netapp.com.
25. Check the Detect client operating system box.
26. Click OK.
27. Click the **Backup Selections** tab.

![Figure 3-97:](image_url)  

28. Click **New**.
29. Click **Browse**...
Figure 3-99:

30. Expand netbackup1.demo.netapp.com in the left pane.
31. Expand the C: drive.
32. Select the BackupData folder.
33. Click OK.
Figure 3-100:

34. Click **OK** to close the dialog window.
Figure 3-101:

35. Click OK to close the Policy window.
3.3.1 Perform a Backup using NetBackup OST

1. Find the nbu1policy, and right click it.
2. Choose Manual Backup....

Figure 3-102:
3. Click OK.
4. Click on the **Activity Monitor** to check the status of the jobs.
5. Once the backup completes successfully, the blue man will display.
6. Double click the **Backup** job to see the job info, and job details.
7. Examine the job details, then click **Close**.
8. Shortly after the first job has completed, the Storage Lifecycle Policy will use the OST plugin to communicate with AltaVault for the second backup job that will become visible in the Activity Monitor. This type will be listed as “Duplication.”

3.3.2 Configure CommVault IntelliSnap for NetApp to Backup to AltaVault

3.3.2 Configure an SMB Share in AltaVault

AltaVault requires an SMB share to communicate with (non-OST) backup applications on Windows. These steps describe the basic configuration process for a share. When configuring for a Unix or Linux backup server, the steps are similar for creating an NFS share.

1. From the main menu select CONFIGURE>STORAGE>SMB.
2. Scroll down to the "Domain" section. Enter \texttt{demo.netapp.com}, with the Username \texttt{Administrator} and the password \texttt{Netapp1!}.

3. Click \texttt{Join Domain}. 
4. After a few seconds the AltaVault appliance joins the domain, and a note appears regarding the DNS settings. The DNS settings should be pre-configured. Optionally, you can confirm this by going to CONFIGURE > NETWORKING > Host Settings and reviewing the DNS Settings. Then return to the SMB section by selecting CONFIGURE > STORAGE > SMB.
5. Click the **Add SMB Share** button at the top of the section that lists the shares.

### SMB

**Pinned Data Information**

- Currently Pinned: 0.00%
- Maximum Pinnable Limit: 50%

5. Enter the following in the “Share Name” field: **CI4Nshare**.
6. Enter the following in the “Local Path” field: **CI4Nshare**.
7. Enter the following in the “Comment” field: **Share for CommVault IntelliSnap for NetApp**.
8. Leave the other values at their default settings. Click the **Add** button.

**Figure 3-111:**

6. Enter the following in the “Share Name” field: **CI4Nshare**.
7. Enter the following in the “Local Path” field: **CI4Nshare**.
8. Enter the following in the “Comment” field: **Share for CommVault IntelliSnap for NetApp**.
9. Leave the other values at their default settings. Click the **Add** button.

**Figure 3-112:**
10. The GUI updates with the new share added and expanded.

11. Click **Home** in the top left of the browser window to return to the main view.

There are several options to optimize each share created on the appliance. Use “disable dedupe” and “disable compression” to reduce the overhead required to process data when you know the data set you are writing to the share does not dedupe or compress well. This saves processing time for the appliance.

The remaining options, “early eviction” and “pin share”, adjust the cache behavior and are mutually exclusive (only one can be set). These features allow an administrator to choose how a data set is managed in the local cache on a per share basis. Data that should be removed from the cache before data from a standard share should be set for early eviction. Early eviction means that when the cache has reached a high water mark, data that has been replicated to the cloud will be removed from the local cache to create free space for new incoming data. Typically, the selection is made for oldest data first, however, early eviction allows the administrator to configure data that is less likely to be needed for a restore to be evicted before data in other shares, that are not set for early eviction.

Pinning a share produces the opposite behavior where data that is pinned will be retained on the appliance. There is an appliance-wide setting to choose the maximum limit for pinnable data. For more details on configuring share options, including setting permissions using Active Directory, refer to the *AltaVault User’s Guide* on the NetApp support site product documentation section.

12. Confirm the share is accessible, by first opening the Windows File Explorer on the Jumphost.

![Figure 3-113](image)

13. Navigate to `\altavault`, and observe the share is available.

14. Open the folder **CI4Nshare**.
Figure 3-114:

15. Right-click, and create a text file. (Example name: “Test File for SMB Share write operation.txt”).

Figure 3-115:

16. Give the file a specific name, as you will reference it in the DR section later in this document.

3.3.2 Connect to SnapProtect CommCell Server

1. Launch the Remote Desktop Manager.
2. Double-click on **spcomm**.

3. From the desktop of the SPCOMM server, click on the **CommVault Logo** shortcut to launch CommVault IntelliSnap for NetApp.

### 3.3.2 Add a Disk Library to the MediaAgent on AltaVault

A library is used by a MediaAgent to communicate and store backup data on a specific device. For the purposes of this configuration, the library created will be configured to point to an AltaVault CIFS share, rather than a local disk volume.

1. Select the **Storage** tab from the top menu, then click on **Expert Storage Configuration**.

2. Identify the MediaAgent to use, and click the **Add** button to select it.
3. Click **OK** to continue.
4. Click **OK** to accept the Information dialog box.

5. When the “Library and Drive Configuration” panel appears, select the Libraries icon, right click it, and select **Add > Disk Library**.
6. Identify the Library name you wish to use, then click **OK**.

7. Provide a base folder name to store the data in. In the Sharing Folder Properties section:
   - If the AltaVault appliance is configured with local permissions, provide the fully qualified CIFS share name to the AltaVault target in the “Local Path” section.
- If the AltaVault appliance is configured with Active Directory, select the **Network Path** section instead. Provide Windows login credentials, and the fully qualified CIFS share name to the AltaVault target.
- Select the “MediaAgent”: **spcomm**.
- Select **Network Path**.
- “Connect As:” **DEMO\Administrator**
- “Password:” **Netapp1!**
- “Folder:” \\altavault\CI4Nshare\disklibrary
- Click **OK** to complete library creation.

![Figure 3-125:](image)

8. Close the window for the “Library and Drive Configuration”.

---

**Figure 3-125:**

8. Close the window for the “Library and Drive Configuration”.
9. From the main console view, expand **Storage Resources > Libraries**. Right click the library just created. Select **Properties**.
10. When the “Properties” window appears, select the **Mount Paths** tab.
11. Set the **Allocate Number of Writers** value of 5 for the “Mount Path Allocation Policy” of the Library.
12. Click **OK**.
3.3.2 Create a Storage Policy to Point to AltaVault

Storage policies act as the primary channels through which data is included in data protection and data recovery operations. A storage policy forms the primary logical entity through which a subclient, or instance, is backed up. Its chief function is to map data from its original location to a physical media. In this example you create a new Storage Policy. For SnapProtect servers with existing storage policies where you would like to add AltaVault, it is possible to modify the existing storage policy and create a copy that uses the previously created disk library that is located on AltaVault.

1. In the “Policies” section of the CommCell console, expand Policies > Storage Policies. Right click, and select New Storage Policy.
2. Provide a unique storage policy name.
3. Click **Next**.
4. Select the previously created library to use for this storage policy.
5. Click Next.
6. Select the “MediaAgent” from the drop down list.
7. Click **Next**.
8. Choose the appropriate retention type and period of time. Check **Retain by jobs** to save that number of snapshots on the volume.

9. Click **Next**.
10. Ensure the Software Encryption option is unchecked, then click **Next**.
11. If prompted for Deduplication, **Uncheck** the Yes checkbox to disable deduplication. You will not need CI4N to manage the deduplication since it is handled by ONTAP.

12. Click **Next**.
13. Select the OnCommand Unified Manager (ocum) system for this policy.
14. Click Next.
15. Review the summary, and click **Finish** to complete the Storage Policy creation.
16. Right click on the storage policy created in the previous step, and choose Properties.

17. Click the SnapShot tab.
18. By default Disable Backup Copy is selected. Select Enable Backup Copy to allow streaming copies of the snapshots.
19. Click OK.
Next, create a Storage Policy operation to copy the snapshot data to the disk library created for the AltaVault.

1. Right-click on the previously created storage policy, choose All Tasks, then Create New Copy.

**Note:** If prompted with a warning, click OK.
2. Enter a name for the copy, for example: `ava-copy`.
3. Add a check next to **Enable Inline Copy** option. (If prompted with a warning, click **OK**).
4. From the drop down menus choose the “Library:” that was created for the AltaVault share.
5. From the drop down menus choose the “MediaAgent:” that will perform the copy.
6. Click the **Retention** tab.
7. Optionally, set the retention for the copy stored on the AltaVault (in the cloud). It is also possible to set extended retention to choose specific copies, such as the monthly full. For more information see the SnapProtect documentation.

8. Click OK.
Figure 3-144:

9. Click **OK** to accept the Default Schedule.
10. The following screen displays the completed storage policy with the primary Snapshot copy, and the AltaVault (cloud) copy.

![Diagram showing completed storage policy with primary Snapshot copy and AltaVault copy](image)

**Figure 3-146:**

### 3.3.2 Assign Storage Policy to Subclient

Prior to running a backup you must first associate the new Storage Policy with the default subclient.
1. In the CommCell Browser directory, navigate to Client Computers > cluster1 > NAS > defaultBackupSet.
2. Right-click on the Subclient Name labeled default, and select Properties.
3. Click the Storage Device tab.
4. In the sub-tab for **Data Storage Policy**, select the “Storage Policy:” created in the previous section.

5. Click **OK**.
3.3.2 Perform a Manual Backup

To test SnapProtect with the AltaVault appliance, you can run a manual backup of a client that uses a storage policy configured in the previous step.

1. Expand the client to back up. In this case, it is the filer that contains the NAS volume to back up. Open the defaultBackupSet to show the subclients.
2. Right click on the subclient file to back up, and select Backup.
3. Use the defaults of **Full** Backup Type, and **Immediate** Job Initiation.
4. Click the **Advanced** button to show the options. Do **NOT** click **OK** yet.
5. Uncheck the **Skip Catalog Phase for SnapProtect Operations** checkbox so that data indexing is performed.

6. Add a check to **Create Backup Copy immediately**.

7. Click **OK** to close the “Advanced Backup Options” dialog.

![Advanced Backup Options dialog](image)

**Figure 3-152:**

8. Click **OK** to initiate the backup.
9. Use the **Job Controller** view within the left tree of the CommCell Console to monitor and control backup jobs. The current running backup jobs are reported under the right panel of the window, and you can access a detailed view by right clicking on the job name and selecting **Details**.

10. After the primary backup completes, you will notice in the Job Controller that the Backup Copy will start as the next Job ID.
11. At any point you can right-click on a job to see events associated with that job, or click on the Event Viewer tab to see the last and previous jobs that completed.
4. Enter This is test 1 before backups to test1.
5. Save and close the file.
6. Launch PuTTY from the desktop.

Figure 3-161:

7. Open the PuTTY session to altavault.
8. Log into the AVA and ping the Intercluster LIF IP to ensure connectivity, then close the session to AVA.

```
ping 192.168.0.121
```

---

3.3.3 Configure AltaVault for SnapMirror

1. Log into the AltaVault with `admin` and `Netapp1!`. 

---

Figure 3-162:

Figure 3-163:
2. Click **Sign In**.

![NetApp AltaVault login interface](image)

3. Navigate to **CONFIGURE > STORAGE > SnapMirror**.
4. Click **Enable**.
SnapMirror Service

Status: **Disabled**

![Image](image1.png)

**Figure 3-166:**

5. Navigate to **MAINTENANCE > APPLIANCE > Service**.

---

SnapMirror Service

Status: **Enabled**

![Image](image2.png)

**Figure 3-167:**

6. Click **Restart**.
7. Return to CONFIGURE > STORAGE > SnapMirror.

8. Scroll down to the “Whitelist IP” section, and click on Add Whitelist IP.
**WhiteList IP**

8. Add WhiteList IP

9. Enter the IP address for the Intercluster SnapMirror LIF on cluster1: **192.168.0.121**.

10. Click **Add**.

---

**Figure 3-171:**

3.3.3 **Configure ONTAP cluster for SnapMirror to AltaVault**

1. Open PuTTY.
2. Open the PuTTY session to `cluster1`.

![PuTTY Configuration](image)

**Figure 3-173:**

3. To add a source snapshot policy issue the following command:

```
snapshot policy create -policy snap_policy1 -prefix1 hourly -snapmirror-label1 ava_hourly -count1 24 -schedule1 hourly -prefix2 daily -snapmirror-label2 ava_daily -count2 7 -schedule2 daily -prefix3 weekly -snapmirror-label3 ava_weekly -count3 5 -schedule3 weekly -enabled true -comment "Source Snapshot Policy"
```

4. To check the policy issue the following command:

```
cluster1::> snapshot policy show
Vserver: cluster1
Policy Name | Number of Schedules | Enabled | Comment
-------------|---------------------|---------|-----------------
default      |                     | true    | Default policy with hourly, daily & weekly schedules.
              | hourly              | 6       | hourly
              | daily               |         |               
              | weekly              |         |               
```

---

**AltaVault Backup to Cloud Setup and Administration**

© 2017 NetApp, Inc. All rights reserved. NetApp Proprietary
5. To assign the policy to the source volume issue the following command and press y:

```
cluster1::> volume modify -volume vol2_CIFS_volume -snapshot-policy snap_policy1
```

Warning: You are changing the Snapshot policy on volume vol2_CIFS_volume to snap_policy1. Any Snapshot copies on this volume from the previous policy will not be deleted by this new Snapshot policy.

Do you want to continue? {y|n}: y

Volume modify successful on volume vol2_CIFS_volume of Vserver svm1.

6. To add a new SnapMirror policy issue the following command:

```
snapmirror policy create ava_policy1 -vserver svm1 -type vault -comment "AVA Vault Policy"
```

7. To add a rule to the policy for hourly retention issue the following command:

```
snapmirror policy add-rule -vserver svm1 ava_policy1 -snapmirror-label ava_hourly -keep 8
```

8. To add a rule to the policy for daily retention issue the following command:

```
snapmirror policy add-rule -vserver svm1 ava_policy1 -snapmirror-label ava_daily -keep 100
```

9. To add a rule to the policy for weekly retention issue the following command:

```
snapmirror policy add-rule -vserver svm1 ava_policy1 -snapmirror-label ava_weekly -keep 50
```

10. Create a SnapMirror relationship between the cluster and altavault. Assign the previously created snapmirror policy, otherwise the xdp default is used, by issuing the following command:

```
snapmirror create -source-path svm1:/vol/vol2_CIFS_volume -destination-path 192.168.0.75:/share/svm1_vol2 -type XDP -policy ava_policy1 -schedule hourly
```

11. To display the status issue the following command:

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

12. To initialize the SnapMirror relationship and begin transferring data, issue the following command:

```
snapmirror initialize -source-path svm1:/vol/vol2_CIFS_volume -destination-path 192.168.0.75:/share/svm1_vol2
```
13. To display the status issue the following command:

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

```
Source Path | Type | Destination Path | State | Relationship | Total | Progress | Healthy | Updated
----------- ---- --------------- -------- -------------- ------- -------- ------- --------
svm1:vol2_CIFS_volume | XDP | 192.168.0.75:/share/svm1_vol2 | Uninitialized | | | |
```

3.3.3 Create SnapShots

In this section, we will manually create backups (snapshots) and transfer them to the AltaVault (snapmirror update). The vault policy created will transfer the scheduled snapshots. We are creating manual snapshot backups to demonstrate the restore process without having to wait on the scheduled snapshots.

1. Make sure you created and added a line to the “test1” file on vol2, do a `dir` from command line to verify it is named “test1.txt”.
2. To perform a backup of this file issue the following command:

```
snapshot create -vserver svm1 -volume vol2_CIFS_volume -snapshot snap1
```
3. To update the SnapMirror to put the snapshot on the destination (AltaVault) issue the following command:

```
snapmirror update -source-path svm1:vol2_CIFS_volume -destination-path 192.168.0.75:/share/svm1_vol2 -s snap1
```
4. Return to the Windows Explorer window at location `\svm1-cifs.demo.netapp.com\vol2`.
5. Open `test1.txt`, and add a second line `This is my second backup of test1`.
6. Save, and close the text file.

7. To create a second snapshot issue the following command:

```
snapshot create -vserver svm1 -volume vol2_CIFS_volume -snapshot snap2
```

![Figure 3-174:]

```
File | Home | Share | View
----- |------ |------- |------
Name |       |        |
BackupData |        |        |
test1

This is test 1 before backups

This is my second backup of test1
```

```
File | Edit | Format | View | Help
----- |------ |-------- |------ |------

This is my second backup of test1
```
8. To perform a SnapMirror update to move the new snapshot to the destination (AltaVault) issue the following command:

```
snapmirror update -source-path svm1:vol2_CIFS_volume -destination-path 192.168.0.75:/share/svm1_vol2 -s snap2
```

9. Return to the AVA Web UI in the browser and return to **CONFIGURE > STORAGE > SnapMirror**. Scroll down to SnapMirror Shares and observe the SnapMirror destination is listed.

10. Click on the **name of the share** to view the snapshots transferred.

![Part of the interface](image)

**Figure 3-175:**

11. Make sure snap1 and snap2 are listed.
3.4 Restore Data from AltaVault

This chapter focuses on lab activities that restore data from backups to the AltaVault performed in previous lab activities dealing with backup operations. Whether data is a local file or in a NetApp Volume, the preferred enterprise backup solution can restore data from the AltaVault cache. In cases where the cache is not available on the AltaVault, either from data rolloff, or a DR scenario in AltaVault, with a simple restore of metadata the AltaVault can pull from the cloud to restore.

3.4.1 Restore data using NetBackup

There are two ways to read the data back from the cloud. The first is to use the backup application to perform a restore and let it request the data. When a file is read and the data no longer exists locally, the AltaVault will read the data from the cloud and send that to NetBackup. This is not always the ideal way to recover data, specifically in the case where the connection to the cloud is slow.

The second method is the use the pre-population feature of the AltaVault appliance. It is possible to list the image files needed for a given restore, or from a recent full backup using the NetBackup catalog query tools. When you know the image files that need to be recovered from, it is possible to go in the Prepopulation page of the AltaVault GUI and select those files to download from the cloud. After the download is complete, the restore operation will restore from the local cache of the appliance.

1. Open the Remote Desktop Connection Manager.
2. Enter session to NetBackup server.

3. From the NetBackup Server, open Windows Explorer.

4. Confirm that the folder “C:\Restore” does not exist on the NetBackup server.
5. Open the **Backup Archive and Restore** console.

![Figure 3-181](image)

6. Click **Select for Restore**.

   A window opens showing the list of backups done. If a dialog is shown saying that there are not backups for this client, navigate to **File > Specify NetBackup Machines > Policy Type** to add the client name you entered when creating the policy. NetBackup is hostname specific; if you gave the short name it will see the fully qualified name as a different client.

![Figure 3-182](image)

7. Expand the **C:** drive in the **All Folders** window pane (bottom left section) to locate a file to restore.
8. Check the box next to the **BackupData** folder.
9. From the main menu choose **Actions > Restore**.
10. Click the **Restore everything to a different location** radio button.
11. In the **Destination**: box enter `c:\Restore`.
12. Click **Start Restore**.
13. To view the restore process, choose Yes when prompted to view the progress.
14. Click Close.

15. It is also possible to return back to the NetBackup Administration Console and view the status of the restore job in the Activity Monitor.
16. Enter password **Netapp1!**, and click **Login**.

![NetBackup Administration Console](image)

17. Click on **Activity Monitor** to find the Restore job.

18. Double-click on the **Restore job**.
19. Click on the **Detailed Status** tab to view additional information.

20. Click **Close**.
21. Using Windows Explorer on the netbackup1 server, view the C:\Restore directory to see the files recovered.
After confirming files have been restored in the folder, minimize the Remote Desktop window to get back to the Jumphost desktop.
3.4.2 Restore data using IntelliSnap

The CommCell Console can also be used to perform restores of backup data for clients. Jobs are not required to perform recovery, but instead NetApp provides a recovery tool. For the purposes of this demonstration the backup data used in this demonstration has files from the SPCOMM server stored in a NetApp Volume sitting in a Storage Virtual Machine accessible from the CIFS share: `\192.168.0.135\vol1`.

1. Launch Windows File Explorer.

2. Navigate to the path:`\svm1-cifs.demo.netapp.com\vol1\BackupData\VMware Tools`.

3. Right-click and delete the `win32` folder.
Figure 3-194:

4. Click Yes to delete the folder.

Figure 3-195:

5. Confirm the folder is gone.
6. Launch the Remote Desktop Connection Manager.

Figure 3-197:

7. Enter session to spcomm server.

Figure 3-198:

8. Enter the CommVault IntelliSnap CommCell Console.
9. From the CommCell Browser, expand and select the defaultBackupSet under Client Computers > cluster1 > NAS > defaultBackupSet.

10. Ensure you click on the tab for the defaultBackupSet.

11. Right click on the subclient named default, then click on Browse & Restore to launch the recovery tool.

12. Click the Advanced Options tab.
13. Select **Browse from copy precedence** with value 3.
14. Click **View Content**.
15. Expand the tree, and select the objects to recover by selecting the **win32** folder.
16. Click **Recover All Selected** to initiate the restore.
17. Change the “Destination client” to `spcomm`.
18. Specify the destination path by clicking `Browse`.
19. Click **New Folder**.
20. Enter the folder name **Restore**.
21. Click **OK**.
22. Click OK.
23. Click OK.
23. Go to the Job Controller tab to monitor the status, or click on the Home menu, and click the Job Controller button and select Show All Jobs.
25. After the job changes to a completed state, return to Windows Explorer and confirm that the folder was restored locally from the AltaVault archive of the NetApp share.

3.4.3 Restore data from ONTAP SnapShots created by SnapMirror destination of AltaVault

This lab activity restores data from a SnapMirror destination when an ONTAP to AltaVault SnapMirror relationship has been established.

3.4.3 Perform a single file SnapRestore of the test1.txt file to the original volume

1. To restore the file from SnapShot on the SnapMirror destination (AltaVault) to the original source volume issue the following command:

   `snapmirror restore -source-path 192.168.0.75:/share/svm1_vol2 -destination-path svm1:vol2_CIFS_volume -source-snapshot snap1 -file-list /test1.txt`
3.4.3 Perform a SnapRestore to a new volume

1. To create a volume to be new home for the data restore issue the following command:

   ```bash
   volume create -vserver svm1 -volume restore_test -aggregate aggr1_01 -type DP -size 2GB
   ```

2. To copy the SnapShot from the SnapMirror destination (AltaVault) to the newly created volume and CIFS share to access the data issue the following command:

   ```bash
   snapmirror restore -source-path 192.168.0.75:/share/svm1_vol2 -destination-path svm1:restore_test -source-snapshot snap1
   ```

3. To mount the volume and define a namespace issue the following command:

   ```bash
   volume mount -vserver svm1 -volume restore_test -junction-path /restore_test
   ```

4. To make the volume accessible via an SMB share issue the following command:

   ```bash
   vserver cifs share create -vserver svm1 -share-name restore_test -path /restore_test
   ```

5. From Windows Explorer on the Jumphost, navigate to `\svm1-cifs.demo.netapp.com\restore_test`.

6. Observe that the “test1” text file is available.

   ![Figure 3-210](image)

   7. Open the **test1** text file, and observe that the copy from the first backup (snap1) was the restore. (Snap2 had an additional line of text).
3.4.4 AltaVault Disaster Recovery

In this section you will simulate a disaster recovery. It is not likely that an appliance would be completely unavailable. However, in the case that it occurs, or in the case that an administrator wants to test disaster recovery, this section describes the process.

This lab uses the existing AltaVault virtual appliance to simulate the disaster. This requires a few steps to wipe the data from the appliance cache.

3.4.4 Simulate Disaster

1. Using the AltaVault Web GUI, navigate to the Configure > Tools menu, and choose Prepopulation.
2. Check the box next to **Cl4Nshare**.
3. Check the box next to **ostshare1cloud**.
4. Check the box next to **ostshare1regular**.
5. Click **Fetch Percent Locally Cached for Selected Files**, and view the results to confirm that the files are present on the AltaVault when 100% is displayed.
6. Using Windows Explorer, navigate to `\altavault\CI4Nshare` to confirm the Test File exists and is accessible.
7. On the desktop of the Jumphost, double-click the **putty** icon.

8. Select **AltaVault** from the list of saved sessions. You need to add it in the master image.
9. Click **Open** to start a session.
10. Log in with credentials username admin, and password Netapp1!
11. Change to Enable-Mode by issuing the `enable` command.
12. Then change to Configure Mode by issuing the `configure terminal` command.
13. Issue the `no service enable` command to stop the optimization service.
14. Issue the `datastore format local` command to format the datastore to remove all the local backup data (the data replicated to the cloud will still exist).
15. Enter `y` when prompted to confirm warning of the format operation.

**Note:** The first step for a disaster recovery with a new appliance is to do the initial setup, and then import the configuration of the missing appliance. This gives the DR appliance the identity of the old appliance, and provides the keys to access the cloud storage to access the data. Since this is a lab simulation using the same virtual appliance, you basically deleted the data from the local appliance, and now it is time to recover the metadata that describes what was replicated to the cloud. This puts the appliance back in the original state, except that only metadata will exist in the cache. None of the previous user data has been copied down from the cloud storage to the cache.
16. Issue the `replication recovery enable` command to start the recovery process.
17. Type `y`, and press `return` when prompted to confirm recovery.
18. Issue the `service enable` command to enable the optimization service.

19. Return to Windows Explorer, and confirm that the Test File is accessible on the share.
20. Return to the AltaVault Web GUI under the “Prepopulation” tag.

21. Select the files again and click **Fetch Percent Locally Cached for Selected Files**. In the current state, you have erased all the local data that was stored on the appliance to simulate a disaster recovery. When you view the percent of each file stored locally, the GUI indicates 0% to show that while the metadata was recovered from cloud storage, the data files were not replicated back to the appliance.
3.4.4 Perform Data Recovery

AltaVault recovery of data is always recommended when using Amazon Glacier (due to the 3-5 hour wait). It is also a preferred method to restore data from any backup application, especially when latency may be an issue. The reason is that AltaVault will delay responding to the requests from the backup application until the bytes are recovered from the cloud.

1. Click **Fetch Percent Locally Cached For Selected Files** again. If you look again at Prepopulation, some files are now all 100% local.
2. Uncheck those with 100%, select only the files less than 100% if there are any, or select all files by checking the share.

3. Click **Prepopulate Selected Files**.

   ![Figure 3-223](image)

4. When prompted click **OK**.
5. Click the **Status** tab. The page may require a refresh to see the status of the job.

   **Note:** The status section will show the Prepopulation jobs and the percent complete. For large backup images being pulled from a slower link, the download process will take some time. Since the lab backups are smaller to a local object storage, the process happens quickly.

6. When the Job status changes to “Completed”, return to the Select File section.

   ![Figure 3-225](image-url)

   **Figure 3-225:**

   7. Click the **Fetch Percent Locally Cached For Selected Files** again.
8. All files will now display 100% for percent locally cached.
3.5 Administer the AltaVault Appliance

3.5
3.5.1 Review AltaVault Reports

You can log in to the AltaVault again using the browser GUI in Firefox and review the reports. The reports show the activity related to the backup including the size of data written to the appliance, the ingest performance and more.

1. Login to the AltaVault admin GUI.
2. From the main menu choose Reports > Front-End Throughput to show the amount data read and written from the AltaVault cache.
3. Click 1h and 5m on the right hand side to zoom the display to cover the past hour and the last 5min.

![Front-End Throughput Report]

Figure 3-228:

4. Switch to the “Back-End Throughput” report to show the data read and written to the cloud.
Figure 3-229:

5. Switch to the “Storage Optimization” report.

Figure 3-230:

Figure 3-231:

7. View the other reports:

- **Storage Optimization** – Shows the amount of data on the appliance, the deduplication and compression factor.
- **Front-End Throughput** – Summarizes the front-end data read in and written out of SMB/NFS/OST.
- **Back-End Throughput** – The performance to/from the cloud.
- **Eviction** – This report will be black as only a recent small backup was done, so no data has been evicted.
- **Replication** – This is an important graph that shows the pending data that needs to be written to the cloud.
- **Cloud Operations** – Put, Get, Post and other operations to the cloud service.

### 3.5.2 AltaVault Operations Tasks

#### 3.5.2 Export the Configuration

Whenever you make configuration changes or set up a new appliance, you should always export the configuration. The configuration is required to perform a disaster recovery using a new appliance. The configuration export also includes the keys used to encrypt the data stored in the cloud. Without these keys there is no way to read the data written. So it is critical to always create a configuration export, and store it in a safe place.

**Note:** Never store the configuration export in the cloud storage used for the backup.

1. From the main menu in the AltaVault GUI, select **Configure > Tools > Setup Wizard.**
2. Choose **Export Configuration**.
3. Click **Export Configuration**.
4. Click **Save File**, or **Cancel**.
5. Click **Exit** to close the export dialog.
6. Click **Exit Wizard** to return to the main view.

### 3.5.2 Reboot or Shutdown Appliance

Whenever you shut down a virtual appliance, always use the GUI to perform the shutdown. The virtual appliance does not have hypervisor tools installed to allow a clean shutdown.

1. From the main menu, choose **Maintenance > Appliance > Reboot/Shutdown**.
2. Click either the **Reboot**, or **Shutdown** buttons as required.

**Warning**: Do not shut down the appliance in Lab on Demand. You will not be able to start the appliance as there are no user controls for starting the VMs.
3.5.3 Using the AltaVault Command Line Interface

This section describes how to use the command line interface (CLI) of the AltaVault appliance. The most common operational features are exposed in the web GUI. The CLI provides additional control over the appliance, and some operations are available only on the CLI.

The CLI provides many commands for troubleshooting, and performing actions that are not very common for an operations staff.

3.5.3 Accessing the CLI

1. Double-click on the putty icon on the desktop of the Jumphost.

![PuTTY Configuration](image)

Figure 3-237:

2. Select altavault from the list of saved sessions.
3. Click Open to start a session.

4. Login with “username” admin, and “password” Netapp1!
Figure 3-239:

The AltaVault CLI provides a network device type user interface with 3 modes, “User-Mode”, “Enable-Mode”, and “Configure-Mode”.

The default session starts in User-Mode.

Enter enable mode by issuing the `enable` command.

Enter configure mode by first going to enable mode, then issuing the `configure terminal` command, or `config t` using the abbreviated syntax.

When using the CLI, it is possible to do the following:

• Autocomplete for commands using tab key.
• Context sensitive help using ?.
• Using arrow keys to view command history.

3.5.3 Configuring the Web GUI Timeout

There is an auto-logout feature for the web GUI, where if the session is idle for 15 minutes the user is logged out of the session. You can adjust this setting using the `[no] web auto-logout <minutes>` command.

1. Login to the ssh command prompt of the AltaVault appliance
2. Enter Enable Mode.
   
   `enable`

3. Enter Configure Mode.
   
   `config t`
4. Set the web auto logout to 60 minutes.
   
   `web auto-logout 60`

5. Make the change persistent.
   
   `configuration write`

3.5.3 Viewing Shares

Using the `show cifs shares` and `show nfs` commands, it is possible to view the active shares and options for them.

Example:

```
altavault # show cifs shares
Share: share1
Path: /share1
Comment: 
Read only: no
Pinned: no
No Dedup: no
No Compression: no
Early Eviction: no
Share: johnbraden
Path: /jbraden
Comment: 
Read only: no
Pinned: no
No Dedup: no
No Compression: no
Early Eviction: no
Share: cifs
Path: /cifs
Comment: Default CIFS share
Read only: no
Pinned: no
No Dedup: no
No Compression: no
Early Eviction: no
altavault #
```

3.5.3 Reboot or Shutdown the Appliance

Issue the `# reload` command to reboot the appliance.

Shutdown the appliance.

⚠️ **Warning**: Do not shut down the appliance in Lab on Demand. You will not be able to start the appliance, as there are no user controls for starting the VMs.

`# reload halt`

3.5.3 Saving the Configuration

`# configuration write`

3.6 Review Cloud Target Configurations

3.6
3.6.1 Review OpenStack Swift Configuration

3.6.1 OpenStack Swift Overview
This lab provides a simple, single server deployment of OpenStack Swift to serve as a target for AltaVault. The lab uses this environment to demonstrate how easy it is to set up a connection to a cloud target. Amazon AWS uses “buckets” as a logical unit of storage in their object storage service in a similar way to solutions like NetApp StorageGRID WebScale. Each object in the bucket consists of data and metadata. OpenStack Swift is the Object Storage solution for OpenStack. OpenStack Swift has “containers” that provide a logical unit of storage for objects that have associated data and metadata. This section demonstrates simple command line operations that show how to create tenants/users, assign roles, create containers, and list contents.

3.6.1 Accessing the OpenStack VM Using Putty
PuTTy is a freeware Windows application that provides a client for terminal or command line communications. It supports several connection protocols such as telnet, rlogin and ssh. This lab uses ssh for the protocol.

If there are windows open on the desktop of the jumphost, minimize them to view the desktop.

1. On the desktop, double-click the putty icon.
2. Select openstack1 from the list of saved sessions.
3. Click Open to start a session.

![PuTTy Configuration](image)

Figure 3-240:

4. Login with username stack, and password Netapp1!

```bash
login as: stack
stack@192.168.0.41's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.13.0-45-generic x86_64)
```
The client for OpenStack can use environment variables for authentication to the management endpoints. There are two files in the stack user’s home directory that contain environment variables for the admin user and the SSAccount user.

5. Issue the `source ./admin-openrc.sh` command to load the admin environment variables.

```
stack@openstack1:~$ source ./admin-openrc.sh
stack@openstack1:~$
```

### 3.6.1 OpenStack Administration

#### 3.6.1 Listing users

To list users in OpenStack issue the `keystone user-list` command.

```
stack@openstack1:~$ keystone user-list
+----------------------------------+-----------+---------+------------------+
|                id                |    name   | enabled |      email       |
+----------------------------------+-----------+---------+------------------+
| f7fcd9fe19314e3ba965c4d15db2c65f | SSaccount |   True  |   root@stack-1   |
| 01b3b9b076684036b51be8321cf188e8 |   admin   |   True  | stack@openstack1 |
| a5cbac35df334075ac7e904c8666724a |   swift   |   True  | root@openstack1  |
+----------------------------------+-----------+---------+------------------+
stack@openstack1:~$
```

#### 3.6.1 Listing tenants

To list tenants in OpenStack issue the `keystone tenant-list` command.

```
stack@openstack1:~$ keystone tenant-list
+----------------------------------+----------+---------+
|                id                |   name   | enabled |
+----------------------------------+----------+---------+
| 3eabe7b1bb614e75895703417b62f640 | SStenant |   True  |
| 04af154ad7e14968a3972b04978539f5 |  admin   |   True  |
| 845075ca1b45498896a798bc9ba2ffe4 | service  |   True  |
+----------------------------------+----------+---------+
stack@openstack1:~$
```

#### 3.6.1 Listing roles

To list roles in OpenStack issue the `keystone role-list` command.

```
stack@openstack1:~$ keystone role-list
+----------------------------------+---------------+
|                id                |      name     |
+----------------------------------+---------------+
| 4cf0741bfedf47e899cf2b1e8b820f  |    _member_   |
| 2065626d35804f7d94fc7659475a85e |     admin     |
| 14e0710c860e407caac89647d8b8948 | swiftoperator |
+----------------------------------+---------------+
stack@openstack1:~$
```
3.6.1 Creating a new user and tenant

To add a new user and allow that user to access swift, issue the following commands.

```bash
keystone user-create --name=johnbraden --pass=Netapp1 --email=jbraden@stack
keystone tenant-create --name=johnbraden --description="Johns Tenant"
keystone user-role-add --user=johnbraden --tenant=johnbraden --role=swiftoperator
```

```bash
stack@openstack1:~$ keystone user-create --name=johnbraden --pass=Netapp1 --email=jbraden@stack
+----------+----------------------------------+
| Property |              Value               |
+----------+----------------------------------+
|  email   |          jbraden@stack           |
| enabled  |               True               |
|    id    | 790bd122c65d435e80eb2e025e42aea0 |
|   name   |            johnbraden            |
| username |            johnbraden            |
+----------+----------------------------------+
stack@openstack1:~$
```

```bash
stack@openstack1:~$ keystone tenant-create --name=johnbraden --description="Johns Tenant"
+-------------+----------------------------------+
|   Property  |              Value               |
+-------------+----------------------------------+
| description |           Johns Tenant           |
|   enabled   |               True               |
|      id     | 1db3d4b58e2445c48f19829146b1a304 |
|     name    |            johnbraden            |
+-------------+----------------------------------+
stack@openstack1:~$
```

```bash
stack@openstack1:~$ keystone user-role-add --user=johnbraden --tenant=johnbraden --role=swiftoperator
stack@openstack1:~$
```

```bash
stack@openstack1:~$ keystone user-list
+----------------------------------+------------+---------+------------------+
|                id                |    name    | enabled |      email       |
+----------------------------------+------------+---------+------------------+
| f7fcd9fe19314e3ba965c4d15db2c65f | SSaccount  |   True  |   root@stack-1   |
| 01b3b9b076684036b51be8321cf188e8 |   admin    |   True  | stack@openstack1 |
| 790bd122c65d435e80eb2e025e42aea0 | johnbraden |   True  | jbraden@stack    |
| a5cbac35df334075ac7e904c8566724a |   swift    |   True  | root@openstack1  |
+----------------------------------+------------+---------+------------------+
stack@openstack1:~$
```

3.6.1 Creating a container (bucket)

Swift refers to a directory style object as a container. Bucket is the Amazon terminology, however, they are sometimes used interchangeably. To create a container in Swift, use the `swift post <container_name>` command.

```bash
stack@openstack1:~$ swift post democnt
stack@openstack1:~$
```

3.6.1 Listing containers for a user

Before listing containers for a user, you need to set the environment variables for the user.

To view the containers created by the SSaccount user, issue the `source ./ss-openrc.sh` command to load the environment variables for that user.

Then, issue the `swift list` command to list the contents for the user in swift.

```bash
stack@openstack1:~$ source ./ss-openrc.sh
stack@openstack1:~$ swift list
democnt
sstest1
stack@openstack1:~$
```

In this example there is only one container (bucket) named “sstest1”. This is the container that was used to configure the AltaVault appliance.
3.6.1 Viewing files in a container

To see the files in a container, perform the same `list` command using the container name. In this example, the container holds the files created by the AltaVault appliance when the backups were performed. You can see there are several files that are common to all AltaVault appliances such as "megastore.guid", which is the file that contains the ID of the appliance that owns the container or bucket.

The `.slab` files contain the user data that was deduped from the share. The `.lm` files contain the metadata that describes how to recreate a file from the data contained in the slabs. A slab file is a group of segments from the deduplication process that are packaged together and written to the cloud storage service.

```
swift list <container_name>
```

```
stack@openstack1:~$ swift list sstest1
0000000000000000.lm
0000000000000000.rbtmd
0000000000000001.lm
0000000000000001.rbtmd
0000000000000007.lm
0000000000000007.rbtmd
0000000000000008.lm
0000000000000008.rbtmd
0000000000000009.lm
0000000000000009.rbtmd
000000000000000A.lm
000000000000000A.rbtmd
000000000001.slab
000000000002.slab
000000000003.slab
000000000004.slab
000000000069.slab
00000000006A.slab
00000000006B.slab
FEFFFFFFFFFF.slab
info.yaml
megastore.guid
rbt_oids.dat
stats.dat
stack@openstack1:~$
```

3.6.1 Viewing permissions for a container

The `swift stat` command provides the status of the tenant associated with the user. If it is entered without additional parameters, it shows a general status of the tenant, including how many containers have been created and how much data has been written to the tenant.

If you supply a container as a parameter, it will list details about the container, including the permissions on the container.

```
stack@openstack1:~$ swift stat sstest1
Account: AUTH_3eabe7b1bb614e75895703417b62f640
Container: sstest1
Objects: 124
Bytes: 439231621
Read ACL: SSaccount
Write ACL: SSaccount
Sync To:
Sync Key:
Accept-Ranges: bytes
X-Storage-Policy: Policy-0
X-Timestamp: 1424500431.67006
X-Trans-Id: txdec64eaba51a4d3cbb924-0057b215be
Content-Type: text/plain; charset=utf-8
stack@openstack1:~$
```
3.6.1 Other OpenStack Administration Commands

It is possible to test upload and download of files using the swift command.

The `swift upload democnt test.txt` command will upload a file in the current directory called “test.txt” to the container called “democnt”.

The `swift download democnt` command will download all the files in the container “democnt”.

For additional commands and parameters, issue the `swift --help keystone --help` command to view the help text.

3.6.2 Review the NetApp StorageGRID WebScale Configuration

1. Launch the link to open the NetApp StorageGRID Webscale Network Management System.

   ![NetApp StorageGRID WebScale](image)

   Figure 3-241:

2. Click **Continue to this website** to bypass the security certificate warning.

   ![Certificate Error](image)

   Figure 3-242:

3. Login using the credentials “username” Vendor, and “password” Netapp1!.

4. Click **Sign In**.
5. Click on Tenants.
6. Examine the Tenant account setup.

**Figure 3-243:**

**Figure 3-244:**

*Note:* The Tenant Login is not available in this version of SGWS. This functionality is introduced in SGWS 10.4. In order to access an S3 compatible private cloud bucket, you must use a third-party application. In this lab the program used is the S3 Browser.

7. From the Jumphost click on the Windows icon.

**Figure 3-245:**

8. Click the down arrow icon.
9. Search for S3.
10. Click on S3 Browser.

11. Examine the Altavault bucket.

For more detailed information on NetApp StorageGRID Webscale 10.x, consider running the lab specific to NetApp StorageGRID.
4 References

The following references were used to create this lab guide.

- *NetApp AltaVault Resources on Support Site*
## 5 Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5.0</td>
<td>June 2017</td>
<td>Initial Release</td>
</tr>
<tr>
<td>1.5.1</td>
<td>June 2017</td>
<td>Added command</td>
</tr>
<tr>
<td>1.5.2</td>
<td>August 2017</td>
<td>Corrected typo</td>
</tr>
<tr>
<td>1.5.3</td>
<td>November 2017</td>
<td>Corrected typo</td>
</tr>
</tbody>
</table>
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.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer’s responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.