VAST Data & Cohesity® NetBackup

Configuration and Best Practice Guide

COHESITY | VAST

Table of Contents

Introduction **3**

VAST Configuration **4**

Create VAST NFS View 4

Create a VAST S3 User 5

Cohesity NBU Configuration **9**

Adding Cloud Configuration Package 9

Windows Installation 10

Linux Installation 11

Adding Device Mapping Files 12

Windows Installation of Device Mapping Files 12

Linux Installation of Device Mapping Files 13

Adding Private Cloud CA Certificate 14

Windows Configuration 15

Linux Configuration 16

Adding Media Servers 16

Adding Client Servers 17

Adding Data Sources 18

Adding a vCenter Server 18

Adding VAST as a Target 20

Advanced Disk with VAST NFS 20

Cloud Storage with VAST S3 26

MSDP Cloud with VAST S3 35

Advanced Solutions **45**

NetBackup Image sharing 45

Configuring a Cloud Recovery Server 45

Restoring Data with Cloud Recovery Server 47

Introduction

VAST Data, for the first time, redefines the economics of flash storage, making flash affordable for all applications, from the highest performance databases to the largest data archives. The concept blends game-changing storage innovations to lower the acquisition cost of flash with an exabyte-scale file and object storage architecture breaking decades of storage tradeoffs.

With the advantage of new, enabling technologies that weren't available before 2018, this new Universal Storage concept can achieve a previously impossible architecture design point. The system combines low-cost hyperscale flash Drives and Storage Class Memory with stateless, containerized storage services all connected over new low-latency NVMe over Fabrics networks to create VAST's Disaggregated Shared Everything (DASE) scale-out architecture. Next-generation global algorithms are applied to this DASE architecture to deliver new levels of storage efficiency, resilience, and scale.

As a market leader in enterprise backup and recovery software, Cohesity NetBackup™ reduces cost and complexity while keeping data secure, compliant and available. NetBackup can scale to any size workload and deliver breakthrough capabilities for virtualized and cloud based deployments that go well beyond what traditional backup practices can achieve. It empowers organizations by improving the resiliency of their applications and infrastructure from edge to core to cloud. From threats such as a ransomware attack to unplanned downtime, NetBackup offers rapid recovery of business-critical data across hybrid, physical, virtual and multi-cloud environments.

VAST Clusters with Cohesity NetBackup jointly deliver an unprecedented level of performance and scalability that's built for today's complex environments. Cohesity NetBackup's ability to scale to petabytes in a single domain is a match made in heaven with the VAST Cluster and its exabyte scale single namespace. In addition, the VAST Cluster introduces Similarity-Based Data Reduction, which reengineers data reduction algorithms to deliver unprecedented storage efficiency. When combined, the result is a fast and highly scalable data protection solution, providing unparalleled levels of restore performance.

This document covers basic configuration steps to integrate NetBackup with a VAST Data cluster. It covers minimal-click VAST Cluster configuration for both NFS and S3 and highlights several examples of data backup and recovery.

This guide will assist individuals who are responsible for the design and deployment of data protection and disaster recovery solutions of virtual machines deployed on a VAST Cluster.

VAST Configuration

This section presents basics steps to be performed on the VAST cluster UI prior to configuring the Cohesity NetBackup Cloud Connector.

Create VAST NFS View

The NFS view created in the following steps can be used for mounting to a Linux system. Then during Advanced Disk Storage Server creation the disk pool can be pointed to this path.

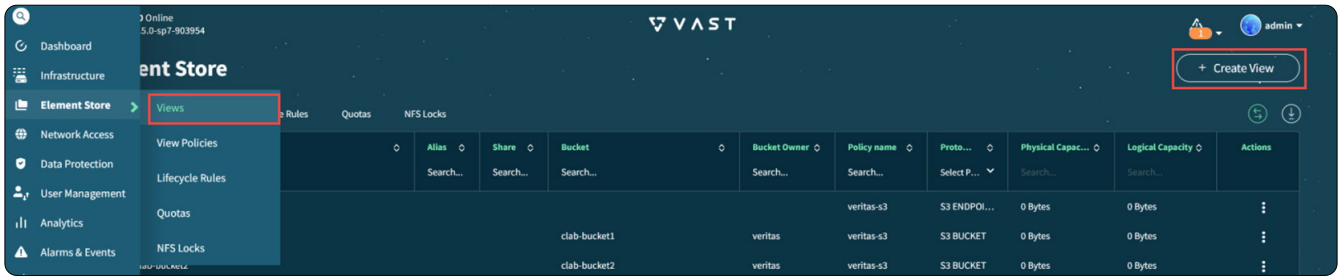


Figure 1 - Creating a New View

To create a new view go to the left column and select ***Element Store*** and select ***Views*** (Figure 1).

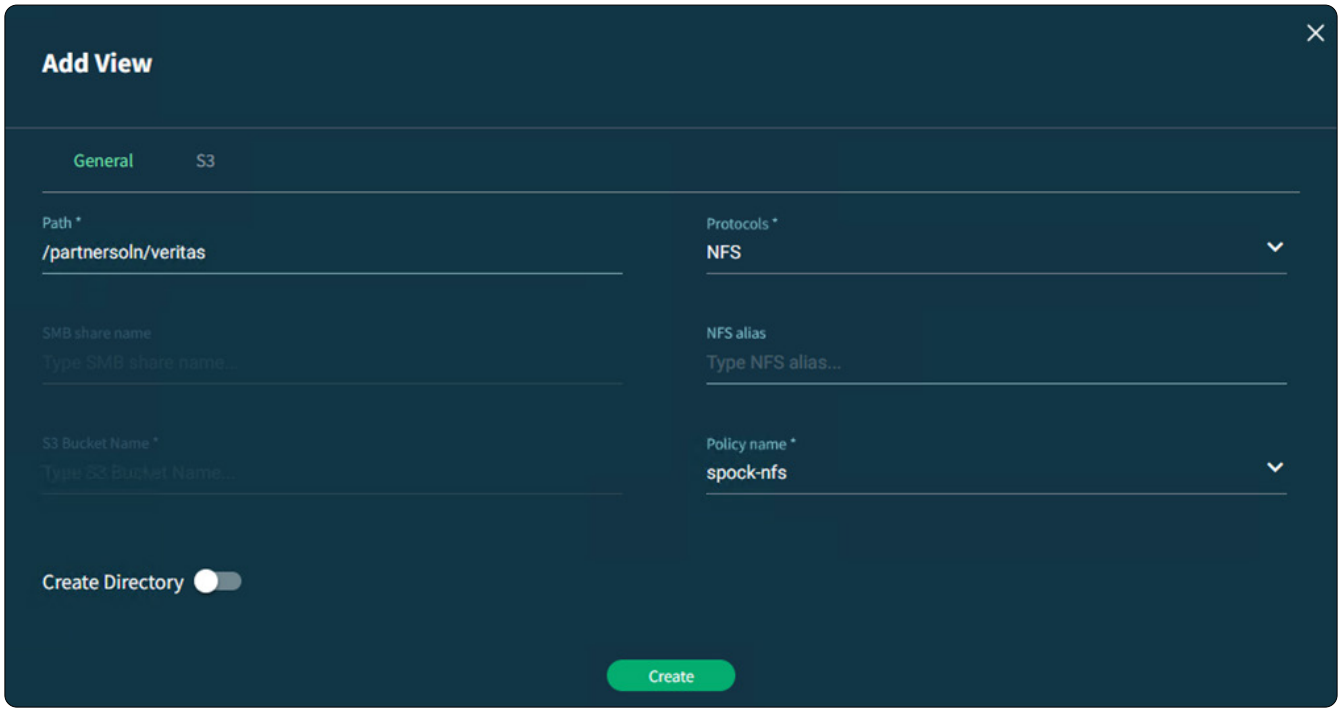


Figure 2 - Add View Wizard

This brings a new ***Add View*** window as shown in Figure 2. Enter in a path that is appropriate for the organization of data within the VAST cluster, select the NFS protocol and assign it to a policy. If this is a new path, slide the ***Create Directory*** toggle over and click ***Create***.

This path can now be mounted to a Media Server and used for the data path during disk pool creation.

Create a VAST S3 User

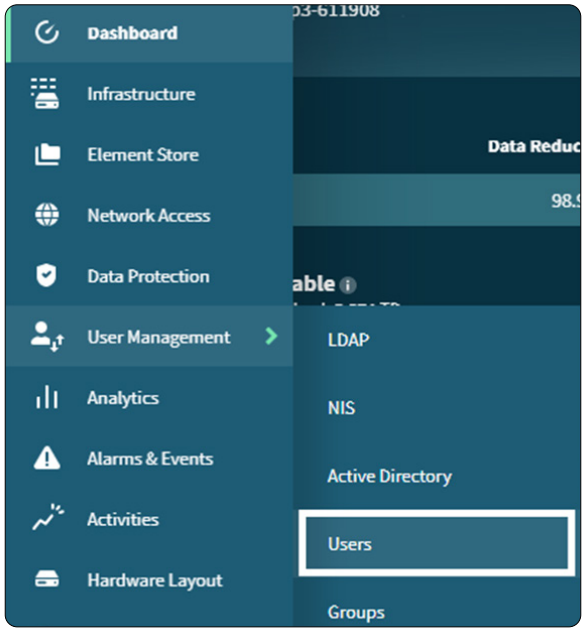


Figure 3 - Selecting Users Category

The ***Add User*** window appears and a username is entered along with any desired UID. This user is granted full S3 credentials but that is not necessary during the Cohesity process of adding an S3 repository.

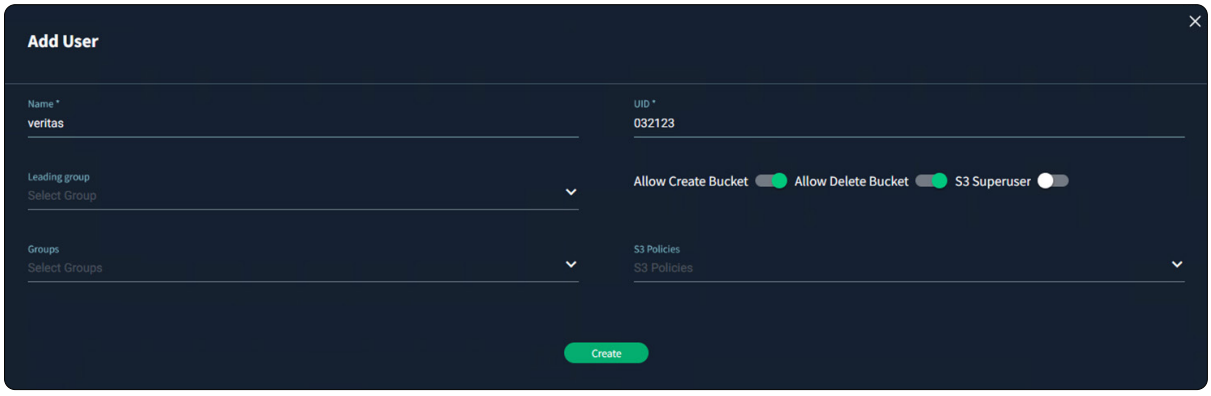


Figure 4 – Creating a New User for S3

After clicking ***Create*** the user will show up in the User Management window Figure 5.

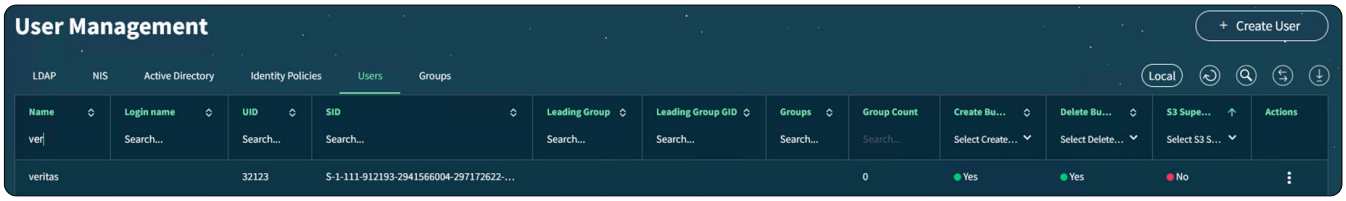


Figure 5 - User Created

Now that the user is created it needs to be edited to create and capture the active and secret keys. On the far right of the user under the action column click on the three dots and select edit (Figure 6).

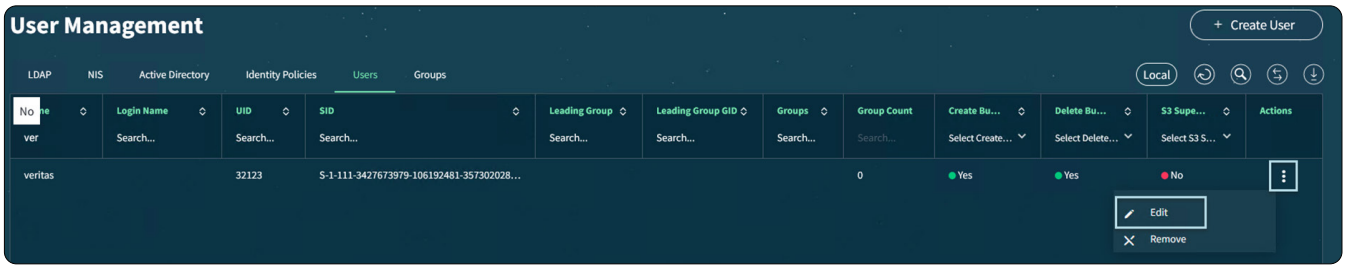


Figure 6 - Update the User

In the ***Update User*** window (Figure 7) click on the ***Create new key*** button to create a new ***Access Key***. Now copy the active key and secret key some place for later. This is the only time when the secret key will be accesible so be sure to store in a safe location. Click Update to close the window.

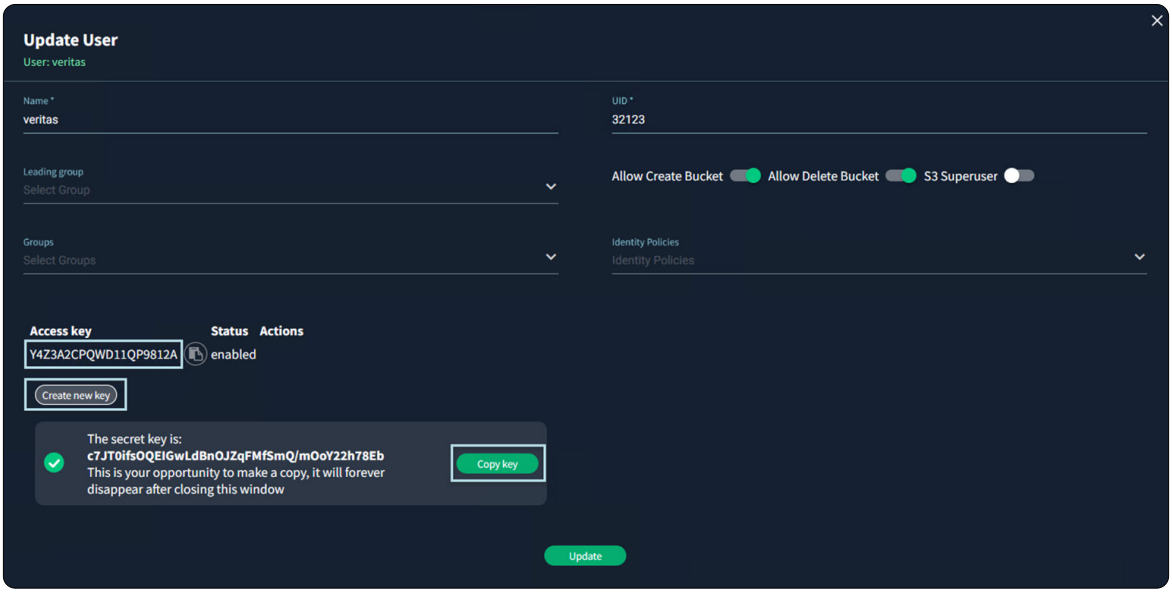


Figure 7 - Capturing Active and Secret Keys

The user will now be used in the creation of a bucket, endpoint or view within the VAST UI. Just as before, when creating a view, from the dashboard go to ***Views*** as shown in Figure 1 and then click ***Create View***. This view is configured as an endpoint only using the S3 Endpoint protocol. Multiple protocols (NFS, S3) can be used on a view. Figure 8 shows the all the settings needed to create the new endpoint. Since this is a new view the create directory toggle is selected.

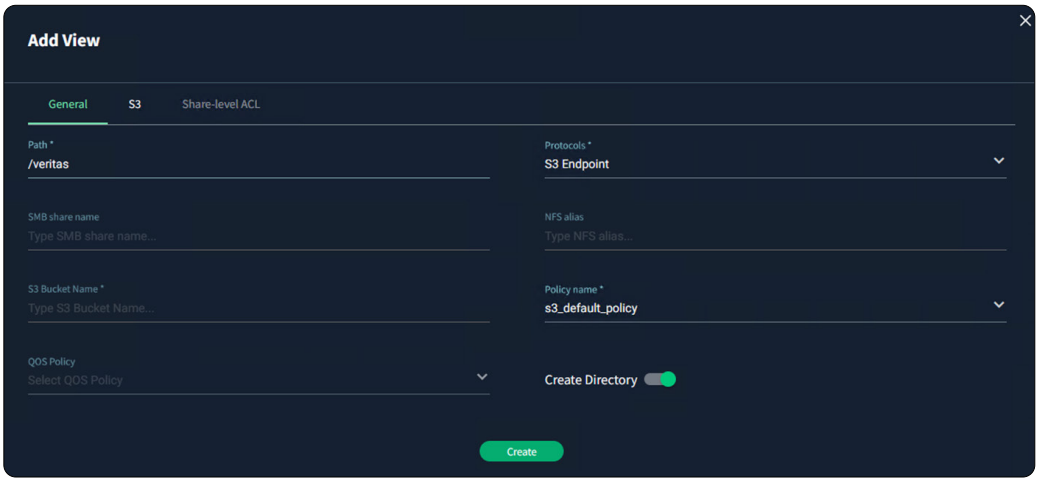


Figure 8 - S3 Endpoint Configuration

The user created previously needs to be given access or ownership of this view. This is done on the S3 tab as shown in Figure 9. When finished click Create from either tab.

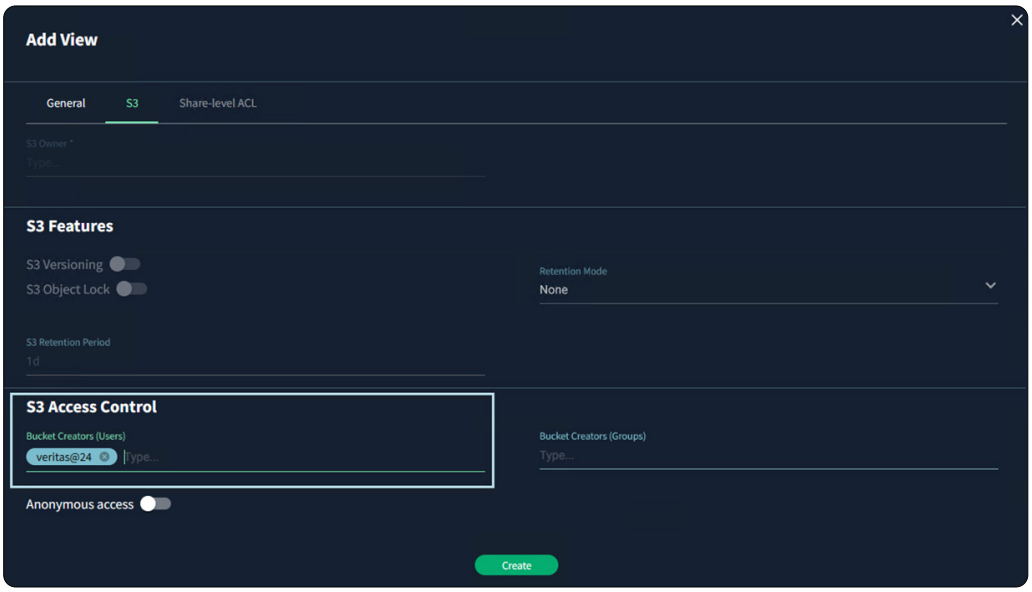


Figure 9 - Adding Bucket Owner (User)

The view (bucket) now shows up in the Element Store as shown in Figure 10.

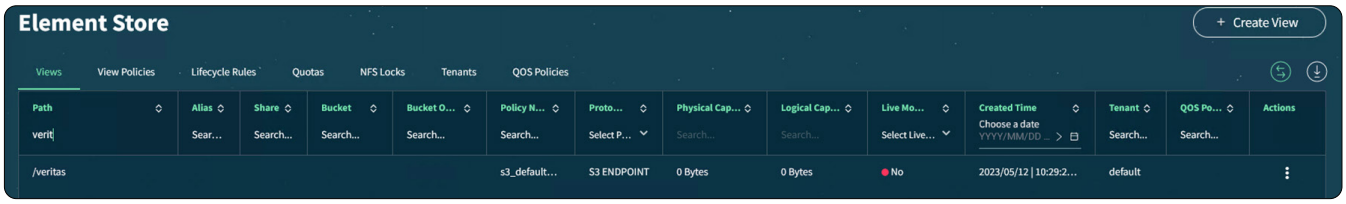


Figure 10 - S3 Bucket Created

Cohesity NBU Configuration

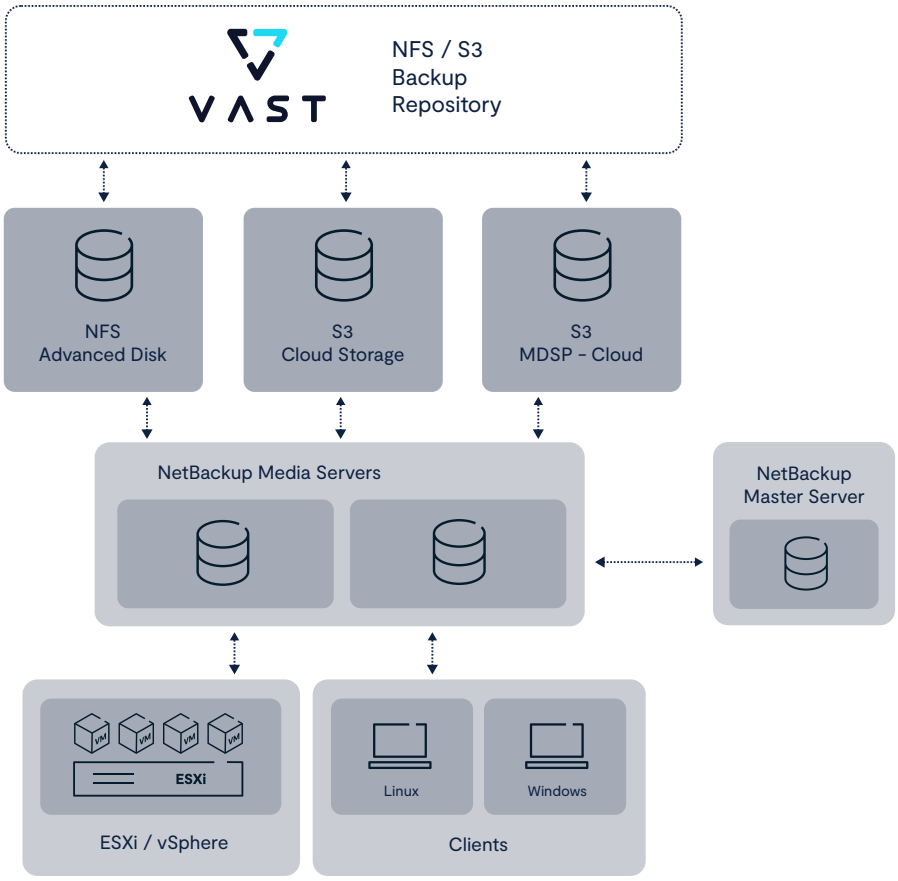


Figure 11 - VAST/Cohesity Deployment Scenarios

This document was written using a NetBackup deployment consisting of one master server and several Linux media servers (Figure 11).

Some prerequisites are needed for NetBackup to function properly with a VAST cluster, specifically, when using S3 to create an MSDP-Cloud (MSDP-C) storage pool. Make sure to review the following sections pertaining to the Cloud Configuration Package and the Device Mapping Files.

Adding Cloud Configuration Package

Before creating any S3 storage server, it's important to install a package provided by Cohesity that integrates VAST into their workflow process. Refer to the Cohesity Hardware and Cloud Storage Compatibility List for versions 9.x and 10.x support[1]. The cloud package is provided for both Windows and Linux Master Server systems. This procedure only needs to be completed on the master server.

After downloading the appropriate package to a temporary folder follow these instructions:

1. https://www.veritas.com/support/en_US/article.100040093

Windows Installation

1. Copy the existing CloudProvider.xml and CloudInstance.xml files from the following location to an alternate location so you can revert back to these files if needed.

Default file location in NetBackup 9.x versions:

```
C:\Program Files\Cohesity\NetBackup\var\global\wmc\cloud
```

Default file location in NetBackup 10.x and later versions:

```
C:\Program Files\Cohesity\NetBackup\var\global\cloud
```

2. Extract the zip file package that is in the temporary folder. This will create two files:

- CloudProvider.xml
- cacert.pem

3. Copy the ***new*** CloudProvider.xml file from the temporary location, in step 2, to the default location mentioned in step 1.

4. Run the following command:

```
<NB _ INSTALL _ PATH>\NetBackup\bin\admincmd\csconfig reinitialize
```

5. Run the following CLI command to confirm that the installation was successful. The command should return a list of cloud providers including VAST Data.

```
<NB _ INSTALL _ PATH>\NetBackup\bin\admincmd\csconfig cldprovider -l
```

The command should output all of the cloud providers including VAST Data. If the command does not output a list of cloud providers or outputs an error message, refer to the troubleshooting section on Cohesity page where the package was downloaded.

Linux Installation

These instructions assume that NetBackup is installed at the default location of /usr/openv/. If NetBackup is installed at a different location, substitute that path for /usr/openv/ in the instructions below:

1. Copy the existing CloudProvider.xml and CloudInstance.xml files from the following location to an alternate location so you can revert back to these files if needed.

Default file location in NetBackup 9.x versions:

```
/usr/openv/var/global/wmc/cloud
```

Default file location in NetBackup 10.x and later versions:

```
/usr/openv/var/global/cloud
```

2. Download and extract the tar file package to the temporary folder. This will create two files in the temporary location:

- CloudProvider.xml
- cacert.pem

3. Copy the ***new*** CloudProvider.xml file from the temporary location, in step 2, to the default location mentioned in step 1.

4. Run the following command:

```
<NB _ INSTALL _ PATH>/NetBackup/bin/admincmd/csconfig reinitialize
```

5. Run the following CLI command to confirm that the installation was successful. The command should return a list of cloud providers including VAST Data.

```
<NB _ INSTALL _ PATH>/NetBackup/bin/admincmd/csconfig cldprovider -l
```

The command should output all of the cloud providers including VAST Data. If the command does not output a list of cloud providers or outputs an error message, refer to the troubleshooting section on Cohesity page where the package was downloaded.

Adding Device Mapping Files

In addition to the Cloud Configuration package there are additional files which integrate VAST more deeply into NetBackup. Device Mapping files are also available and are used by the NetBackup Enterprise Media Manager database to determine which protocols and settings to use to communicate with storage devices. They are also used by the Device Configuration Wizard to automatically configure new devices.

Along with the cloud configuration package it is essential to install these files for proper functionality of the S3 MSDP-C storage server. The file only needs to be installed on the Master Server however the Device Manager (ltid) needs to be restarted for all Media Servers.

Note: This installation only highlights installation of the external_types.txt file and not the external_robotics.txt for robotics devices. See the Device Mappings download page for instructions on installing the robotics file.

Ensure the file downloaded is for the appropriate NetBackup version and operating system. As of publication there are two versions available, one for NetBackup 10.x and higher and one for NetBackup 7.x-9.x. The installation location on NetBackup versions is the same for all of them.

Windows Installation of Device Mapping Files

```
C:\Program Files\Cohesity\Volmgr\bin
```

The instructions below assume that NetBackup is installed in the default location of **C:\Program Files\Cohesity**. If NetBackup is installed in a different location, substitute that path for **C:\Program Files\Cohesity**in the instructions below:

1. Download and extract the new mappings file package to a temporary directory:

```
C:\temp\Mapping Files - Windows>dir
 Volume in drive C has no label.
 Volume Serial Number is F0A5-7B7A
 Directory of C:\temp\Mapping Files - Windows
05/10/2023 09:20 AM  <DIR>     .
05/10/2023 09:20 AM  <DIR>     ..
05/10/2023 09:18 AM      23,299 Mappings _ CRC _ v1174.zip    <-- NetBackup 10.x
05/10/2023 09:18 AM      23,345 Mappings _ v1174.zip          <-- NetBackup 9.x
```

This will create three files in the temporary location:

- Readme.txt
- external_types.txt
- external_robotics.txt

2. Copy the external_types.txt file from the temporary location to the master server at:

```
C:\Program Files\Cohesity\NetBackup\var\global\
```

If desired, backup or move the existing file to a safe location in case there is a need to revert back.

(For NetBackup High Availability environments, copy the file to the shared disk.)

3. Update the NetBackup Enterprise Media Manager database with the new device mappings version. This only needs to be done once and must be run from the Master/EMM Server. Use the command format below:

```
C:\Program Files\Cohesity\Volmgr\bin\tpext -loadEMM
C:\Program Files\Cohesity\Volmgr\bin\tpext -get _ dev _ mappings
```

4. Restart Device Manager (ltid) on each Media Server.

5. Verify that the version that is now stored in the Enterprise Media Manager database is the same as that which is in the file stored on the Media Server:

```
C:\Program Files\Cohesity\Volmgr\bin>tpext -get _ dev _ mappings _ ver
device mappings version in the EMM database is 1.174
device mappings version from the local file is 1.174
Local device mappings file is up-to-date
```

Linux Installation of Device Mapping Files

The instructions below assume that NetBackup is installed in the default location of **/usr/openv/.** If NetBackup is installed in a different location, substitute that path for **/usr/openv/** in the instructions below:

6. Download and extract the new mappings file package to a temporary directory and run:

```
tar -xvf Mappings _ CRC _ v1174.tar
```

(Above command is for NetBackup 10.x. NetBackup 9.x file is Mappings_v1174.tar)

This will create three files in the temporary location:

- Readme.txt
- external_types.txt
- external_robotics.txt

7. Copy the external_types.txt file from the temporary location to /usr/openv/var/global on the Primary/EMM Server. If desired, backup or move the existing file to a safe location in case there is a need to revert back.

```
cp /temp _ dir/external _ types.txt /usr/openv/var/global/
```

(For NetBackup High Availability environments, copy the file to the shared disk.)

8. Update the NetBackup Enterprise Media Manager database with the new device mappings version. This only needs to be done once and must be run from the Master/EMM Server. Use the command format below:

```
/usr/openv/volmgr/bin/tpext -loadEMM
/usr/openv/volmgr/bin/tpext -get _ dev _ mappings
```

9. Restart Device Manager (ltid) on each Media Server.

10. Verify that the version that is now stored in the Enterprise Media Manager database is the same as what is in the file stored on the Media Server:

```
/usr/openv/volmgr/bin/tpext -get _ dev _ mappings _ ver
```

Adding Private Cloud CA Certificate

To ensure that an S3 Storage server can be created the CA Certifcate that is on the VAST cluster (See https://support.vastdata.com for more information on creating a CA Certificate) must be added to the Cohesity file ***cacert.pem***.

To query the VAST cluster for the current CA certificate chain an openssl command can be used both from Linux or Windows (installation of the package may be necessary). An example command is given below with the format –

Virtual IP Pool.VAST Cluster.domain

```
openssl s _ client -connect Cohesity.tmphx-10.vastdata.lab:443 -showcerts
```

The returned output should contain the certificate chain as in the text below.

```
-----BEGIN CERTIFICATE-----
MIIF+jCCBOKgAwIBAgITQwAAAAQAWcgmumCZ1wAAAAAABDANBgkqhkiG9w0BAQsF

Data Removed for Brevity

upyH+npXDdvJKrzUsUPWJQ18gZDqMBULApmqyF58is2umozjYTXTTl9qEM2lnejd
iZB9lNcTvjiO9fWVSQJbU8Ntj3Gh4+daoacajTK1Oqv2e45ENxn0R/bh+N9gyw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgIQXID1vrrk64xDyI3G+jrc2DANBgkqhkiG9w0BAQsFADBT

Data Removed for Brevity

MRMwEQYKCZImiZPyLGQBGRYDbGFiMRgwFgYKCZImiZPyLGQBGRYIdmFzdGRhdGEx
dJyJsSPurVUiFH0dlnSd6O2mNvIpWVlGAYlW+nufAckQJaAPmfmX
-----END CERTIFICATE-----
```

Now, simply append the certificate in the cacert.pem file. The file will need to be modified temporarily with proper write permissions. This only needs to be done on the media server(s) that will access the bucket. As with all certificates copy everything and include the header and footer of the certificate.

Note: The location of the cacert.pem varies based on the platform and the NetBackup version. They are all addressed next.

Windows Configuration

NetBackup 9.x:

The location of the cacert.pem file for NetBackup 9.x is:

```
<installation-path>NetBackup\var\global\wmc\cloud\cacert.pem
```

NetBackup 10.x:

The location of the cacert.pem file for NetBackup 10.x is:

```
<installation-path>\NetBackup\var\global\cloud
```

Linux Configuration

NetBackup 9.x:

The location of the cacert.pem file for NetBackup 9.x is:

```
/usr/openv/var/global/wmc/cloud/
```

NetBackup 10.x:

The location of the cacert.pem file for NetBackup 10.x is:

```
/usr/openv/var/global/cloud/
```

Adding Media Servers

The NetBackup architecture and data flow involve backing up data to storage that is connected to servers, designated as media servers. A few quick steps are discussed here to highlight the basics of setting up a media server.

One of the most important installation steps is to ensure that any media server is reachable through their IP address, hostname and FQDN. Ensure that both forward and reverse lookups are possible. Once the media server software is installed it may not show up automatically within the NetBackup Master Server. If that is the case the following CLI commands can help resolve the issue and add the new media server.

To ensure the media servers are properly resolving hostname and IP address use the following from the Master Server:

```
C:\Program Files\Cohesity\NetBackup\bin>bpclntcmd -hn linmedia-04
host linmedia-04: LINMEDIA-04.SLI.VASTDATA.COM at 10.61.206.60
aliases:    LINMEDIA-04.SLI.VASTDATA.COM    linmedia-04    10.61.206.60
```

The above command confirms that the media server is resolving from its hostname. Similar to an ping command, this command ensures the host is simply reachable

```
C:\Program Files\Cohesity\NetBackup\bin>bpclntcmd -ip 10.61.206.60
host 10.61.206.60: 10.61.206.60 at 10.61.206.60
aliases:    10.61.206.60
```

To manually add the new media server perform the following command:

```
C:\Program Files\Cohesity\NetBackup\bin\admincmd>nbemmcmd -addhost -machinename
linmedia-11.sli.vastdata.com -machinetype media -masterserver nbuwin2.sli.vastdata.com
-NetBackupversion 9.1.0.1 -operatingsystem linux
NBEMMCMD, Version: 9.1.0.1
Command completed successfully.
```

The media server should now show as in Figure 12 but the following command can also be issued:

```
C:\Program Files\Cohesity\NetBackup\bin\admincmd>nbemmcmd -listhosts
NBEMMCMD, Version: 9.1.0.1
The following hosts were found:
server                  nbuwin2
master                  nbuwin2
media                   linmedia-01.sli.vastdata.com
virtual_machine         selab-vcenter.sli.vastdata.com
media                   winmedia-02.sli.vastdata.com
client                  nbulin-204-9.sli.vastdata.com
media                   linmedia-04.sli.vastdata.com
Command completed successfully.
```

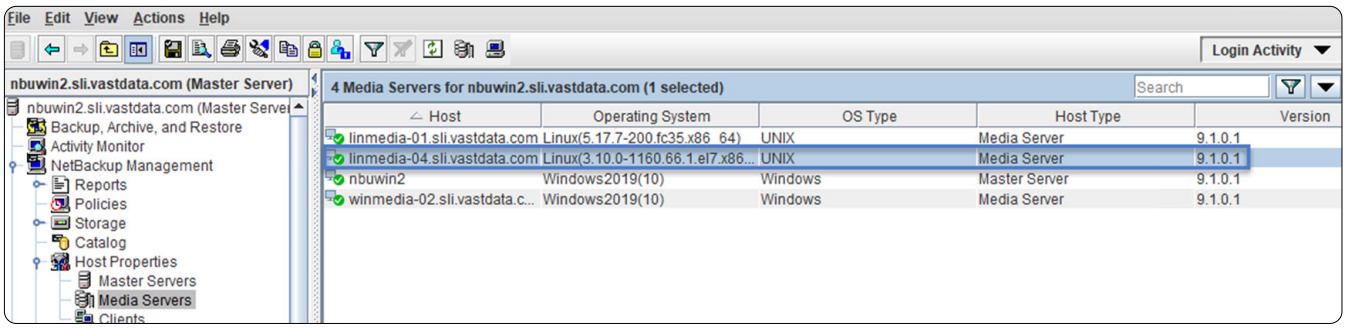


Figure 12 - New Media Server Added

Adding Client Servers

Adding a client server through the command line is essentially the same as adding a media server except the ***'machinetype'*** is different as in the following command:

```
C:\Program Files\Cohesity\NetBackup\bin\admincmd>nbemmcmd -addhost -machinename
nbulin-204-9.sli.vastdata.com -machinetype client -masterserver nbuwin2.sli.vastdata.com
```

Note: Clients may not even show up even with the above command until added into a policy.

Adding Data Sources

The example below is the simple task of adding a vCenter Server to the Master Server.

Adding a vCenter Server

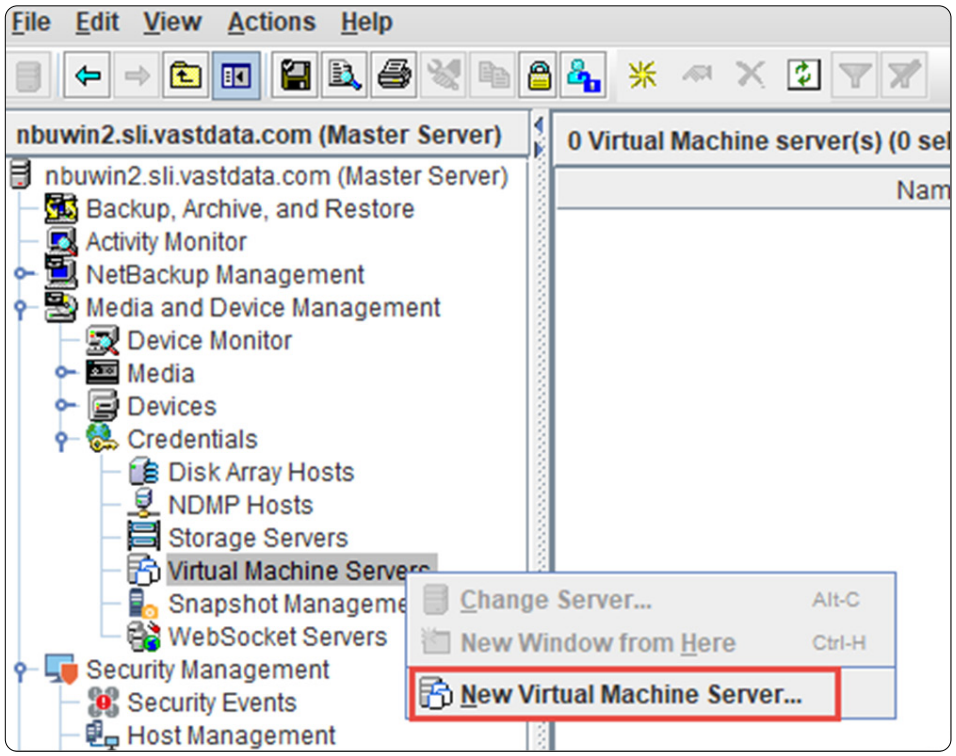


Figure 13 - Adding a New Virtual Machine Server

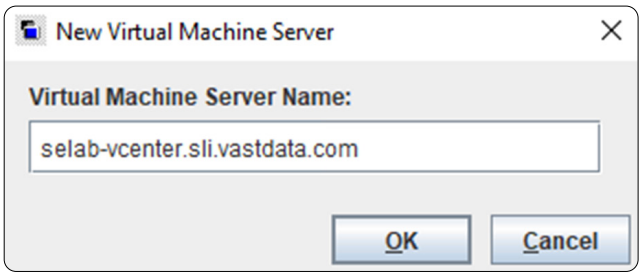


Figure 14 - Adding the Virtual Machine Server

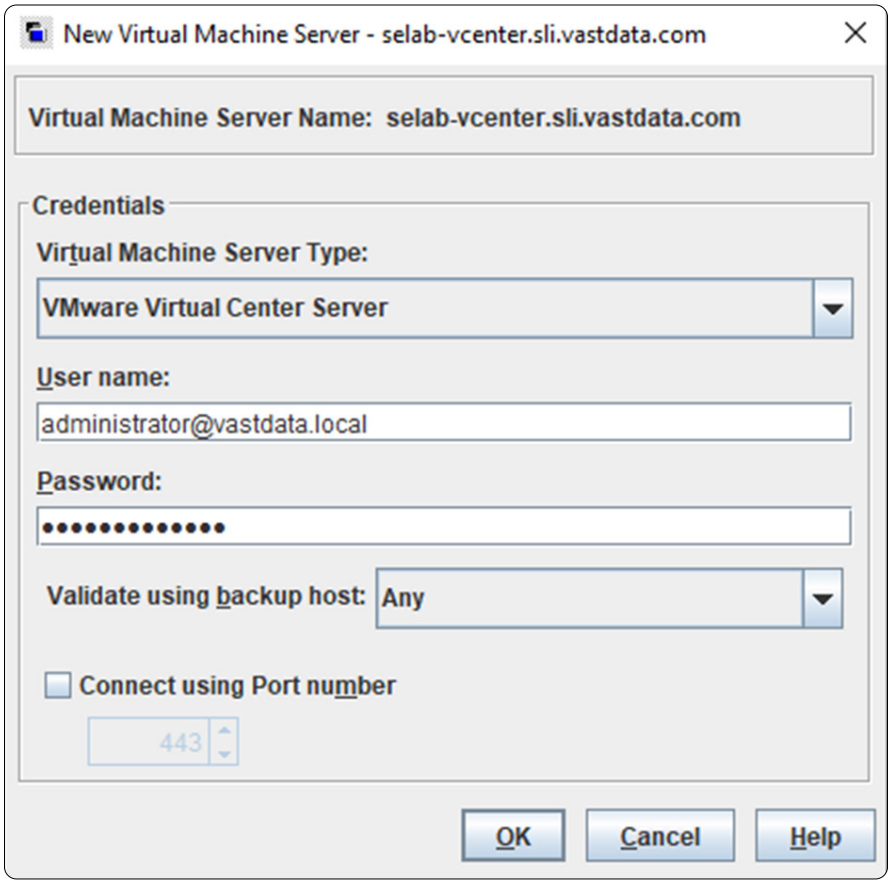


Figure 15 - Credentials for the Virtual Machine Server

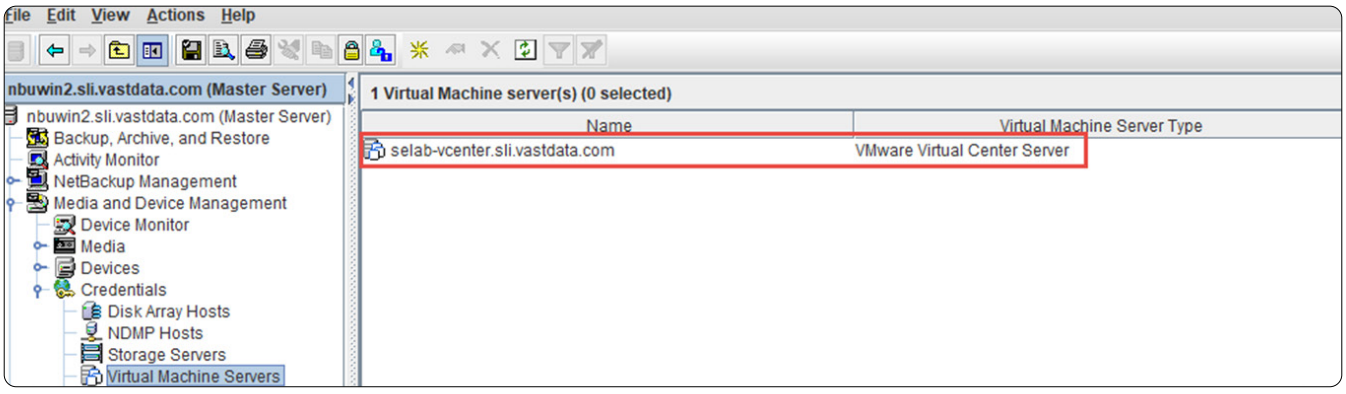


Figure 16 - Successfully Added Virtual Machine Server

Adding VAST as a Target

The work flow for adding storage begins in the Credentials section of Cohesity and proceeds

- Credentials → Storage Servers
- Devices → Diskpool
- NetBackup Management → Storage Units

Cohesity NBU UI walks the user through all of the steps in the creation process but pausing after each step is also available.

Advanced Disk with VAST NFS

Using an Advanced Disk configuration optionwith VAST is a simple way to backup to storage but keep in mind that a lot of the Cohesity functionality is not available for Advanced Disks. If data simply needs to be backed up then this is a reasonable option.

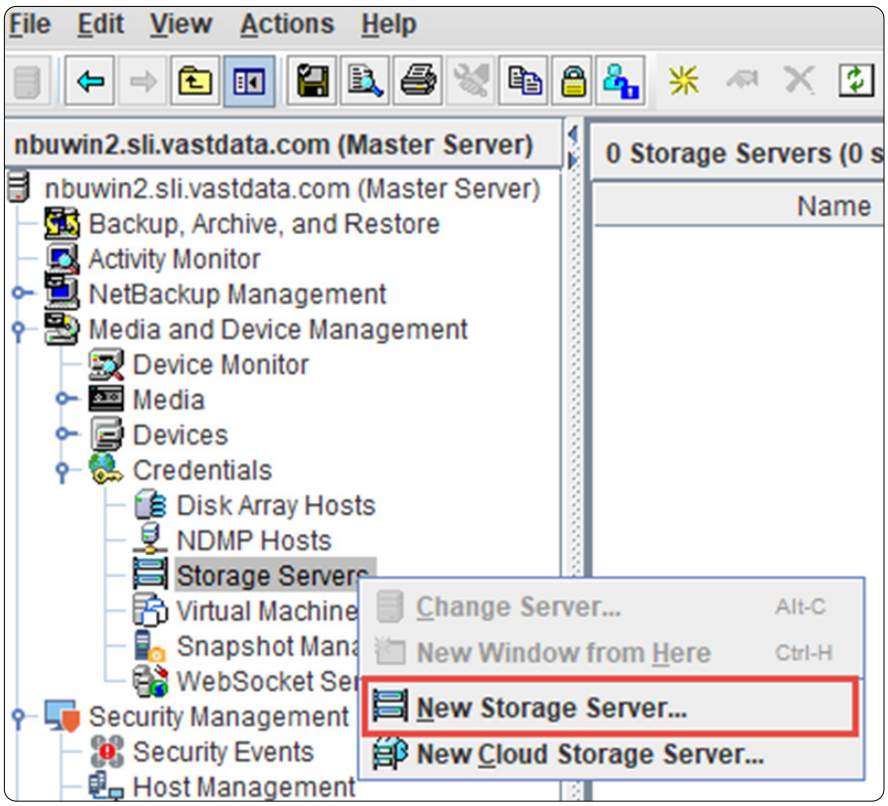


Figure 17 - Create New Storage Server

To start, right click on ***Storage Servers*** underneath ***Credentials*** and a select ***New Storage Server*** (Figure 17). A Storage Server Configuation Wizard window opens up (Figure 18). Select ***AdvancedDisk*** and click ***Next***.

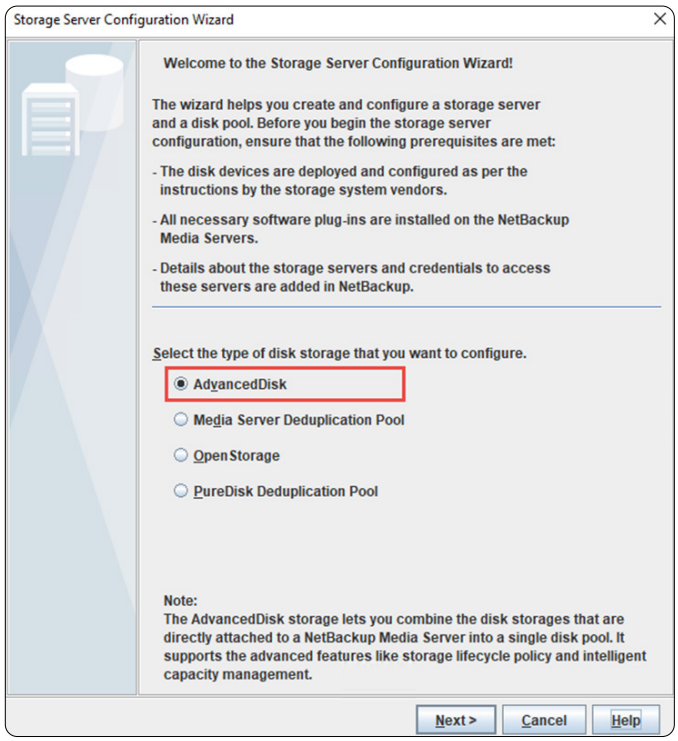


Figure 18 - Selecting Storage Server Type as Advanced Disk

On the next window (Figure 19), select the Media Server that will be used to write to the VAST cluster.

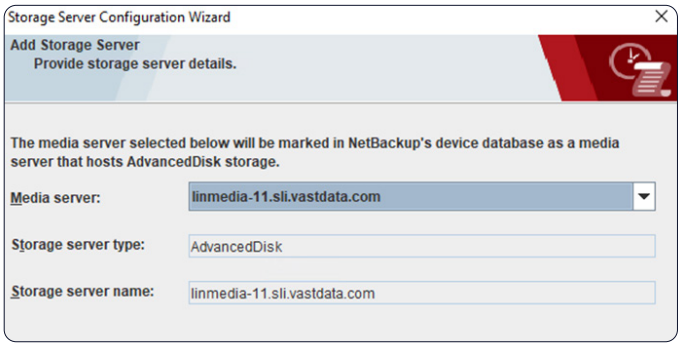


Figure 19 - Selecting the Media Server

The next window (Figure 20) is a summary of the settings. Review the setings and click ***Next.***

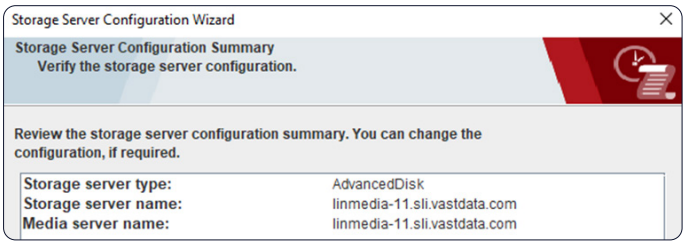


Figure 20 - Review Storage Server Settings

In Figure 21, it shows the successful creation of the Storage Server. It also allows the user to exit the workflow or continue on creating the Disk Pool. Click ***Next*** to continue on.

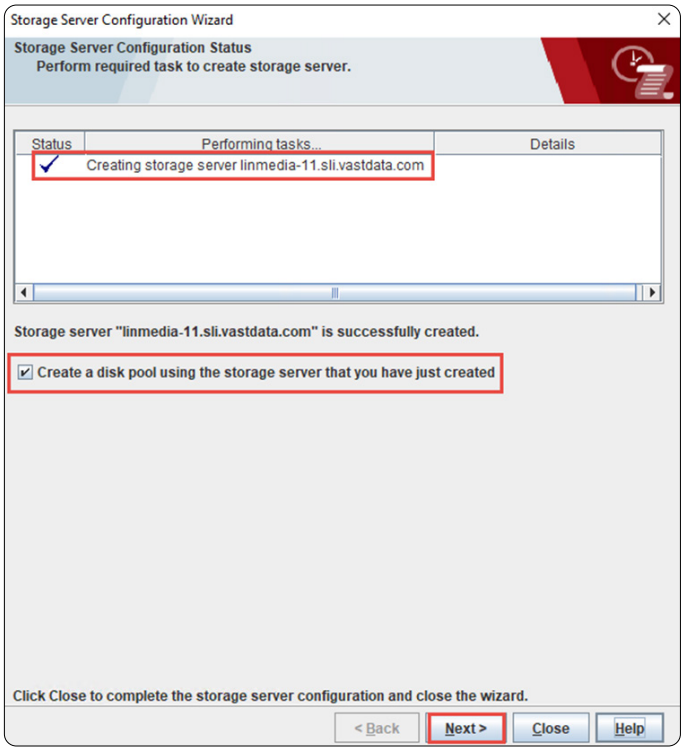


Figure 21 - Successfully Created Storage Server

The next step is the process of selecting the VAST Data volume that's been mounted to the Media Server. If this has not been completed yet then visit the section - Create VAST NFS View.

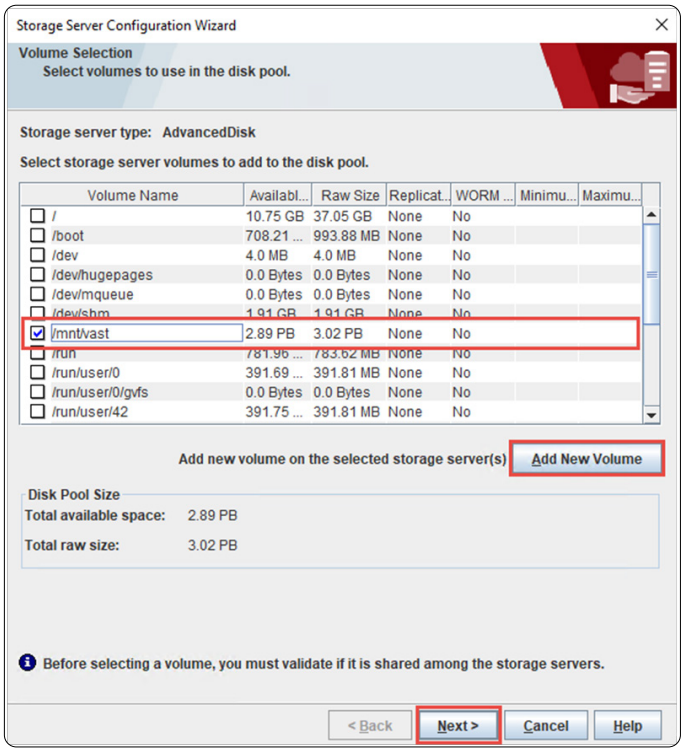


Figure 22 - Select Storage Server Volume for Disk Pool

Once an appropriate volume is mounted to the Media Server but does not show in the list in Figure 22 then click ***Add New Volume***. This will bring up a window as shown in Figure 23.



Figure 23 - Adding New Volume

Enter in the appropriate path and click ***Validate and Add***. The volume should now show as in Figure 22. Check the box for that volume and click ***Next***.

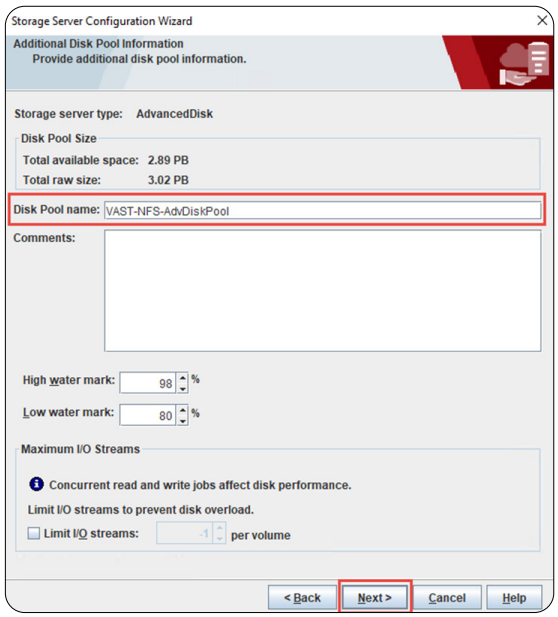


Figure 24 – Adding Disk Pool Name

In the next window (Figure 24), add a name for the Disk Pool and review the other settings if needed and then click ***Next.***

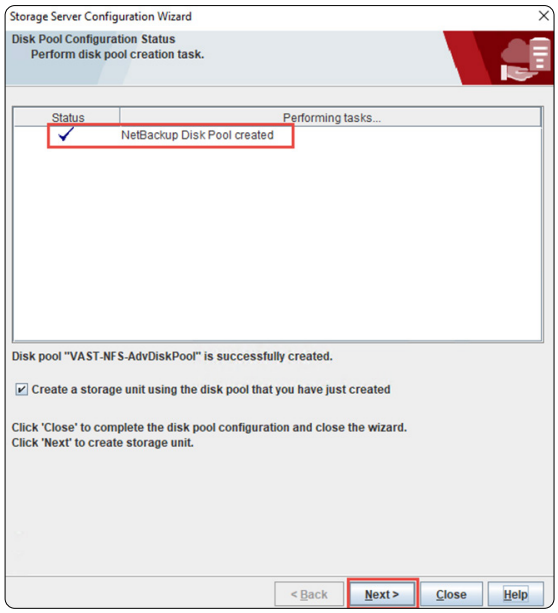


Figure 25 – Successful Creation of the Disk Pool

Figure 25 shows the successful creation of the Disk Pool. Click ***Next*** to continue on to the Storage Unit creation.

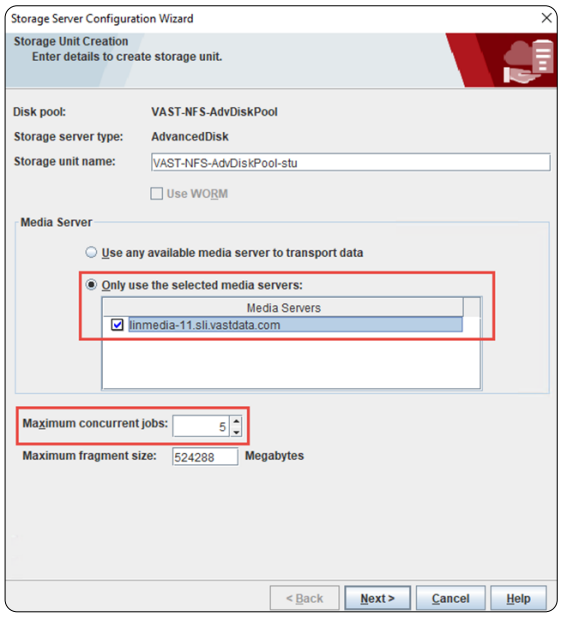


Figure 26 - Configuration of the Storage Unit

Enter a name for the Storage Unit as shown in Figure 26. Also, here is where the user can select which and how many Media Servers are able to write to the storage unit. In this example, only one specific Media Server has been given access to transport the data. Click ***Next*** to continue.

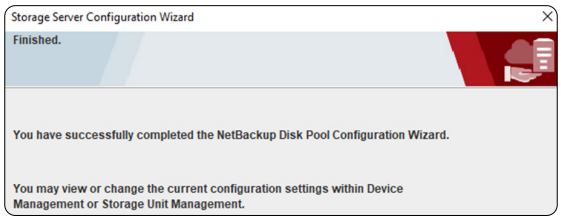


Figure 27 - Successful Creation of the Storage Unit

The next window (Figure 27) simply highlights the successful creation of the Storage Unit.

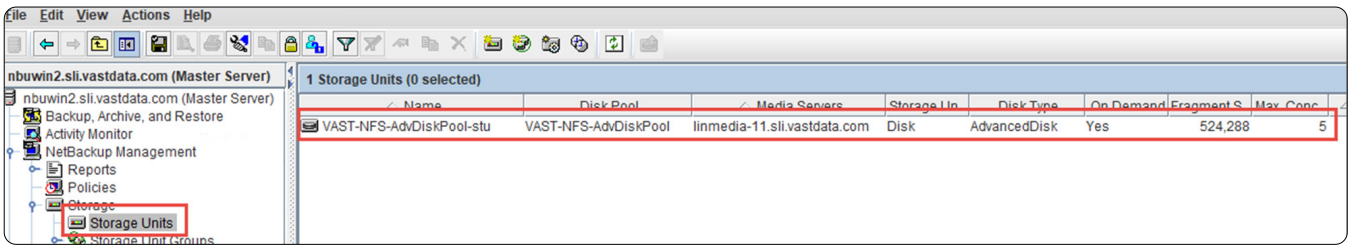


Figure 28 - Verfication of the Storage Unit

Looking under ***NetBackup Management → Storage*** and then highlighting ***Storage Units*** verifies that the Storage Unit is now available for backups (Figure 28) and can be assigned to policies.

Cloud Storage with VAST S3

Cloud storage with S3 is similar to an Advanced Disk in its functionality. It is a basic backup destination with limited NetBackup features, but works well for most environments.

The process for creating an S3 Storage Unit starts the same as was described for an Advanced Disk but in this scenario ***New Cloud Storage Server*** is selected instead (Figure 29).

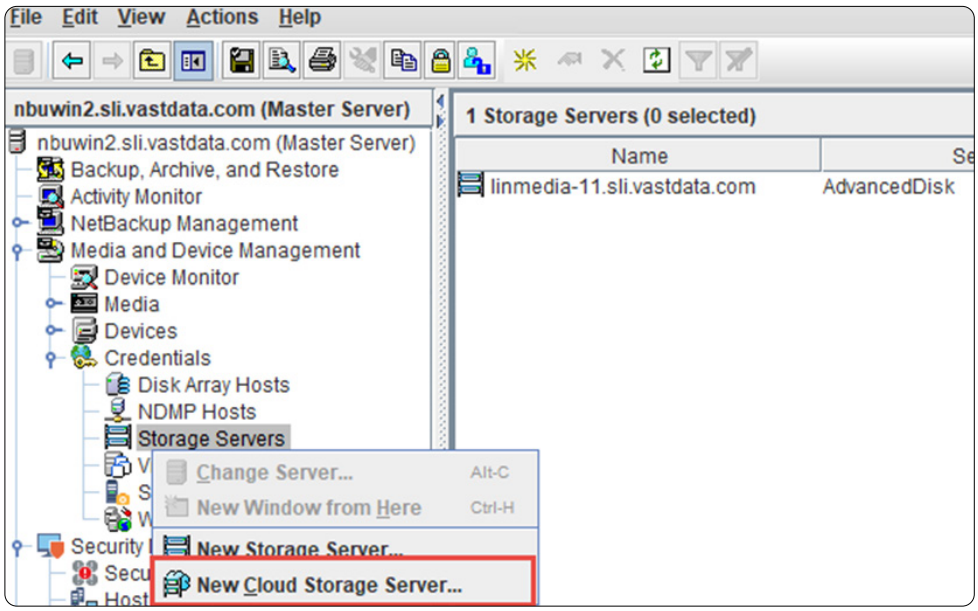


Figure 29 - Create New Cloud Storage Server

The next window (Figure 30) brings to attention a number of prerequisites that are needed for creating a Cloud Storage Server. Most of the concerns were addressed in previous sections of this document, specifically:

- Security Certificate – Section: Adding Private Cloud CA Certificate
- Credentials – Section: Create a VAST S3 User
- Storage Provider – Section: Adding Cloud Configuration Package

Not listed in the prerequisite list but is also needed is:

- Device Mapping - Section: Adding Device Mapping Files

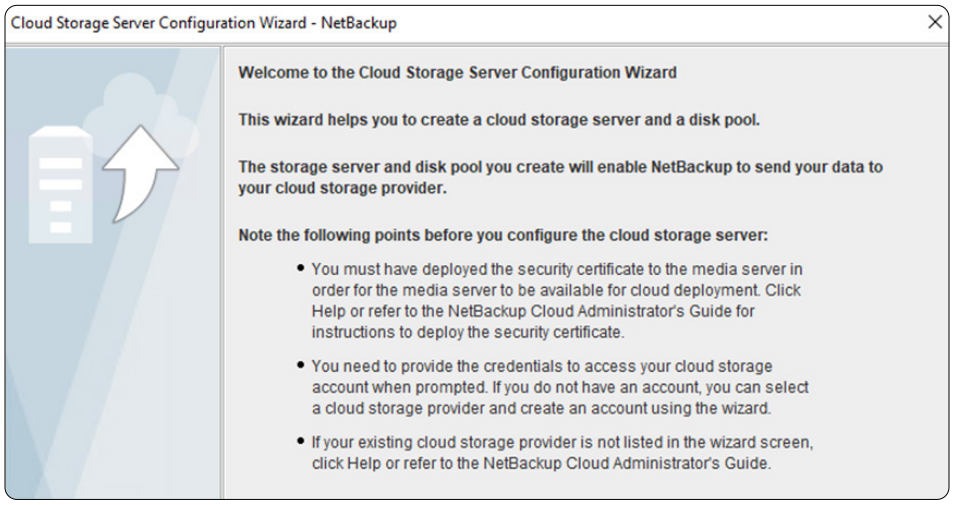


Figure 30 - Key Points Before Creating Cloud Storage Server

Once the key points have been addressed click ***Next***.

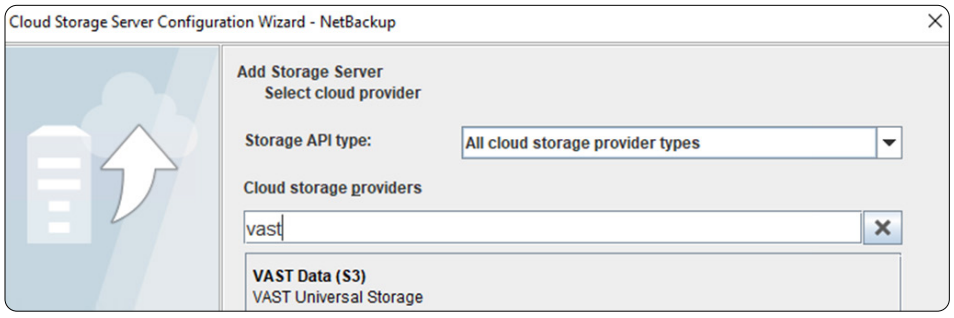


Figure 31 - Selecting VAST Data as the Storage Provider

In the next window (Figure 31) search for VAST as the cloud provider by either typing in a name to filter or simply scroll through the list to find VAST. Select it and then click ***Next.***

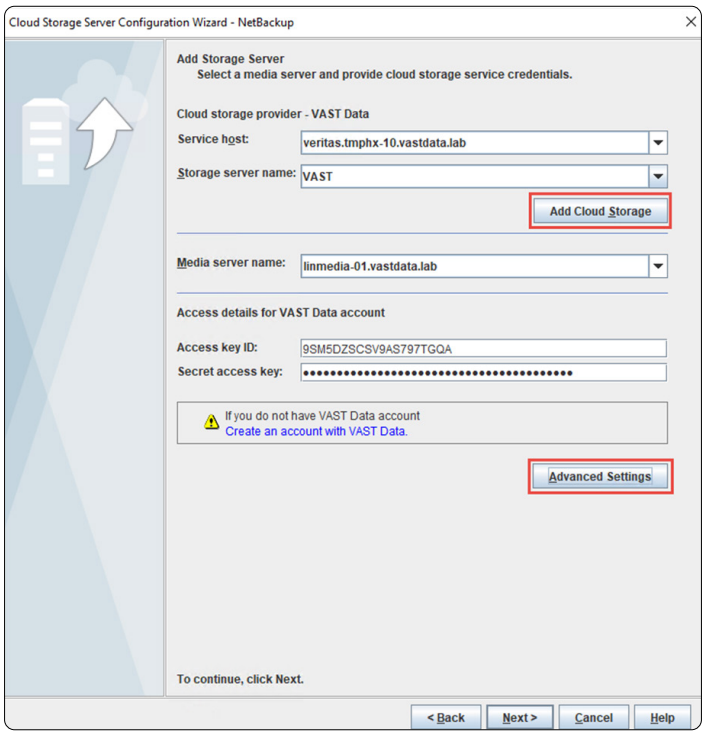


Figure 32 - Configuring the Cloud Storage

Figure 32 highlights several tasks needed to configure the Cloud Storage. The fields show an already configured setup so we'll return to this figure in a bit. To create one click on the ***Add Cloud Storage*** button as shown in the figure.

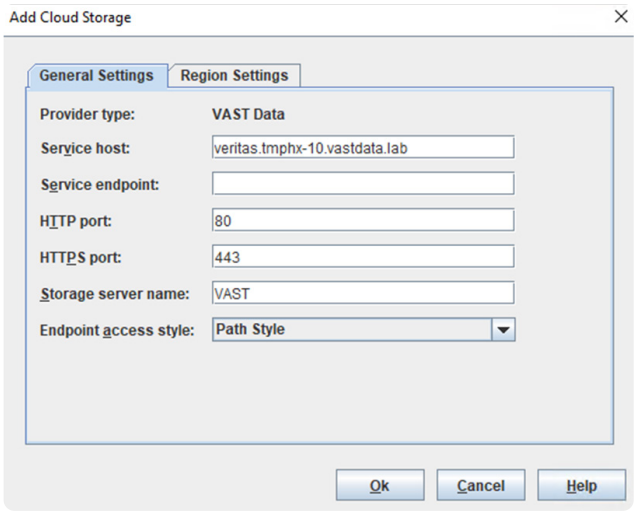


Figure 33 - Adding VAST Cloud Storage

This brings up the Add Cloud Storage window as shown in Figure 33. The service host here is the VAST VIP appended to the DNS name of the cluster. On the VAST cluster, a simple S3 Endpoint was created without any alias, therefore the Service Endpoint is left empty. Using an endpoint allows NetBackup to create and delete buckets from within the software. A single service host can be used multiple times to connect to but it is only created once.

Note: Creating multiple service hosts would be a way to segregate various backup groups within the same VAST cluster. This would be achieved by creating various VIPs within VAST and then creating the corresponding NetBackup Service Hosts.

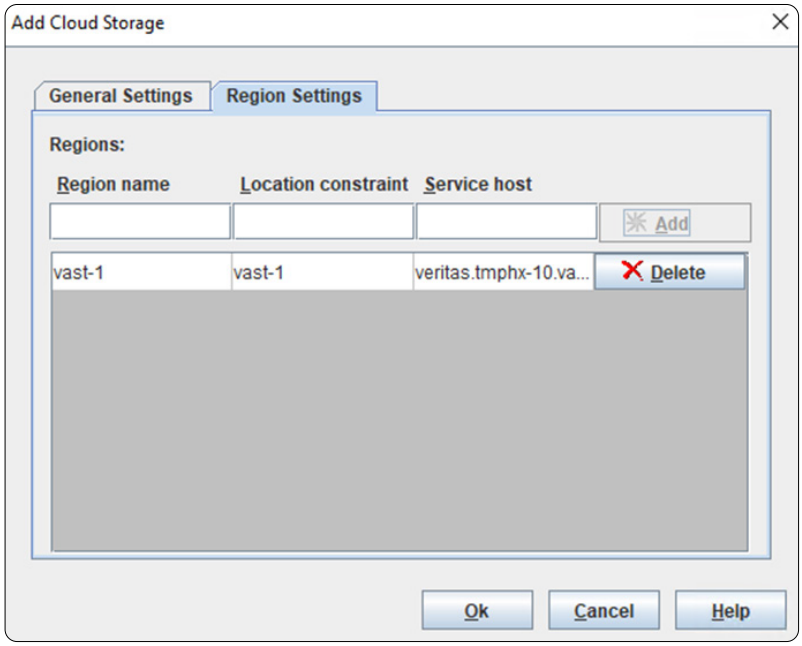


Figure 34 - Configuring the Region

Clicking on the Region Settings brings up the window as shown in Figure 34. Make sure to use 'vast-1' as both the region name and location constraint. The Service host entry should match the same from the General Settings tab.

Note: It is critical that the region name and location constraint be 'vast-1' or 'VAST-1'.

Once both tabs are filled out, click ***OK***. The options that are shown for ***Service Host*** and ***Storage Server Name*** should now be available as shown in Figure 32.

Enter the access and secret access keys that were created for the S3 User (See - Create a VAST S3 User). Finally click on the ***Advanced Settings*** button. This will bring up the window as show in Figure 35.

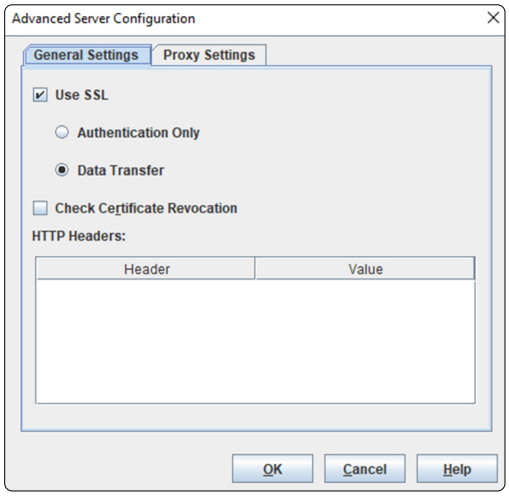


Figure 35 - Advanced Server Configuration

Ensure that the ***Check Certificate Revocation*** box is unchecked, the ***Use SSL*** is selected with the ***Data Transfer*** option and then click OK. Then click ***Next*** to move onto the next window.

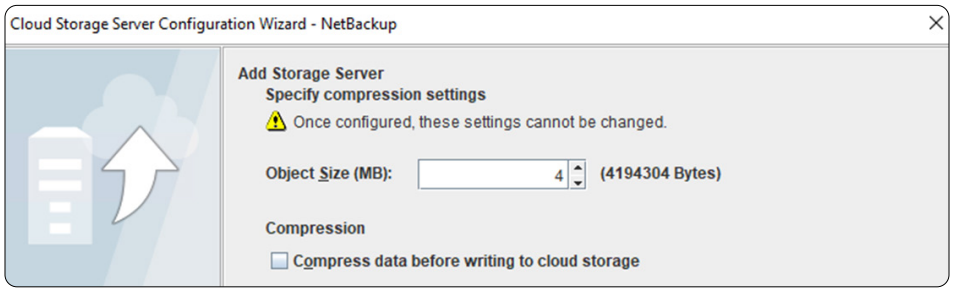


Figure 36 - Configuring Additional Settings

Figure 36 allows the user to configure object size and compression. Here the object size was left as the default and compression was left off, as the VAST cluster has compression enabled by default. The compression setting is specific to each customer's environment and careful thought should be used in addressing this setting. Accept the warning window (not shown) that compression object size settings cannot be changed later. Review all of the settings in the next window and click ***Next*** and the Storage Server creation will begin.

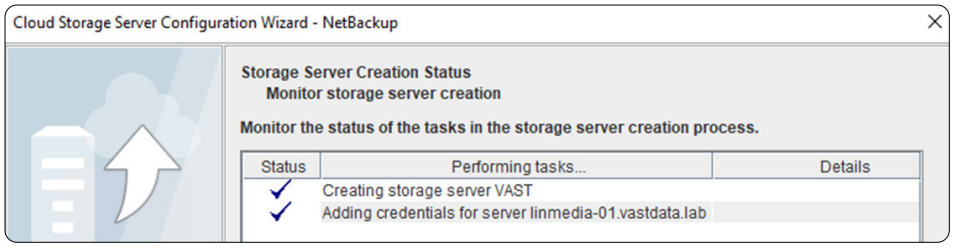


Figure 37 - Successful Creation of S3 MSDP Storage Server

When the Storage Server creation completes you will receive the message shown in Figure 37.

Note: To ensure that the second phase completes properly make sure the VAST CA Certificate has been appended to the cacert.pem file. This is discussed in the section – Adding Private Cloud CA Certificate.

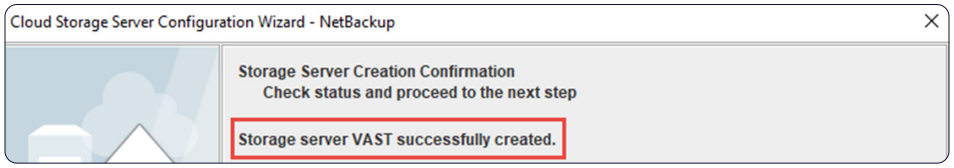


Figure 38 - Confirmation Storage Server Created

An additional confirmation is shown in Figure 38 and allows the user to exit the workflow if desired. However, click ***Next*** to continue creating the Disk Pool.

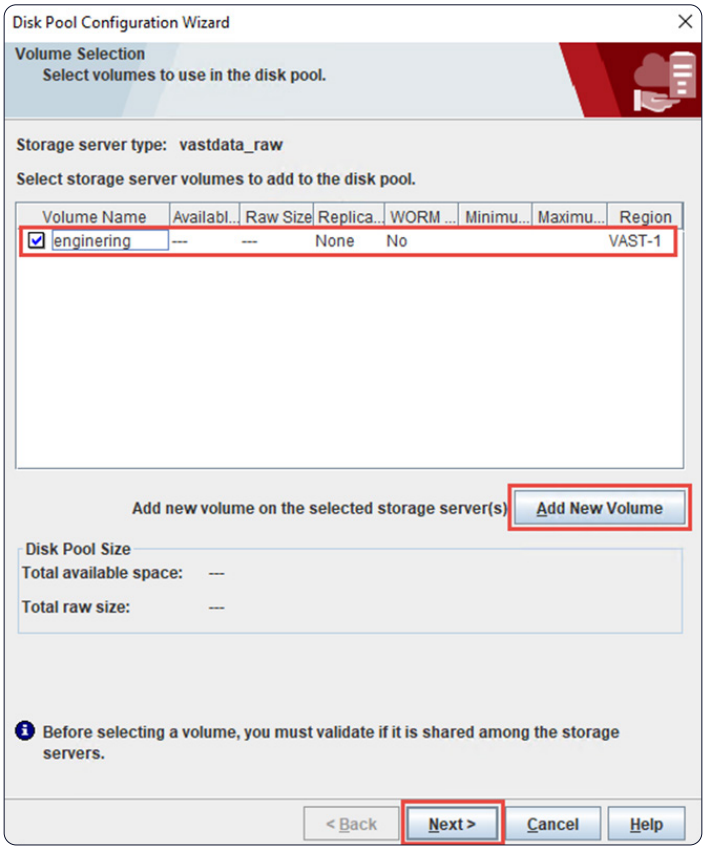


Figure 39 - Select Disk Pool Volume (Bucket)

Figure 39 shows the volume (bucket) selection window and one already selected. If there are none available then one needs to be created and that is done by clicking the ***Add New Volume*** button.

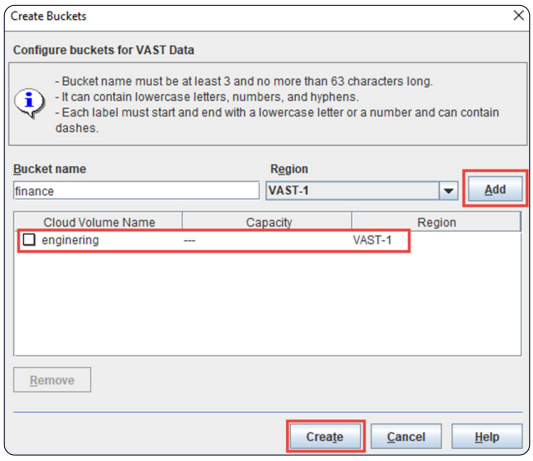


Figure 40 - Create Bucket

In the ***Create Buckets*** window (Figure 40), enter a Bucket Name and Region and then Click ***Add***. The bucket will appear in the lower part of the window. Create as many buckets as needed and then click ***Create***. This will now return to the Disk Pool wizard (Figure 39) where the newly created bucket(s) are now available. Select the bucket and click ***Next***.

Note: Only one volume should be used for a disk pool. Do not select multiple volumes.

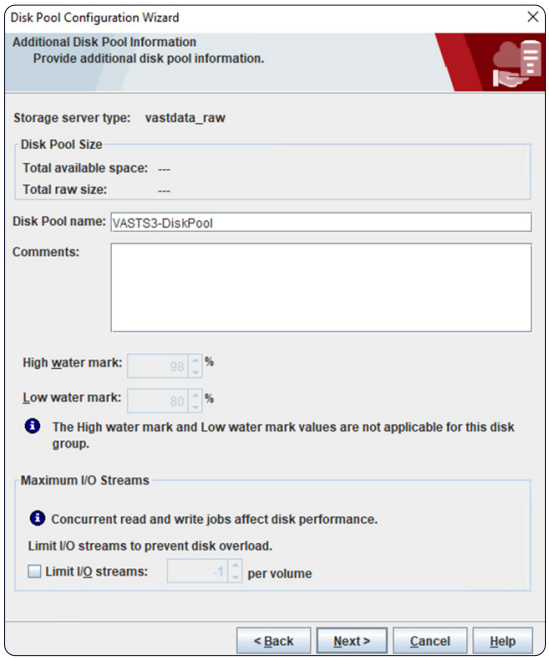


Figure 41 - Naming the Disk Pool

In Figure 41 the Disk Pool was given a name. There are some additional limit settings that are configurable but are left at their defaults. After clicking ***Next*** confirm everything on the summary window and then click ***Next*** again.

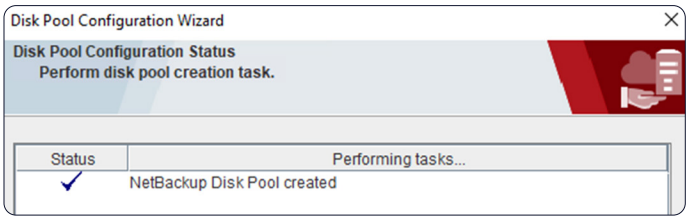


Figure 42 - Successful Creation of the Disk Pool

When the Disk Pool creation finishes the result appears as in Figure 42. This window is also another opportunity to exit the workflow but click Next so the final step of creating the Storage Unit can be completed.

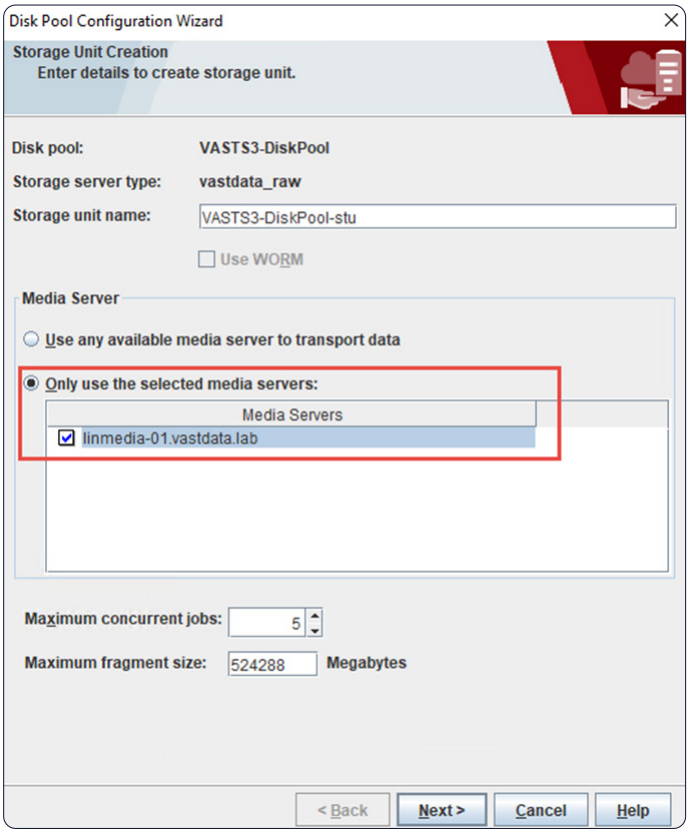


Figure 43 - Storage Unit Configuration

In the ***Storage Unit Creation*** window (Figure 43) give the Storage Unit a name or accept the default name. The Media Server selection is identical to the process when creating an Advanced Disk where specific Media Servers can be selected to transport data. The maximums that are at the bottom are environment specific. In this setup it can easily support 5 concurrent jobs so that setting has been increased accordingly. Click ***Next*** to continue.

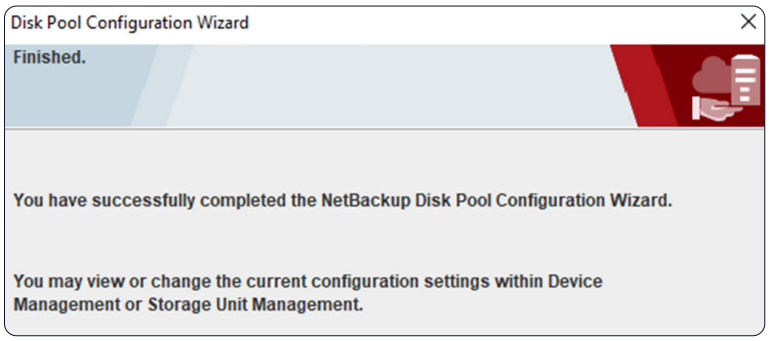


Figure 44 - Successful Storage Unit Creation

Successful creation of the Storage Unit is highlighted in Figure 44 and then verified under Storage ➔ Storage Units (Figure 45).

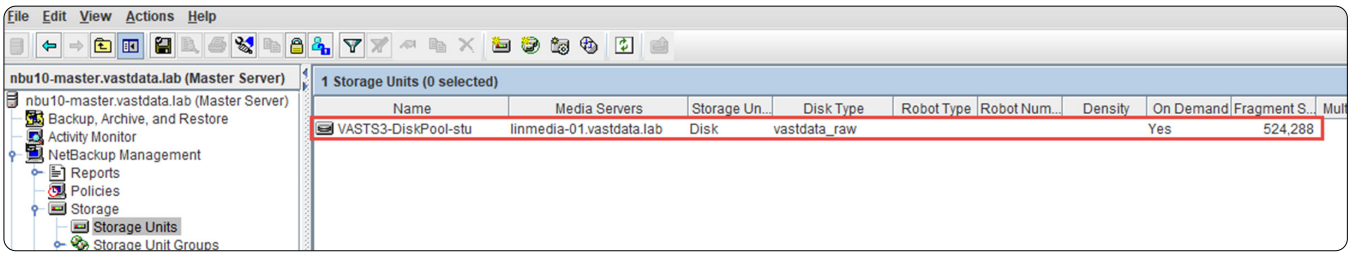


Figure 45 - Confirmation Cloud Storage Unit Creation

MSDP Cloud with VAST S3

A relatively new concept for Cohesity NetBackup is MSDP Cloud or MSDP-C, which incorporates many of the benefits of the Media Server Deduplication Pool (MSDP) with the disk pool created from cloud storage. This is a direct result of the VAST cloud connector that is discussed in the section - Adding Cloud Configuration Package.

Note: Check the latest Cohesity NetBackup HCL for a list of the current functionality that MSDP Cloud offers since not all of the MSDP benefits are currently available.

Below is an example of how to configure an MSDP Cloud Storage Server, a disk pool with a VAST S3 Bucket and a storage unit. This will be done from the Web UI since the cloud disk pool creation is not available through the JAVA UI.

Starting on the left side of the Web UI go to ***Storage*** and select ***Storage configuration*** (Figure 46).

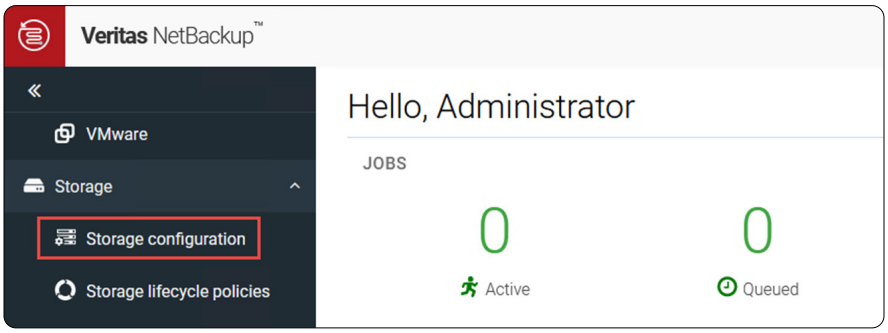


Figure 46 - Select Storage Configuration

This will bring up the Storage configuration window. Click on the ***Add*** button to add a new storage server (Figure 47).

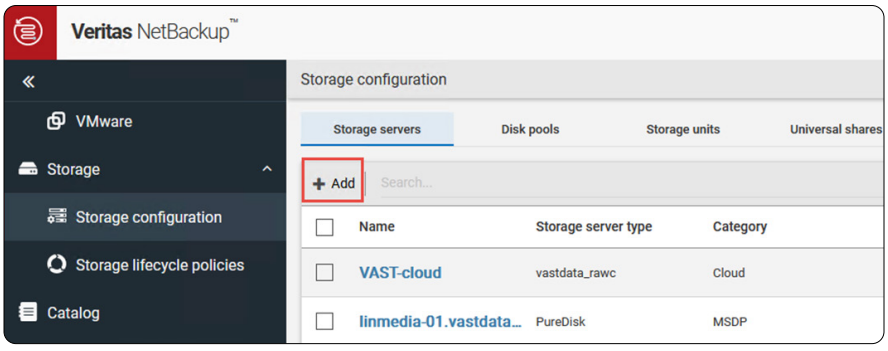


Figure 47 - Add Storage

The Add Storage server window appears and, in this example, select ***Media Server Deduplication Pool (MSDP)*** as shown in Figure 48.

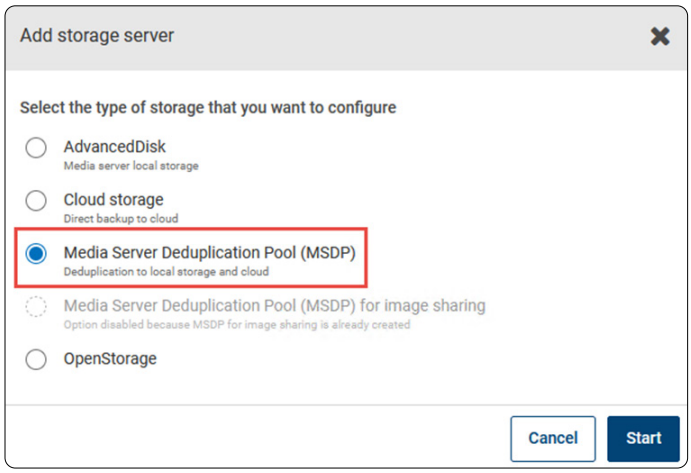


Figure 48 - MSDP Selected

In the ***Add MSDP Storage server window*** (Figure 49) select the media server to be used and this will pop up the Select Media Server shown in Figure 50. Select the appropriate media server and then click ***Select***.

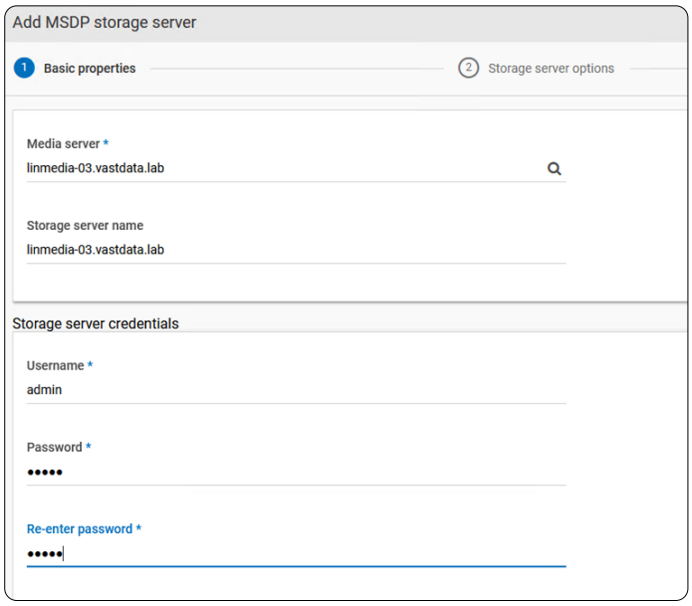


Figure 49 - Media Server and storage server credentials

Add a username and login credentials. The user name and password are only particular to this storage but make note of the credentials in case maintenance is needed later. Click ***Next*** when finished.

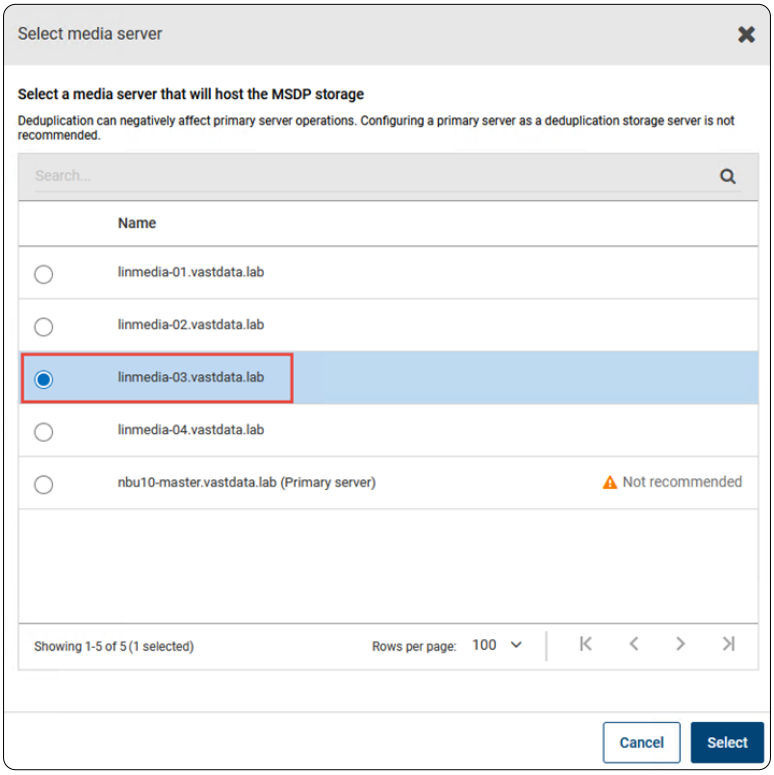


Figure 50 - Selecting Media Server for MSDP

On the next window (Figure 51) add the ***Storage path*** for the installation of the deduplication engine and other files.

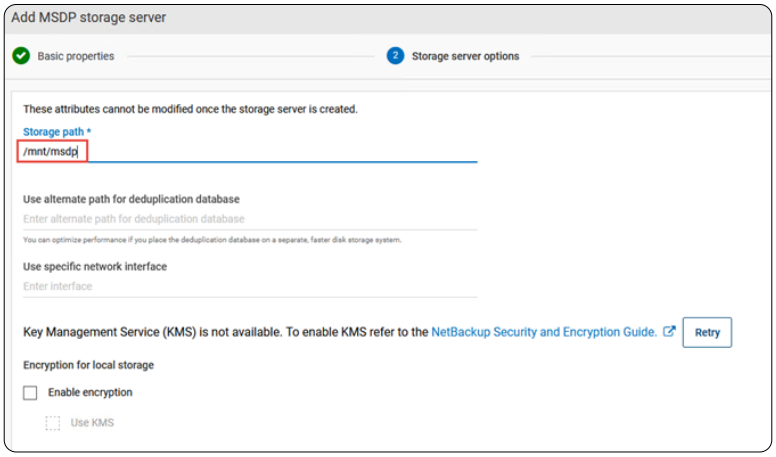


Figure 51 - Storage Path for MSDP installation

Here encryption is disabled. If you choose to enable encryption, the VAST cluster will not be able to deduplicate the data, resulting in more usable storage being consumed. The benefit of using S3 in this scenario is that the connection to the bucket and cloud are already secure. Disabling encryption maximizes VAST deduplication and similarity data reduction for better storage utilization.

NOTE: There are often scenarios where encrypting data is required for security purposes. Please consult with your IT Security team if you have questions.

The next screen (Figure 52) is simply another chance to add additional media servers to this storage server for additional compute and to handle the initial NetBackup deduplication.

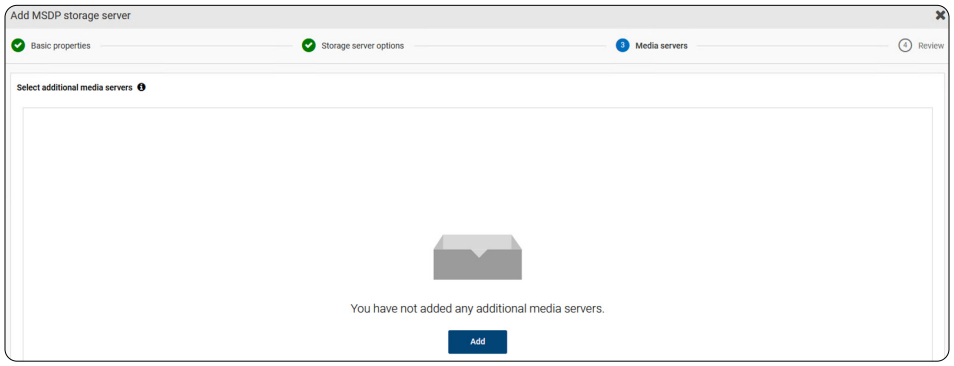


Figure 52 - Option to Add Additional Media Servers

Review the settings on the next window (not shown) and click ***Save***. Once the storage server has been created it will show up as in Figure 53.

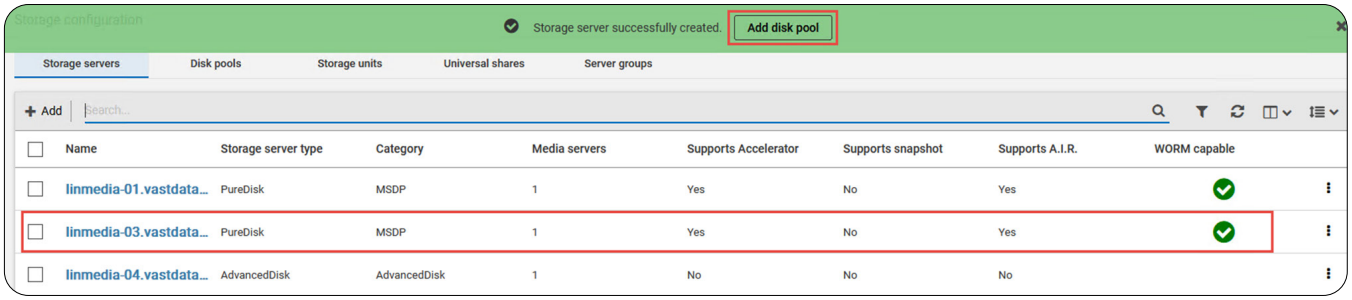


Figure 53 - MSDP Storage Server Successfully Created

Taking the easy handoff and clicking the green ***Add disk pool*** button at the top immediately pops up the Add disk pool window (Figure 54). The media server should already be selected. Give the disk pool a name and click ***Next***.

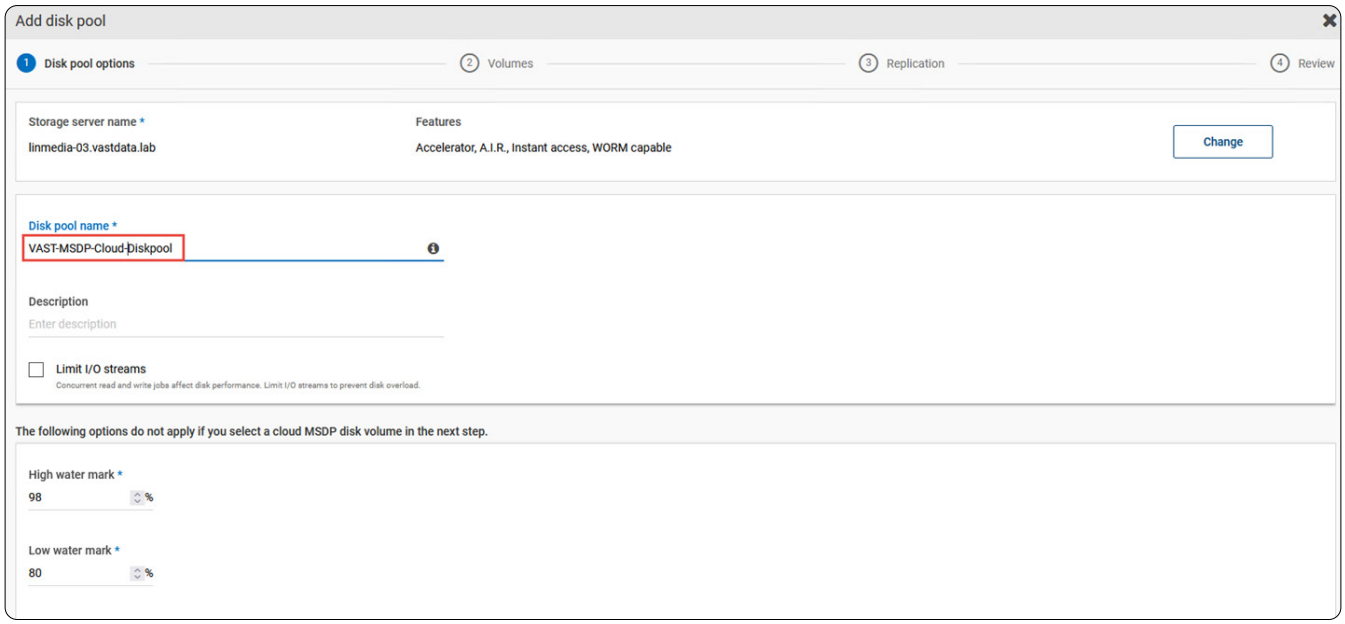


Figure 54 - Disk Pool Name

The next window (Figure 55) is where a volume is selected for the disk pool. The default volume is the disk used by the media server. To create an S3 volume click on ***Add volume.***

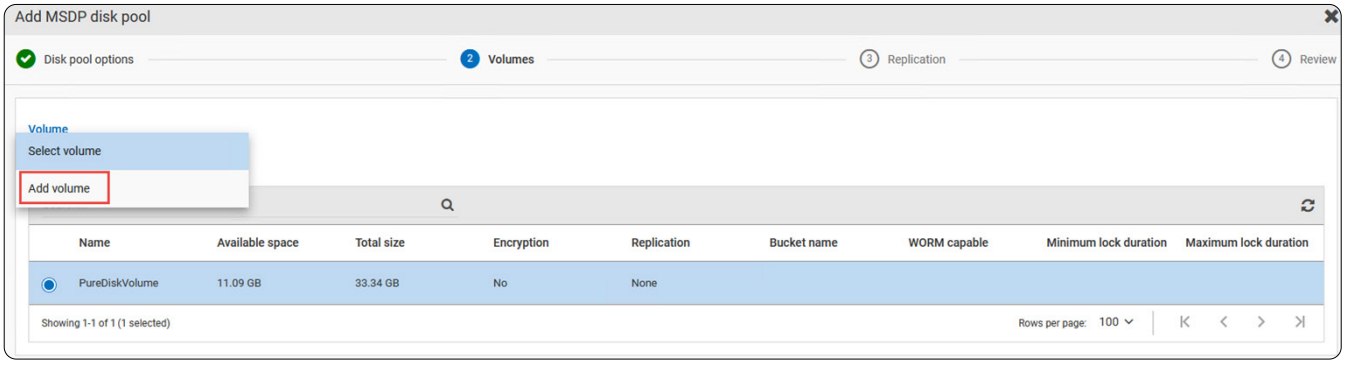


Figure 55 - Add Volume to Disk Pool

Now in the ***Add MSDP disk pool*** window (Figure 56) give the volume a name and then click on ***Cloud storage provider***. This will open up another window where a text search for VAST brings up the choice as shown in Figure 57.

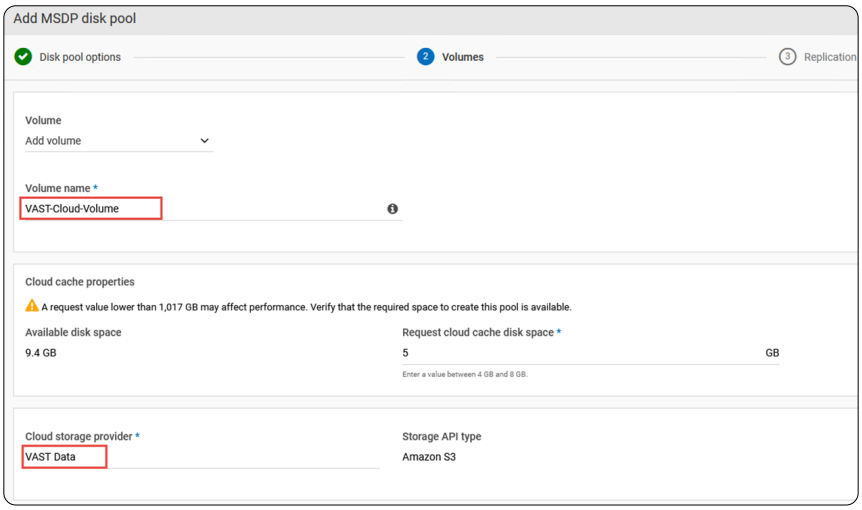


Figure 56 - Volume Name and Cloud Storage Provider

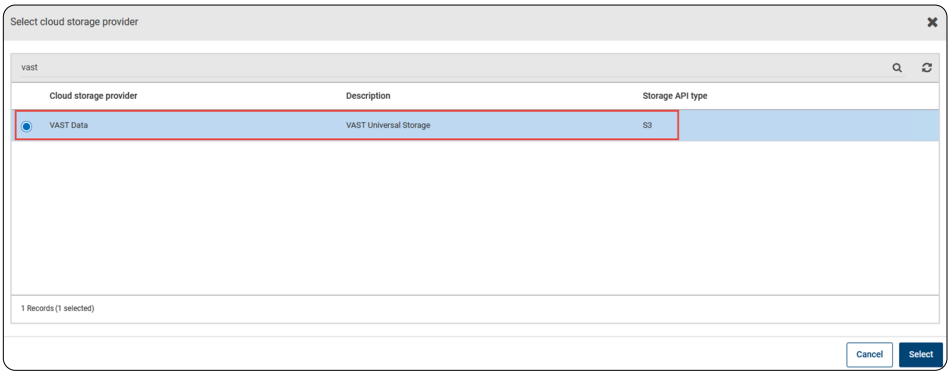


Figure 57 - Selecting VAST Data Cloud Provider

After selecting VAST and scrolling further down the page the ***Region*** is selected (Figure 58). If one is not available then it can be added in the same way as shown and described for Figure 33 and Figure 34.

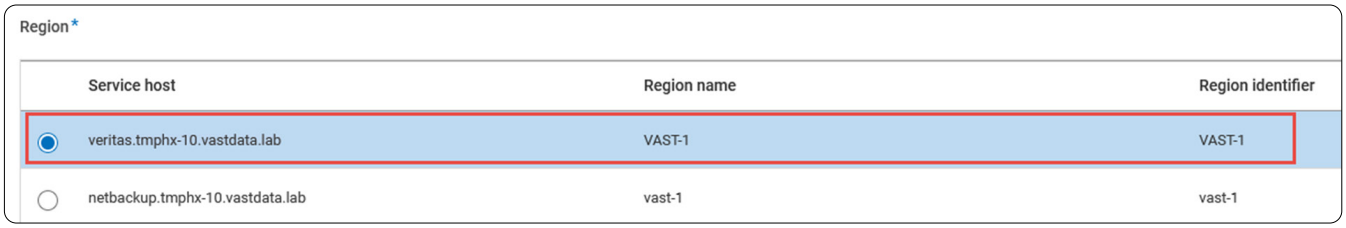


Figure 58 - Selecting VAST Data Configured Service Host

Scrolling ever further down the ***Add MSDP disk pool window***, enter the S3 user credential and confirm the Check certificate revocation is unchecked.

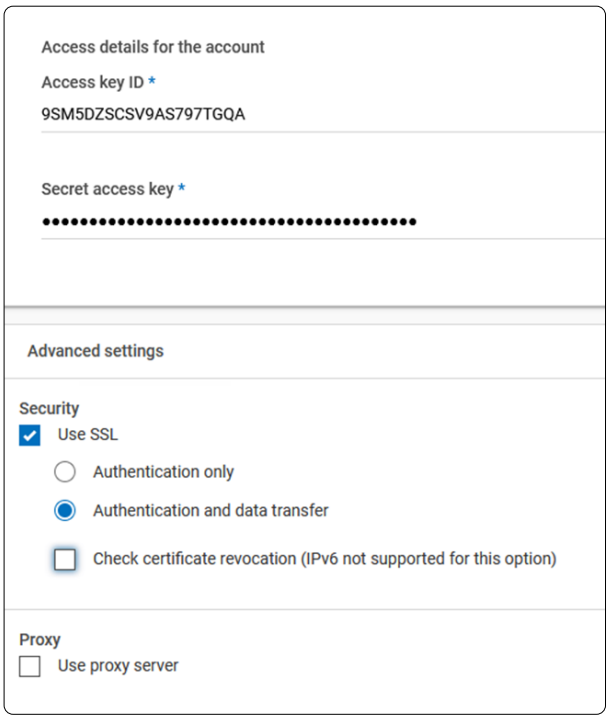


Figure 59 - User Credentials for VAST Data Service Host

Finally, at the bottom of the window is the Cloud bucket selection (Figure 60). A known bucket can just be entered or a list of buckets can be generated by clicking the ***Retrieve list***. Clicking ***Retrieve list*** will test the S3 connection settings and bring up a list of buckets that that particular S3 user is able to see.

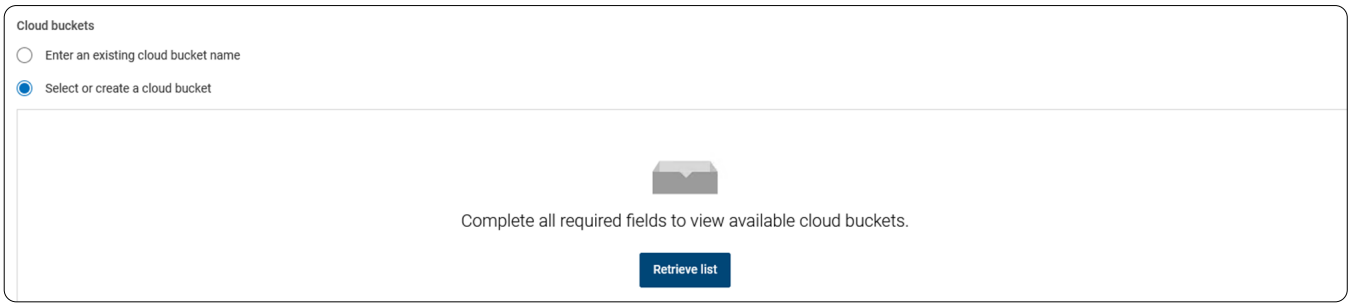


Figure 60 - Selecting VAST Cloud Bucket

Select an existing bucket or add one by clicking the plus button (not shown). Clicking the add button brings up the ***Add a bucket*** window shown in Figure 61. Enter a bucket name and VAST-1 as the region and click ***Add***.

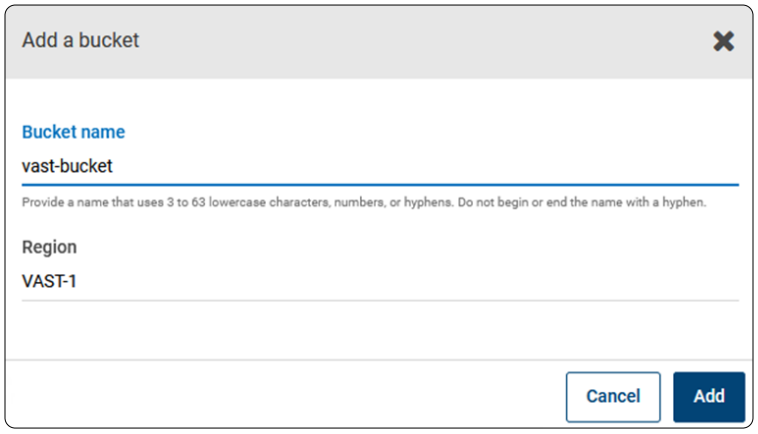


Figure 61 - Adding Bucket to VAST

Now that the bucket has been added it will show up in the list (Figure 62). Select it and click ***Next***.

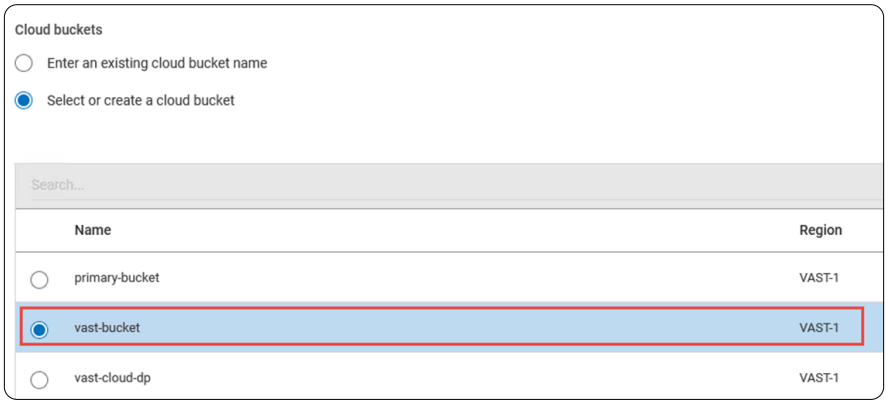


Figure 62 - Selecting Newly Created VAST Bucket

Review the settings for the disk pool and click ***Finish*** when ready.

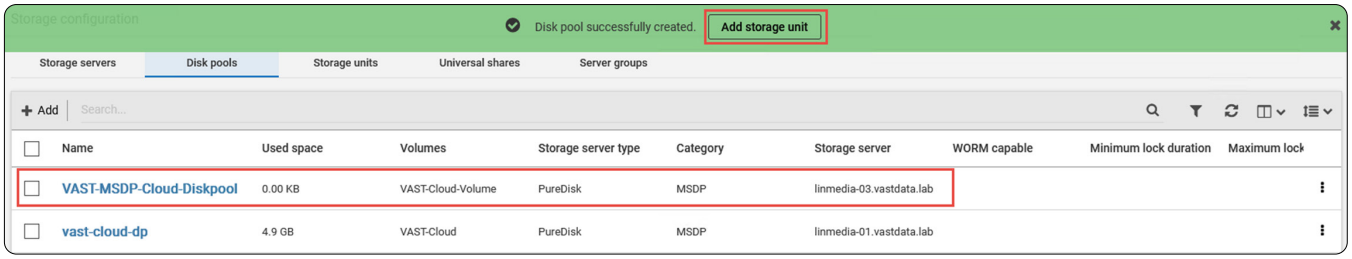


Figure 63 - Disk Pool Successfully Created on VAST Cloud

The disk pool is now created as shown in Figure 63. Click on the green ***Add storage unit*** button at the top. This brings up the window as shown in Figure 64. Give the storage unit a name and adjust the other settings as needed and then click Next.

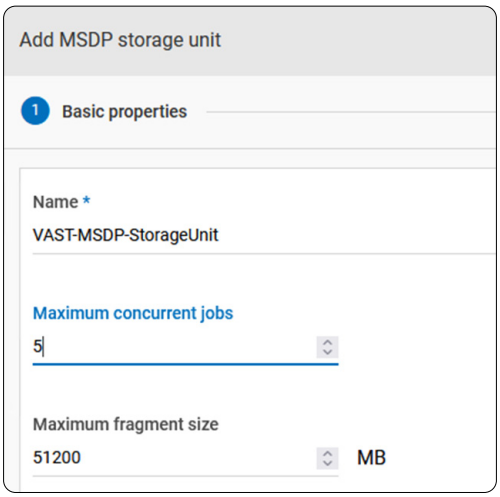


Figure 64 - Creating Storage Unit

Select the disk pool (Figure 65) that was created in the previous step and click ***Next.***

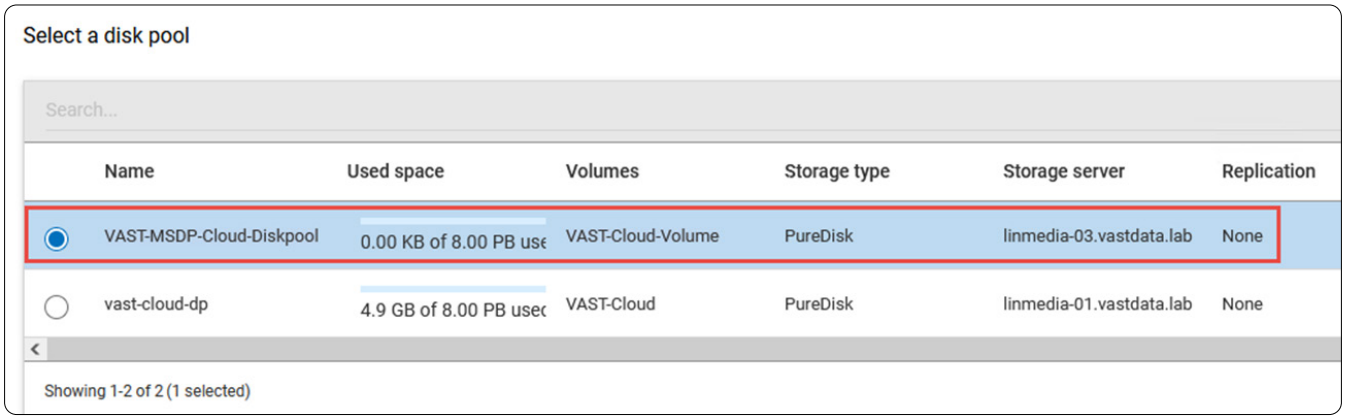


Figure 65 - Selecting Disk Pool for Storage Unit

Select the appropriate media server access (Figure 66) and click ***Next***, review the settings and click ***Save*** when ready.

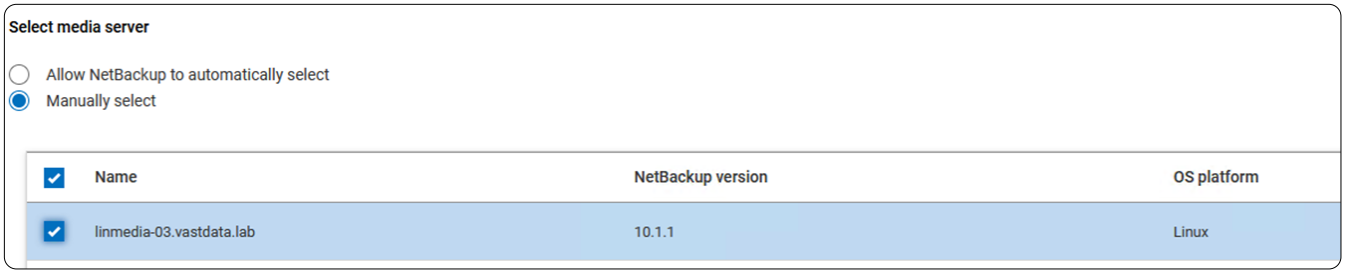


Figure 66 - Selecting Media Servers for Storage Unit

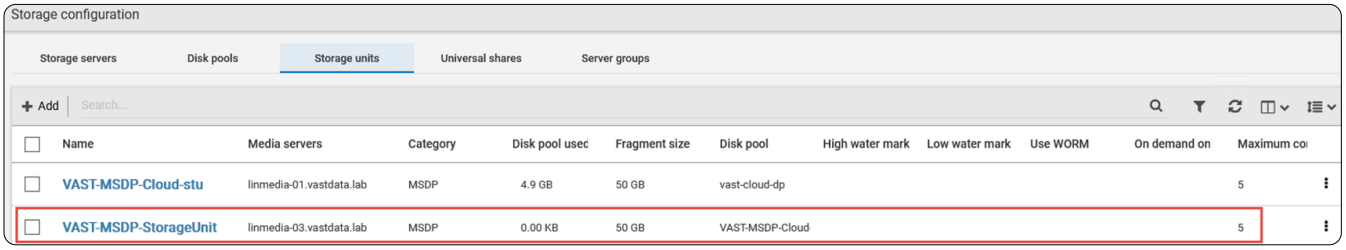


Figure 67 - Storage Unit Successfully Created

Once the storage unit is created, it will look like the one highlighted in Figure 67. The MSDP-Cloud storage server can now be assigned to policies.

Advanced Solutions

This section covers concepts beyond the creation of storage servers, disk pools and storage units looking at topics such disaster recovery, replication and duplication (not deduplication).

NetBackup Image sharing

Image sharing is a NetBackup concept that allows for the import and recovery of a backup catalog and the backup image from a cloud backup when access to the primary server is compromised. This is possible because not only is the data image backed up into the cloud but so is the catalog. This allows full access to the backed-up data.

The recovery requires a single-purpose, fully installed NetBackup Master Server, called a Cloud Recovery Server, which can either be run in the cloud or on a physical server. It is configured as a unique option of an MSDP storage server with access to the exact same Volume Name and bucket in the disk pool of the data that needs to be recovered.

The following sections highlight how to create a Cloud Recovery Server and how to recover data using it.

Configuring a Cloud Recovery Server

Currently, this server can only be installed on Linux. The installation process is very similar to any other Linux install, however, check the Cohesity NetBackup documentation for the latest specifications and installation tips for this server.

Once installed bring up the WEB UI to complete the configuration. This server will need the same tasks discussed earlier:

1. CloudProvide.xml – See section Linux Installation Adding Cloud Configuration Package
2. Device Mappings – See section Adding Device Mapping Files
3. CA Certificate – Since this server will be both the Master and Media Server it will need the CA certificate appended in the cacert.pem file. See section Adding Private Cloud CA Certificate

Once those tasks are complete a storage server needs to be created starting off in the same way discussed in the section - MSDP Cloud with VAST S3. The only difference for this storage server is it will be configured as shown in Figure 68. The selection is specific to a Cloud Recovery Server and only one can be configured on this server as it is single purpose system.

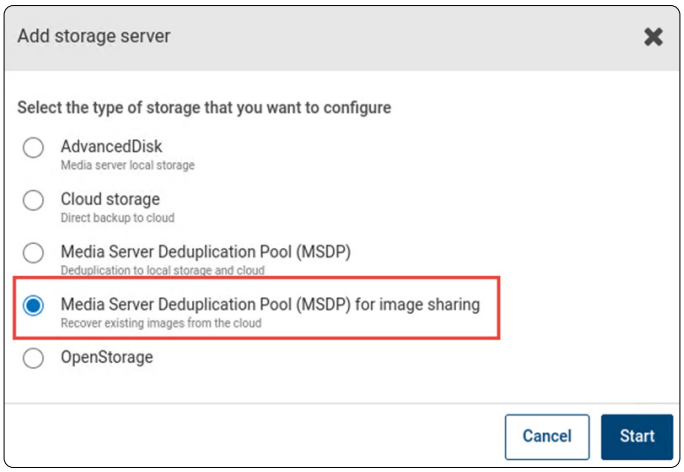


Figure 68 - Cloud Recovery Server Configured for Image Sharing

After selecting ***Media Server Deduplication Pool(MSDP) for Image Sharing*** click ***Start***. This continues the same process for an MSDP-Cloud Storage Server creation as before. Once completed it will look like what is shown in Figure 69. The ***Category*** column shows, ***MSDP for Image sharing***, which is specific for a cloud recovery server.

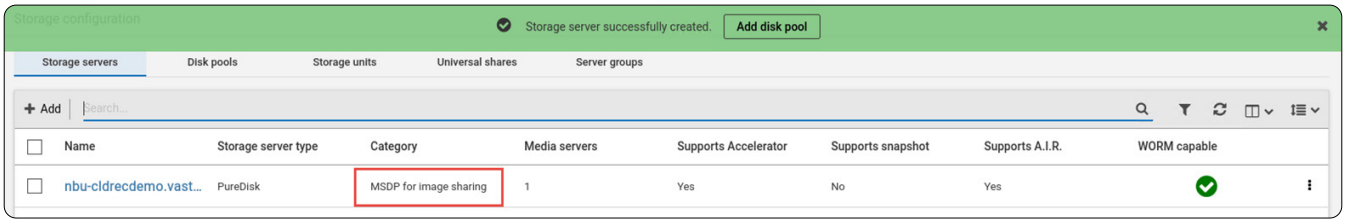


Figure 69 - Successful Creation of Cloud Recovery Storage Server

The last step to compete is the creation of a cloud disk pool pointing to the exact same Volume Name and bucket that is being used to backup data with an MSDP-Cloud storage server.

For ease, simply click on the green ***Add disk pool*** at the top and complete the disk pool creation process. This again, is the exact same process as when creating the MSDP-C disk pool. In this example, shown in Figure 70, the volume name matches the volume shown previously in Figure 56.

Note: It is imperative that the Volume selected matches the volume of the MSDP-C disk pool where data needs to be recovered.

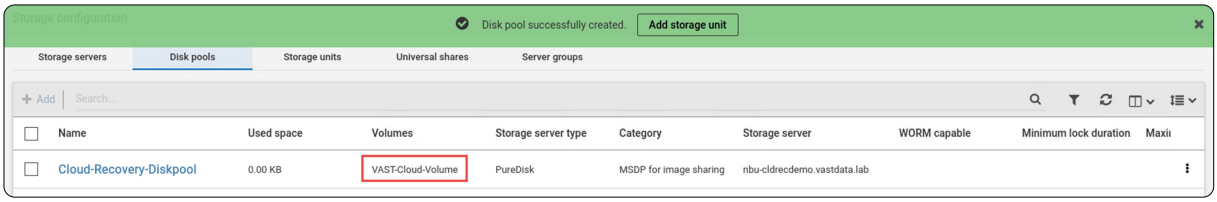


Figure 70 - Successful Creation of Cloud Recovery Disk Pool

A storage unit does not need to be created to recover data from the cloud. At this point the Cloud Recovery Server is ready to recover from this particular volume and bucket.

Restoring Data with Cloud Recovery Server

To recover data that has been backed up into the cloud with an MSDP-C storage server it is amazingly simple with a Cloud Recovery Server. If the primary server is unavailable use the following steps to recover the data with the Cloud Recovery Server.

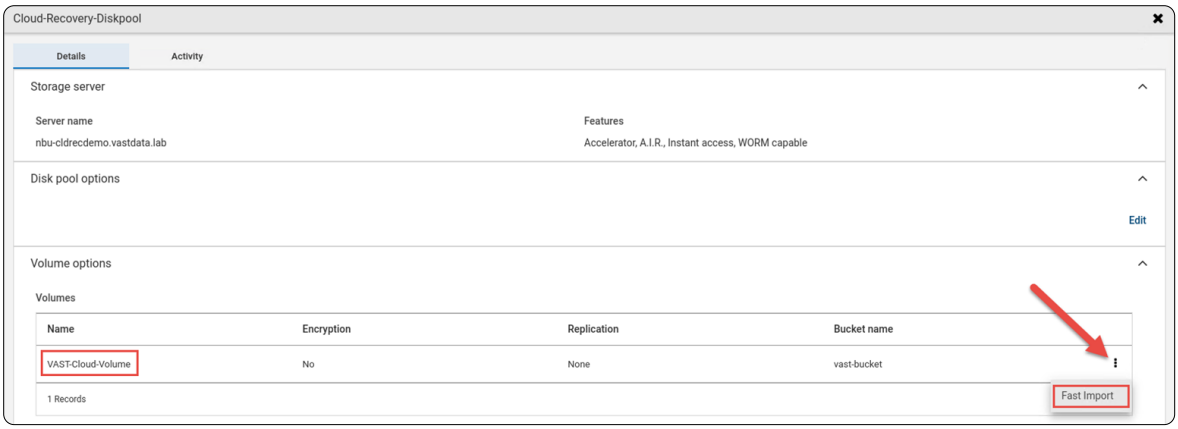


Figure 71 - Selecting Fast Import for Volume

Login to the Cloud Recovery Server Web UI and go to the Disk Pool tab (Figure 70). Click on the ***Name*** of the disk pool and this will open the Details window of that disk pool. Scroll down to the ***Volume*** options section and find the Volume where the data has been backed up to and on the far right of the volume there are three vertical dots, click on that and select ***Fast Import*** (Figure 71).

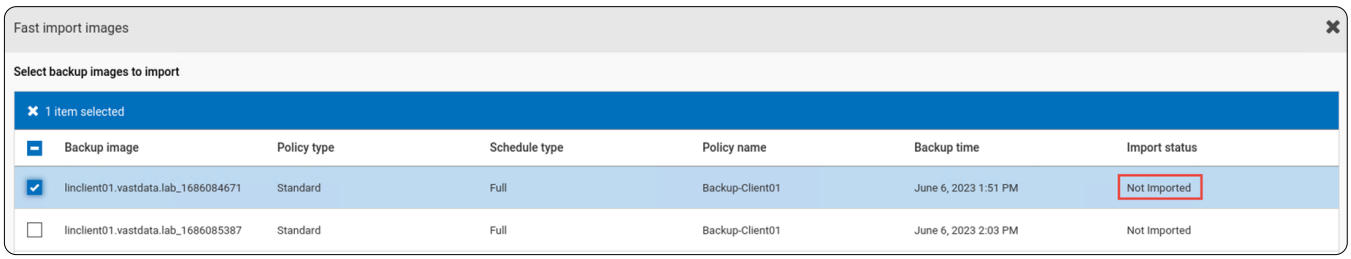


Figure 72 - Selecting the Appropriate Backup to Import

The recovery server will then scan the bucket looking for catalog files of backup images and will list them as shown in Figure 72. Select the appropriate backup image and then click ***Import*** (not shown in image). Now that the image has been imported, data can be recovered.

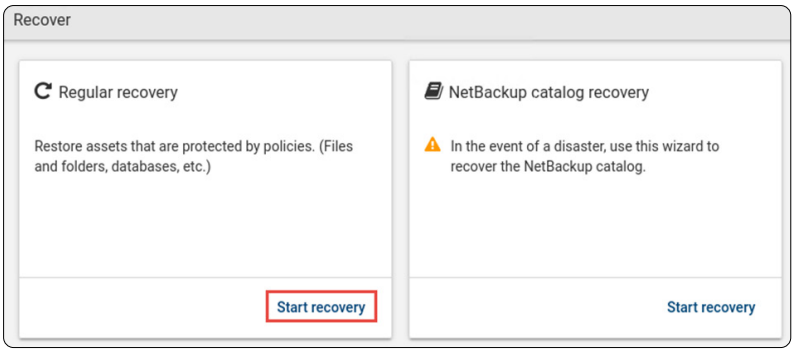


Figure 73 - Starting a Regular Recovery

To do a recovery, click on ***Recovery*** on the left side of the Web UI and then select ***Start recovery*** under ***Regular Recovery*** (Figure 73). Now a little knowledge of the backup policy is necessary to complete the form shown in Figure 74.

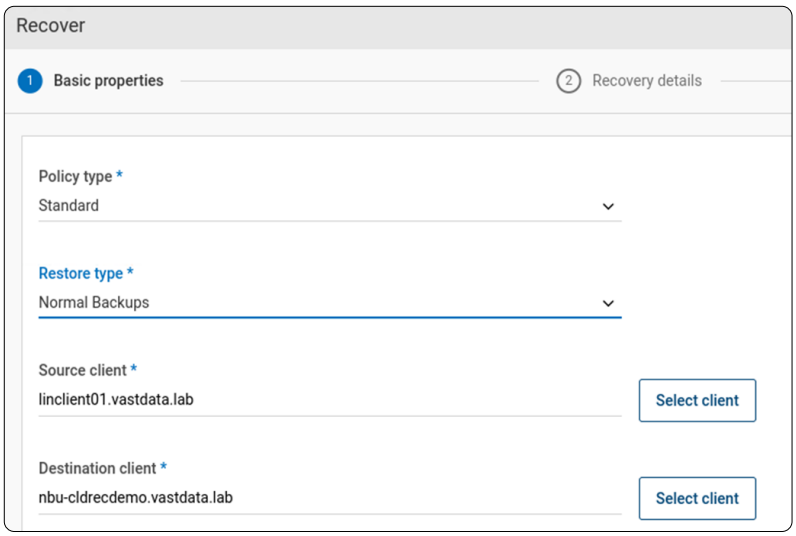


Figure 74 - Specifying Source and Destination of Recovered Data

The Java UI assists the user in filling out this form but knowing the ***Policy Type*** is the critical piece of information. In this example some files were backed up with a ***Standard*** policy. The recovery destination is going to a local directory on this recovery server but it could be restored to an NFS mount from another VAST cluster or another NetBackup client. Click ***Next*** when completed with this form.

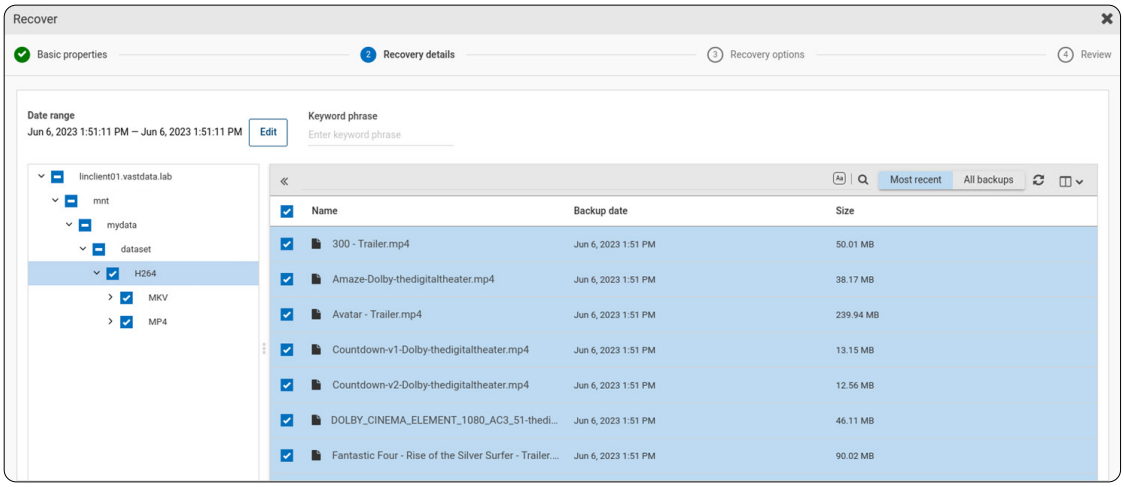


Figure 75 - Selecting Data to Restore

A directory structure now shows all the contents of the data. After selecting the top-level directory to select all of the data, click ***Next***. Keeping things simple all the files will be restored to a different location as shown in Figure 76. The rest of settings are left as default and ***Next*** is clicked.



Figure 76 - Selecting Location to Restore Files

Review the restore information on the summary page (not shown) and then click ***Start Recovery***. The recovery can be monitored from the Activity monitor. Once it completes, check the directory and all of the selected files should be recovered to that location.



For more information on Universal Storage and how it can help you solve your application problems, reach out to us at hello@vastdata.com.

©2025 VAST Data, Inc. All rights reserved. All trademarks belong to their respective owners.