

Veritas Alta™ Recovery Vault Deployment Guide

Cloud-based Storage-as-a-Service to
Isolated Cloud Data Vault

*This paper is designed to highlight the steps customers will need
to perform to setup and use Veritas Alta™ Recovery Vault*

*For more information on Veritas products and solutions,
visit www.veritas.com*

TABLE OF CONTENTS

TARGET AUDIENCE	4
INTRODUCTION	4
EXECUTIVE SUMMARY	4
WHY VERITAS ALTA RECOVERY VAULT	4
LOOKING TO GET VERITAS ALTA RECOVERY VAULT?.....	5
HOW TO USE THIS DEPLOYMENT GUIDE.....	5
ADDITIONAL RESOURCES	6
WHERE TO DOWNLOAD THE SOFTWARE	6
PREREQUISITES	7
NETBACKUP 10.2 AND ABOVE FOR AZURE AND 10.4 AND ABOVE FOR AWS	7
Emergency Engineering Binaries (EEB).....	7
Media Server.....	8
Primary Server.....	9
NETBACKUP 10.1.X AND BELOW FOR AZURE AND 10.3 AND BELOW FOR AWS	9
Emergency Engineering Binaries (EEB).....	9
Media Server.....	9
Ports.....	10
Communication Test.....	10
ALL VERSIONS OF NETBACKUP	11
AWS and Azure Public IP Addresses.....	11
Azure ExpressRoute with Microsoft Peering.....	11
Microsoft vNet Peering	12
AWS Direct Connect Hosted Connection	12
Necessary Information.....	14
Information about Archive Tier Limitations.....	14
IMMUTABILITY/WORM.....	15
SHORT LIVED TOKEN BASED AUTHENTICATION.....	15
MIGRATING FROM ACCESS KEY TO TOKEN-BASED AUTHENTICATION FOR AZURE	17
MIGRATING FROM ACCESS KEY TO TOKEN-BASED AUTHENTICATION FOR AWS	19
PROXY SERVER UPDATE FOR ALTA RECOVERY VAULT	20
CONNECTING TO YOUR NEW STORAGE ACCOUNT IN AZURE.....	21
NETBACKUP 10.4 OR LATER.....	21
NETBACKUP 10.3	34
NETBACKUP 10.2	46
NETBACKUP 10.1.1 OR EARLIER	58
CONNECTING TO YOUR NEW STORAGE ACCOUNT IN AWS	70
NETBACKUP 10.4 OR LATER.....	70
NETBACKUP 10.3	83
NETBACKUP 10.2 OR EARLIER.....	94
CREATING AN ALTA RECOVERY VAULT BACKUP POLICY.....	105
RESTORING DATA FROM ALTA RECOVERY VAULT.....	111
CONSUMPTION REPORTING	114
GENERATING A NEW STORAGE ACCOUNT CREDENTIAL TOKEN	116

Revision History

Version	Date	Changes	Author
1.00	10/27/2021	Initial Version	Neil Glick
1.01	11/4/2021	Updated to reflect that customers will create their own storage buckets. Also added an appendix to show how to create the container using an explorer tool.	Neil Glick
1.02	3/22/2022	Updated for AWS and Immutability.	Neil Glick
1.03	6/7/2022	Split Azure and AWS. Added more best practices.	Neil Glick
1.04	11/10/2022	Veritas Alta rebranding, archive tier added, more best practices.	Neil Glick
1.05	2/14/2023	Added token-based authentication.	Neil Glick
1.06	5/17/2023	Immutability re-write	Neil Glick
1.07	5/17/2023	Immutability notes	Ramya Kalyanam
1.08	8/2/2023	Immutability through web UI	Neil Glick
1.09	11/1/2023	Added AWS Direct Connect, 10.3 and 10.1.1 deployment steps.	Neil Glick
1.10	03/01/2024	AWS token support, Azure and AWS archive updates, reporting, creating policies, restoring data and more best practices.	Neil Glick

1.11	08/19/2024	Update for proxy server, corrections, make document easier to use.	Neil Glick
------	------------	--	------------

Target Audience

This document is for customers interested in learning more about Veritas Alta Recovery Vault and how to implement it.

Introduction

Executive Summary

Veritas Alta Recovery Vault is a cloud-based data vault designed to protect applications and infrastructure from threats that target backup data, by immutably isolating an off-site data copy in the cloud with a virtual air gap. With Alta Recovery Vault, there is no need to build, manage, and protect a physical site to isolate backup data.

Why Veritas Alta Recovery Vault

In a few short years, the adoption of public cloud-based data protection-as-a-service has grown significantly. This trend is placing the onus on data owners to deliver on data protection SLAs, data sovereignty, security, and ransomware resiliency.

Traditional approaches to cloud data protection aren't keeping pace with IT complexity, growing threats, or economic expectations.

Alta Recovery Vault provides a fully managed cloud data protection tier that's seamlessly integrated in NetBackup. With Alta Recovery Vault, Veritas customers can be confident that their data is secure in the cloud and protected from ransomware, is disaster recovery ready, and is able to meet compliance and governance requirements.

Alta Recovery Vault is the right technology at the right time. Alta Recovery Vault not only simplifies the process of provisioning new storage in the cloud, it also reduces risks. All storage as-a-service resources are provisioned and managed from within NetBackup's locked-down security and role-based authentication policies. Eliminating separate accounts and user interfaces across cloud providers helps ensure that security and compliance policies are in check. And because Alta Recovery Vault is an integral feature of NetBackup, customer cloud storage benefits from all its capabilities.

Veritas only supports immutable storage for Alta Recovery Vault. Non immutable storage leaves backups vulnerable to malicious attacks.

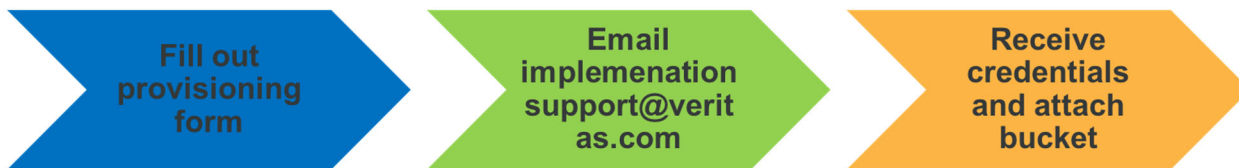
See [Veritas Knowledge Base Article 100055803](#) for more information on Alta Recovery Vault and immutability.

With Alta Recovery Vault you can:

- **Reduce Risks** – Crucial cloud security, retention, and compliance managed within NetBackup.
- **Scale Limitlessly** – Efficiently manage data growth without compromising manageability.
- **Lower Total Cost of Ownership (TCO)** – Predictable as-a-service subscription. Zero hidden costs.
- **Automate Resiliency** – Intelligent cloud policies and air-gapped multi-cloud isolation protect data from ransomware and other threats.

Looking to Get Veritas Alta Recovery Vault?

Veritas Alta™ Recovery Vault – Easy as 1,2,3



How to Use This Deployment Guide

The implementation of Alta Recovery Vault will require certain prerequisites and the possibility of patches before a connection can be made to your new storage.

It is strongly recommended to use the [Alta Recovery Vault Pre-Install Checklist](#) to help ensure proper prerequisites and Emergency Engineering Binaries (EEBs) have been applied to your environment.

This most efficient way to use this deployment guide is to navigate to the Table of Contents and find the Prerequisites section. From there, navigate to the version of NetBackup you are currently running and what Cloud Storage Provider you wish to connect to.

Each prerequisite section will contain what ports will need to be opened, necessary patches and connection tests that will help ensure the ports are ready to connect to your new storage.

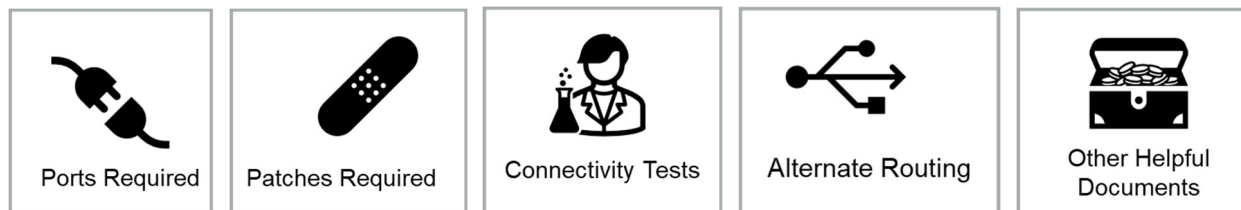
After the prerequisites section, the guide discusses how connection will be made to the CSP and if you would like to use alternate connectivity methods other than the default HTTPS.

Next comes the discussion regarding immutability of your data and how Veritas handles it.

The following section discusses short lived token-based authentication and how to create your credential that will be necessary to connect to your storage. You can create the credential now or create it when you are in the process of connecting to your storage.

The following three sections are for migrations from previous versions of Alta Recovery Vault. If you are not migrating a proxy server or upgrading to token-based authentication, go back to the Table of Contents and find the “Connecting To Your New Storage Account In...” section. Navigate which version of NetBackup you are currently running and which CSP you’ll connect to.

Click on the icons below to link to the required sections.



Additional Resources

Along with this deployment guide, the following resources will help your implementation of Alta Recovery Vault.

1. [Veritas Alta Recovery Vault: Setting up Immutable Storage Part 1 of 2](#)
2. [Veritas Alta Recovery Vault: Backup, Recovery, and Expiring Immutable Storage Part 2 of 2](#)
3. [Veritas Alta Recovery Vault Short Lived Token Based Authentication Overview](#)
4. [Veritas Alta Recovery Vault Security Guide](#)
5. [Veritas Alta Recovery Vault Azure ExpressRoute Overview](#)
6. [Veritas Alta Recovery Vault AWS Direct Connect](#)
7. [Veritas Alta Recovery Vault Pre-Install Checklist](#)
8. [Veritas Alta Recovery Vault Image Sharing and Disaster Recovery](#)
9. [Veritas Alta Recovery Vault Troubleshooting Guide](#)

Where to Download The Software

Alta Recovery Vault is already part of NetBackup and there is no additional software to install.

AWS – Alta Recovery Vault with AWS can be used with NetBackup 9.1 and later.

Azure – Alta Recovery Vault with Azure can be used with NetBackup 10.0 and later.

Note: The minimum version for Azure short lived tokens is NetBackup 10.2

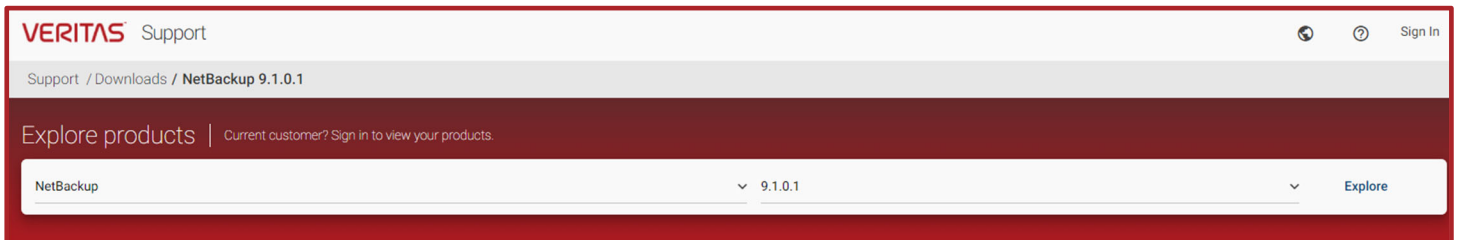
The minimum version for AWS short lived tokens is NetBackup 10.4.

It is recommended to use the latest version of NetBackup with Alta Recovery Vault since it will contain all the new product and security features. Review the [Alta Recovery Vault Pre-Install Checklist](#) to ensure you have the latest EEBs applied and are following all best practices. See the Emergency Engineering Binaries (EEB) section to learn more.

If you would like to run Alta Recovery Vault on NetBackup 10.1 or earlier, proceed to the [Veritas Support and Downloads](#) page to download necessary EEBs.

Note: Additional EEBs not available on the download page may be necessary for earlier versions of NetBackup. Contact your account representative or Veritas Support for more information.

1. After you are on the download page, enter in your version of NetBackup and click **Explore**.



2. Click **Updates** and search for Veritas Alta Recovery Vault.



Prerequisites

Review and implement the following prerequisites before the Alta Recovery Vault implementation.

Note: It is a best practice to download and fill out the [Alta Recovery Vault Pre-Install Checklist](#) to assist in your implementation.

Note: NetBackup 9.1 is the earliest version to support AWS Alta Recovery Vault.

Note: NetBackup 10.0 is the earliest version to support Azure for Alta Recovery Vault.

NetBackup 10.2 and Above for Azure and 10.4 and above for AWS Emergency Engineering Binaries (EEB)

Many versions of NetBackup require that NetBackup EEBs be applied to the primary and/or media servers that connect to Alta Recovery Vault. To download EEBs, navigate to the [Veritas Software Download Site](#). Each .zip file contains the EEBs and a README file with the installation instructions. EEBs are updated on a regular basis, so it's important to apply the most recent version of the EEB on your primary or media server.

Note: Follow the instructions in the README file in the .zip EEB file. Some EEBs must be installed on the primary and/or on the media server and may not be applied if other EEBs have already been applied. If you have any questions regarding patching your primary or media servers, contact Veritas Support for more assistance.

Note: The [Veritas Alta Recovery Vault Pre-Install Checklist](#) lists most of the EEBs necessary, however please check with Veritas Support before implementing Alta Recovery Vault to ensure you have the latest EEBs in place.

Media Server

Alta Recovery Vault uses MSDP Direct Cloud Tiering (MSDP-C) functionality in NetBackup. MSDP-C can be configured on CentOS, RHEL-based and SUSE media servers, NetBackup appliances (NetBackup Appliance, Flex Appliance, or Flex Scale) or Alta Data Protection (Cloud Scale).

Note: Microsoft Windows Media Servers are not supported for Alta Recovery Vault.

Ports

Port 443 – Communication to the external storage bucket requires TCP port 443 to be open outbound so the NetBackup API can communicate with the storage bucket through HTTPS. If you do not wish to open TCP port 443 outbound and choose to use products like Azure ExpressRoute or AWS Direct Connect, see the [Veritas Alta Recovery Vault Security Profile](#) for more information.

Port 80 – Veritas checks for certificate revocation to ensure the certificates are valid, which means that TCP port 80 needs to be opened outbound on the media server configured for MSDP-C unless you do not wish to check for certificate revocation. To remove this certificate validation, simply uncheck certificate revocation when creating the disk pool.

Advanced settings

Security

Use SSL

Authentication only

Authentication and data transfer

Check certificate revocation (IPv6 not supported for this option)

Note: For more information on Alta Recovery Vault security, see the [Veritas Alta Recovery Vault Security Profile](#).

Primary Server

Ports

Port 443 – Alta Recovery Vault uses the NetBackup primary server to communicate with the Veritas secure short lived token server. A proxy server can also be used if direct connection to the internet is not available. (This step can be seen later in this guide.)

Communication Test

Check the connectivity with the Alta Recovery Vault service on the NetBackup Primary server with the following curl command to ensure communication can occur.

```
curl -v https://rvltapi.nr1.archivecloud.net/api/servicestatus/info
```

Note: Look for “Connected to rvltapi.nr1.archivecloud.net (52.52.233.219) port 443 (#0)” for a successful connection.

NetBackup 10.1.x and Below for Azure and 10.3 and below for AWS Emergency Engineering Binaries (EEB)

NetBackup versions 9.0.0.1, 9.1.0.1, 10.0.0.1 and 10.1 require that NetBackup EEBs be applied to the primary and/or media servers that connect to Alta Recovery Vault. To download EEBs, navigate to the [Veritas Software Download Site](#). Each .zip file contains the EEBs and a README file with the installation instructions. EEBs are updated on a regular basis, so it’s important to apply the most recent version of the EEB on your primary or media server.

Note: Follow the instructions in the README file in the .zip EEB file. Some EEBs must be installed on the primary and/or on the media server and may not be applied if other EEBs have already been applied. If you have any questions regarding patching your primary or media servers, contact Veritas Support for more assistance.

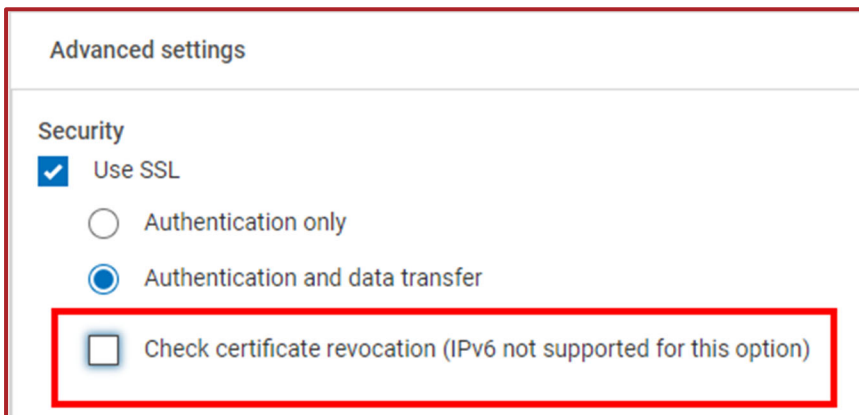
Media Server

Alta Recovery Vault uses MSDP Direct Cloud Tiering (MSDP-C) functionality in NetBackup. MSDP-C can be configured on CentOS, RHEL-based and SUSE media servers, NetBackup appliances (NetBackup Appliance, Flex Appliance, or Flex Scale) or Alta Data Protection (Cloud Scale).

Ports

Port 443 – Communication to the external storage bucket requires TCP port 443 to be open outbound so the NetBackup API can communicate with the storage bucket through HTTPS. If you do not wish to open TCP port 443 outbound and choose to use products like Azure ExpressRoute or AWS Direct Connect, see the [Veritas Alta Recovery Vault Security Profile](#) for more information.

Port 80 – Veritas checks for certificate revocation to ensure the certificates are valid, which means that TCP port 80 needs to be opened outbound on the media server configured for MSDP-C unless you do not wish to check for certificate revocation. To remove this certificate validation, simply uncheck certificate revocation when creating the disk pool.



Advanced settings

Security

Use SSL

Authentication only

Authentication and data transfer

Check certificate revocation (IPv6 not supported for this option)

Note: For more information on Alta Recovery Vault security, see the [Veritas Alta Recovery Vault Security Profile](#).

Communication Test

Check the connectivity with the Alta Recovery Vault service on the NetBackup media server with the following curl command.

Azure:

```
curl -v https://<storageaccount>.blob.core.windows.net
```

AWS:

```
curl -v https://<s3bucket>.s3.dualstack.us-east-1.amazonaws.com
```

All Versions of NetBackup

AWS and Azure Public IP Addresses

You may want to allowlist IP addresses that Azure and AWS use to connect to your service. See the following for more information:

Azure: <https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519>

AWS: <https://docs.aws.amazon.com/quicksight/latest/user/regions.html>

Azure ExpressRoute with Microsoft Peering

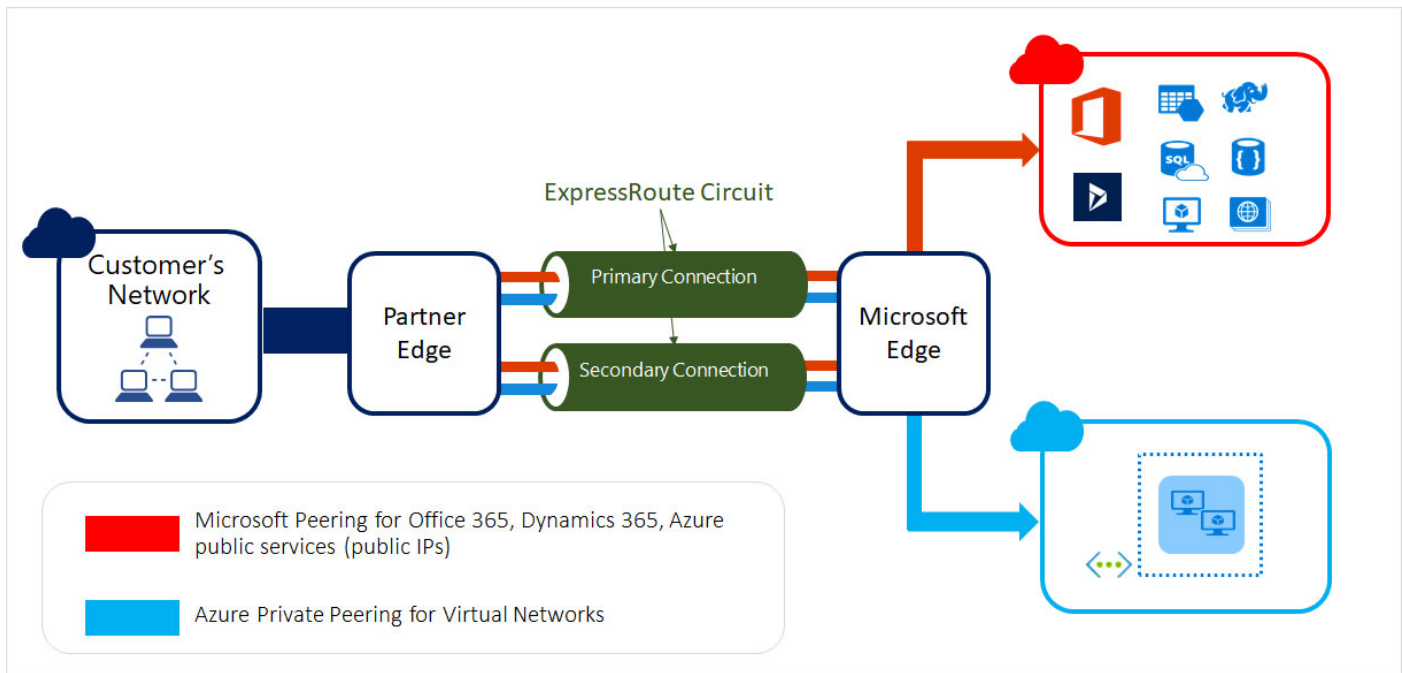
Alta Recovery Vault has been tested and certified to use Azure ExpressRoute. To use Azure ExpressRoute to connect to Alta Recovery Vault storage in Azure, customers should use Azure ExpressRoute “Microsoft Peering”, and not Azure “Private Peering”.

The differences are described on Microsoft’s site: <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings>

With an ExpressRoute configured for Microsoft Peering, in the past, Microsoft used to send all the prefixes for public IPs. Now, customers should configure a route filter first, which is a Border Gateway Protocol (BGP) community value for the prefixes you want to receive to the storage region (such as East US or West US 2, etc.) you have chosen for your Alta Recovery Vault Azure storage.

Please review Microsoft’s guide on setting up a route filter for the prefixes you want to receive:

<https://learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal>



For more information on our testing with Azure ExpressRoute, see the [Veritas Alta Recovery Vault ExpressRoute Overview Guide](#).

Microsoft vNet Peering

Veritas does not recommend using Microsoft vNet Peering for Alta Recovery Vault. vNet Peering is cost prohibitive when it is used for backup and restore purposes. The least expensive vNet Peering is within the same region, at \$0.01 per GB for both inbound or outbound traffic and charged at both ends of the peered networks. Both Veritas as well as the end user would incur costs which will lead to transfers out of the same region that are 3.5x to 16x more expensive, depending on the regions used.

vNet Peering also requires non-overlapping IP addresses, and Alta Recovery Vault is a multi-tenant environment. As multiple customers are connecting to their storage in the same Veritas Azure subscription, there could be overlap with IP ranges with other future customers and we would not be able to support future customers' requests.

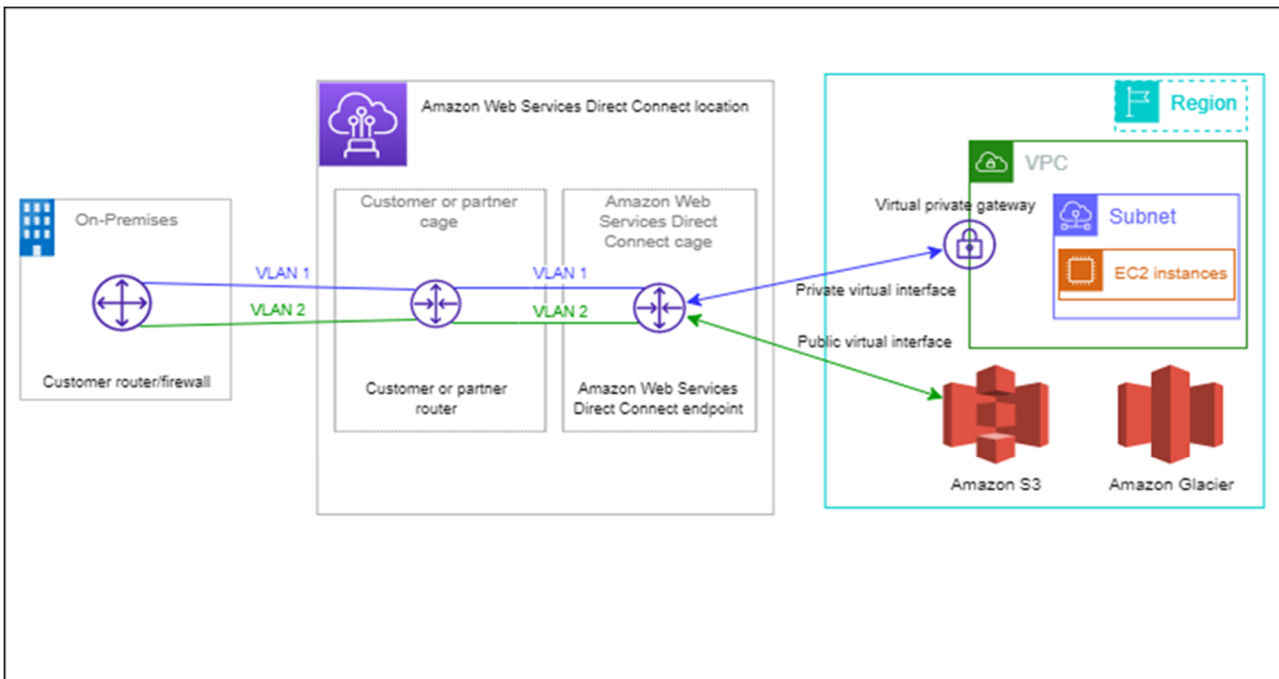
AWS Direct Connect Hosted Connection

Alta Recovery Vault has been tested and certified to use AWS Direct Connect using a hosted connection. AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to public AWS services (for example, to Amazon

S3) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the Region with which it is associated. You can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.

While in transit, your network traffic remains on the AWS global network and never touches the public internet. This reduces the chance of hitting bottlenecks or unexpected increases in latency. When creating a new connection, you can choose a hosted connection provided by an AWS Direct Connect Delivery Partner or choose a dedicated connection from AWS—and deploy at over 100 AWS Direct Connect locations around the globe. For more information: <https://aws.amazon.com/directconnect/>

The following diagram shows a high-level overview of how AWS Direct Connect interfaces with your network.



For more information on our testing with AWS Direct Connect, see the [Veritas Alta Recovery Vault Direct Connect Overview Guide](#).

Necessary Information

The first step to your journey to storage-as-a-service is to contact your Veritas account manager. Your account manager will collect the necessary information needed to provision your Alta Recovery Vault storage account.

Following are examples of the information you might provide:

- Cloud provider(s)
- Data center region
- Number of buckets
- Size of the buckets (2.4PB per disk volume)
- Veritas account representative
- Veritas partner name
- Immutability support requirements
- **Note:** Non-Immutable storage is not available in Alta Recovery Vault.

After the necessary information has been collected, the Veritas Alta Recovery Vault Provisioning Team creates the storage account, enabling you to create cloud buckets in the cloud provider.

Note for Azure Customers – Use the NetBackup web UI to attach to the new storage account and create the desired cloud bucket(s) or use the cloud buckets created by the Veritas Alta Recovery Vault Provisioning Team.

Note for AWS Customers –The cloud buckets are created, and the names are given to you by the Veritas Alta Recovery Vault Provisioning Team.

Information about Archive Tier Limitations

The introduction of Archive Tier gives backup administrators even more flexibility when using Alta Recovery Vault storage-as-a-service. However, you should review the NetBackup Cloud Administrators Guide and NetBackup Deduplication Guide regarding NetBackup capabilities while using specific cloud vendor archive tiers.

AWS https://www.veritas.com/content/support/en_US/doc/58500769-157138736-0/v113989222-157138736

Azure https://www.veritas.com/content/support/en_US/doc/58500769-157138736-0/v135373405-157138736

https://www.veritas.com/content/support/en_US/doc/25074086-156145854-0/v144509100-156145854

Immutability/WORM

Immutability/WORM gives you the ability to write once, and read many, to your Alta Recovery Vault storage and select how long you would like the images to be retained. In the event of a threat actor/malware compromise, immutability prevents the threat actor from expiring your backup images in Alta Recovery Vault or manipulating the data in any way.

Alta Recovery Vault currently only supports Governance mode (also known as enterprise mode). Governance immutability gives users special permissions to disable the retention lock and then delete the image.

Governance mode allows users to accelerate the expiration of images, compliance mode does not allow this. Alta Recovery Vault is closer to compliance mode because no users have the ability to shorten a lock duration since the customer is not the cloud tenant for the storage.

Note: Only the cloud administrator user can disable the retention lock and then delete the image if required. For Alta Recovery Vault, Veritas is the cloud administrator.

When requesting storage from Veritas, your Alta Recovery Vault storage buckets, created by Veritas, will have immutability enabled. All NetBackup Cloud Storage Units must be created with Governance mode immutability enabled in order to ensure that data is written in an immutable format.

Note: For more information on immutability and the `msdpclutil` command, refer to the NetBackup Deduplication Guide:

https://www.veritas.com/support/en_US/doc/25074086-159245004-0/v152917675-159245004.

https://www.veritas.com/support/en_US/doc/25074086-149019166-0/v149102641-149019166.

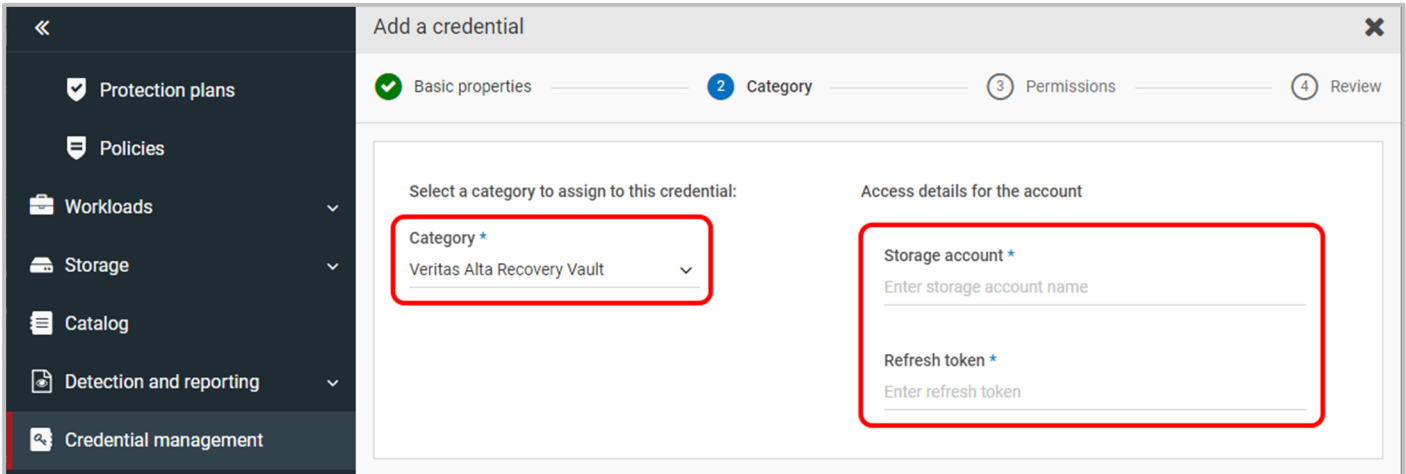
Short lived token based authentication

Veritas provides the ability to connect to Alta Recovery Vault cloud storage in Azure and AWS using token-based credentials provided by Veritas. Enhanced security of token-based credentials further minimizes the risk window when authenticating users or devices in the NetBackup zero trust model by providing a credential management mechanism that uses short lived tokens instead of standard credentials. This new mechanism uses refresh tokens as its security input and generates a new access token periodically before the existing tokens expire.

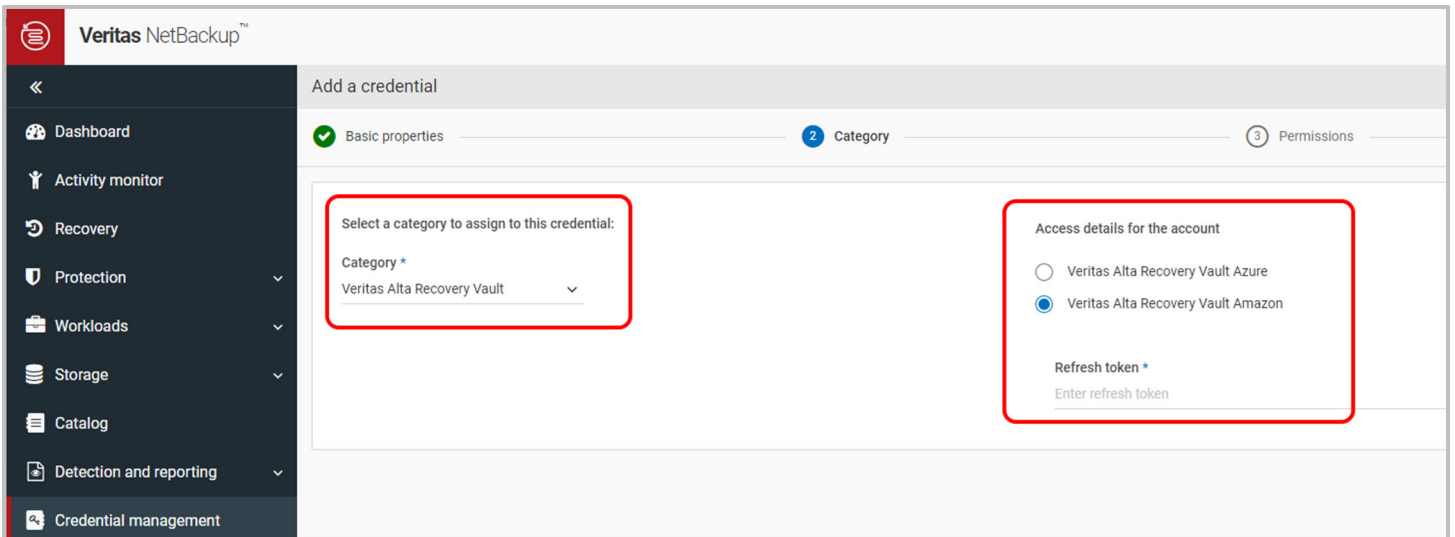
Note: The minimum version for Azure short lived tokens is NetBackup 10.2

The minimum version for AWS short lived tokens is NetBackup 10.4.

For Azure users: Take the storage account and refresh token given to you by Veritas and create a new credential under the Credential Management tab in the NetBackup WebUI.



For AWS users: Take the refresh token given to you by Veritas and create a new credential under the Credential Management tab in the NetBackup WebUI.



Use the credential created when connecting to your Alta Recovery Vault cloud storage in Azure or AWS.

Note: These credentials should be unique. Duplicate entries might lead to failures in configuration or with NetBackup jobs. If you need to update your refresh token for any reason, use the edit option and update the

existing storage account instead of creating a new credential with same storage account and new refresh token.

Migrating from Access Key to Token-Based Authentication for Azure

To migrate from access key to token-based authentication, the media server connected to the Alta Recovery Vault must be upgraded to NetBackup 10.2 or later. Currently the command line interface (CLI) is needed to complete the migration.

An attribute called “Need Token Renew” (NTR) will be set to “No” after the upgrade and it must be set to “Yes.”

1. Check to see what the NTR is set as on your storage server after the media server has been upgraded to 10.2 or later.
 - a. `<install path>/netbackup/bin/admincmd/csconfig cldinstance -i`

```
root@slv014--1 /usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -i -in Veritas-Alta-Recovery-Vault-Azure
Cloud Instance Name      : Veritas-Alta-Recovery-Vault-Azure
Provider Type           : vazure
Service API Type        : Azure
Service Host            : blob.core.windows.net
Service Endpoint        : <empty>
Service HTTP Port       : 80
Service HTTPS Port      : 443
Service URL Style       : Virtual Hosted Style
Customizable            : No
Storage Server          : Veritas-
Use SSL                 : DATA
Use CRL                 : Yes
Need Token Renew        : Yes
Storage Tier            : ACCOUNT_ACCESS_TIER
Use Proxy               : NONE
Proxy Host              : <NA>
Proxy Port              : <NA>
Use Proxy Tunneling     : <NA>
Proxy Authentication Type : <NA>
Credentials Broker      : CREDENTIALS_PROMPT
Storage Server          : si-
Use SSL                 : DATA
Use CRL                 : Yes
Need Token Renew        : Yes
Storage Tier            : ACCOUNT_ACCESS_TIER
Use Proxy               : NONE
Proxy Host              : <NA>
Proxy Port              : <NA>
Use Proxy Tunneling     : <NA>
Proxy Authentication Type : <NA>
Credentials Broker      : CREDENTIALS_PROMPT
Storage Server          : si-
Use SSL                 : DATA
Use CRL                 : Yes
Need Token Renew        : No
Storage Tier            : ACCOUNT_ACCESS_TIER
Use Proxy               : NONE
Proxy Host              : <NA>
Proxy Port              : <NA>
Use Proxy Tunneling     : <NA>
Proxy Authentication Type : <NA>
Credentials Broker      : CREDENTIALS_PROMPT
```

Note: As seen in the image above, the first two storage servers are new media servers and the third is an upgrade. The NTR is currently set to No and needs to be flipped to Yes.

2. Run the following command for the storage server that needs NTR flipped to Yes.
 - a. `<install path>/netbackup/bin/admincmd/csconfig cldinstance -us -in <Your_Cloud_Instance_Name> -sts <Alias_Name> -ntr 1`
 - Example: `/usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -us -in Veritas-Alta-Recovery-Vault-Azure -sts storageserver.com_myvolume -ntr 1`
3. Run the following command to ensure your NTR has been set to Yes.

- a. `<install path>/netbackup/bin/admincmd/csconfig cldinstance -i`

4. (CLI) –

- a. Update the cloud alias credentials using `nbdevconfig`
- b. Create or update a text config file with the new credentials.
- c. Set `IsuCloudUser` to the credential name you created using Credential Management
- d. Fill in `IsuCloudPassword` with a dummy string
- e. Example content of the file:

```
V7.5 "operation" "update-Isu-cloud" string
V7.5 "IsuName" "myvolume" string
V7.5 "cmsCredName" "credentialname" string
V7.5 "IsuCloudBucketName" "mybucket" string
V7.5 "IsuCloudBucketSubName" "myvolume" string
<install path>/netbackup/bin/admincmd/nbdevconfig -setconfig -stype PureDisk -
storage_server <storage_server> -configlist <config file path>
```

5. (Web UI) - Navigate to **Storage > Storage configuration > Disk pools** and select the disk pool your Alta Recovery Vault is located in. Under **Associate credentials**, replace the existing credential.

Note: Upgrading the MSDP server to use the new credential requires a restart of the MSDP service.

The screenshot shows the Veritas NetBackup web interface. The left sidebar contains navigation options: Policies, Workloads, Storage, Storage configuration, Storage lifecycle policies, Devices, Catalog, Detection and reporting, Anomaly detection, Malware detection, Paused protection, Usage, Credential management, Hosts, Host properties, Deployment management, and Bare Metal Restore. The main content area displays a table of disk pools with columns for Name, Encryption, Replication, Bucket name, WORM capable, Minimum lock duration, and Maximum lock duration. Below the table, the 'Cloud details' section shows Storage provider (NetBackup Recovery Vault Azure), Storage API type (Azure), and Storage tier (Account access tier). The 'Region' section shows Service host (blob.core.windows.net). The 'Associate credentials' section contains a table with columns for Credential name, Tag, and Description. A red box highlights the 'Replace' button in the bottom right corner of the 'Associate credentials' table.

Migrating from Access Key to Token-Based Authentication for AWS

To migrate from access key to token-based authentication, the media server connected to the Alta Recovery Vault must be upgraded to NetBackup 10.4 or later. Currently the command line interface (CLI) is needed to complete the migration.

An attribute called “Need Token Renew” (NTR) will be set to “No” after the upgrade and it must be set to “Yes.”

1. Check to see what the NTR is set as on your storage server after the media server has been upgraded to 10.4 or later.
 - a. `<install path>/netbackup/bin/admincmd/csconfig cldinstance -i`

2. Run the following command for the storage server that needs NTR flipped to Yes.
 - a. `<install path>/netbackup/bin/admincmd/csconfig cldinstance -us -in <Your_Cloud_Instance_Name> -sts <Alias_Name> -ntr 1`
 - i. Example: `/usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -us -in Veritas-Alta-Recovery-Vault-AWS -sts storageserver.com_myvolume -ntr 1`

3. Run the following command to ensure your NTR has been set to Yes.
 - a. `<install path>/netbackup/bin/admincmd/csconfig cldinstance -i`

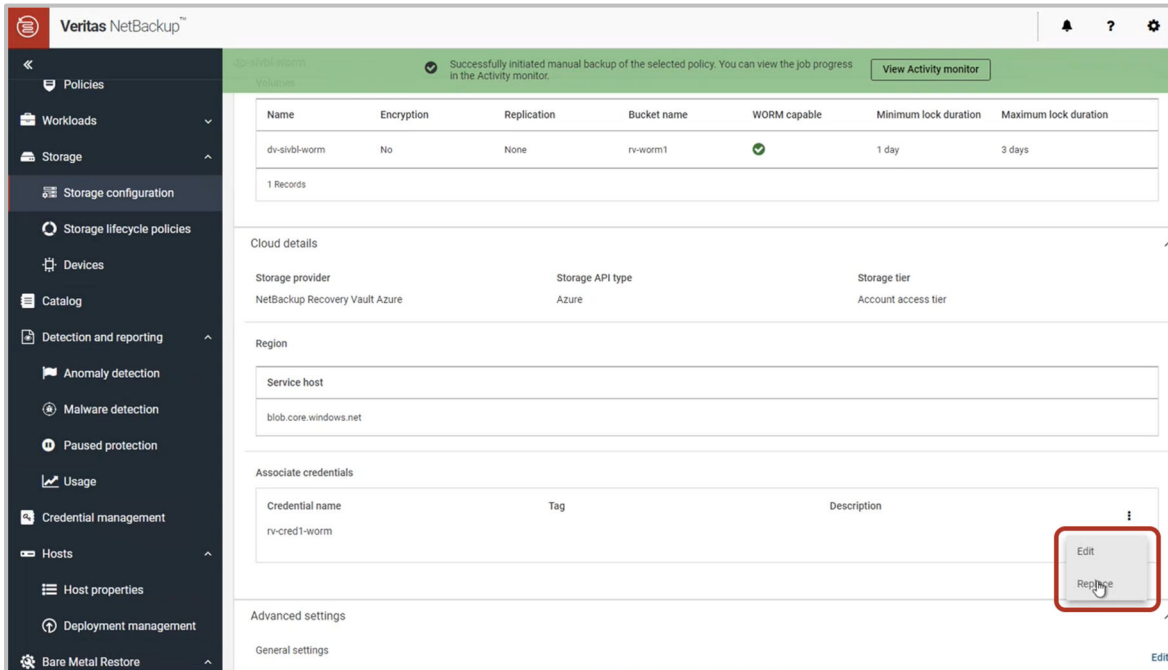
4. (CLI) –
 - a. Update the cloud alias credentials using `nbdevconfig`
 - b. Create or update a text config file with the new credentials.
 - c. Set `IsuCloudUser` to the credential name you created using Credential Management
 - d. Fill in `IsuCloudPassword` with a dummy string
 - e. Example content of the file:

```
V7.5 "operation" "update-lsu-cloud" string
V7.5 "IsuName" "myvolume" string
V7.5 "cmsCredName" "credentialname" string

V7.5 "IsuCloudBucketName" "mybucket" string
V7.5 "IsuCloudBucketSubName" "myvolume" string
<install path>/netbackup/bin/admincmd/nbdevconfig -setconfig -stype PureDisk -
storage_server <storage_server> -configlist <config file path>
```

- (Web UI) - Navigate to **Storage > Storage configuration > Disk pools** and select the disk pool your Alta Recovery Vault is located in. Under **Associate credentials**, replace the existing credential.

Note: Upgrading the MSDP server to use the new credential requires a restart of the MSDP service.



PROXY SERVER UPDATE FOR ALTA RECOVERY VAULT

To change a proxy server configured for Alta Recovery Vault in NetBackup the following steps are necessary.

Update the information of the cloud instance

- For a NetBackup Primary server running on Linux connect via ssh. If NetBackup is on Flex or Flex Scale use `sudo -i` to become root.
- Examine the storage server name and current proxy server configuration on the cloud instance:
 - If Alta Recovery Vault is on Azure, use the command:


```
/usr/opencv/netbackup/bin/admincmd/csconfig cldinstance -i -in Veritas-Alta-Recovery-Vault-Azure
```
 - If Alta Recovery Vault is on AWS, use the command:


```
/usr/opencv/netbackup/bin/admincmd/csconfig cldinstance -i -in Veritas-Alta-Recovery-Vault-Amazon
```

Note: The parameter `-in <instance_name>` depends on your NetBackup version of cloud configuration file. The command

```
/usr/opencv/netbackup/bin/admincmd/csconfig cldinstance -l
```

will display the list of cloud providers available.

3. Update the current proxy configuration using the command below

```
a. /usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -us -in  
    <instance_name> -sts <storage_server_name> -pxtype HTTP -pxhost  
    <proxy_ip> -pxport <proxy_port>
```

4. Update the information on the NetBackup WebUI.

- a. Open the NetBackup WebUI, select Storage, then Disk Storage.
- b. Under Disk Pools, select the Disk Pool used by Alta Recovery Vault by clicking on its name.
- c. Use the Edit button on the Disk Pool Advanced Settings and update the Proxy information as needed.

CONNECTING TO YOUR NEW STORAGE ACCOUNT IN AZURE

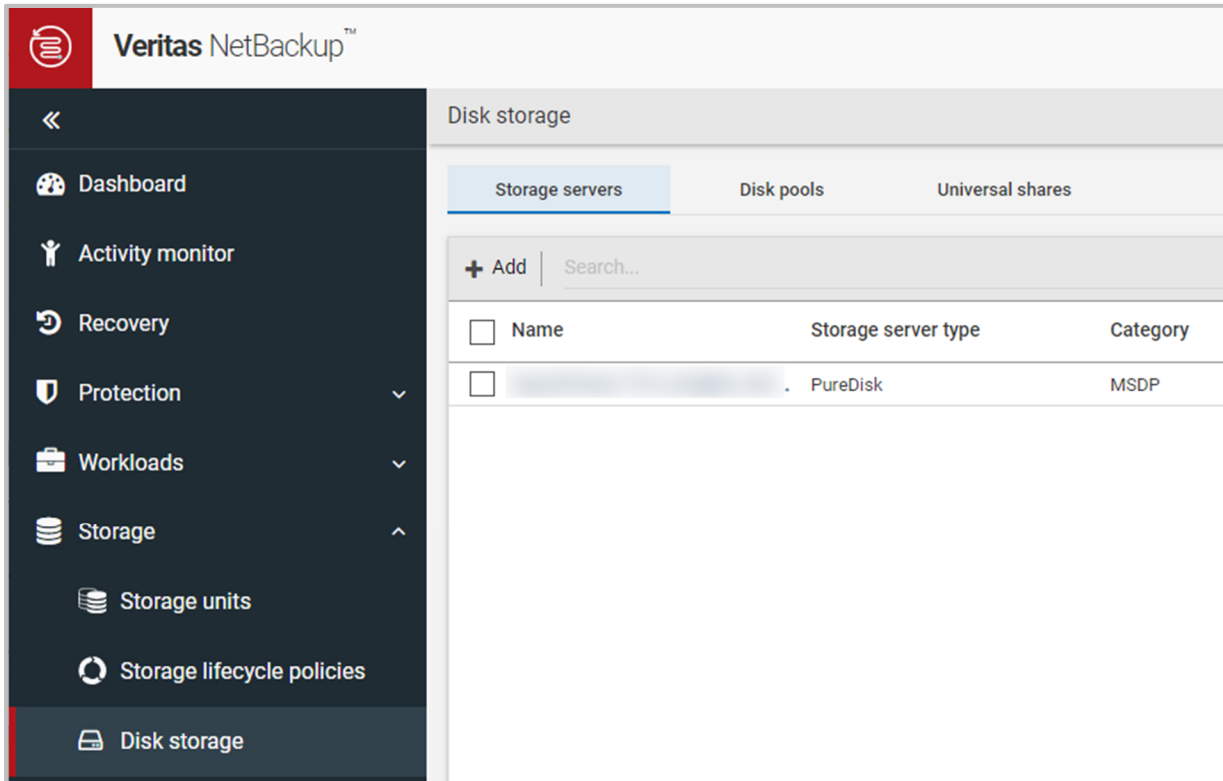
NetBackup 10.4 or later

Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

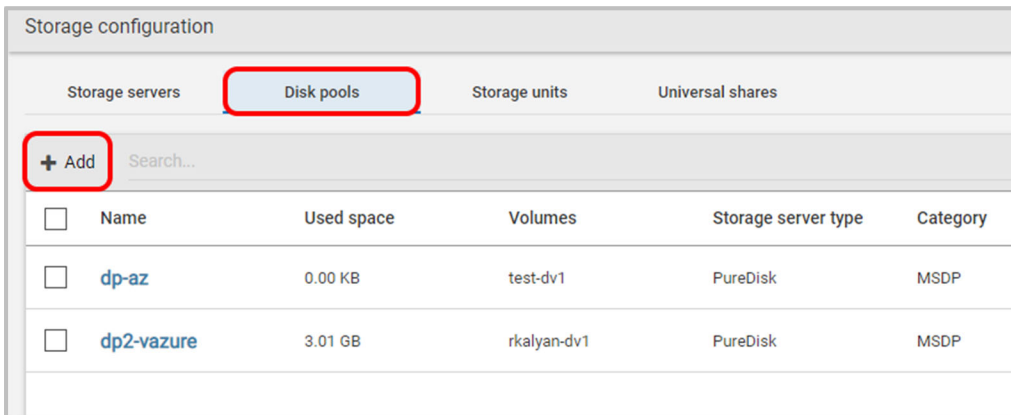
1. Ensure your storage server has been created.
 - a. Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*:
https://www.veritas.com/content/support/en_US/doc/25074086-159245004-0/v24332600-159245004

2. From within your NetBackup primary server web UI, navigate to **Storage > Disk Storage**

You should see your storage server(s) listed.



3. Click the **Disk pools** tab and click **+ Add**.



4. First, enter the details for disk pool options.

- a. Select the storage server name where this disk pool will reside. In this example, the choice is the storage server seen in step 1 of this procedure.
- b. Provide a name for the disk pool. This example uses “ngpool1”.
- c. If you choose, provide a description for the pool.
- d. Select **Limit I/O streams** if desired. This option could help limit disk I/O contention.
- e. Click **Next** at the bottom of the page to continue. (Not seen in the image.)

The screenshot shows the 'Add disk pool' configuration window with the 'Disk pool options' step selected. The 'Storage server name' is 'siv'. The 'Disk pool name' is 'ngpool1'. There is a 'Description' field with the placeholder 'Enter description'. A checkbox for 'Limit I/O streams' is present with a tooltip: 'Concurrent read and write jobs affect disk performance. Limit I/O streams to prevent disk overload.' Below this, a note states: 'The following options do not apply if you select a cloud MSDP disk volume in the next step.' There are two water mark settings: 'High water mark' at 98% and 'Low water mark' at 80%.

5. Next, you're brought to the Volumes page. In the example you can see that there are already three volumes created, but you want to add your new Alta Recovery Vault volume. Click **Volume > Select volume**.

The screenshot shows the 'Add MSDP disk pool' configuration window with the 'Volumes' step selected. A dropdown menu labeled 'Volume' is open, showing 'Select volume'. Below is a search bar and a table of existing volumes.

Name	Available space	Total size	Encryption
PureDiskVolume	753.88 GB	885.38 GB	No
test-dv1	8.00 PB	8.00 PB	No
rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

6. Click **Add volume** to begin the process.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Select volume

Add volume

	Name	Available space	Total size	Encryption
<input type="radio"/>	PureDiskVolume	753.88 GB	885.38 GB	No
<input type="radio"/>	test-dv1	8.00 PB	8.00 PB	No
<input type="radio"/>	rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

7. Provide a name for the new volume and click **Cloud storage provider**.

Add MSDP disk pool

✓ Disk pool options 2 Volumes 3 Replication

Volume

Add volume

Volume name *
ngvolume1

Cloud cache properties

⚠ A request value lower than 1,017 GB may affect performance. Verify that the required space to create this pool is available.

Available disk space: 146.57 GB

Request cloud cache disk space *
73 GB
Enter a value between 4 GB and 117 GB.

Cloud storage provider *
Select cloud storage provider

Storage API type
-

8. Search for “Veritas Alta Recovery Vault Azure” and the following Cloud storage providers appear. For this example, you will choose **Veritas Alta Recovery Vault Azure**.

Select cloud storage provider		
Search...		
Cloud storage provider	Description	Storage API type
<input checked="" type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure

9. After you select the cloud storage provider, you’re taken back to the Add MSDP disk pool screen. Select the Storage tier you purchased and the Azure region to be used.

Note: Choices for Storage Tier are:

Alta Recovery Vault Standard – AZURE

or

Alta Recovery Vault Archive - AZURE

Note: If you’ve purchased archive tier, select Alta Recovery Vault Archive - AZURE. You have a choice to archive again every 3 to 30 days.

Note: For archive tier, ensure your cloud vendor provides archive support in the desired region. If archive tier is not supported in the region, this feature will not function correctly.

Note: The region is provided by the Veritas Alta Recovery Vault Provisioning Team.

Cloud storage provider *	Storage API type
Veritas Alta Recovery Vault Azure	Microsoft Azure
Storage tier	
Alta Recovery Vault Standard - AZURE	
Region *	
Service host	
<input checked="" type="radio"/> blob.core.windows.net	

Cloud storage provider *

Veritas Alta Recovery Vault Azure

Storage API type

Microsoft Azure

Storage tier

Alta Recovery Vault Archive - AZURE



Archive again after

3



days

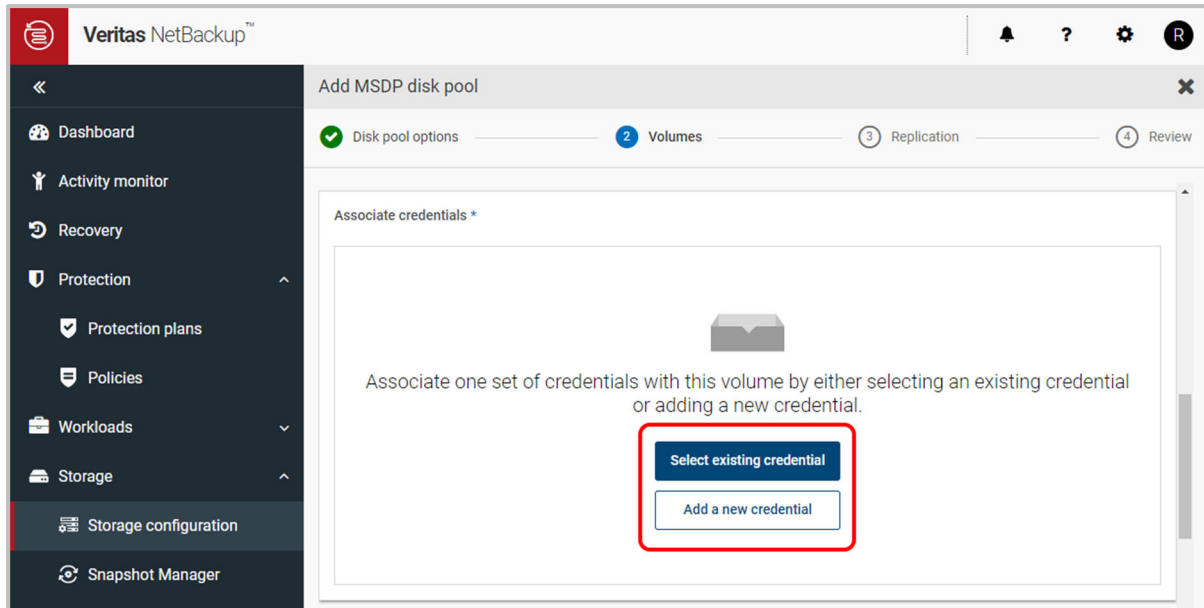
Region *

Service host



blob.core.windows.net

10. Click **Select existing credential** if you've already created your credential from the Short-Lived Token Based Authentication section earlier in this document. If not, click **Add a new credential** and create a new credential using the storage account and refresh token given to you by Veritas.



Note: You can create multiple disk volumes/buckets using the same credentials. There is no need to add multiple credentials for the same storage account.


Note: The storage account, short lived tokens, and access keys are provided by the Veritas Alta Recovery Vault Provisioning Team.

Access details for Azure account

Storage account *

rvlrcust001

Access key *

..... 

11. In the WORM section is where you set the immutability time duration. During the Lock duration the image is locked. For more information regarding immutability, see the [Veritas Knowledge Base Article 100055803](https://www.veritas.com/learn/whitepapers/100055803) for more information on Alta Recovery Vault and immutability.

Note: WORM and Enterprise mode are selected by default and cannot be changed.

WORM

Use object lock
NetBackup retrieves the object lock information from cloud storage, ensures that the target

Retention mode ⓘ

Compliance

Enterprise

Lock duration ⓘ

Minimum lock duration

1 Day

Maximum lock duration

1 Year

12. In Advanced settings, enter the required Security or Proxy preferences.

Note: If you do not want to open port 80 externally, you will need to uncheck “Check certificate revocation”, For more information on check certificate revocation, see the following: https://en.wikipedia.org/wiki/Certificate_revocation_list#:~:text=In%20cryptography%2C%20a%20certifi%20revocation,should%20no%20longer%20be%20trusted%22.

Note: A proxy server can be used if wanted. Check the box seen below and enter the required information for the proxy server.

Add MSDP disk pool

1 Disk pool options 2 Volumes 3 Replication

Advanced settings

Security

Use SSL

Authentication only

Authentication and data transfer

Check certificate revocation (IPv6 not supported for this option)

Proxy

Use proxy server

13. Click **Select or create a cloud bucket** and then click **Retrieve list**. This process logs into Azure using the credentials provided earlier.

Note: If the Retrieve List operation is successful, the credentials to connect to the Azure storage are correct.

Cloud buckets

Enter an existing cloud bucket name

Select or create a cloud bucket

Complete all required fields to view available cloud buckets.

Retrieve list

14. A new bucket can also be created using the **+ Add** button in the NetBackup web UI after you connect to the new storage account. Listed below is the Alta Recovery Vault cloud bucket “rvlrcust001c1”. The name of your cloud bucket will be different; the one below is for reference only.

Cloud buckets

Enter an existing cloud bucket name

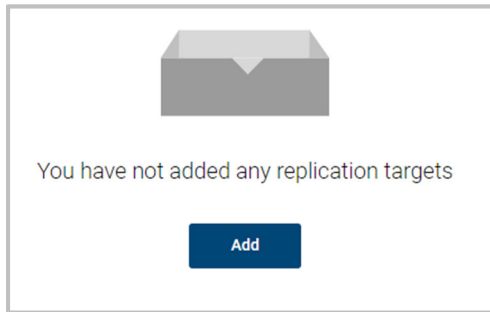
Select or create a cloud bucket

+ Add

Search... 🔍 ↻

Name
<input type="radio"/> rvlrcust001c1

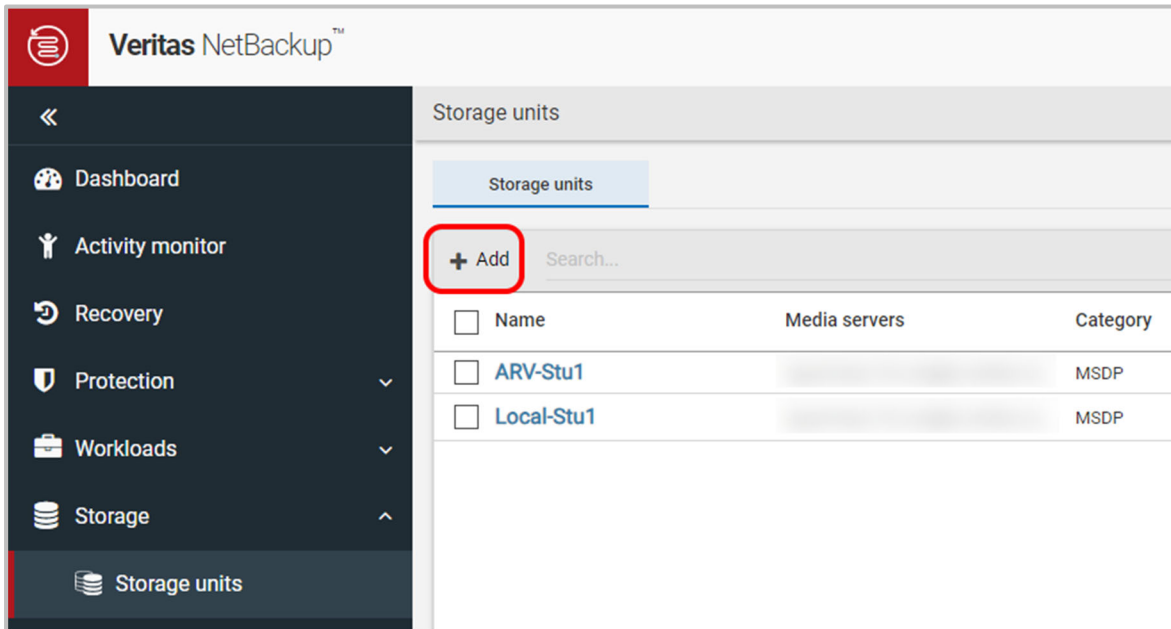
15. If you would like to set up replication targets, they can be set up now. If none are needed, click **Next**. (Not shown in the image.)



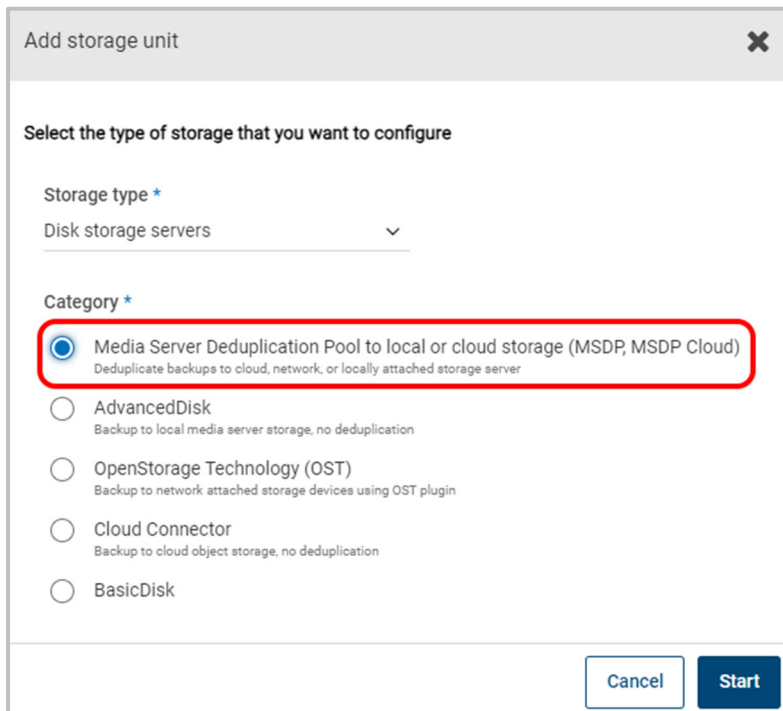
16. The next page is a summary page. If everything looks good, create the new disk pool. In this example, the new "ngpool1" has been created.

Storage configuration							
Storage servers		Disk pools		Storage units		Universal shares	
+ Add Search...							
<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category		
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP		
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP		
<input type="checkbox"/>	ngpool1	0.00 KB	ngvolume1	PureDisk	MSDP		

17. Next, add a storage unit so you can use your new Alta Recovery Vault storage. Under Storage > Storage Units, click **+ Add**.



18. Select **Media Server Deduplication Pool to local or cloud storage (MSDP, MSDP Cloud)** and click **Start**.



19. Provide a new MSDP storage unit name and select the desired **Maximum concurrent jobs** and **Maximum fragment size**. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

1 Basic properties

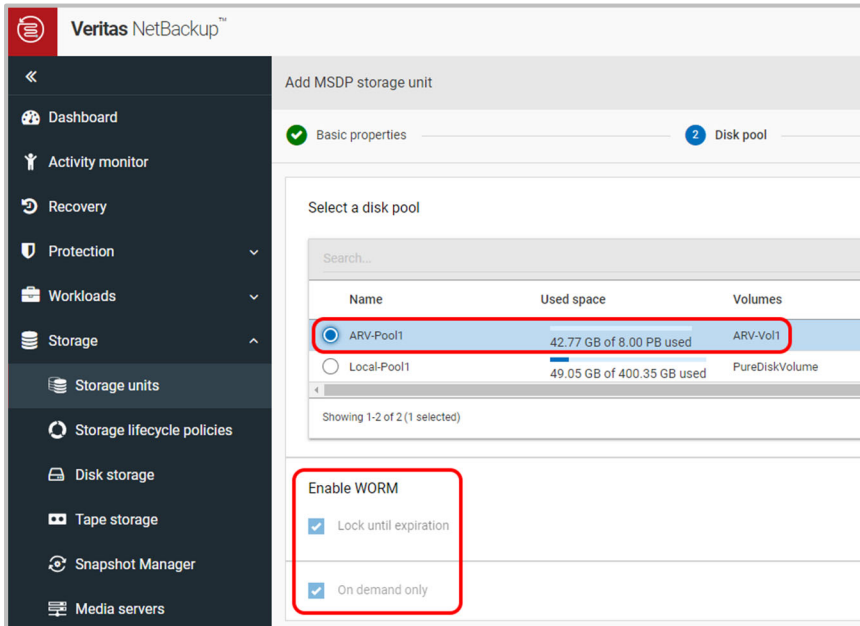
Name *
ngstorage1

Maximum concurrent jobs
1

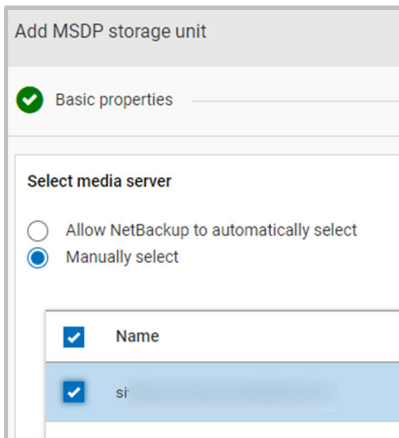
Maximum fragment size
51200 MB

20. Select the Alta Recovery Vault volume created earlier. Click **Next** to continue. (Not shown in the image.)

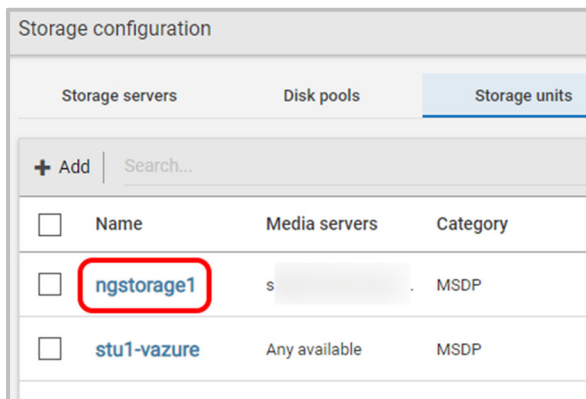
Note: Enable WORM will be checked by default and cannot be un-checked.



21. Select the media server you wish to use. Click **Next** to continue. (Not shown in the image.)



22. Here you can see your new “ngstorage1” storage unit successfully created.



The new Alta Recovery Vault storage can now be used for backups.

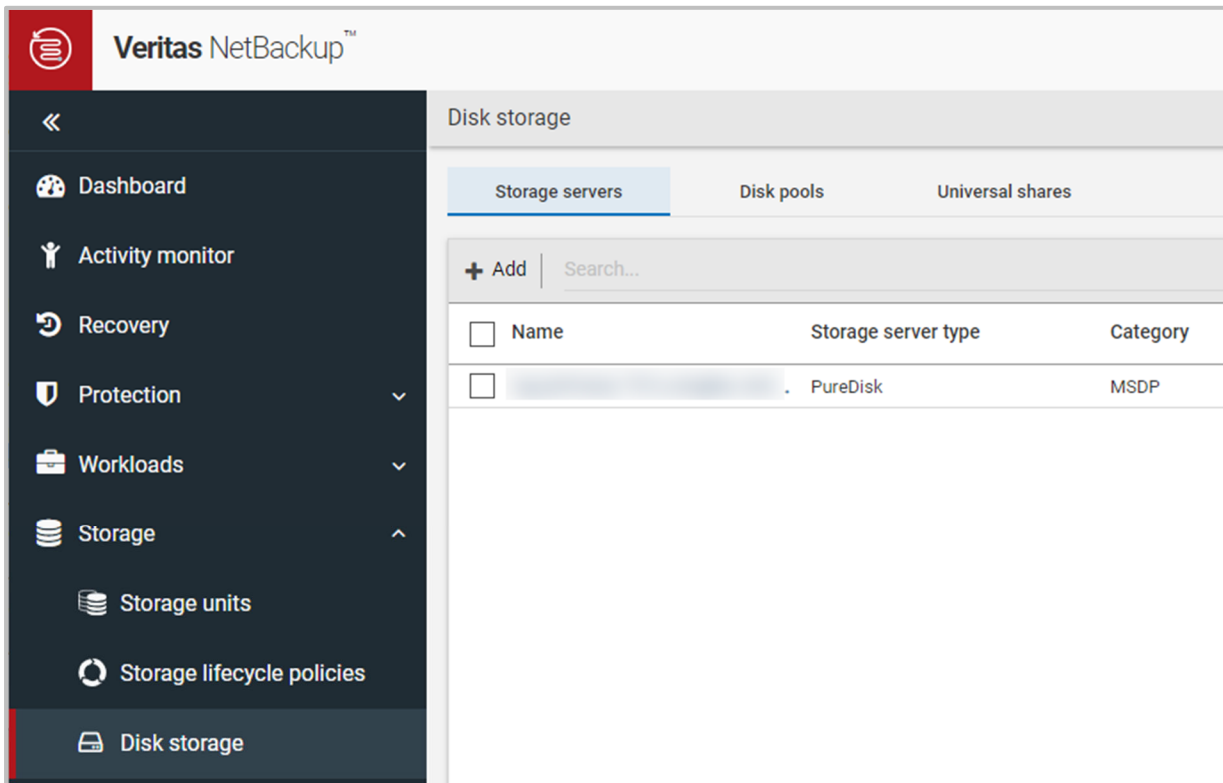
NetBackup 10.3

Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

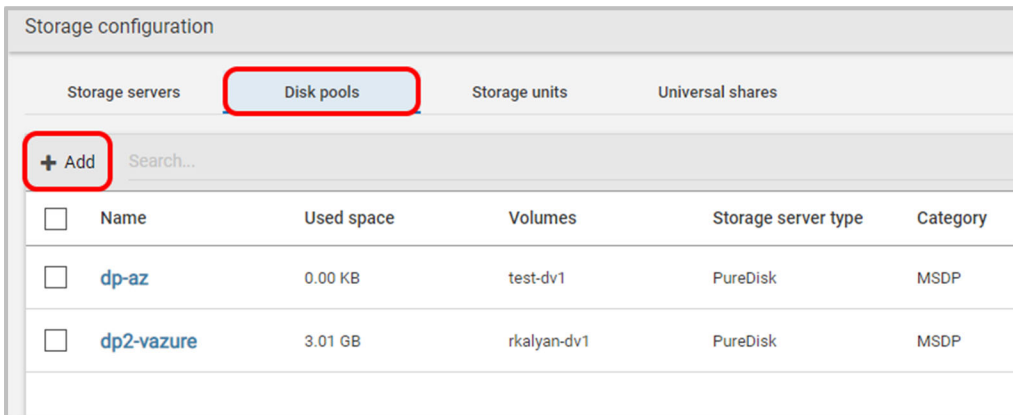
1. Ensure your storage server has been created.
 - a. Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*:
https://www.veritas.com/content/support/en_US/doc/25074086-159245004-0/v24332600-159245004

2. From within your NetBackup primary server web UI, navigate to **Storage > Disk Storage**

You should see your storage server(s) listed.



3. Click the **Disk pools** tab and click **+ Add**.



4. First, enter the details for disk pool options.

- f. Select the storage server name where this disk pool will reside. In this example, the choice is the storage server seen in step 1 of this procedure.
- g. Provide a name for the disk pool. This example uses “ngpool1”.
- h. If you choose, provide a description for the pool.
- i. Select **Limit I/O streams** if desired. This option could help limit disk I/O contention.
- j. Click **Next** at the bottom of the page to continue. (Not seen in the image.)

The screenshot shows the 'Add disk pool' configuration window with the 'Disk pool options' step selected. The 'Storage server name' is 'siv'. The 'Disk pool name' is 'ngpool1'. The 'Description' field is empty. The 'Limit I/O streams' checkbox is unchecked. Below this, a note states: 'The following options do not apply if you select a cloud MSDP disk volume in the next step.' Underneath, there are two water mark settings: 'High water mark' at 98% and 'Low water mark' at 80%.

5. Next, you're brought to the Volumes page. In the example you can see that there are already three volumes created, but you want to add your new Alta Recovery Vault volume. Click **Volume > Select volume**.

The screenshot shows the 'Add MSDP disk pool' configuration window with the 'Volumes' step selected. A dropdown menu labeled 'Volume' is open, showing 'Select volume'. Below this is a search bar and a table of existing volumes.

Name	Available space	Total size	Encryption
PureDiskVolume	753.88 GB	885.38 GB	No
test-dv1	8.00 PB	8.00 PB	No
rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

6. Click **Add volume** to begin the process.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Select volume

Add volume

	Name	Available space	Total size	Encryption
<input type="radio"/>	PureDiskVolume	753.88 GB	885.38 GB	No
<input type="radio"/>	test-dv1	8.00 PB	8.00 PB	No
<input type="radio"/>	rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

7. Provide a name for the new volume and click **Cloud storage provider**.

Add MSDP disk pool

✓ Disk pool options 2 Volumes 3 Replication

Volume

Add volume

Volume name *
ngvolume1

Cloud cache properties

⚠ A request value lower than 1,017 GB may affect performance. Verify that the required space to create this pool is available.

Available disk space: 146.57 GB

Request cloud cache disk space *
73 GB
Enter a value between 4 GB and 117 GB.

Cloud storage provider *
Select cloud storage provider

Storage API type
-

8. Search for “Veritas Alta Recovery Vault Azure” and the following Cloud storage providers appear. For this example, you will choose **Veritas Alta Recovery Vault Azure**.

Select cloud storage provider		
Search...		
Cloud storage provider	Description	Storage API type
<input checked="" type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure

9. After you select the cloud storage provider, you’re taken back to the Add MSDP disk pool screen. Select the Storage tier you would like and the Azure region to be used.

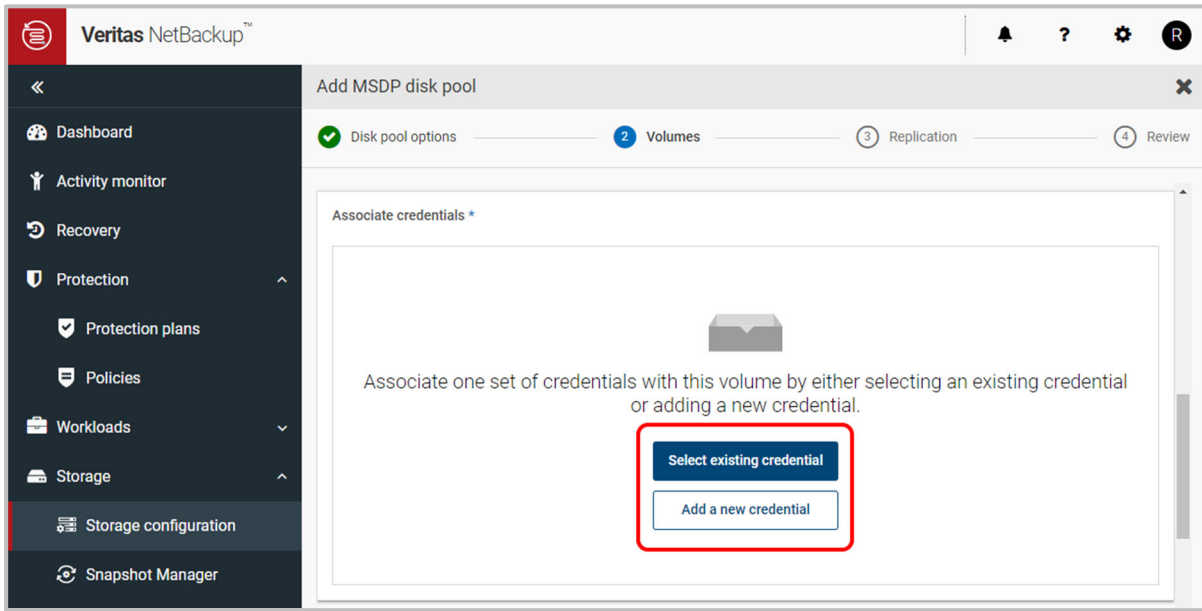
Note: The region is provided by the Veritas Alta Recovery Vault Provisioning Team.

The image shows two side-by-side screenshots of the 'Add MSDP disk pool' configuration interface. Both screenshots show the 'Disk pool options' section with a '2 Volumes' indicator. The left screenshot shows the 'Storage tier' dropdown set to 'Account access tier' and the 'Region' dropdown set to 'blob.core.windows.net'. The right screenshot shows the 'Storage tier' dropdown set to 'Archive' and the 'Archive again after' field set to '3 days'. Red boxes highlight these specific settings in both screenshots.

If you’ve purchased archive tier, click **Account access tier** and select **Archive**. You have a choice to archive again every 3 to 30 days.

Note: For archive tier, ensure your cloud vendor provides archive support in the desired region. If archive tier is not supported in the region, this feature will not function correctly.

10. Click **Select existing credential** if you've already created your credential from the Short-Lived Token Based Authentication section earlier in this document. If not, click **Add a new credential** and create a new credential using the storage account and refresh token given to you by Veritas.



Note: You can create multiple disk volumes/buckets using the same credentials. There is no need to add multiple credentials for the same storage account.


Note: The storage account, short lived tokens, and access keys are provided by the Veritas Alta Recovery Vault Provisioning Team.

Access details for Azure account

Storage account *

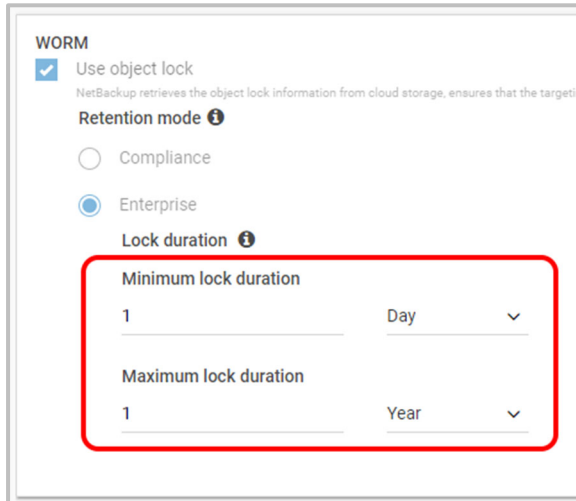
rvlrcust001

Access key *

..... 

11. In the WORM section is where you set the immutability time duration. During the Lock duration the image is locked. For more information regarding immutability, see the [Veritas Knowledge Base Article 100055803](https://www.veritas.com/learn/whitepapers/100055803) for more information on Alta Recovery Vault and immutability.

Note: WORM and Enterprise mode are selected by default and cannot be changed.

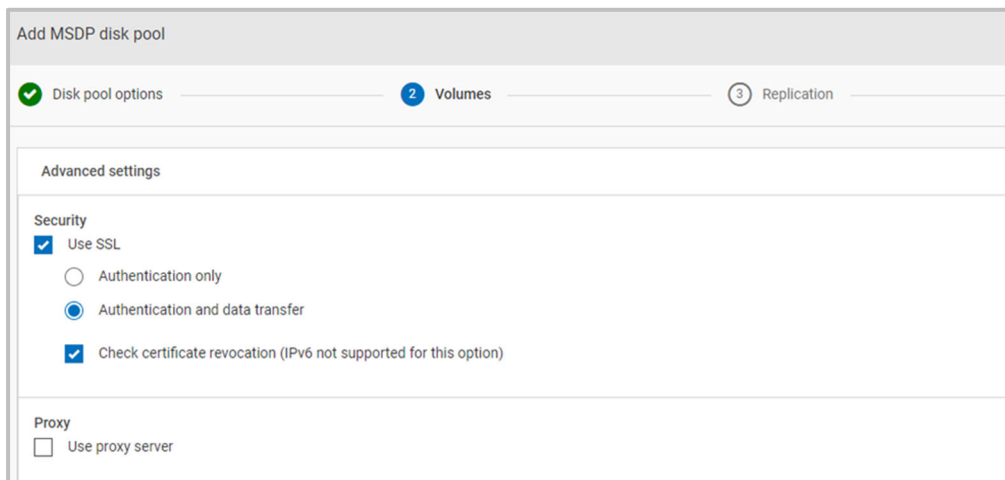


The screenshot shows the 'WORM' configuration section. It includes a checked checkbox for 'Use object lock'. Below it, the 'Retention mode' is set to 'Enterprise' (selected with a radio button). The 'Lock duration' section is highlighted with a red box and contains two fields: 'Minimum lock duration' set to '1 Day' and 'Maximum lock duration' set to '1 Year'.

12. In Advanced settings, enter the required Security or Proxy preferences.

Note: If you do not want to open port 80 externally, you will need to uncheck “Check certificate revocation”, For more information on check certificate revocation, see the following: https://en.wikipedia.org/wiki/Certificate_revocation_list#:~:text=In%20cryptography%2C%20a%20certificate%20revocation,should%20no%20longer%20be%20trusted%22.

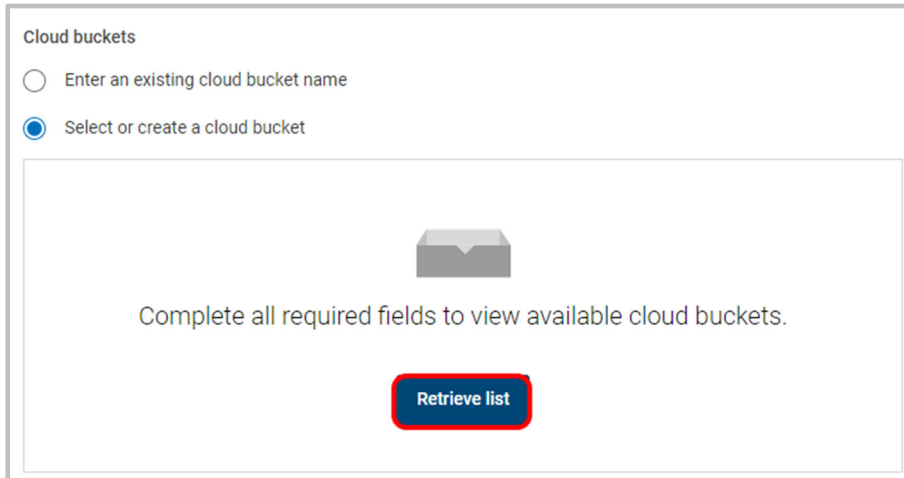
Note: A proxy server can be used if wanted. Check the box seen below and enter the required information for the proxy server.



The screenshot shows the 'Add MSDP disk pool' configuration interface. It has three tabs: 'Disk pool options' (selected), 'Volumes', and 'Replication'. Under 'Advanced settings', the 'Security' section has 'Use SSL' checked, 'Authentication and data transfer' selected, and 'Check certificate revocation (IPv6 not supported for this option)' checked. The 'Proxy' section has 'Use proxy server' unchecked.

13. Click **Select or create a cloud bucket** and then click **Retrieve list**. This process logs into Azure using the credentials provided earlier.

Note: If the Retrieve List operation is successful, the credentials to connect to the Azure storage are correct.



Cloud buckets

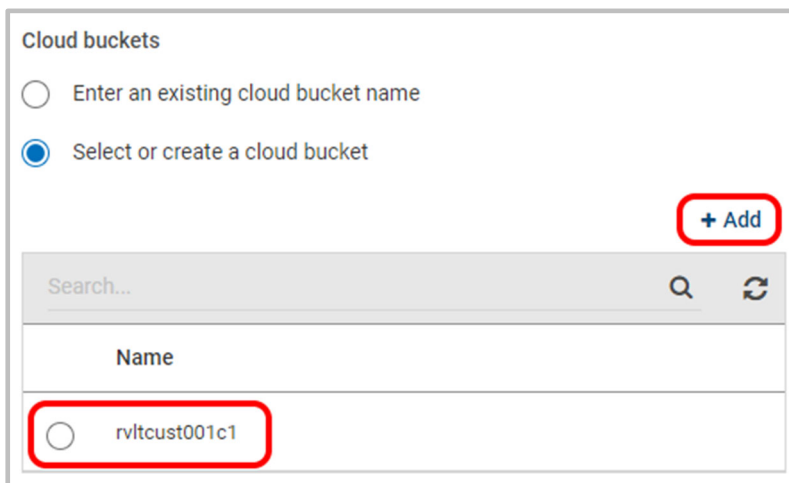
Enter an existing cloud bucket name

Select or create a cloud bucket

Complete all required fields to view available cloud buckets.

Retrieve list

14. A new bucket can also be created using the **+ Add** button in the NetBackup web UI after you connect to the new storage account. Listed below is the Alta Recovery Vault cloud bucket “rvlrcust001c1”. The name of your cloud bucket will be different; the one below is for reference only.



Cloud buckets

Enter an existing cloud bucket name

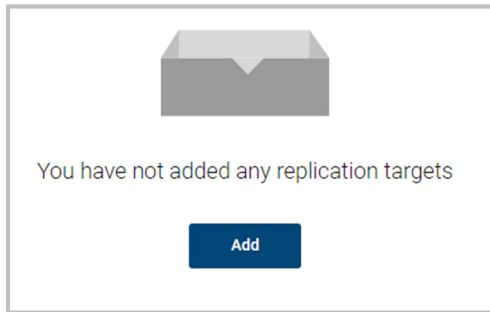
Select or create a cloud bucket

+ Add

Search... 🔍 ↻

Name
<input type="radio"/> rvlrcust001c1

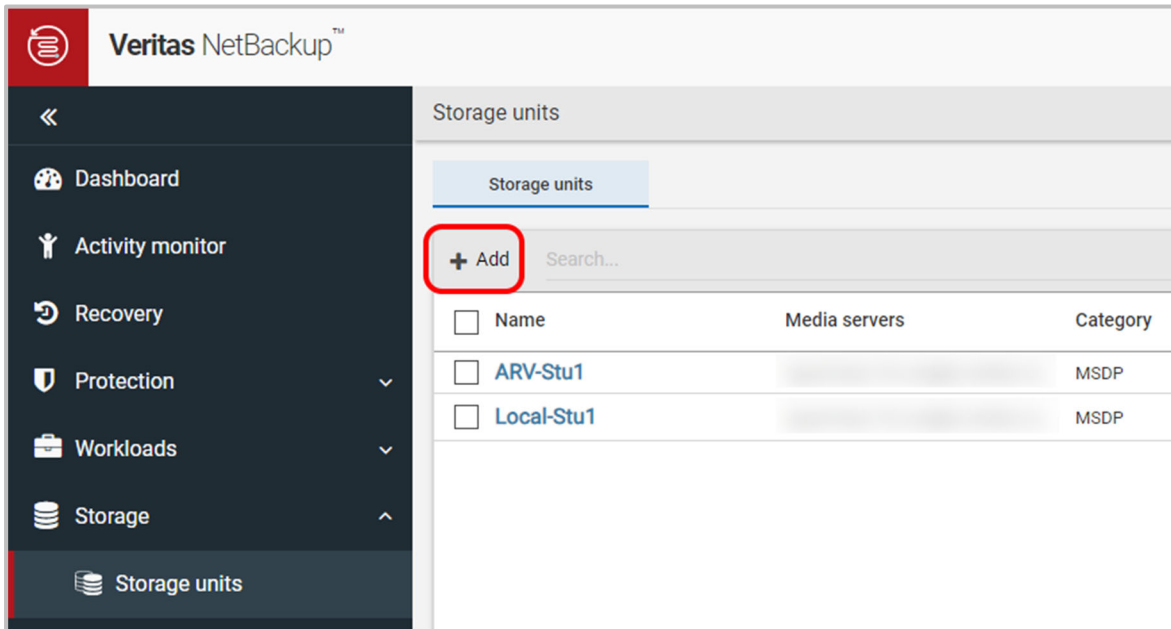
15. If you would like to set up replication targets, they can be set up now. If none are needed, click **Next**. (Not shown in the image.)



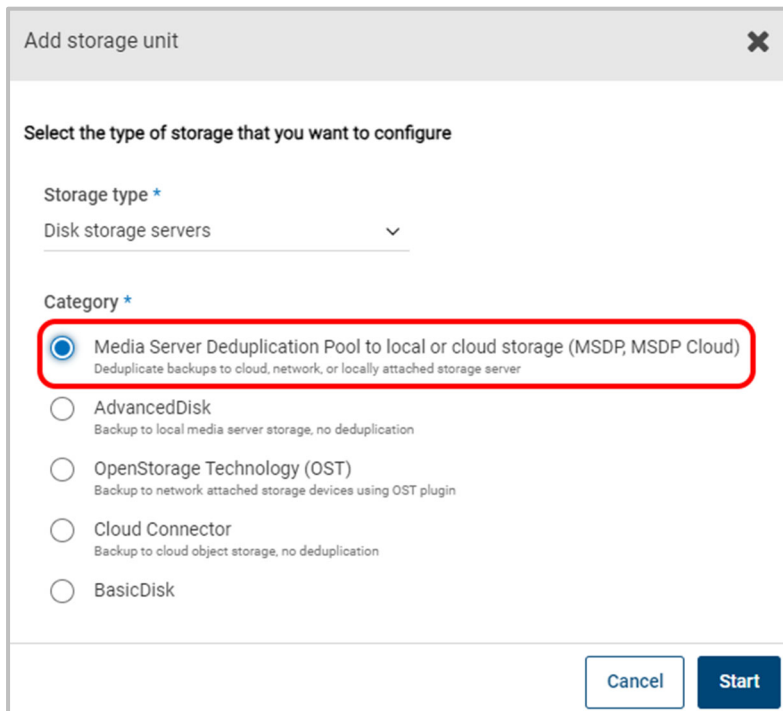
16. The next page is a summary page. If everything looks good, create the new disk pool. In this example, the new "ngpool1" has been created.

Storage configuration							
Storage servers		Disk pools		Storage units		Universal shares	
+ Add Search...							
<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category		
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP		
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP		
<input type="checkbox"/>	ngpool1	0.00 KB	ngvolume1	PureDisk	MSDP		

17. Next, add a storage unit so you can use your new Alta Recovery Vault storage. Under Storage > Storage Units, click **+ Add**.



18. Select **Media Server Deduplication Pool to local or cloud storage (MSDP, MSDP Cloud)** and click **Start**.



19. Provide a new MSDP storage unit name and select the desired **Maximum concurrent jobs** and **Maximum fragment size**. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

1 Basic properties

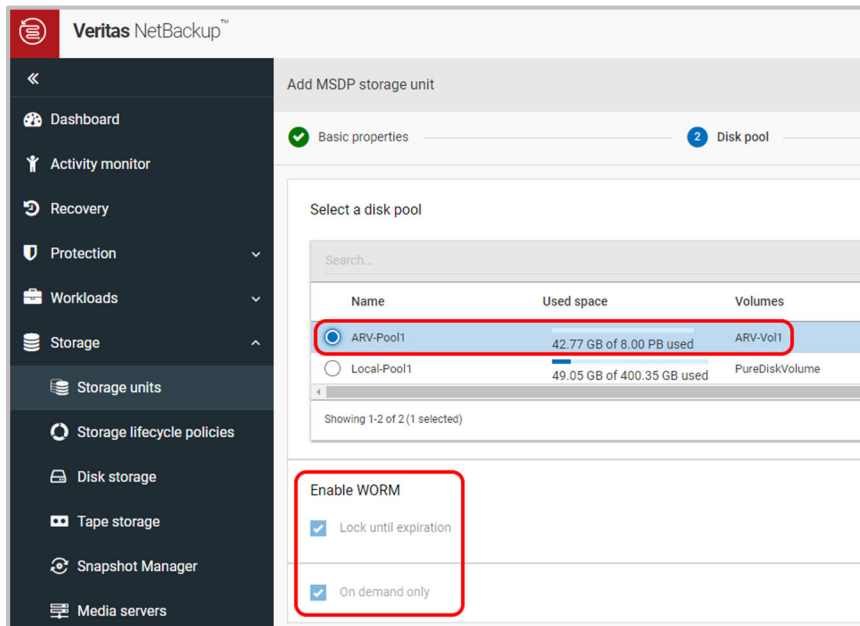
Name *
ngstorage1

Maximum concurrent jobs
1

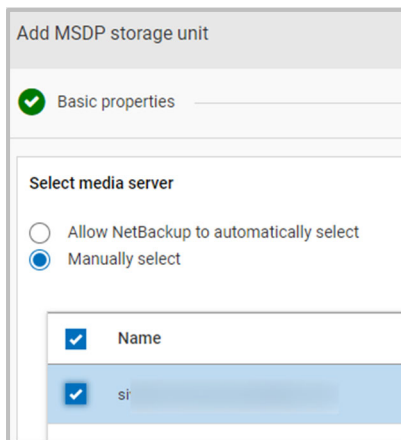
Maximum fragment size
51200 MB

20. Select the Alta Recovery Vault volume created earlier. Click **Next** to continue. (Not shown in the image.)

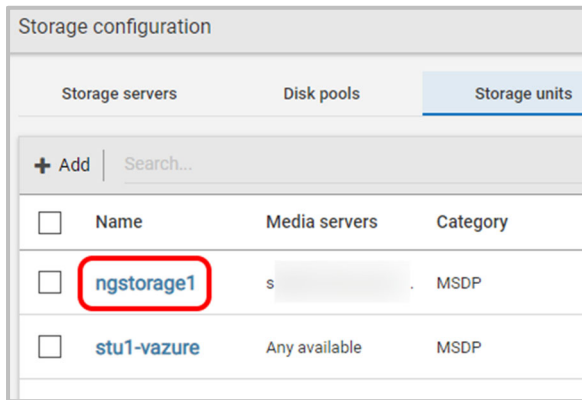
Note: Enable WORM will be checked by default and cannot be un-checked.



21. Select the media server you wish to use. Click **Next** to continue. (Not shown in the image.)



22. Here you can see your new “ngstorage1” storage unit successfully created.



23. The new Alta Recovery Vault storage can now be used for backups.

Netbackup 10.2

Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

1. Ensure your storage server has been created.
 - a. Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*: https://www.veritas.com/content/support/en_US/doc/25074086-159245004-0/v24332600-159245004
2. Log into the console of your media server that is your MSDP storage server you created in step 1.
3. A Volume and a Volume Container must be created at the CLI before they can be created in the web UI.
4. Run the following command to create the volume and volume container (without archive):
 - a. `/usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -as -in NetBackup-Recovery-Vault-Azure -sts <storage_server_name> -pctype NONE -lsu_name <lsu_name>`
 - b. Example:
 - i. `/usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -as -in Veritas-Alta-Recovery-Vault-Azure -sts MSDP-FQDN.com -pctype NONE -lsu_name my-lsu-name`
 - ii. OUTPUT:
 1. *Successfully added storage server(s): <storage_server_name>_lsu_name*
 2. *Example:*
 - a. *Successfully added storage server(s): MSDP-FQDN.com_my-lsu-name*
5. Run the following command to create the volume and volume container (with archive):

a. `/usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -as -in Veritas-Alta-Recovery-Vault-Azure -sts <Storage_Server_Name> -pstype NONE -lsu_name <lsu-name> -storage_tier ARCHIVE -post_rehydration_period <# of days>`

b. Example:

i. `/usr/opensv/netbackup/bin/admincmd/csconfig cldinstance -as -in Veritas-Alta-Recovery-Vault-Azure -sts MSDP-FQDN.com -pstype NONE -lsu_name my-lsu-name -storage_tier ARCHIVE -post_rehydration_period 3`

6. Navigate to `/usr/opensv/pdde/pdcr/bin/` on the command line of your media server.

7. Set environment variables for Azure.

a. Azure with short lived tokens (two new variables highlighted in yellow):

- i. `# export MSDPC_REGION=<your region>`
- ii. `# export MSDPC_PROVIDER=vazure`
- iii. `# export MSDPC_ACCESS_KEY=<the credential name you create in the web UI>`
- iv. `# export MSDPC_SECRET_KEY=<this is a dummy value, enter anything>`
- v. `# export MSDPC_ENDPOINT=https://xxxx.blob.core.windows.net/`
"xxxx" is the Storage Account Name
- vi. `# export MSDPC_MASTER_SERVER=<name_of_your_primary_with_fqdn>`
- vii. `#export MSDPC_ALIAS=<output from commands 4 or 5>`

b. Azure Example:

- i. `# export MSDPC_REGION=<your region like "West US 2">`
- ii. `# export MSDPC_PROVIDER=vazure`
- iii. `# export MSDPC_ACCESS_KEY= <RV-Credential1>`
- iv. `# export MSDPC_SECRET_KEY=<my_dummy_secret>`
- v. `# export MSDPC_ENDPOINT=<your endpoint such as https:// rvlcust001c1.blob.core.windows.net>`
- vi. `# export MSDPC_MASTER_SERVER=<widget.widgets.are.us.com>`
- vii. `#export MSDPC_ALIAS=MSDP-FQDN.com_my-lsu-name`

Note: MSDP-C variables highlighted in yellow are new variables added in 10.2. These are necessary for immutability to function properly with Azure.

8. Run the following command with your immutability inputs:

- a. `./msdpclutil create -b <container_name> -v <some_volumename> --mode GOVERNANCE --min time --max time -l expirationdate --enable_sas`
- b. Example `./msdpclutil create -b rvlcust001c1 -v rk-v01 --mode GOVERNANCE --min 1D --max 1Y -l 2024-10-24 --enable_sas`

Governance mode (also known as enterprise mode):

Users require special permissions to disable the retention lock and then delete the image. Only the cloud administrator user can disable the retention lock and then delete the image if required.

Note: '--enable_sas' in the above command is not needed if you are using NB 10.1.x or earlier than NB 10.2

9. A list of the immutable buckets can be seen with the following command:
 - a. `./msdpclutil list -b nameofcontainer`
 - b. Example `./msdpclutil list -b jzh-worm-bucket07`

Note: '--enable_sas' in the above command is not needed if you are using NB 10.1.x or earlier than NB 10.2

10. Now that the immutable container (bucket) has been configured on the command line, the immutable disk pool can be created.
11. Go to the NetBackup web UI and navigate to **Storage > Storage configuration**.

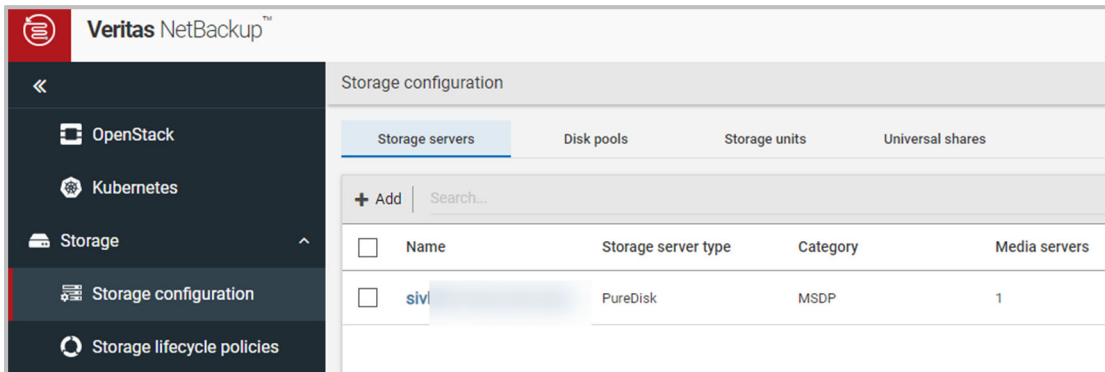
After you receive the storage access keys and the volume and volume container has been created on your media server's CLI, it's time to connect to the new storage container (bucket) in NetBackup through the web UI.

Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*:

https://www.veritas.com/content/support/en_US/doc/25074086-149019166-0/v24332600-149019166

1. From within your NetBackup primary server web UI, navigate to **Storage > Storage configuration**.

You should see your storage servers listed.



2. Click the **Disk pools** tab and click **+ Add**.

Storage configuration					
Storage servers	Disk pools	Storage units	Universal shares		
<input type="checkbox"/> + Add Search...					
<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP

3. Enter the details for disk pool options.

- Select the storage server name where this disk pool will reside. In this example, the choice is the storage server seen in step 1 of this procedure.
- Provide a name for the disk pool. This example uses “ngpool1”.
- If you choose, provide a description for the pool.
- Select **Limit I/O streams** if desired. This option could help limit disk I/O contention.
- Click **Next** at the bottom of the page to continue. (Not seen in the image.)

1 Disk pool options
2 Volumes
3 Replication
4 Review

Storage server name *

Features

Accelerator, A.I.R., Instant access, WORM capable

[Change](#)

Disk pool name *

Description

Enter description

Limit I/O streams
Concurrent read and write jobs affect disk performance. Limit I/O streams to prevent disk overload.

The following options do not apply if you select a cloud MSDP disk volume in the next step.

High water mark
98 %

Low water mark
80 %

4. Next, you're brought to the Volumes page. In the example you can see that there are already three volumes created, but you want to add your new Alta Recovery Vault volume. Click **Volume > Select volume**.

The screenshot shows the 'Add MSDP disk pool' interface. At the top, there are two progress indicators: 'Disk pool options' (checked) and 'Volumes' (2). Below this, a dropdown menu labeled 'Volume' is open, showing 'Select volume' as the selected option. Below the dropdown is a search bar and a table of existing volumes.

	Name	Available space	Total size	Encryption
<input type="radio"/>	PureDiskVolume	753.88 GB	885.38 GB	No
<input type="radio"/>	test-dv1	8.00 PB	8.00 PB	No
<input type="radio"/>	rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

5. Click **Add volume** to begin the process.

The screenshot shows the 'Add MSDP disk pool' interface. At the top, there are two progress indicators: 'Disk pool options' (checked) and 'Volumes' (2). Below this, a dropdown menu labeled 'Volume' is open, showing 'Add volume' as the selected option. Below the dropdown is a search bar and a table of existing volumes.

	Name	Available space	Total size	Encryption
<input type="radio"/>	PureDiskVolume	753.88 GB	885.38 GB	No
<input type="radio"/>	test-dv1	8.00 PB	8.00 PB	No
<input type="radio"/>	rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

6. Provide a name for the new volume and click **Cloud storage provider**.

Note: Name the volume the same as you did using the msdpclutil command.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Add volume ▾

Volume name *
ngvolume1 ⓘ

Cloud storage provider *
Select cloud storage provider

Storage API type
-

7. Search for “veritas” and the following Cloud storage providers appear. For this example, you will choose **Veritas Alta Recovery Vault Azure**.

Select cloud storage provider

Search...

Cloud storage provider	Description	Storage API type
<input checked="" type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure

8. After you select the cloud storage provider, you're taken back to the Add MSDP disk pool screen. Select the Storage tier you would like and the Azure region to be used.

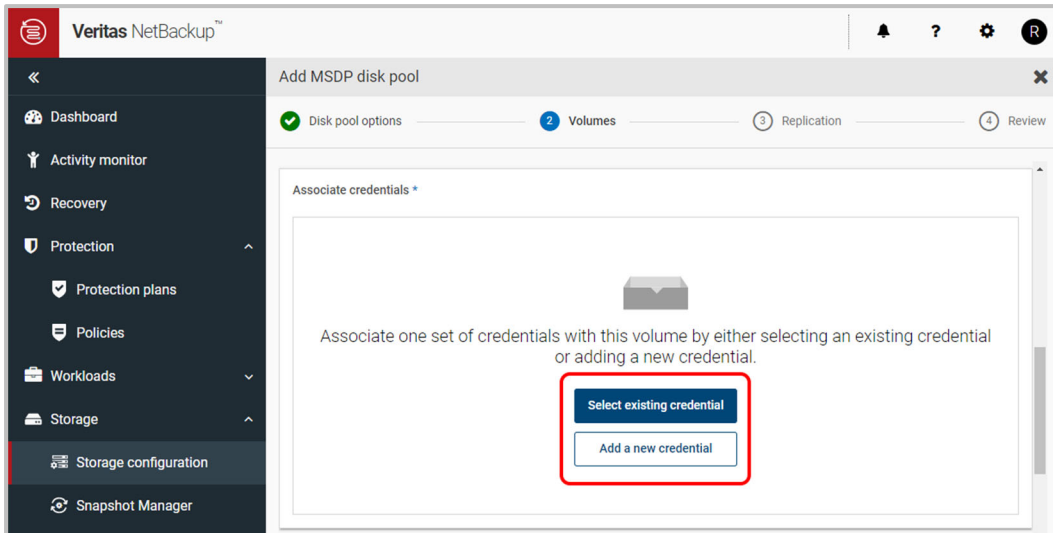
Note: The region is provided by the Veritas Alta Recovery Vault Provisioning Team.

The image displays two side-by-side screenshots of the 'Add MSDP disk pool' configuration interface. Both screenshots show a progress bar at the top with 'Disk pool options' checked and 'Volumes' at step 2. The left screenshot shows the 'Storage tier' dropdown menu set to 'Account access tier' and the 'Region*' dropdown menu set to 'blob.core.windows.net'. The right screenshot shows the 'Storage tier' dropdown menu set to 'Archive' and the 'Archive again after' field set to '3 days'. Red boxes highlight these specific settings in both screenshots.

If you've purchased archive tier, click **Account access tier**, and select **Archive**. You have a choice to archive again every 3 to 30 days.

Note: For archive tier, ensure your cloud vendor provides archive support in the desired region. If archive tier is not supported in the region, this feature will not function correctly.

9. Click **Select existing credential** if you've already created your credential from the Short-Lived Token Based Authentication section earlier in this document. If not, click **Add a new credential** and create a new credential using the storage account and refresh token given to you by Veritas.



Note: You can create multiple disk volumes/buckets using the same credentials. There is no need to add multiple credentials for the same storage account.

Note: The storage account, short lived tokens, and access keys are provided by the Veritas Alta Recovery Vault Provisioning Team.

Access details for Azure account

Storage account *

rvlrcust001

Access key *

.....

10. In Advanced settings, enter the required Security, Proxy, or WORM preferences.

Note: If you do not want to open port 80 externally, you will need to uncheck "Check certificate revocation", For more information on check certificate revocation, see the following: https://en.wikipedia.org/wiki/Certificate_revocation_list#:~:text=In%20cryptography%2C%20a%20certificate%20revocation,should%20no%20longer%20be%20trusted%22.

Note: Ensure to check the **WORM > Use object lock** checkbox.

Note: If you have not completed the CLI steps earlier in the document, the Web UI will give you an error when trying to connect to your Alta Recovery Vault storage.

Add MSDP disk pool

1 Disk pool options — 2 Volumes — 3 Replication

Advanced settings

Security

- Use SSL
- Authentication only
- Authentication and data transfer
- Check certificate revocation (IPv6 not supported for this option)

Proxy

- Use proxy server

WORM


- Use object lock

NetBackup retrieves the Object Lock information from Cloud storage. Ensure that the targeting bucket is created, and the Object Lock mode is set. Refer to the NetBackup Deduplication Guide for more details.

11. Click **Select or create a cloud bucket** and then click **Retrieve list**. This process logs into Azure using the credentials provided earlier.

Cloud buckets

- Enter an existing cloud bucket name
- Select or create a cloud bucket



Complete all required fields to view available cloud buckets.

Retrieve list

12. A new container (bucket) can also be created using the **+ Add** button in the web UI after you connect to the new storage account. Listed below is the Alta Recovery Vault cloud bucket “rvltcust001c1”. The name of your cloud bucket will be different; the one below is for reference only.

Cloud buckets

Enter an existing cloud bucket name

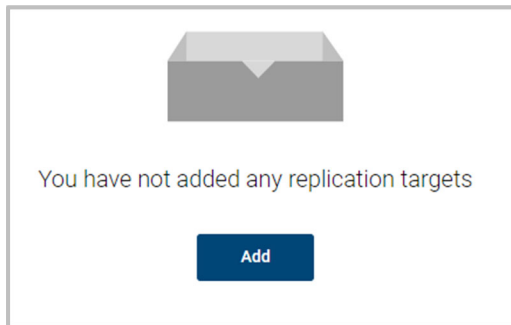
Select or create a cloud bucket

+ Add

Search...

Name
<input type="radio"/> rvltcust001c1

13. If you would like to set up replication targets, they can be set up now. If none are needed, click **Next**. (Not shown in the image.)



14. The next page is a summary page. If everything looks good, create the new disk pool. In this example, the new “ngpool1” has been created.

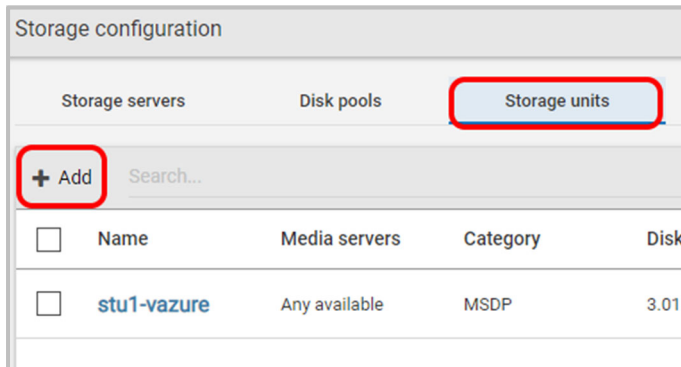
Storage configuration

Storage servers | **Disk pools** | Storage units | Universal shares

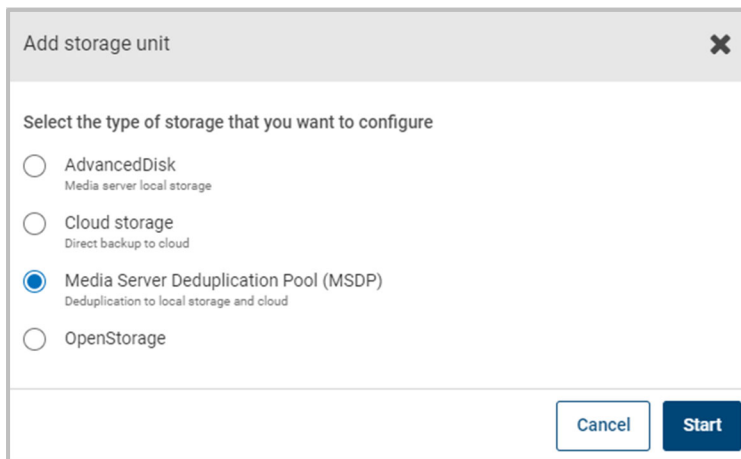
+ Add | Search...

<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP
<input type="checkbox"/>	ngpool1	0.00 KB	ngvolume1	PureDisk	MSDP

15. Next, add a storage unit so you can use your new Alta Recovery Vault storage. Click the **Storage units** tab and click **+ Add**.



16. Select **Media Server Deduplication Pool (MSDP)** and click **Start**.



17. Provide a new MSDP storage unit name and select the desired **Maximum concurrent jobs** and **Maximum fragment size**. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

1 Basic properties

Name *
ngstorage1

Maximum concurrent jobs
1

Maximum fragment size
51200 MB

18. Select the Alta Recovery Vault volume created earlier. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

Basic properties 2 Disk pool

Select a disk pool

Search...

Name	Used space	Volumes	Storage type	Storage server
<input type="radio"/> dp-az	0.00 KB of 8.00 PB used	test-dv1	PureDisk	si
<input type="radio"/> dp2-vazure	3.01 GB of 8.00 PB used	rkalyan-dv1	PureDisk	si
<input checked="" type="radio"/> ngpool1	0.00 KB of 8.00 PB used	ngvolume1	PureDisk	si

Showing 1-3 of 3 (1 selected)

19. Select the media server you wish to use. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

✓ Basic properties

Select media server

Allow NetBackup to automatically select

Manually select

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	si

20. Here you can see your new “ngstorage1” storage unit successfully created.

Storage configuration

Storage servers Disk pools **Storage units**

+ Add Search...

<input type="checkbox"/>	Name	Media servers	Category
<input type="checkbox"/>	ngstorage1	s	MSDP
<input type="checkbox"/>	stu1-vazure	Any available	MSDP

21. The new Alta Recovery Vault storage can now be used for backups.

NetBackup 10.1.1 or earlier

Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

1. Ensure your storage server has been created.
 - a. Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*: https://www.veritas.com/content/support/en_US/doc/25074086-149019166-0/v24332600-149019166
2. Log into the console of your media server that is your MSDP storage server you created in step 1.

3. Navigate to `/usr/opensv/pdde/pdcr/bin/` on the command line of your media server.

Set environment variables for Azure.

- a. Azure:
 - i. `# export MSDPC_ACCESS_KEY=xxxx(Your Storage Account)`
 - ii. `# export MSDPC_SECRET_KEY=yyyyyyyyyyyyyy (Your Access Key)`
 - iii. `# export MSDPC_REGION=<selectedregion>`
 - iv. `# export MSDPC_PROVIDER=vazure`
 - v. `#export MSDPC_ENDPOINT="https://<container>.blob.core.windows.net/"`
- b. Azure Example:
 - i. `# export MSDPC_ACCESS_KEY=<giventoyoubyVeritas> (Your Storage Account)`
 - ii. `# export MSDPC_SECRET_KEY=<giventoyoubyVeritas> (Your Access Key)`
 - iii. `# export MSDPC_REGION=<"East US 1">`
 - iv. `# export MSDPC_PROVIDER=vazure`
 - v. `#export MSDPC_ENDPOINT="https://<container>.blob.core.windows.net/"`

Governance mode (also known as enterprise mode):

Users require special permissions to disable the retention lock and then delete the image. Only the cloud administrator user can disable the retention lock and then delete the image if required.

4. Run the following command with your immutability inputs:
 - a. `./msdpclutil create -b <container_name> -v volumename --mode GOVERNANCE --min time --max time -l expirationdate`
 - b. Example `./msdpclutil create -b jzh-worm-bucket07 -v jzh-b01-v02 --mode GOVERNANCE --min 1D --max 1Y -l 2024-10-24`
5. A list of the immutable containers (buckets) can be seen with the following command:
 - a. `./msdpclutil list -b nameofcontainer`
 - b. Example `./msdpclutil list -b jzh-worm-bucket07`
6. Now that the immutable bucket has been configured on the command line, the immutable disk pool can be created.
7. Go to the NetBackup web UI and navigate to **Storage > Storage configuration**.

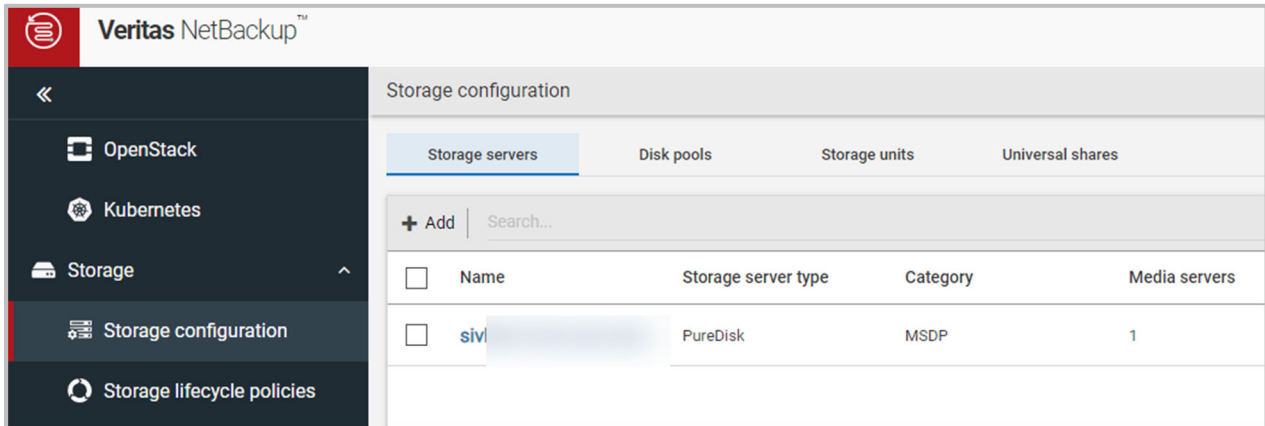
After the volume and volume container have been created on your media server's CLI, it's time to connect to the new storage container (bucket) in NetBackup through the Web UI.

Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*:

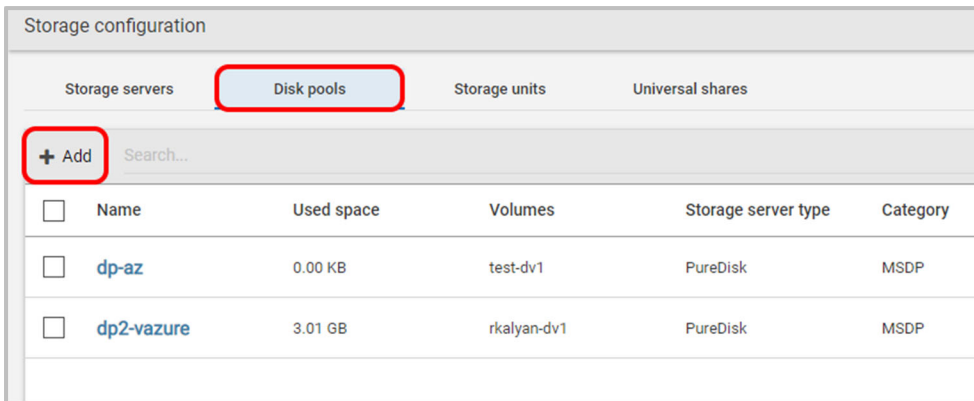
https://www.veritas.com/content/support/en_US/doc/25074086-149019166-0/v24332600-149019166

On your primary server web UI, navigate to **Storage > Storage configuration**.

1. You should see your storage servers listed.



2. Click the **Disk pools** tab and click **+ Add**.



3. First, you enter in the details for disk pool options.

- a. Select the storage server name where this disk pool will reside. In this example, the choice is the storage server seen in step 1 of this procedure.
- b. Provide a name for the disk pool. This example uses “ngpool1”.
- c. If you choose, provide a description for the pool.
- d. Select **Limit I/O streams** if desired. This option could help limit disk I/O contention.
- e. Click **Next** at the bottom of the page to continue. (Not shown in the image.)

The screenshot shows a configuration window titled "Add disk pool" with a close button (X) in the top right corner. The window is divided into four steps: 1. Disk pool options (active), 2. Volumes, 3. Replication, and 4. Review.

Storage server name *
siv

Features
Accelerator, A.I.R., Instant access, WORM capable

Change

Disk pool name *
ngpool1

Description
Enter description

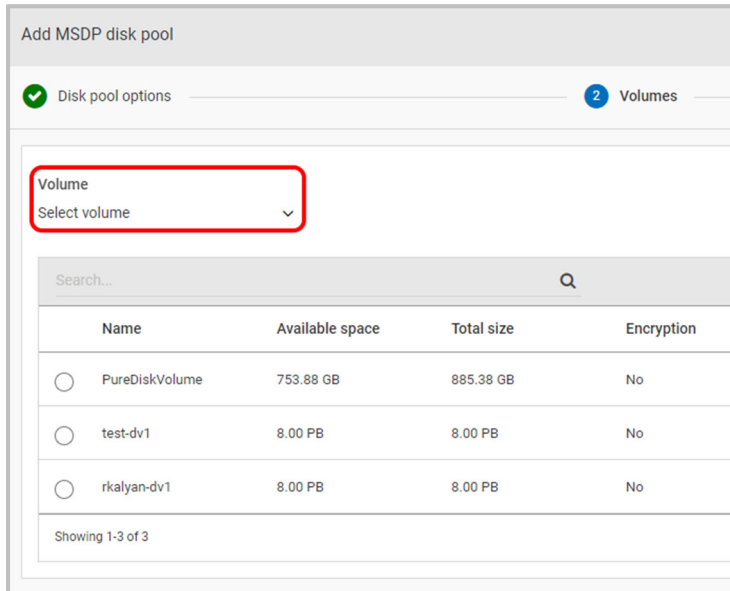
Limit I/O streams
Concurrent read and write jobs affect disk performance. Limit I/O streams to prevent disk overload.

The following options do not apply if you select a cloud MSDP disk volume in the next step.

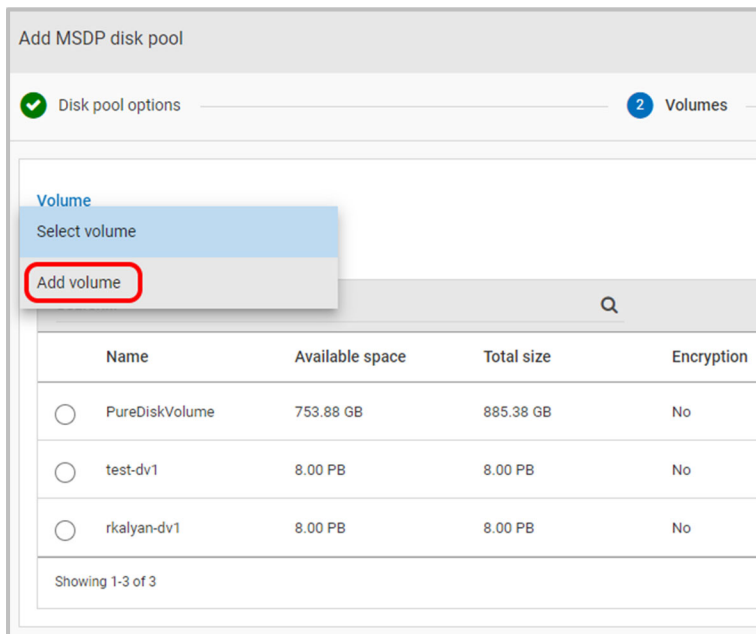
High water mark
98 %

Low water mark
80 %

4. Next, you'll be brought to the Volumes page. As you can see, there are already three volumes created, but you want to add your new Alta Recovery Vault volume. Click **Volume > Select volume**.



5. Click **Add volume** to begin the volume add process.



6. Provide a name for the new volume and click **Cloud storage provider**.

Note: If WORM is being used, the volume name should be same as the volume created using msdpclutil. For more information, see immutability section.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Add volume

Volume name *
ngvolume1

Cloud storage provider *
Select cloud storage provider

Storage API type

7. Search for “veritas” and the following Cloud storage providers appear. For this example, the choice is **Veritas Alta Recovery Vault Azure**.

Select cloud storage provider

Search...

Cloud storage provider	Description	Storage API type
<input checked="" type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure

8. After you select the cloud storage provider, you're taken back to the Add MSDP disk pool screen. Select Account Access Tier as the **Storage tier** and select **blob.core.windows.net** for the Region.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Add volume

Volume name *

ngvolume1

Cloud storage provider * Storage API type

Veritas Alta Recovery Vault Azure Microsoft Azure

Storage tier

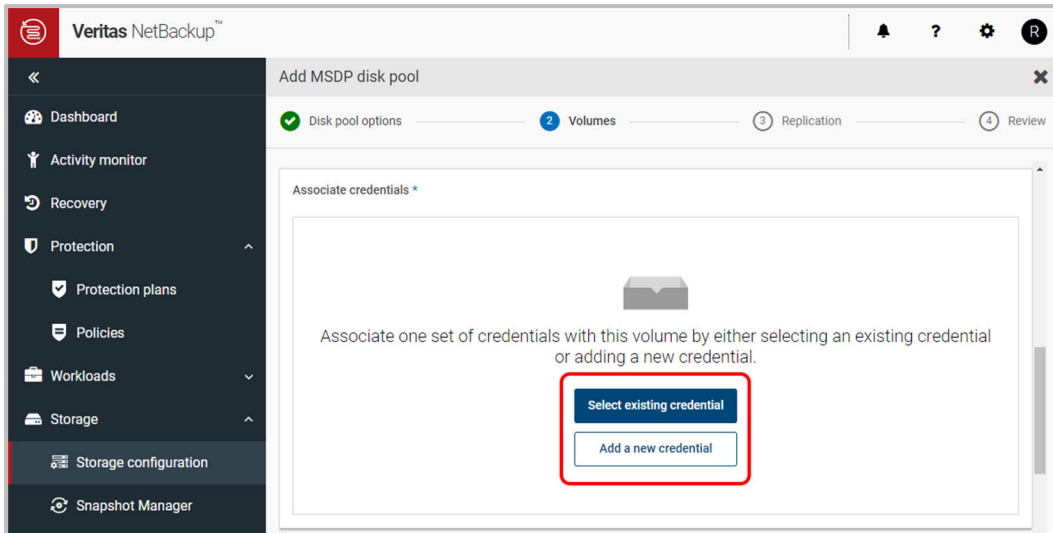
Account access tier

Region *

Service host

blob.core.windows.net

9. Click **Select existing credential** if you've already created your credential from the Short-Lived Token Based Authentication section earlier in this document. If not, click **Add a new credential** and create a new credential using the storage account and refresh token given to you by Veritas.



Note: You can create multiple disk volumes/buckets using the same credentials. There is no need to add multiple credentials for the same storage account.

If you are using NetBackup 10.1.1 or earlier, enter the storage account and Access key for Azure.

Note: The storage account, short lived tokens, and access keys are provided by the Veritas Alta Recovery Vault Provisioning Team.

The image shows a form titled 'Access details for Azure account'. It has two main sections. The first section is 'Storage account *' with a text input field containing 'rvlrcust001'. The second section is 'Access key *' with a text input field filled with dots, indicating a masked password. There is a small eye icon to the right of the access key field to toggle visibility.

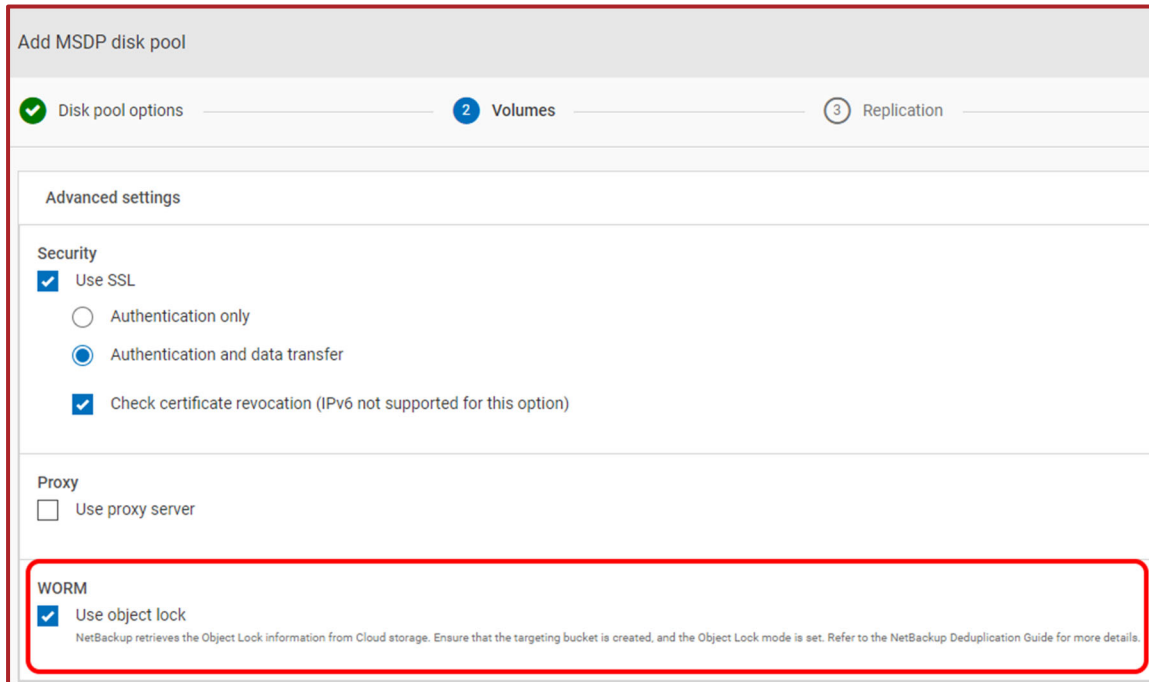
10. In Advanced settings, enter the required Security, Proxy, or WORM preferences.

Note: If you do not want to open port 80 externally, you will need to uncheck “Check certificate revocation”, For more information on check certificate revocation, see the following:

https://en.wikipedia.org/wiki/Certificate_revocation_list#:~:text=In%20cryptography%2C%20a%20certificate%20revocation,should%20no%20longer%20be%20trusted%22.

Note: Ensure to check the **WORM > Use object lock** checkbox.

Note: If you have not completed the CLI steps earlier in the document, the Web UI will give you an error when trying to connect to your Alta Recovery Vault storage.



Add MSDP disk pool

1 Disk pool options — 2 Volumes — 3 Replication

Advanced settings

Security

- Use SSL
 - Authentication only
 - Authentication and data transfer
- Check certificate revocation (IPv6 not supported for this option)

Proxy

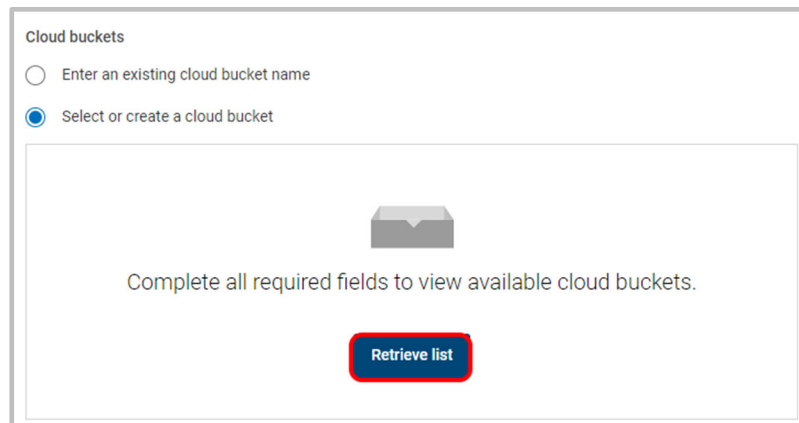
- Use proxy server

WORM

- Use object lock

NetBackup retrieves the Object Lock information from Cloud storage. Ensure that the targeting bucket is created, and the Object Lock mode is set. Refer to the NetBackup Deduplication Guide for more details.

11. Click **Select or create a cloud bucket** and then click **Retrieve list**. This process logs into Azure using the credentials provided earlier.



Cloud buckets

- Enter an existing cloud bucket name
- Select or create a cloud bucket

Complete all required fields to view available cloud buckets.

Retrieve list

12. A new bucket can also be created using the **+ Add** button in the NetBackup web UI after you connect to the new storage account. Listed below is the Alta Recovery Vault cloud bucket “rvltcust001c1”. The name of your cloud bucket will be different; the one below is for reference only.

Cloud buckets

Enter an existing cloud bucket name

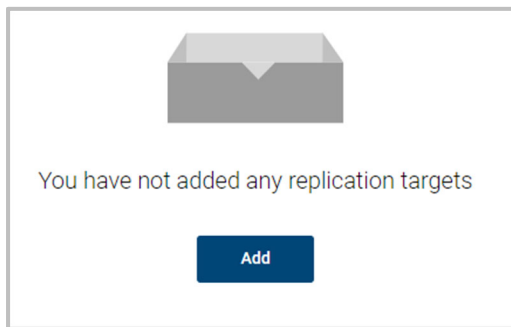
Select or create a cloud bucket

+ Add

Search...

Name
<input type="radio"/> rvlcust001c1

13. If you would like to set up replication targets, they can be set up now. If none are needed, click **Next**. (Not shown in the image.)



14. The next page is a summary page. If everything looks good, create the new disk pool. In this example, the new “ngpool1” has been created.

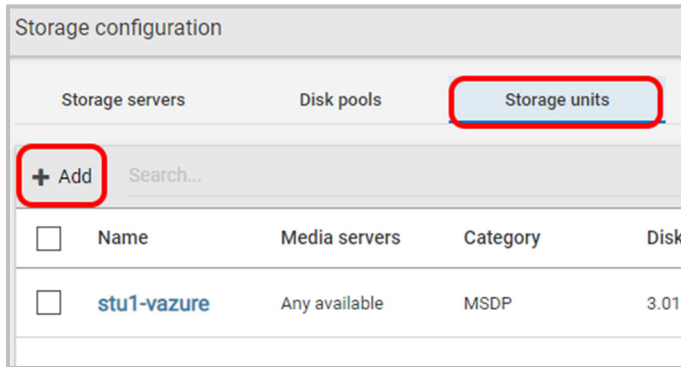
Storage configuration

Storage servers | **Disk pools** | Storage units | Universal shares

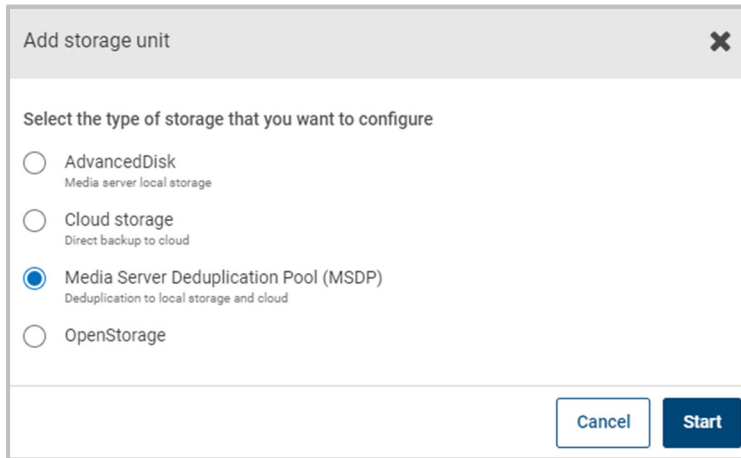
+ Add | Search...

<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP
<input type="checkbox"/>	ngpool1	0.00 KB	ngvolume1	PureDisk	MSDP

15. Next, add a storage unit so you can use your new Alta Recovery Vault storage. Click the **Storage units** tab and click **+ Add**.



16. Select **Media Server Deduplication Pool (MSDP)** and click **Start**.



17. Provide a new MSDP storage unit name and select the desired **Maximum concurrent jobs** and **Maximum fragment size**. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

1 Basic properties

Name *
ngstorage1

Maximum concurrent jobs
1

Maximum fragment size
51200 MB

18. Select the Alta Recovery Vault volume created earlier. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

Basic properties 2 Disk pool

Select a disk pool

Search...

Name	Used space	Volumes	Storage type	Storage server
<input type="radio"/> dp-az	0.00 KB of 8.00 PB used	test-dv1	PureDisk	si
<input type="radio"/> dp2-vazure	3.01 GB of 8.00 PB used	rkalyan-dv1	PureDisk	si
<input checked="" type="radio"/> ngpool1	0.00 KB of 8.00 PB used	ngvolume1	PureDisk	si

Showing 1-3 of 3 (1 selected)

19. Select the media server you wish to use. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

Basic properties

Select media server

Allow NetBackup to automatically select

Manually select

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	si

20. Here you can see your new “ngstorage1” storage unit successfully created.

Storage configuration

Storage servers Disk pools **Storage units**

+ Add Search...

<input type="checkbox"/>	Name	Media servers	Category
<input type="checkbox"/>	ngstorage1	s	MSDP
<input type="checkbox"/>	stu1-vazure	Any available	MSDP

21. The new Alta Recovery Vault storage can now be used for backups.

CONNECTING TO YOUR NEW STORAGE ACCOUNT IN AWS

NetBackup 10.4 or later

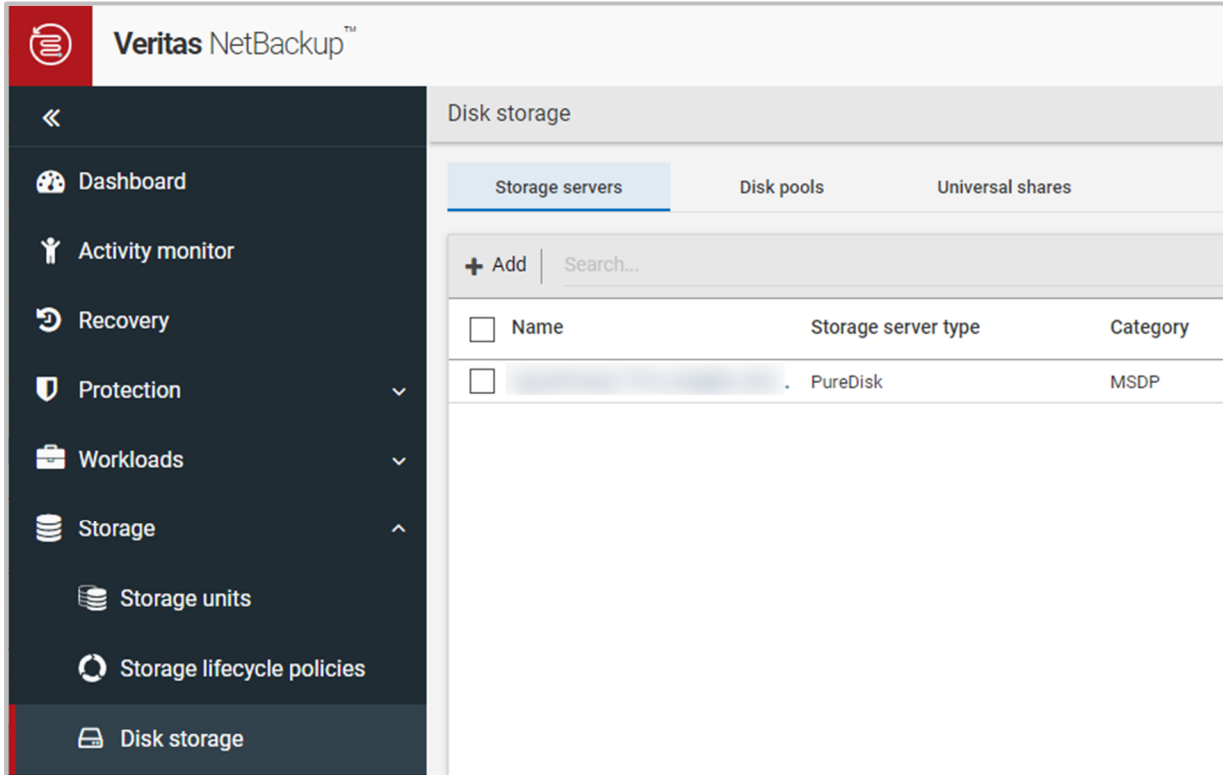
Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

1. Ensure your storage server has been created.

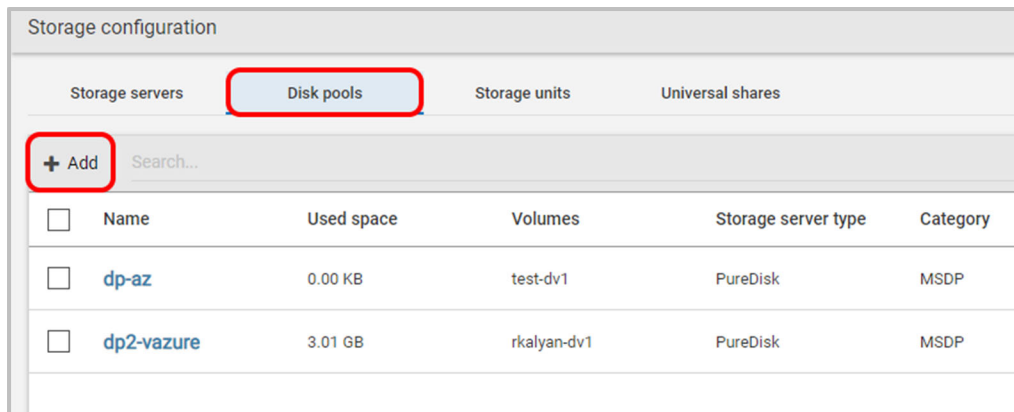
- a. Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*: https://www.veritas.com/content/support/en_US/doc/25074086-159245004-0/v24332600-159245004

2. From within your NetBackup primary server web UI, navigate to **Storage > Disk Storage**

You should see your storage server(s) listed.



3. Click the **Disk pools** tab and click **+ Add**.



4. First, enter the details for disk pool options.

- k. Select the storage server name where this disk pool will reside. In this example, the choice is the storage server seen in step 1 of this procedure.
- l. Provide a name for the disk pool. This example uses “ngpool1”.
- m. If you choose, provide a description for the pool.
- n. Select **Limit I/O streams** if desired. This option could help limit disk I/O contention.
- o. Click **Next** at the bottom of the page to continue. (Not seen in the image.)

The screenshot shows the 'Add disk pool' configuration window with the 'Disk pool options' step selected. The 'Storage server name' is 'siv'. The 'Disk pool name' is 'ngpool1'. There is a 'Description' field with the placeholder 'Enter description'. A checkbox for 'Limit I/O streams' is present with a tooltip: 'Concurrent read and write jobs affect disk performance. Limit I/O streams to prevent disk overload.' Below this, a note states: 'The following options do not apply if you select a cloud MSDP disk volume in the next step.' There are two water mark settings: 'High water mark' at 98% and 'Low water mark' at 80%.

5. Next, you're brought to the Volumes page. In the example you can see that there are already three volumes created, but you want to add your new Alta Recovery Vault volume. Click **Volume > Select volume**.

The screenshot shows the 'Add MSDP disk pool' configuration window with the 'Volumes' step selected. A dropdown menu labeled 'Volume' is open, showing 'Select volume'. Below is a search bar and a table of existing volumes.

Name	Available space	Total size	Encryption
PureDiskVolume	753.88 GB	885.38 GB	No
test-dv1	8.00 PB	8.00 PB	No
rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

6. Click **Add volume** to begin the process.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Select volume

Add volume

	Name	Available space	Total size	Encryption
<input type="radio"/>	PureDiskVolume	753.88 GB	885.38 GB	No
<input type="radio"/>	test-dv1	8.00 PB	8.00 PB	No
<input type="radio"/>	rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

7. Provide a name for the new volume and click **Cloud storage provider**.

Add MSDP disk pool

✓ Disk pool options 2 Volumes 3 Replication

Volume

Add volume

Volume name *
ngvolume1

Cloud cache properties

⚠ A request value lower than 1,017 GB may affect performance. Verify that the required space to create this pool is available.

Available disk space: 146.57 GB

Request cloud cache disk space *
73 GB
Enter a value between 4 GB and 117 GB.

Cloud storage provider *
Select cloud storage provider

Storage API type
-

8. Search for “Veritas Alta Recovery Vault Amazon” and the following Cloud storage providers appear. For this example, you will choose **Veritas Alta Recovery Vault Amazon**.

Select cloud storage provider		
Search...		
Cloud storage provider	Description	Storage API type
<input type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input checked="" type="radio"/> Veritas Alta Recovery Vault Amazon	Veritas Alta Recovery Vault Amazon Storage Service	S3
<input type="radio"/> Veritas Alta Recovery Vault Amazon Government	Veritas Alta Recovery Vault Amazon Storage Service	S3

9. After you select the cloud storage provider, you’re taken back to the Add MSDP disk pool screen. Select the Storage tier you purchased and the AWS region to be used.

Note: Choices for Storage Tier are:

Alta Recovery Vault Standard – AWS

or

Alta Recovery Vault Archive - AWS

Note: If you’ve purchased archive tier, select Alta Recovery Vault Archive - AWS.

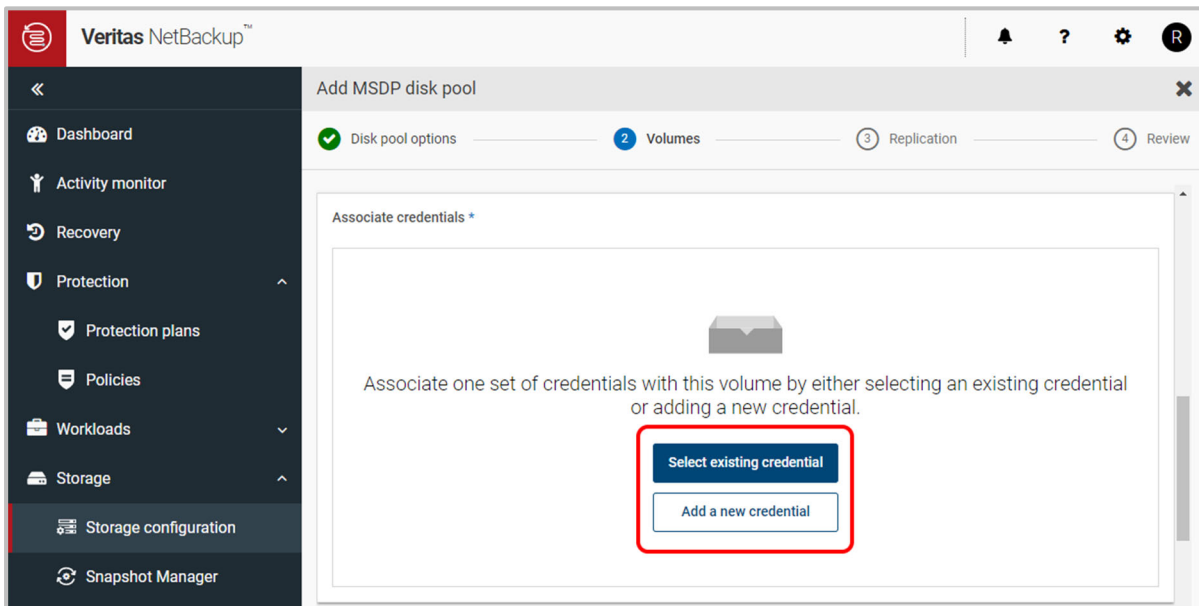
Note: For archive tier, ensure your cloud vendor provides archive support in the desired region. If archive tier is not supported in the region, this feature will not function correctly.

Note: The region is provided by the Veritas Alta Recovery Vault Provisioning Team.

Cloud storage provider *	Storage API type	
Veritas Alta Recovery Vault Amazon	Amazon S3	
Storage class		
Alta Recovery Vault Standard - AWS		
Region *		
Service host	Region name	Region identifier
<input checked="" type="radio"/> s3.dualstack.us-east-1.amazonaws.com	US East (N. Virginia)	us-east-1
<input type="radio"/> s3.dualstack.us-west-1.amazonaws.com	US West (Northern California)	us-west-1
<input type="radio"/> s3.dualstack.us-west-2.amazonaws.com	US West (Oregon)	us-west-2
<input type="radio"/> s3.dualstack.eu-west-1.amazonaws.com	EU (Ireland)	eu-west-1
<input type="radio"/> s3.dualstack.ap-east-1.amazonaws.com	Asia Pacific (Hong Kong)	ap-east-1

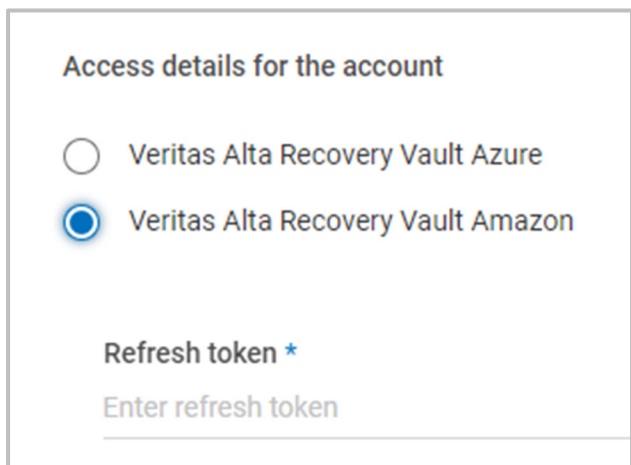
Cloud storage provider *	Storage API type	
Veritas Alta Recovery Vault Amazon	Amazon S3	
Storage class		
Alta Recovery Vault Archive - AWS		
Region *		
Service host	Region name	Region identifier
<input checked="" type="radio"/> s3.dualstack.us-east-1.amazonaws.com	US East (N. Virginia)	us-east-1
<input type="radio"/> s3.dualstack.us-west-1.amazonaws.com	US West (Northern California)	us-west-1
<input type="radio"/> s3.dualstack.us-west-2.amazonaws.com	US West (Oregon)	us-west-2
<input type="radio"/> s3.dualstack.eu-west-1.amazonaws.com	EU (Ireland)	eu-west-1
<input type="radio"/> s3.dualstack.ap-east-1.amazonaws.com	Asia Pacific (Hong Kong)	ap-east-1

10. Click **Select existing credential** if you've already created your credential from the Short-Lived Token Based Authentication section earlier in this document. If not, click **Add a new credential** and create a new credential using the storage account and refresh token given to you by Veritas.



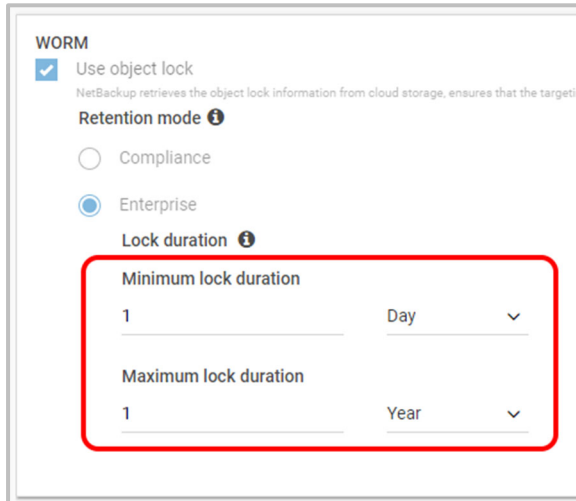
Note: You can create multiple disk volumes/buckets using the same credentials. There is no need to add multiple credentials for the same storage account.

Note: Refresh tokens are provided by the Veritas Alta Recovery Vault Provisioning Team.



11. In the WORM section is where you set the immutability time duration. During the Lock duration the image is locked. For more information regarding immutability, see the [Veritas Knowledge Base Article 100055803](#) for more information on Alta Recovery Vault and immutability.

Note: WORM and Enterprise mode are selected by default and cannot be changed.

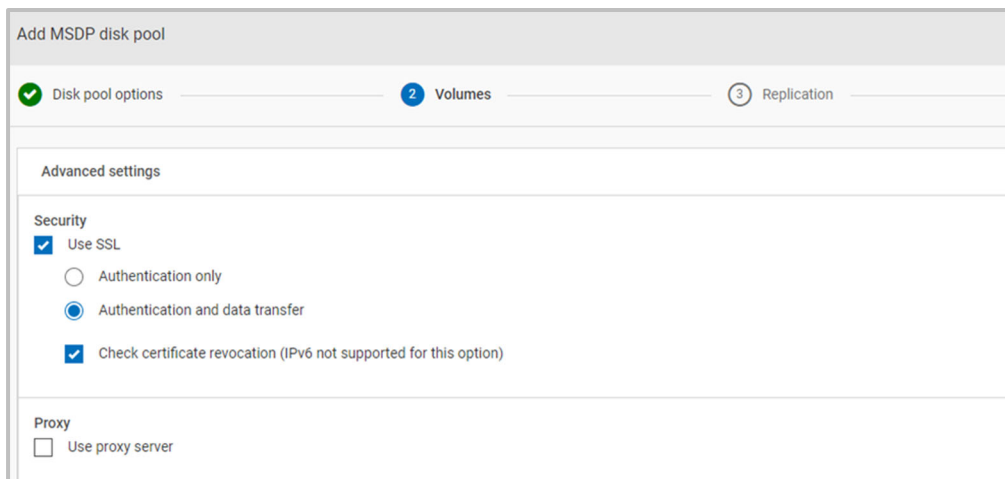


The screenshot shows the 'WORM' configuration section. It includes a checked checkbox for 'Use object lock'. Below it, the 'Retention mode' is set to 'Enterprise' (selected with a radio button). The 'Lock duration' section is highlighted with a red box and contains two fields: 'Minimum lock duration' set to '1 Day' and 'Maximum lock duration' set to '1 Year'.

12. In Advanced settings, enter the required Security or Proxy preferences.

Note: If you do not want to open port 80 externally, you will need to uncheck “Check certificate revocation”, For more information on check certificate revocation, see the following: https://en.wikipedia.org/wiki/Certificate_revocation_list#:~:text=In%20cryptography%2C%20a%20certificate%20revocation,should%20no%20longer%20be%20trusted%22.

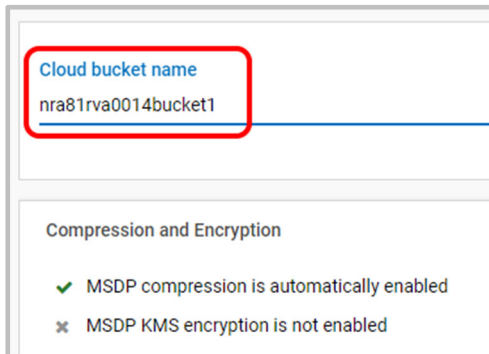
Note: A proxy server can be used if wanted.



The screenshot shows the 'Add MSDP disk pool' configuration interface. It has three tabs: 'Disk pool options' (selected), 'Volumes', and 'Replication'. Under 'Advanced settings', the 'Security' section has 'Use SSL' checked, 'Authentication and data transfer' selected, and 'Check certificate revocation (IPv6 not supported for this option)' checked. The 'Proxy' section has 'Use proxy server' unchecked.

13. Enter the cloud bucket name.

Note: This name is provided by the Veritas Alta Recovery Vault Provisioning Team. The one shown below is for reference only. After entering the cloud bucket name, click **Next**. (Not shown in the image.)

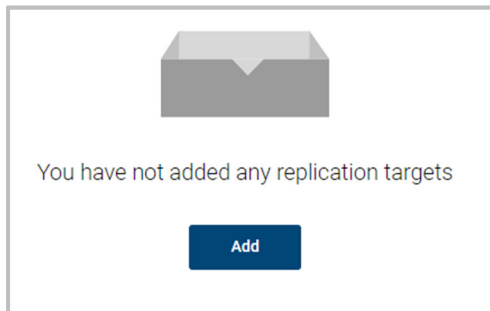


Cloud bucket name
nra81rva0014bucket1

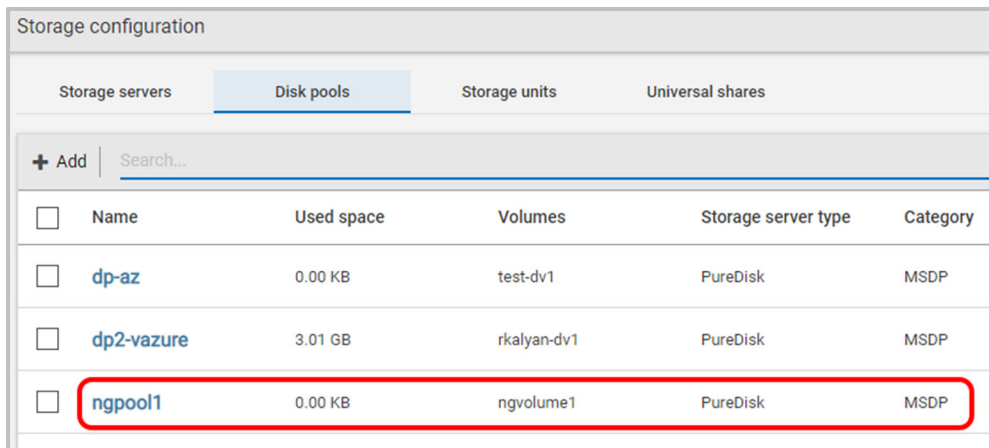
Compression and Encryption

- ✓ MSDP compression is automatically enabled
- ✗ MSDP KMS encryption is not enabled

14. If you would like to set up replication targets, they can be set up now. If none are needed, click **Next**. (Not shown in the image.)

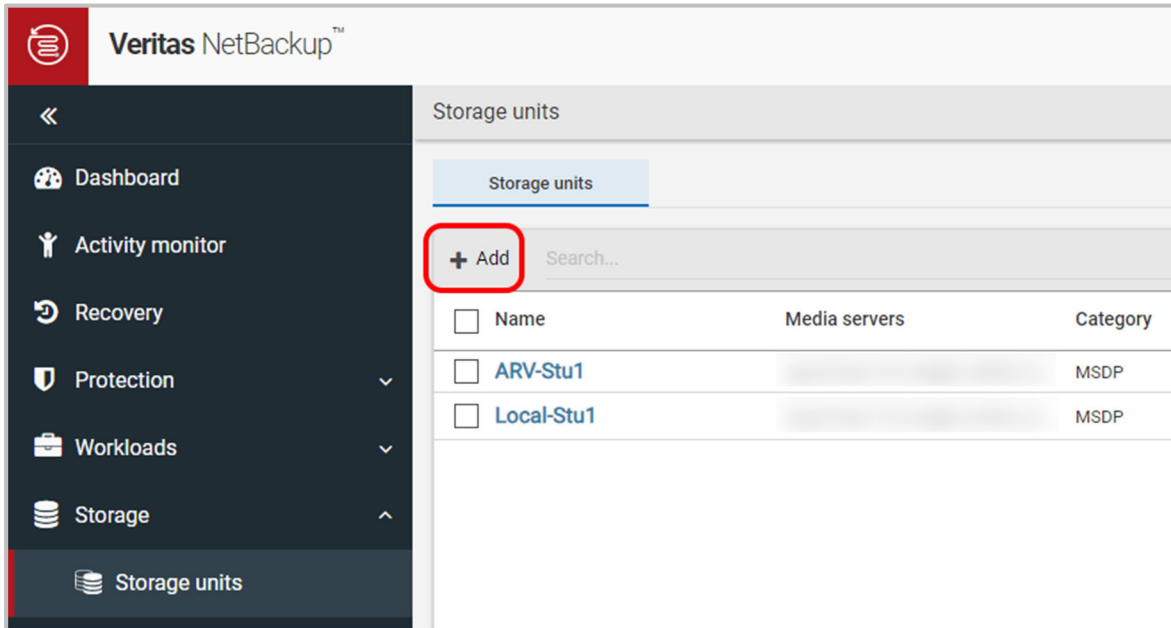


15. The next page is a summary page. If everything looks good, create the new disk pool. In this example, the new “ngpool1” has been created.



Storage configuration							
Storage servers		Disk pools		Storage units		Universal shares	
+ Add Search...							
<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category		
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP		
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP		
<input type="checkbox"/>	ngpool1	0.00 KB	ngvolume1	PureDisk	MSDP		

16. Next, add a storage unit so you can use your new Alta Recovery Vault storage. Under Storage > Storage Units, click **+ Add**.



17. Select **Media Server Deduplication Pool to local or cloud storage (MSDP, MSDP Cloud)** and click **Start**.

Add storage unit

Select the type of storage that you want to configure

Storage type *

Disk storage servers

Category *

Media Server Deduplication Pool to local or cloud storage (MSDP, MSDP Cloud)
Deduplicate backups to cloud, network, or locally attached storage server

AdvancedDisk
Backup to local media server storage, no deduplication

OpenStorage Technology (OST)
Backup to network attached storage devices using OST plugin

Cloud Connector
Backup to cloud object storage, no deduplication

BasicDisk

Cancel Start

18. Provide a new MSDP storage unit name and select the desired **Maximum concurrent jobs** and **Maximum fragment size**. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

1 Basic properties

Name *

ngstorage1

Maximum concurrent jobs

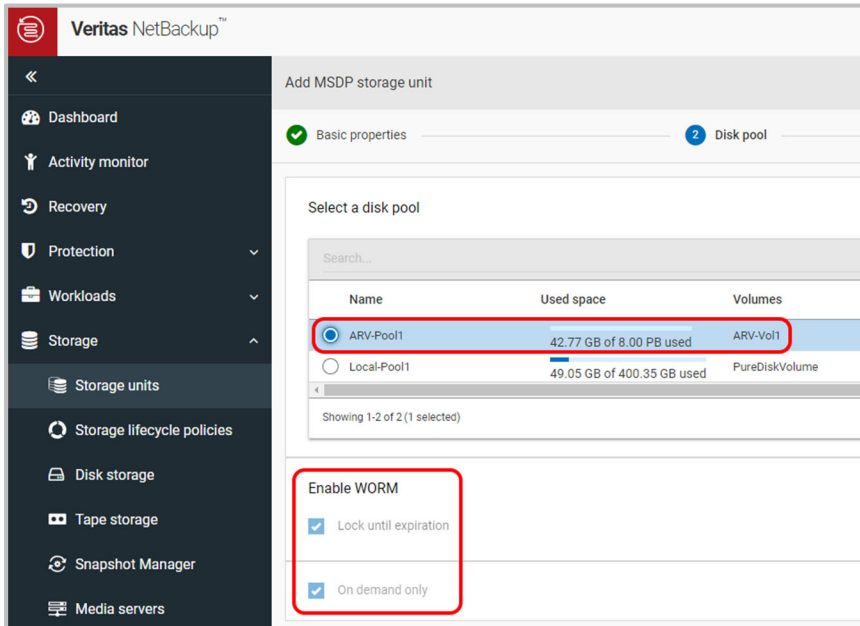
1

Maximum fragment size

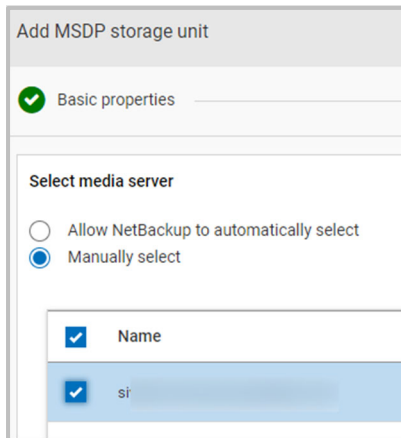
51200 MB

19. Select the Alta Recovery Vault volume created earlier. Click **Next** to continue. (Not shown in the image.)

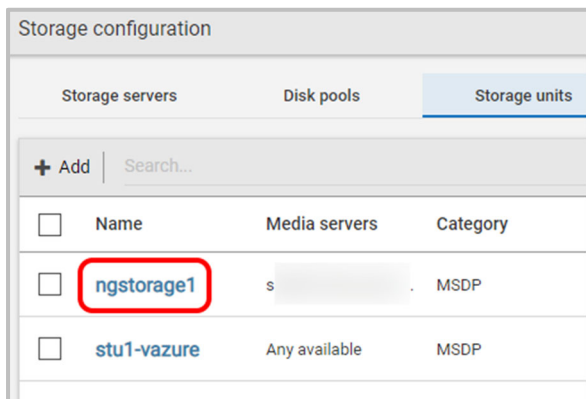
Note: Enable WORM will be checked by default and cannot be un-checked.



20. Select the media server you wish to use. Click **Next** to continue. (Not shown in the image.)



21. Here you can see your new “ngstorage1” storage unit successfully created.



The new Alta Recovery Vault storage can now be used for backups.

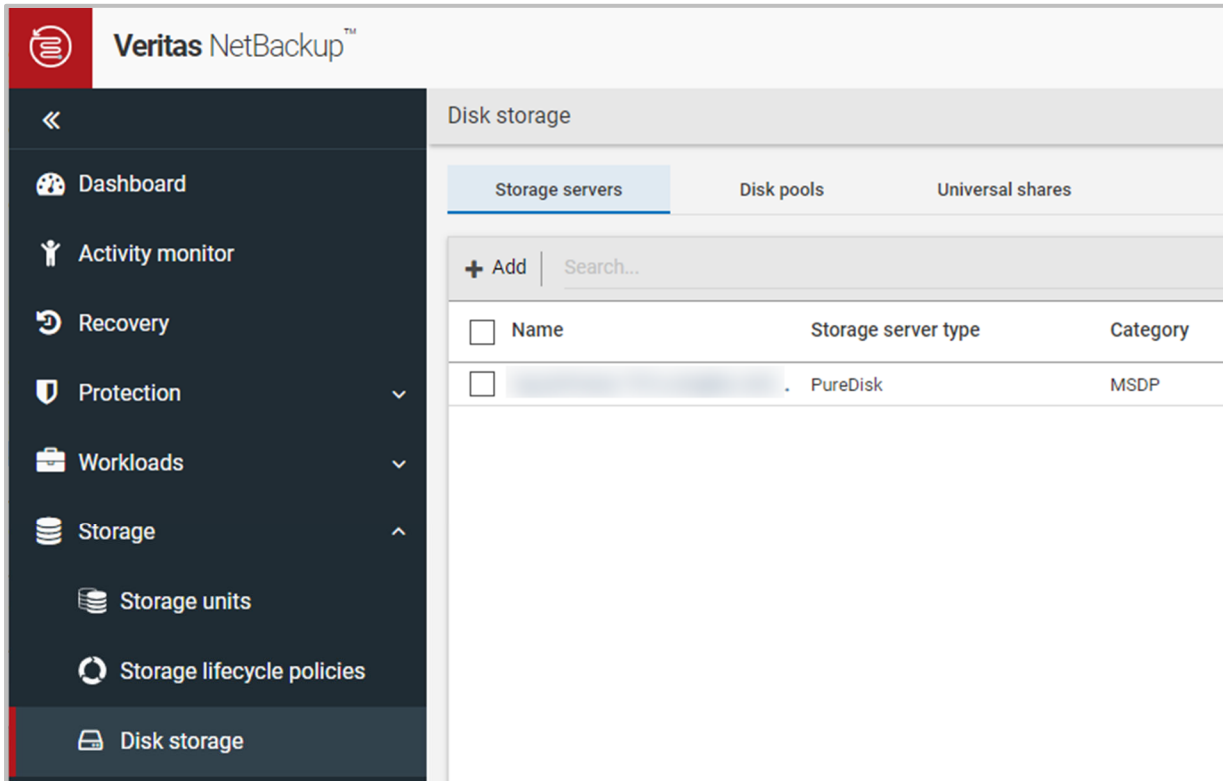
NetBackup 10.3

Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

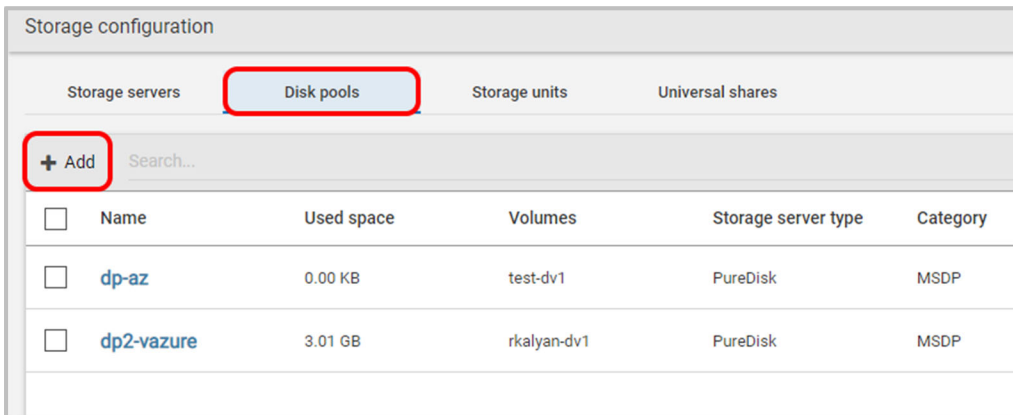
1. Ensure your storage server has been created.
 - a. Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*:
https://www.veritas.com/content/support/en_US/doc/25074086-159245004-0/v24332600-159245004

2. From within your NetBackup primary server web UI, navigate to **Storage > Disk Storage**

You should see your storage server(s) listed.



3. Click the **Disk pools** tab and click **+ Add**.



4. First, enter the details for disk pool options.

- p. Select the storage server name where this disk pool will reside. In this example, the choice is the storage server seen in step 1 of this procedure.
- q. Provide a name for the disk pool. This example uses “ngpool1”.
- r. If you choose, provide a description for the pool.
- s. Select **Limit I/O streams** if desired. This option could help limit disk I/O contention.
- t. Click **Next** at the bottom of the page to continue. (Not seen in the image.)

The screenshot shows the 'Add disk pool' configuration window with the 'Disk pool options' step selected. The 'Storage server name' is 'siv'. The 'Disk pool name' is 'ngpool1'. The 'Description' field is empty. The 'Limit I/O streams' checkbox is unchecked. Below the main form, there is a note: 'The following options do not apply if you select a cloud MSDP disk volume in the next step.' Under this note, there are two water mark settings: 'High water mark' at 98% and 'Low water mark' at 80%.

5. Next, you're brought to the Volumes page. In the example you can see that there are already three volumes created, but you want to add your new Alta Recovery Vault volume. Click **Volume > Select volume**.

The screenshot shows the 'Add MSDP disk pool' configuration window with the 'Volumes' step selected. A dropdown menu labeled 'Volume' is open, showing 'Select volume'. Below the dropdown is a search bar and a table of existing volumes.

Name	Available space	Total size	Encryption
PureDiskVolume	753.88 GB	885.38 GB	No
test-dv1	8.00 PB	8.00 PB	No
rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

6. Click **Add volume** to begin the process.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Select volume

Add volume

	Name	Available space	Total size	Encryption
<input type="radio"/>	PureDiskVolume	753.88 GB	885.38 GB	No
<input type="radio"/>	test-dv1	8.00 PB	8.00 PB	No
<input type="radio"/>	rkalyan-dv1	8.00 PB	8.00 PB	No

Showing 1-3 of 3

7. Provide a name for the new volume and click **Cloud storage provider**.

Add MSDP disk pool

✓ Disk pool options 2 Volumes 3 Replication

Volume

Add volume

Volume name *
ngvolume1

Cloud cache properties

⚠ A request value lower than 1,017 GB may affect performance. Verify that the required space to create this pool is available.

Available disk space: 146.57 GB

Request cloud cache disk space *
73 GB
Enter a value between 4 GB and 117 GB.

Cloud storage provider *
Select cloud storage provider

Storage API type
-

8. Search for “Veritas Alta Recovery Vault Amazon” and the following Cloud storage providers appear. For this example, you will choose **Veritas Alta Recovery Vault Amazon**.

Select cloud storage provider		
Search...		
Cloud storage provider	Description	Storage API type
<input type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input checked="" type="radio"/> Veritas Alta Recovery Vault Amazon	Veritas Alta Recovery Vault Amazon Storage Service	S3
<input type="radio"/> Veritas Alta Recovery Vault Amazon Government	Veritas Alta Recovery Vault Amazon Storage Service	S3

9. After you select the cloud storage provider, you’re taken back to the Add MSDP disk pool screen. Select **GLACIER_IR** as the **Storage class**.

The image shows two side-by-side screenshots of the 'Add MSDP disk pool' configuration screen. Both screenshots show the 'Disk pool options' and 'Volumes' tabs. The 'Volume' section is expanded, showing 'Volume name *' set to 'ngvolume1'. The 'Cloud storage provider *' is set to 'Veritas Alta Recovery Vault Amazon' and the 'Storage API type' is 'Amazon S3'. In the left screenshot, the 'Storage class' dropdown menu is open, and 'GLACIER_IR' is selected and highlighted with a red box. In the right screenshot, the 'Storage class' dropdown menu is open, and 'Glacier Deep Archive' is selected and highlighted with a red box.

If you’ve purchased Archive tier, click **Storage class**, and select **Glacier Deep Archive**.

Note: For archive tier, ensure your cloud vendor provides archive support in the desired region. If archive tier is not supported in the region, this feature will not function correctly.

10. Next, enter the Region, Access Key ID, and Secret Access Key.

Note: These are provided by the Veritas Alta Recovery Vault Provisioning Team.

Region *

	Service host	Region name	Region identifier
<input type="radio"/>	s3.dualstack.us-east-1.amazonaws.com	US East (N. Virginia)	us-east-1
<input type="radio"/>	s3.dualstack.us-west-1.amazonaws.com	US West (Northern California)	us-west-1
<input type="radio"/>	s3.dualstack.us-west-2.amazonaws.com	US West (Oregon)	us-west-2
<input type="radio"/>	s3.dualstack.eu-west-1.amazonaws.com	EU (Ireland)	eu-west-1

Access details for the account

Access key ID *

Enter access key ID

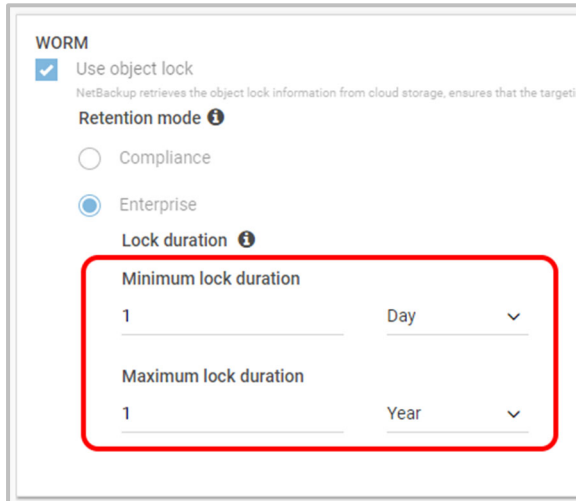
Secret access key *

Enter secret access key



11. In the WORM section is where you set the immutability time duration. During the Lock duration the image is locked. For more information regarding immutability, see the [Veritas Knowledge Base Article 100055803](https://www.veritas.com/learn/whitepapers/100055803) for more information on Alta Recovery Vault and immutability.

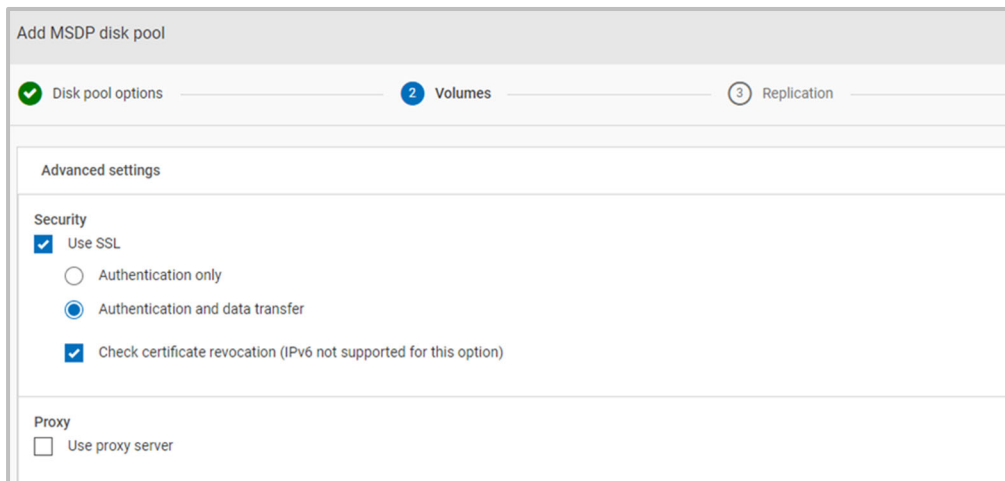
Note: WORM and Enterprise mode are selected by default and cannot be changed.



The screenshot shows the 'WORM' configuration section. It includes a checked checkbox for 'Use object lock'. Below it, the 'Retention mode' is set to 'Enterprise' (selected with a radio button). The 'Lock duration' section is highlighted with a red box and contains two fields: 'Minimum lock duration' set to '1' with a unit dropdown set to 'Day', and 'Maximum lock duration' set to '1' with a unit dropdown set to 'Year'.

12. In Advanced settings, enter the required Security or Proxy preferences.

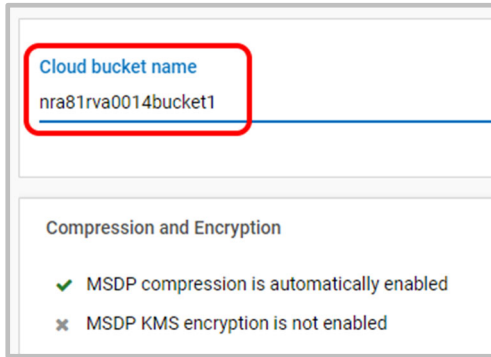
Note: If you do not want to open port 80 externally, you will need to uncheck “Check certificate revocation”, For more information on check certificate revocation, see the following: https://en.wikipedia.org/wiki/Certificate_revocation_list#:~:text=In%20cryptography%2C%20a%20certifi%20revocation,should%20no%20longer%20be%20trusted%22.



The screenshot shows the 'Add MSDP disk pool' configuration interface. It has three tabs: 'Disk pool options' (checked), 'Volumes' (selected), and 'Replication'. Under the 'Advanced settings' section, there are two sub-sections: 'Security' and 'Proxy'. In the 'Security' section, 'Use SSL' is checked, 'Authentication and data transfer' is selected, and 'Check certificate revocation (IPv6 not supported for this option)' is checked. In the 'Proxy' section, 'Use proxy server' is unchecked.

13. Enter the cloud bucket name.

Note: This name is provided by the Veritas Alta Recovery Vault Provisioning Team. The one shown below is for reference only. After entering the cloud bucket name, click **Next**. (Not shown in the image).

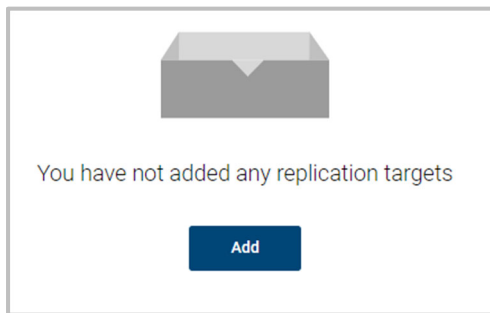


Cloud bucket name
nra81rva0014bucket1

Compression and Encryption

- ✓ MSDP compression is automatically enabled
- ✗ MSDP KMS encryption is not enabled

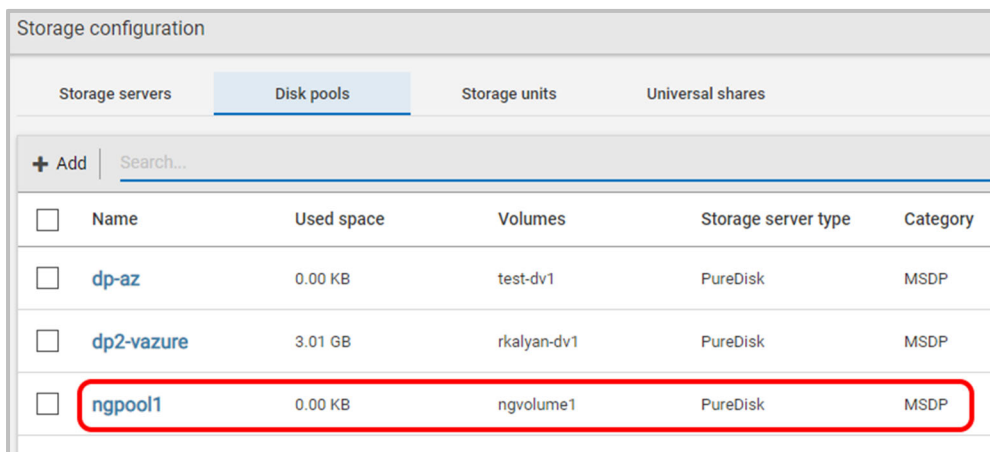
14. If you would like to set up replication targets, they can be set up now. If none are needed, click **Next**. (Not shown in the image.)



You have not added any replication targets

Add

15. The next page is a summary page. If everything looks good, create the new disk pool. In this example, the new “ngpool1” has been created.



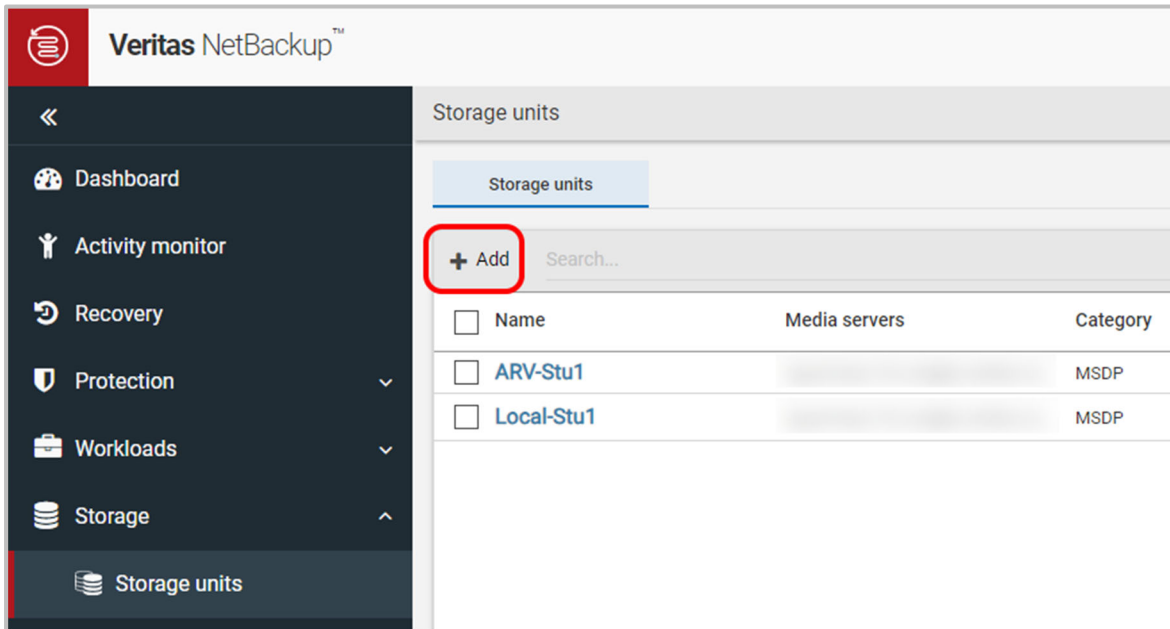
Storage configuration

Storage servers | **Disk pools** | Storage units | Universal shares

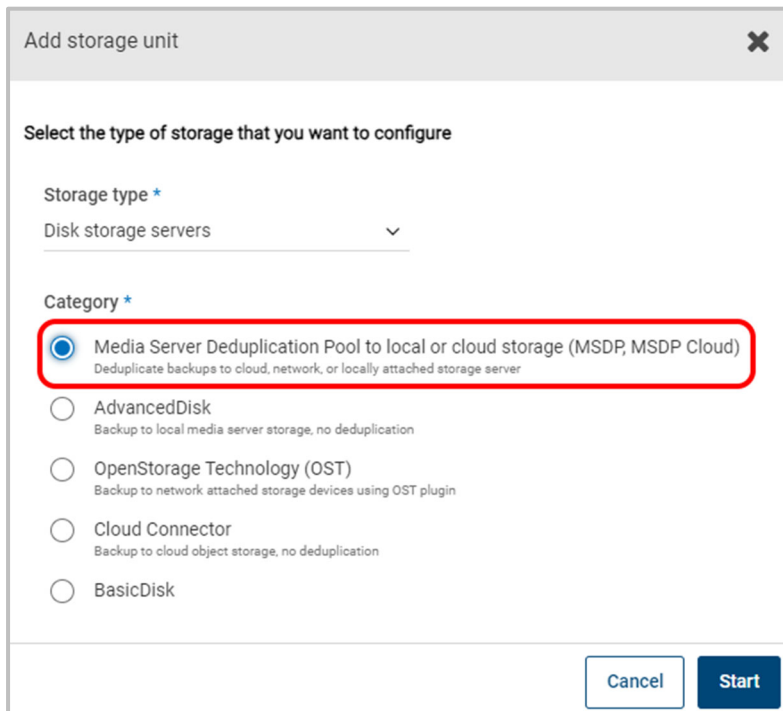
+ Add | Search...

<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP
<input type="checkbox"/>	ngpool1	0.00 KB	ngvolume1	PureDisk	MSDP

16. Next, add a storage unit so you can use your new Alta Recovery Vault storage. Under Storage > Storage Units, click **+ Add**.



17. Select **Media Server Deduplication Pool to local or cloud storage (MSDP, MSDP Cloud)** and click **Start**.



18. Provide a new MSDP storage unit name and select the desired **Maximum concurrent jobs** and **Maximum fragment size**. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

1 Basic properties

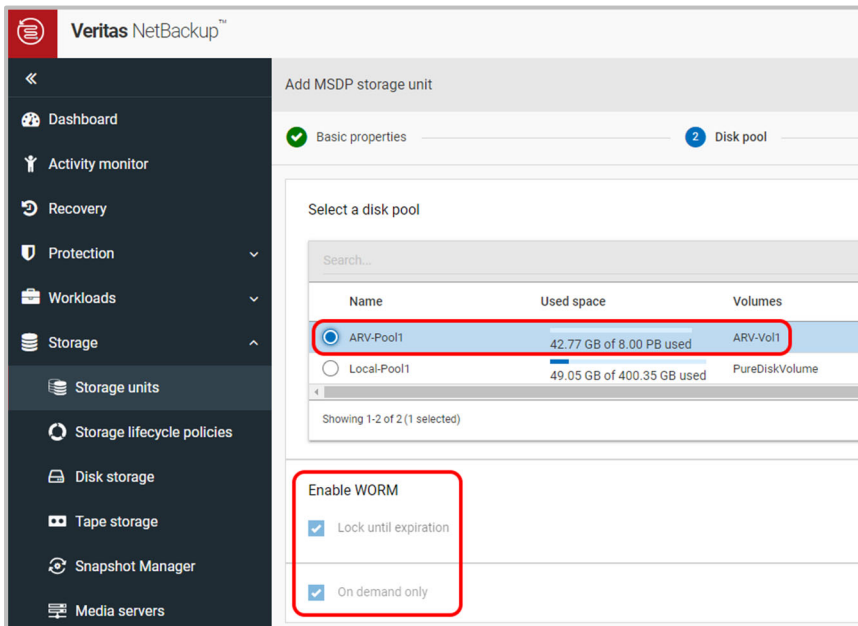
Name *
ngstorage1

Maximum concurrent jobs
1

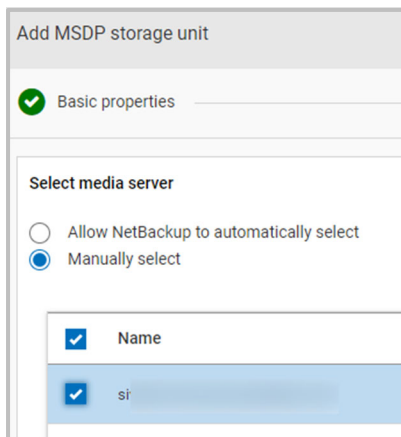
Maximum fragment size
51200 MB

19. Select the Alta Recovery Vault volume created earlier. Click **Next** to continue. (Not shown in the image.)

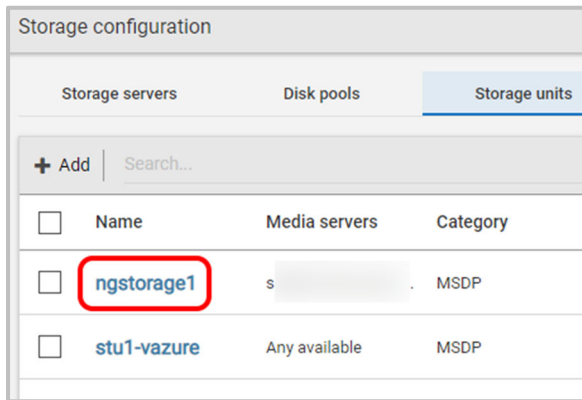
Note: Enable WORM will be checked by default and cannot be un-checked.



20. Select the media server you wish to use. Click **Next** to continue. (Not shown in the image.)



21. Here you can see your new “ngstorage1” storage unit successfully created.



22. The new Alta Recovery Vault storage can now be used for backups.

NetBackup 10.2 or Earlier

Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

1. Ensure your storage server has been created.
 - a. Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*: https://www.veritas.com/content/support/en_US/doc/25074086-149019166-0/v24332600-149019166
2. Log into the console of your media server that is your MSDP storage server you created in step 1.
3. Navigate to `/usr/opensv/pdde/pdcr/bin/` on the command line of your media server.

Set environment variables for AWS

- a. AWS:
 - i. `# export MSDPC_ACCESS_KEY=xxxx (Your Access Key)`
 - ii. `# export MSDPC_SECRET_KEY=yyyyyyyyyyyyyy (Your Secret Key)`
 - iii. `# export MSDPC_REGION=<selectedregion>`
 - iv. `# export MSDPC_PROVIDER=vamazon`
- b. AWS Example
 - i. `# export MSDPC_ACCESS_KEY=<givetoyoubyVeritas> (Your Access Key)`
 - ii. `# export MSDPC_SECRET_KEY=<giventoyoubyVeritas> (Your Secret Key)`
 - iii. `# export MSDPC_REGION=<your region like us-east-1>`
 - iv. `# export MSDPC_PROVIDER=vamazon`

Governance mode (also known as enterprise mode):

Users require special permissions to disable the retention lock and then delete the image. Only the cloud administrator user can disable the retention lock and then delete the image if required.

4. Run the following command with your immutability inputs (non-archive)

- a. `./msdpclutil create -b containernamegivenbyveritas -v volumename --mode GOVERNANCE --min time --max time -l expirationdate --storageclass GLACIER_IR`
- b. **Example** `./msdpclutil create -b jzh-worm-bucket07 -v jzh-b01-v02 --mode GOVERNANCE --min 1D --max 1Y -l 2024-10-24 --storageclass GLACIER_IR`

5. Run the following command with your immutability inputs (archive)

- a. `./msdpclutil create -b containernamegivenbyveritas -v volumename --mode GOVERNANCE --min time --max time -l expirationdate`
- b. **Example** `./msdpclutil create -b jzh-worm-bucket07 -v jzh-b01-v02 --mode GOVERNANCE --min 1D --max 1Y -l 2024-10-24`

Note: When running `msdpclutil` for AWS **without** archive, the storage class must be set. Choose `GLACIER_IR` when setting up non-archive AWS storage.

Note: When running `msdpclutil` for AWS **with** archive, do **NOT** include the storage class.

6. A list of the immutable containers (buckets) can be seen with the following command:

- a. `./msdpclutil list -b nameofcontainer`
- b. **Example** `./msdpclutil list -b jzh-worm-bucket07`

7. Now that the immutable bucket has been configured on the command line, the immutable disk pool can be created.

8. Go to the NetBackup web UI and navigate to **Storage > Storage configuration**.

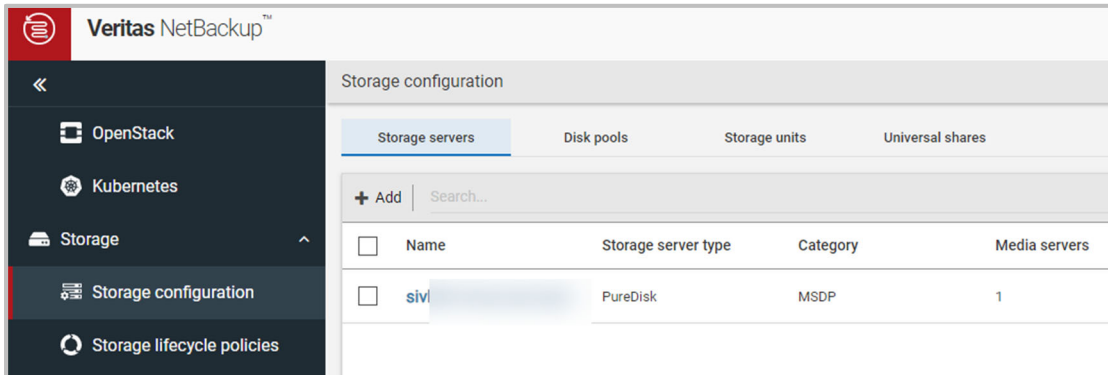
After the volume and volume container have been created on your media server's CLI, it's time to connect to the new storage bucket in NetBackup through the Web UI.

Note that this document assumes you already have an MSDP storage server created. For more information on how to add a storage server, see the *NetBackup Deduplication Guide*:

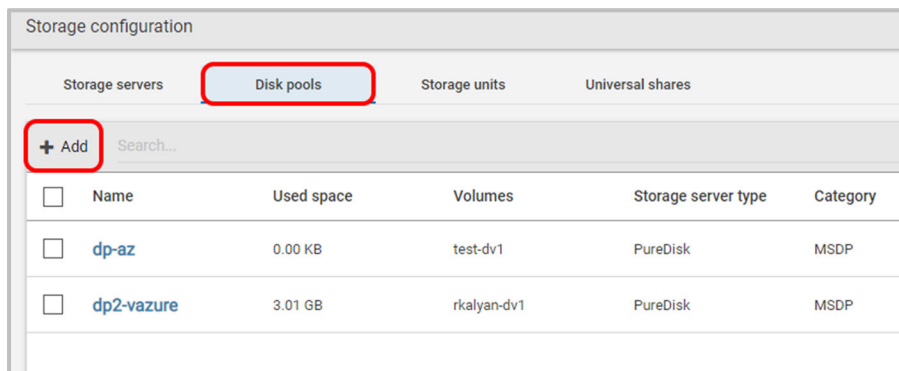
https://www.veritas.com/content/support/en_US/doc/25074086-149019166-0/v24332600-149019166

9. From within your NetBackup primary server web UI, navigate to **Storage > Storage configuration**.

You should see your storage servers listed.



10. Click the **Disk pools** tab and click **+ Add**.



11. Enter the details for disk pool options.

- f. Select the storage server name where this disk pool will reside. In this example, the choice is the storage server seen in step 1 of this procedure.
- g. Provide a name for the disk pool. This example uses “ngpool1”.
- h. If you choose, provide a description for the pool.
- i. Select **Limit I/O streams** if desired. This option could help limit disk I/O contention.
- j. Click **Next** at the bottom of the page to continue. (Not seen in the image.)

The screenshot shows a configuration window titled "Add disk pool" with a close button (X) in the top right corner. The window is divided into four steps: 1. Disk pool options (active), 2. Volumes, 3. Replication, and 4. Review.

Storage server name *
siv

Features
Accelerator, A.I.R., Instant access, WORM capable

Change

Disk pool name *
ngpool1

Description
Enter description

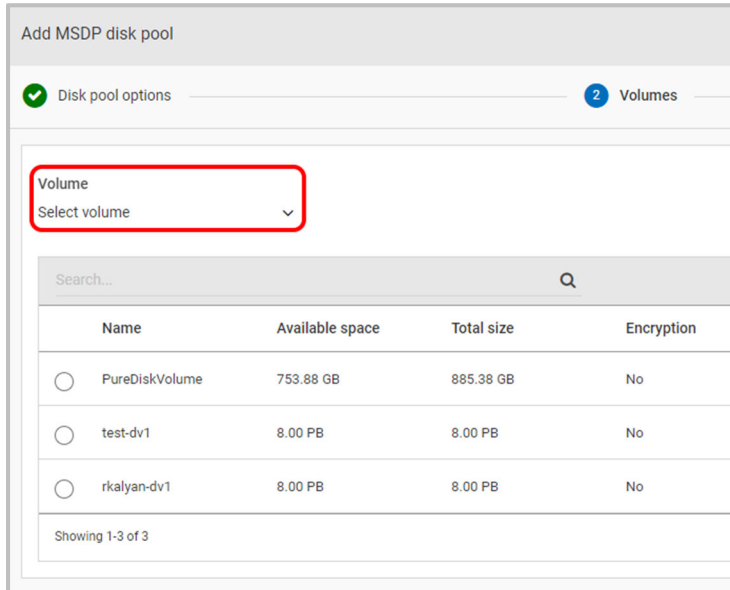
Limit I/O streams
Concurrent read and write jobs affect disk performance. Limit I/O streams to prevent disk overload.

The following options do not apply if you select a cloud MSDP disk volume in the next step.

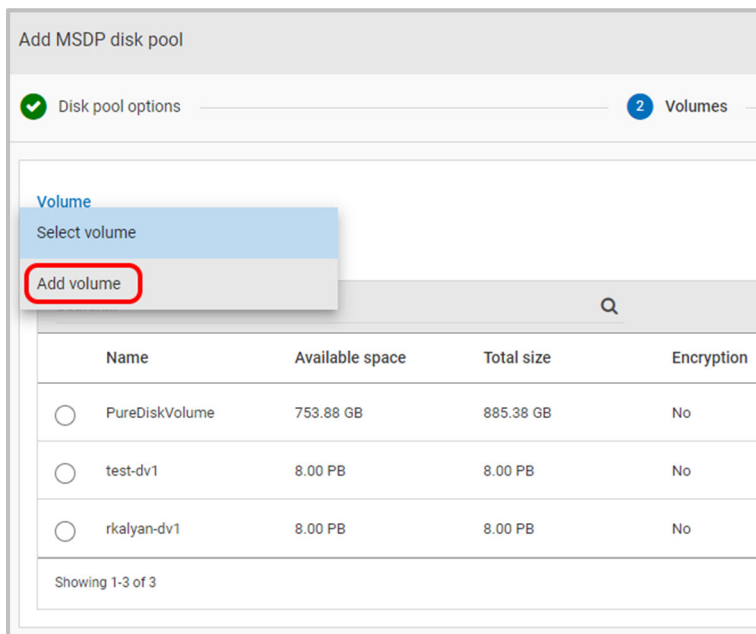
High water mark
98 %

Low water mark
80 %

12. Next, you're brought to the Volumes page. In the example you can see that there are already three volumes created, but you want to add your new Alta Recovery Vault volume. Click **Volume > Select volume**.



13. Click **Add volume** to begin the process.



14. Provide a name for the new volume and click **Cloud storage provider**.

Note: Name the volume the same as you did using the msdpclutil command.

Add MSDP disk pool

✓ Disk pool options 2 Volumes

Volume

Add volume ▾

Volume name *
ngvolume1 ⓘ

Cloud storage provider *
Select cloud storage provider

Storage API type
-

15. Search for “Veritas Alta Recovery Vault Amazon” and the following Cloud storage providers appear. For this example, you will choose **Veritas Alta Recovery Vault Amazon**.

Cloud storage provider	Description	Storage API type
<input type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input checked="" type="radio"/> Veritas Alta Recovery Vault Amazon	Veritas Alta Recovery Vault Amazon Storage Service	S3
<input type="radio"/> Veritas Alta Recovery Vault Amazon Government	Veritas Alta Recovery Vault Amazon Storage Service	S3

16. After you select the cloud storage provider, you're taken back to the Add MSDP disk pool screen. Select **GLACIER_IR** as the **Storage class**.

The image shows two side-by-side screenshots of the 'Add MSDP disk pool' configuration interface. Both screenshots show the 'Volumes' step (indicated by a '2' in a blue circle) and the 'Storage class' dropdown menu. In the left screenshot, the 'Storage class' is set to 'GLACIER_IR'. In the right screenshot, the 'Storage class' is set to 'Glacier Deep Archive'. Other fields visible include 'Volume name' (ngvolume1), 'Cloud storage provider' (Veritas Alta Recovery Vault Amazon), and 'Storage API type' (Amazon S3).

Note: For archive tier, ensure your cloud vendor provides archive support in the desired region. If archive tier is not supported in the region, this feature will not function correctly.

17. Next, enter the Region, Access Key ID, and Secret Access Key.

Note: These are provided by the Veritas Alta Recovery Vault Provisioning Team.

The image shows a screenshot of the 'Region' selection screen. The 'Region' dropdown is expanded, showing a list of regions with their service hosts, region names, and region identifiers. The 'us-east-1' region is highlighted with a red box. Below the list, the 'Access details for the account' section is also highlighted with a red box, showing fields for 'Access key ID' and 'Secret access key'.

Service host	Region name	Region identifier
<input type="radio"/> s3.dualstack.us-east-1.amazonaws.com	US East (N. Virginia)	us-east-1
<input type="radio"/> s3.dualstack.us-west-1.amazonaws.com	US West (Northern California)	us-west-1
<input type="radio"/> s3.dualstack.us-west-2.amazonaws.com	US West (Oregon)	us-west-2
<input type="radio"/> s3.dualstack.eu-west-1.amazonaws.com	EU (Ireland)	eu-west-1

Access details for the account

Access key ID *

Enter access key ID

Secret access key *

Enter secret access key

18. In Advanced settings, enter the required Security, Proxy, or WORM preferences.

Note: If you do not want to open port 80 externally, you will need to uncheck “Check certificate revocation”, For more information on check certificate revocation, see the following:

https://en.wikipedia.org/wiki/Certificate_revocation_list#:~:text=In%20cryptography%2C%20a%20certificate%20revocation,should%20no%20longer%20be%20trusted%22.

Note: Ensure to check the **WORM > Use object lock** checkbox.

Note: If you have not completed the CLI steps earlier in this section, the WebUI will give you an error when trying to connect to your Alta Recovery Vault storage.

The screenshot shows the 'Add MSDP disk pool' configuration page. At the top, there are three progress indicators: '1 Disk pool options' (checked), '2 Volumes' (active), and '3 Replication'. Below this is the 'Advanced settings' section, which is divided into three sub-sections: 'Security', 'Proxy', and 'WORM'. In the 'Security' section, 'Use SSL' is checked, 'Authentication and data transfer' is selected with a radio button, and 'Check certificate revocation (IPv6 not supported for this option)' is checked. In the 'Proxy' section, 'Use proxy server' is unchecked. In the 'WORM' section, 'Use object lock' is checked and highlighted with a red box. Below this checkbox, there is a note: 'NetBackup retrieves the Object Lock information from Cloud storage. Ensure that the targeting bucket is created, and the Object Lock mode is set. Refer to the NetBackup Deduplication Guide for more details.'

19. Enter the cloud bucket name.

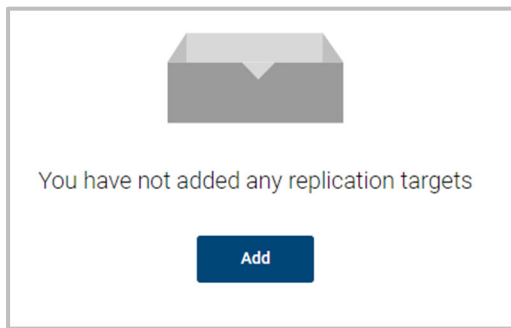
Note: This name is provided by the Veritas Alta Recovery Vault Provisioning Team. The one shown below is for reference only. After entering the cloud bucket name, click **Next**. (Not shown in the image).

Cloud bucket name
nra81rva0014bucket1

Compression and Encryption

- ✓ MSDP compression is automatically enabled
- ✗ MSDP KMS encryption is not enabled

20. If you would like to set up replication targets, they can be set up now. If none are needed, click **Next**. (Not shown in the image.)



21. The next page is a summary page. If everything looks good, create the new disk pool. In this example, the new “ngpool1” has been created.

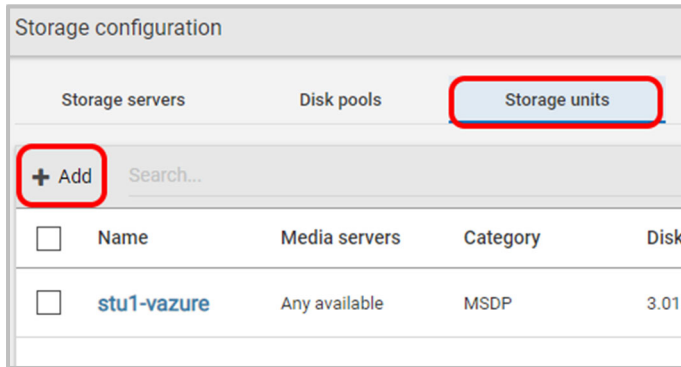
Storage configuration

Storage servers | **Disk pools** | Storage units | Universal shares

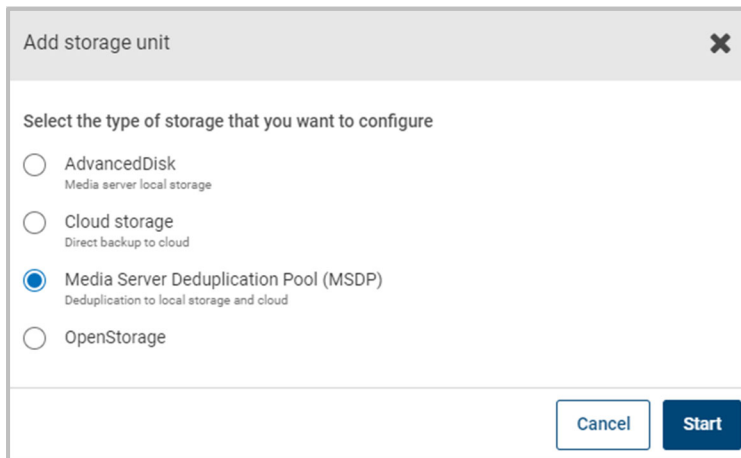
+ Add | Search...

<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category
<input type="checkbox"/>	dp-az	0.00 KB	test-dv1	PureDisk	MSDP
<input type="checkbox"/>	dp2-vazure	3.01 GB	rkalyan-dv1	PureDisk	MSDP
<input type="checkbox"/>	ngpool1	0.00 KB	ngvolume1	PureDisk	MSDP

22. Next, add a storage unit so you can use your new Alta Recovery Vault storage. Click the **Storage units** tab and click **+ Add**.



23. Select **Media Server Deduplication Pool (MSDP)** and click **Start**.



24. Provide a new MSDP storage unit name and select the desired **Maximum concurrent jobs** and **Maximum fragment size**. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

1 Basic properties

Name *
ngstorage1

Maximum concurrent jobs
1

Maximum fragment size
51200 MB

25. Select the Alta Recovery Vault volume created earlier. Click **Next** to continue. (Not shown in the image.)

Add MSDP storage unit

Basic properties 2 Disk pool

Select a disk pool

Search...

Name	Used space	Volumes	Storage type	Storage server
<input type="radio"/> dp-az	0.00 KB of 8.00 PB used	test-dv1	PureDisk	si
<input type="radio"/> dp2-vazure	3.01 GB of 8.00 PB used	rkalyan-dv1	PureDisk	si
<input checked="" type="radio"/> ngpool1	0.00 KB of 8.00 PB used	ngvolume1	PureDisk	si

Showing 1-3 of 3 (1 selected)

26. Select the media server you wish to use. Click **Next** to continue. (Not shown in the image.)

The screenshot shows a configuration window titled "Add MSDP storage unit". At the top, there is a section for "Basic properties" with a green checkmark. Below this is the "Select media server" section, where the radio button for "Manually select" is selected. A list of media servers is displayed below, with "Name" and "si" selected. The "si" entry is highlighted in blue.

27. Here you can see your new “ngstorage1” storage unit successfully created.

The screenshot shows the "Storage configuration" window with the "Storage units" tab selected. The table below lists the storage units:

<input type="checkbox"/>	Name	Media servers	Category
<input type="checkbox"/>	ngstorage1	s	MSDP
<input type="checkbox"/>	stu1-vazure	Any available	MSDP

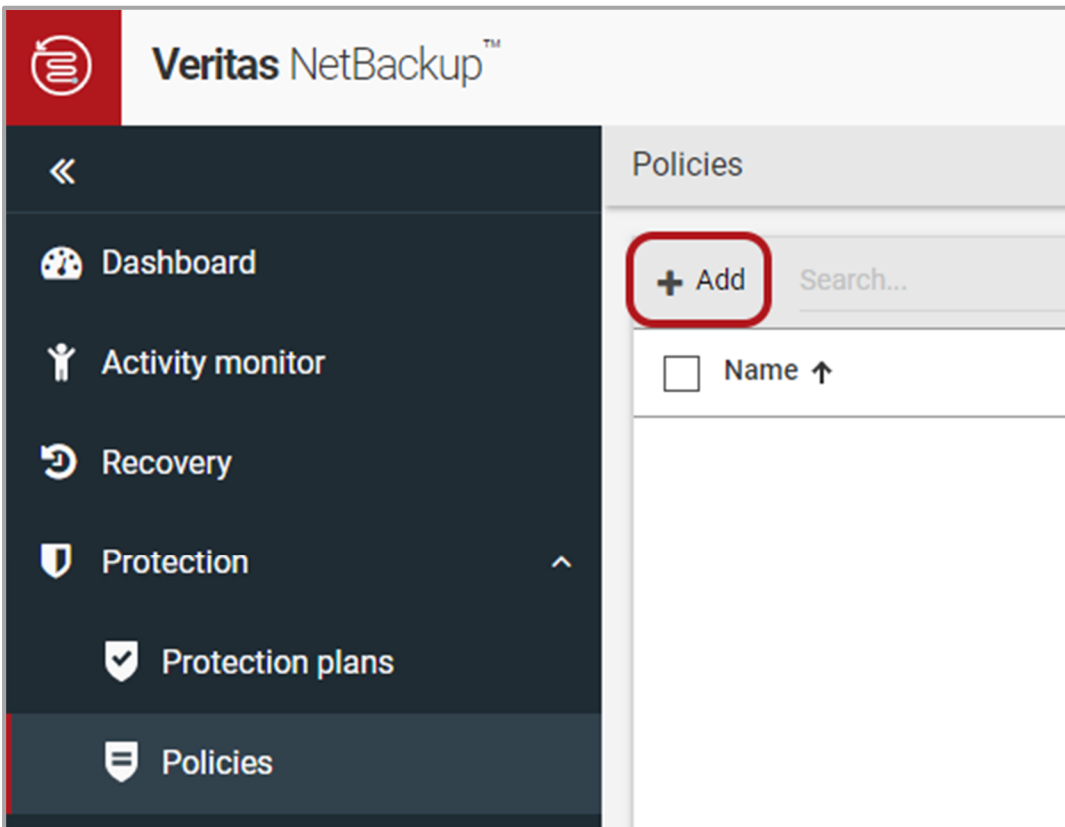
28. The new Alta Recovery Vault storage can now be used for backups.

Creating an Alta Recovery Vault Backup Policy

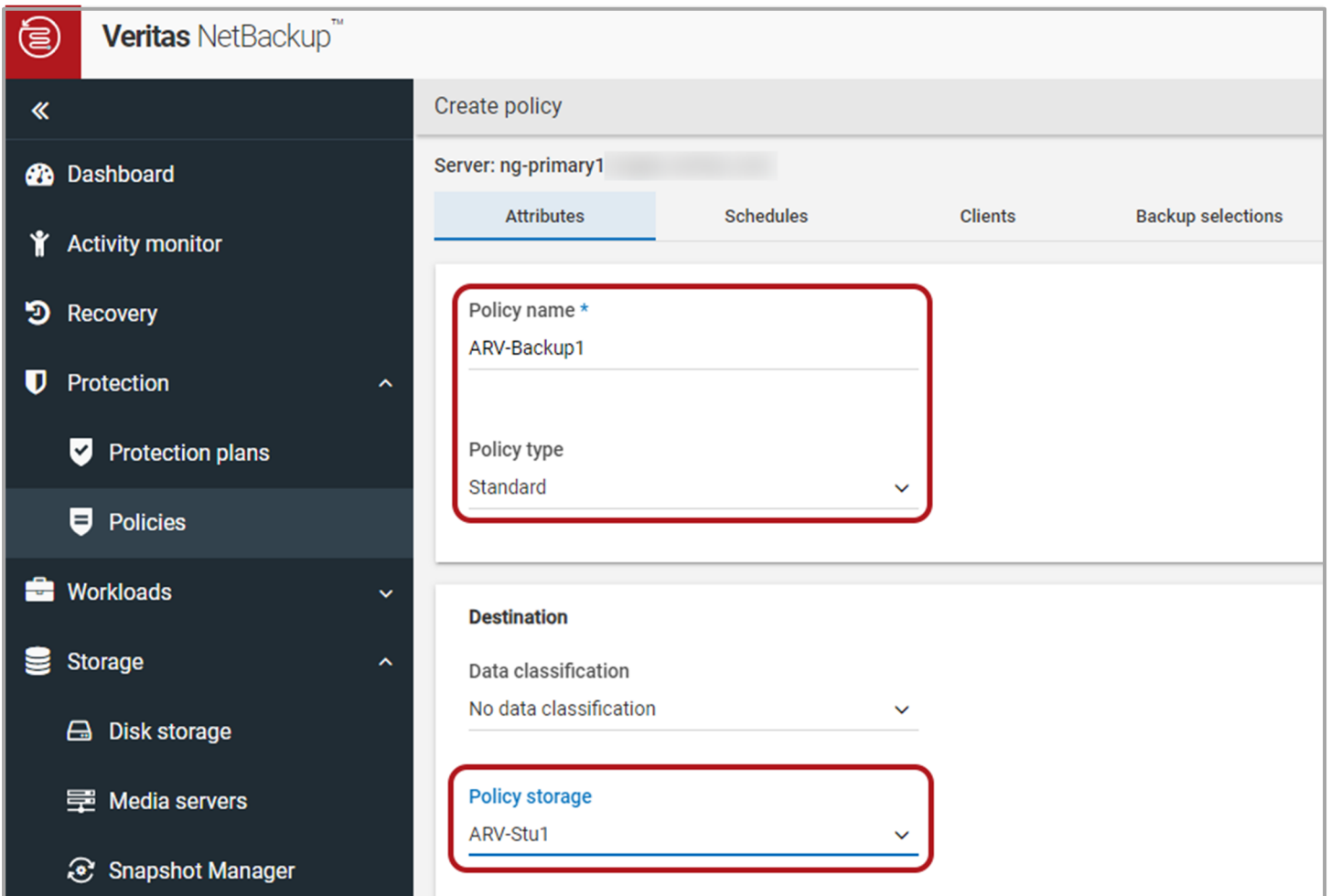
Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

Once the new storage unit(s) have been created it's time to create a backup policy using the Alta Recovery Vault storage.

1. Navigate to Protection > Policies and click on the +Add button.



2. There are many options for Attributes for your backup that can be selected to customize the backup to your needs. For this example, you want to be sure to choose the storage unit created with Alta Recovery Vault.



3. The next step is to add a schedule to the policy. Name your schedule and select from the attributes listed.

Note: The backup policy retention must be less than the WORM max retention period otherwise the policy creation will fail.

Add schedule

Attributes Start window Exclude dates

Name *
ARV-Sched1 ⓘ

Type of backup *
Full backup ▾

Synthetic backup
 Accelerator forced rescan

Destination

Multiple copies

Override policy storage selection
ARV-Stu1 ▾

Override policy volume pool
NetBackup ▾

Schedule type

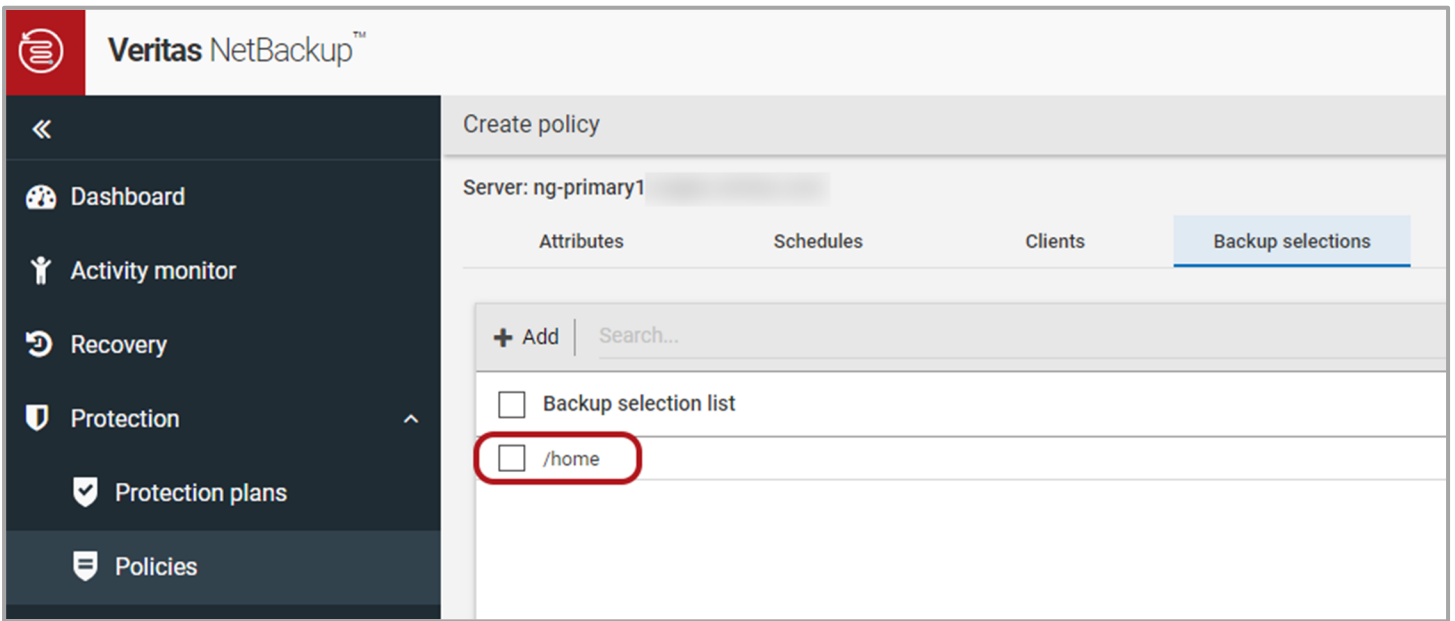
Calendar
 Retries allowed after the run day

Frequency
1 week

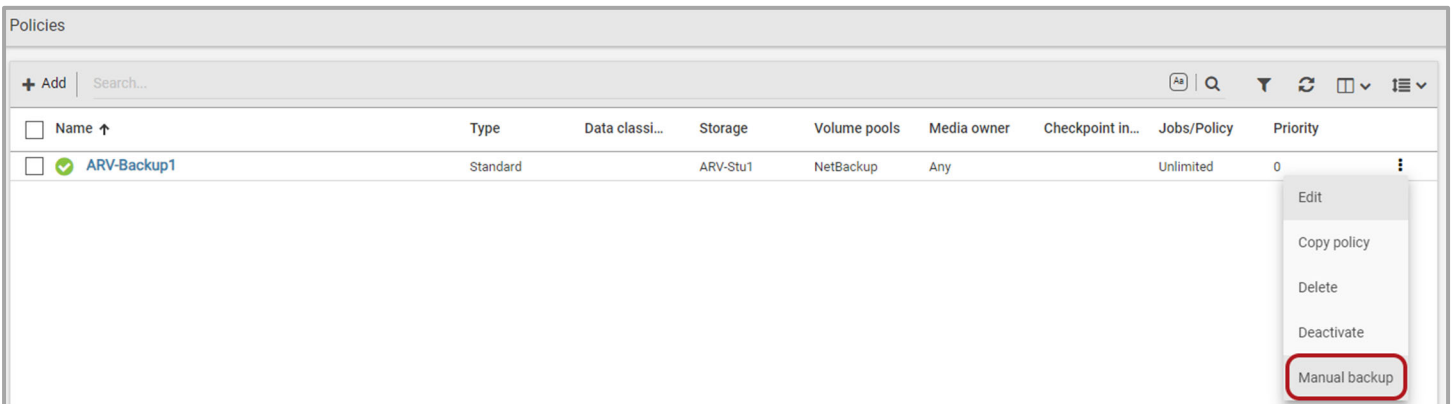
Retention *
2 weeks (Retention Level 1)

Media multiplexing
1

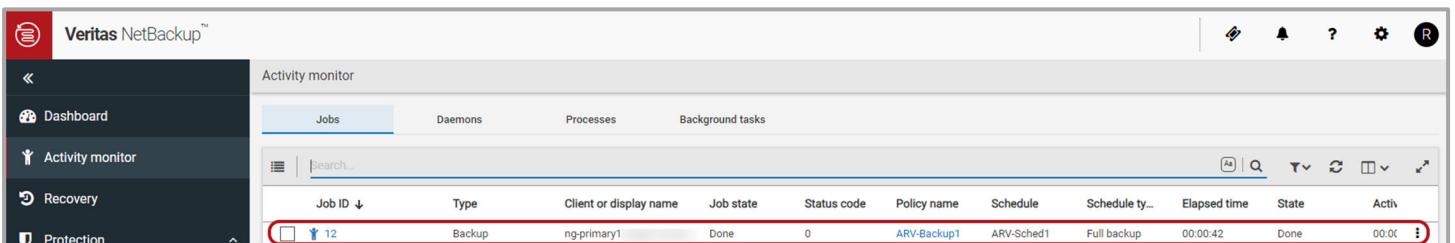
4. Select the start window and any exceptions you'd like to create.



7. Once the policy has been created you can wait for the start time for the backup to initiate. In this example a manual backup is started.



8. Checking the activity monitor will show you the progress state of your new Alta Recovery Vault backup.

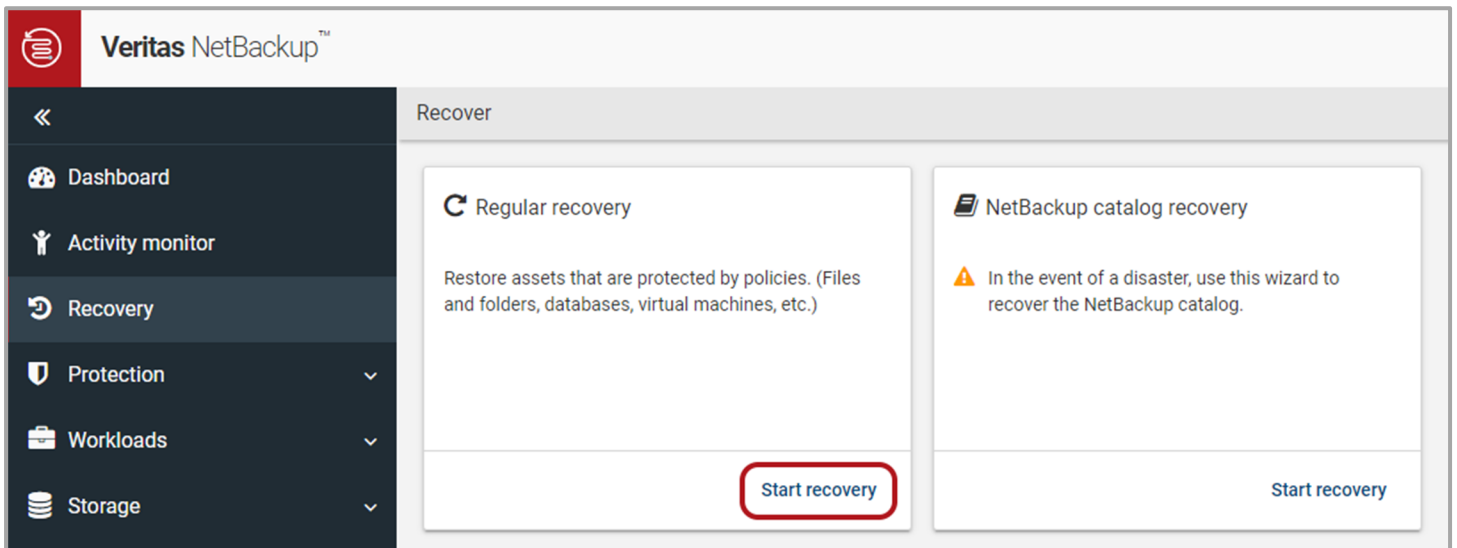


Restoring Data from Alta Recovery Vault

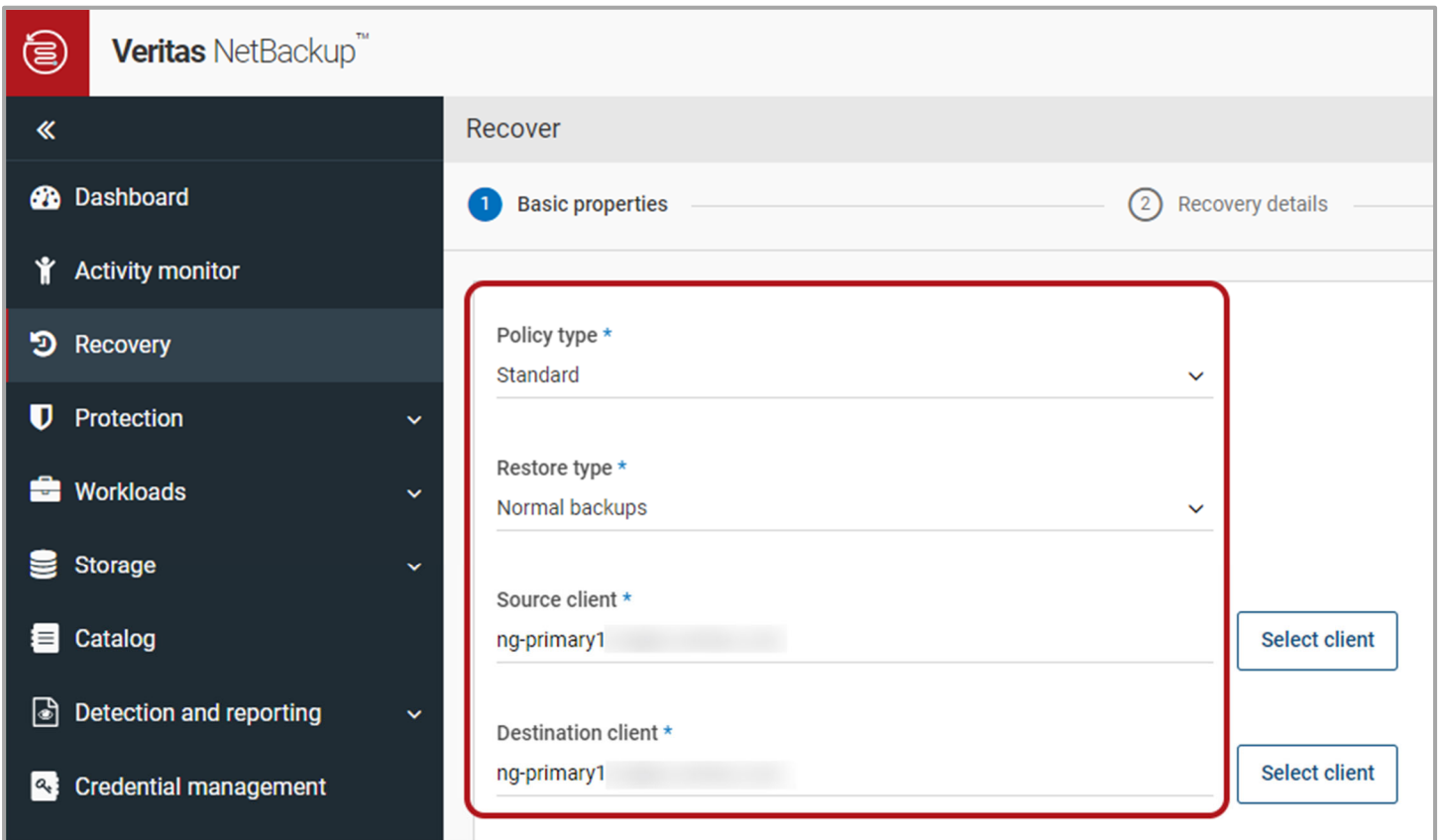
Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

Restoring data from Alta Recovery Vault is simple and follows the same process as restoring a standard MSDP storage unit.

1. Click on Recovery in the navigation bar and select start recovery from the regular recovery box.



2. Select Standard Policy Type, Normal Backups as the Restore Type and finally select the source and destination clients.



3. Select the date range for the restore and what files you'd like restored. Since Alta Recovery Vault is built right into NetBackup, restores are simple and intuitive.

Recover

Basic properties 2 Recovery details 3 Recovery options

Date range

Keyword phrase

Scan for malware before recovery ⓘ
 Additional malware scanning options are available in the next

ng-primary1.engba.veritas.com

- home
 - backups
 - bkadmin
 - .mozilla

Search file or directory name

Name	Backup date	Size
<input type="checkbox"/> .bash_logout	Mar 25, 2024 11:33 AM	18 B
<input type="checkbox"/> .bash_profile	Mar 25, 2024 11:33 AM	141 B
<input type="checkbox"/> .bashrc	Mar 25, 2024 11:33 AM	376 B
<input type="checkbox"/> .mozilla	Mar 25, 2024 11:33 AM	-
<input type="checkbox"/> .zshrc	Mar 25, 2024 11:33 AM	658 B
<input checked="" type="checkbox"/> important_file1	Mar 25, 2024 11:33 AM	500 MB
<input checked="" type="checkbox"/> important_file2	Mar 25, 2024 11:33 AM	300 MB
<input checked="" type="checkbox"/> important_file3	Mar 25, 2024 11:33 AM	2 GB

4. The final step is to customize your recovery options, which allow for even more flexibility for the file restore(s).

Recover

Basic properties 2 Recovery details 3 Recovery options

Restore target

Restore everything to original location

Restore everything to a different location

Restore individual directories and files to different locations

Create and restore to new virtual hard disk file

Recovery options

Allow overwrite of existing files

Restore directories without crossing mount points

Restore directories without access-control attributes (Windows clients only)

Rename hard links

Rename soft links

Media server

Default Select

Job priority *

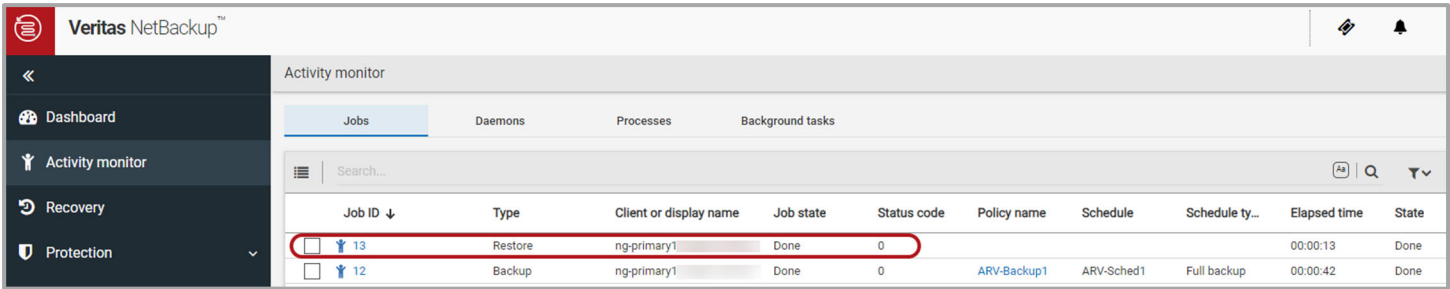
90000

A higher number is greater priority.

5. Review the summary of the review and when everything looks good, click on start recovery.



6. From the Activity Monitor you can see the status of your Alta Recovery Vault restore.

A screenshot of the Veritas NetBackup Activity Monitor interface. The left sidebar shows navigation options: Dashboard, Activity monitor, Recovery, and Protection. The main area is titled "Activity monitor" and has tabs for Jobs, Daemons, Processes, and Background tasks. The "Jobs" tab is active, showing a table of job details. A red circle highlights the first row of the table, which represents a restore job.

Job ID ↓	Type	Client or display name	Job state	Status code	Policy name	Schedule	Schedule ty...	Elapsed time	State
13	Restore	ng-primary1	Done	0				00:00:13	Done
12	Backup	ng-primary1	Done	0	ARV-Backup1	ARV-Sched1	Full backup	00:00:42	Done

Consumption Reporting

Note: Having trouble installing Alta Recovery Vault? See the [Alta Recovery Vault Troubleshooting Guide](#).

The amount of consumed and available Veritas Alta Recovery Vault storage can be easily observed in the Alta View user interface. View the total storage consumptions of your purchased Alta Recovery Vault storage. See the consumption report of standard and archive storage categories on Azure and AWS cloud providers. Also, view storage details including name, cloud provider name, region, used space, immutability type, and storage tier. For more information contact your Veritas Account Team.

To learn more about Veritas Alta View check out:

[Alta View Overview Guide](#)

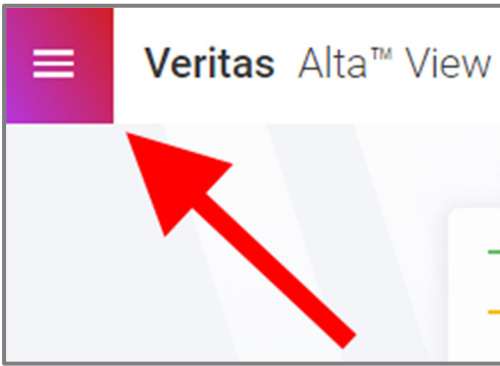
[Get Started with Veritas Alta View Today](#)

[Ready for Veritas Alta View?](#)

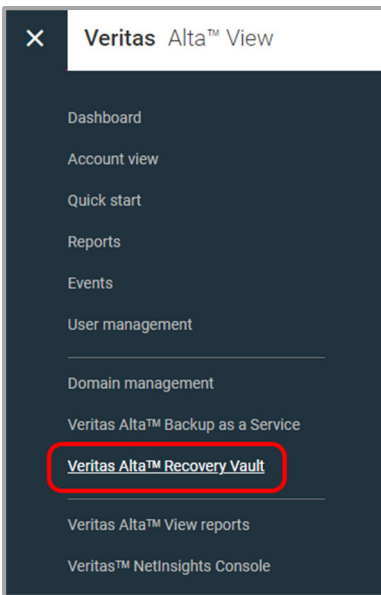
[Overview: Veritas Alta View](#)

[Veritas Alta View – Getting Started](#)

1. From the Alta View console, click on the three horizontal lines in the upper left corner.



2. From the menu select Veritas Alta Recovery Vault.



3. You will now be able to see all of your Alta Recovery Vault storage at a simple glance. The charts are dynamic as well and can be clicked on to see specific types of data.



4. Further down the page all your storage containers from both Azure and AWS, standard and archive will show in further detail.

Export to CSV | Search for Storage name, Used space, Cloud providers, Region, Immutability, Provisioned for, Storage tier

Storage name	Used space ↓	Cloud providers	Region	Immutability	Provisioned for	Storage tier
nrv [redacted]	39.37 TB	Azure	westus2	Yes	NetBackup / Alta Data Protection	Standard
nrv [redacted]	2.18 TB	Azure	westus2	Yes	NetBackup / Alta Data Protection	Standard
nrv [redacted]	1.07 TB	Azure	southcentralus	Yes	NetBackup / Alta Data Protection	Standard
nra [redacted]	424.21 GB	AWS	us-east-1	Yes	NetBackup / Alta Data Protection	Standard
nrv [redacted]	404.73 GB	Azure	southcentralus	Yes	NetBackup / Alta Data Protection	Standard
nrv [redacted]	101.77 GB	Azure	eastus	Yes	NetBackup / Alta Data Protection	Standard
nrv [redacted]	26.58 GB	Azure	westus2	Yes	NetBackup / Alta Data Protection	Standard
nra [redacted]	25.49 GB	AWS	us-east-1	Yes	NetBackup / Alta Data Protection	Standard
nra [redacted]	25.49 GB	AWS	us-west-1	Yes	NetBackup / Alta Data Protection	Standard
nrv [redacted]	25.27 GB	Azure	eastus	Yes	NetBackup / Alta Data Protection	Standard

Showing 1-10 of 68 | Rows per page: 10 | K < > X

Generating a New Storage Account Credential Token

In the event you require a new storage account credential token, you can either contact Veritas Support or you can generate a new token right from Veritas Alta View. The following are reasons for needing a new token:

1. Your Primary with the Alta Recovery Vault credential is shut off for more than 30 days.
2. You re-apply your token to the same credential.
3. Your Primary is destroyed and needs to be re-built.
4. You would like to build a Cloud Recovery Server (CRS) and perform Image Sharing.

Note: See the [Veritas Alta Recovery Vault Image Sharing and Disaster Recovery](#) for more information.

To generate a new token:

1. From Alta View, click on the Veritas Alta Recovery Vault tab on the left side.
2. Search for your Storage Account name.
3. Look for the column labeled Actions.
4. Click on the Generate Token link. This will create a new token that can be used for your replacement Primary token or can be used on your CRS Image Sharing server (Alternate Primary).

The screenshot displays the Veritas Alta View interface. The top navigation bar includes the Veritas logo and 'Veritas Alta™ View'. A left sidebar contains various management options, with 'Veritas Alta™ Recovery Vault' highlighted. The main content area shows 'Recovery Vault storage usage overview' with two bar charts: 'Archive storage overview' and 'Standard storage overview'. Below these charts is a table of storage accounts. The table has columns for 'Storage name', 'Used space', 'Cloud providers', 'Immutability', 'Actions', 'Storage tier', and 'Region'. The 'Actions' column for the first row contains a red 'Generate token' button. A search bar above the table contains the text 'Storage Account Name'.

Storage name	Used space ↓	Cloud providers	Immutability	Actions	Storage tier	Region
	23.09 GB	Azure	Yes	Generate token	Standard	westus

Conclusion

Veritas Alta Recovery Vault not only simplifies the process of provisioning new storage in the cloud, it reduces risk, allows for limitless scalability, lowers TCO and automates resiliency. Through seamless integration with NetBackup together with an easy-to-use UI, management and monitoring of cloud storage resources and retention policies, provisioning storage, and protecting your data has never been easier.

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at [veritas.com](https://www.veritas.com). Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
[veritas.com](https://www.veritas.com)

For specific country offices
and contact numbers,
please visit our website.

VERITAS™