In-Cloud Data Recovery with Veritas Alta Recovery Vault

Cloud-based Storage-as-a-Service

This paper is designed to highlight the steps customers will need to perform Image Sharing with Veritas Alta™ Recovery Vault.

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

September 2024

TABLE OF CONTENTS

Revision History

Version	Date	Changes	Author
1.00	06/2022	Initial Version	Neil Glick
1.01	01/2023	Rebrand	Neil Glick
1.02	9/21/2023	Updates for 10.3	Neil Glick
1.03	8/27/2024	Security and version updates.	Neil Glick

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 Veritas Alta Recovery Vault, there is no need to build, manage, and protect a physical site to isolate backup data.

Target Audience

This document is targeted at customers interested in learning about using Veritas Alta Recovery Vault, Cloud Recovery Servers and Image Sharing to restore critical data anywhere you need it.

Why NetBackup Alta Recovery Vault and Image Sharing

Image Sharing is not new to NetBackup, but with the introduction of NetBackup Alta Recovery Vault, users can combine the strengths of both technologies to copy data from a primary site to an alternate site in a different domain or in the cloud.

NetBackup Alta Recovery Vault provides a fully managed cloud data protection tier that’s seamlessly integrated in NetBackup. With NetBackup Alta Recovery Vault and Image Sharing, Veritas customers can copy their mission critical data and restore it using a completely autonomous primary server located off site. In the event the primary server is compromised, mission critical data can be restored to the alternate site and continue to meet compliance and governance requirements.

Image Sharing and Veritas Alta Recovery Vault Prerequisites and Requirements

Using Image Sharing with Veritas Alta Recovery Vault is simple, but some prerequisites will need to be met for Image Sharing and Veritas Alta Recovery Vault to work together:

1. Image Sharing is supported on both Azure and AWS.
2. Archive tiers are not supported for Image Sharing on Azure or AWS.
3. Image Sharing requires an alternate NetBackup primary server be available on a different domain or cloud environment. This is generally achieved by deploying a NetBackup Cloud Recovery Server, which is an all-in-one node that includes both a primary and media server.
4. The Media Server Deduplication Pool (MSDP) for Image Sharing will need to be created at the alternate site.

   Note: In NetBackup 10.5 and above an existing Primary server can be used, but a new MSDP for Image Sharing must be created and added to the existing domain.

5. When creating the MSDP storage server, the alternate primary server must be chosen, which cannot be a media server. (For NetBackup 10.4 and below)

6. The name of the backup volume used at the alternate site must match the name of the volume at the primary site.
7. The Veritas Alta Recovery Vault cloud bucket used for primary backups will need to be used at the alternate site.
8. Veritas Alta Recovery Vault account credentials will need to be available or already in use.
    a. A new token for Azure. Contact your Veritas Account team to receive a new token.
    b. A new token for AWS. Contact your Veritas Account team to receive a new token.

You do not need to make any changes on the primary server as long as the data you wish to copy to the alternate site is located on a Veritas Alta Recovery Vault SaaS MSDP-C disk pool. If you do not have Veritas Alta Recovery Vault, contact your Veritas NetBackup Account Manager for a demonstration and additional documentation on the benefits of the SaaS offering.

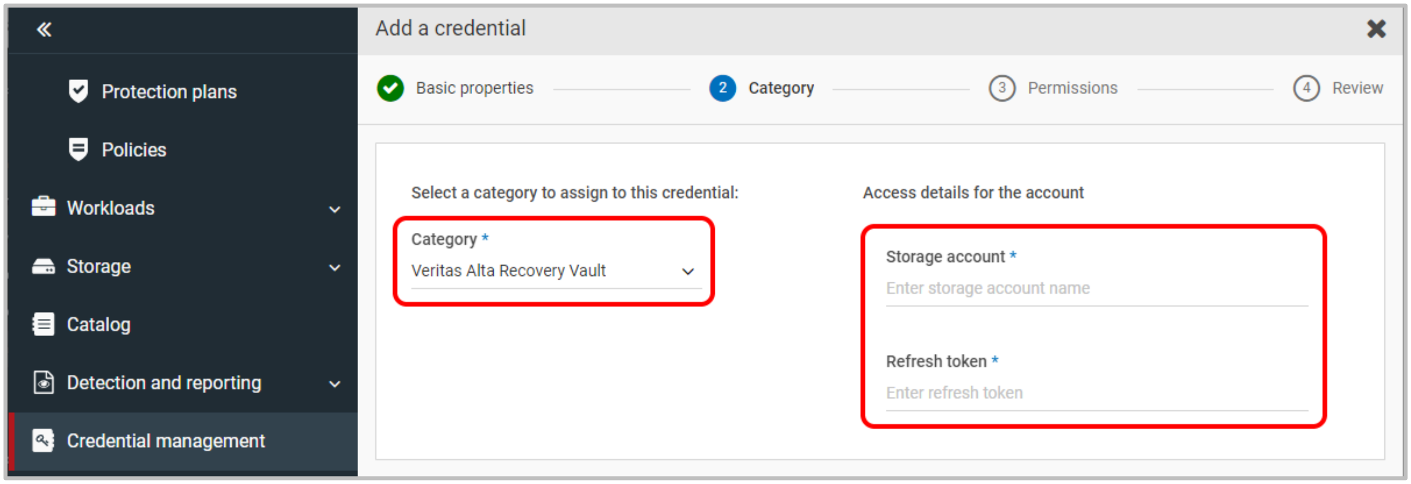
Short lived token based authentication

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 SAS 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.



Add a credential

Basic properties — 2 Category — 3 Permissions — 4 Review

Select a category to assign to this credential:

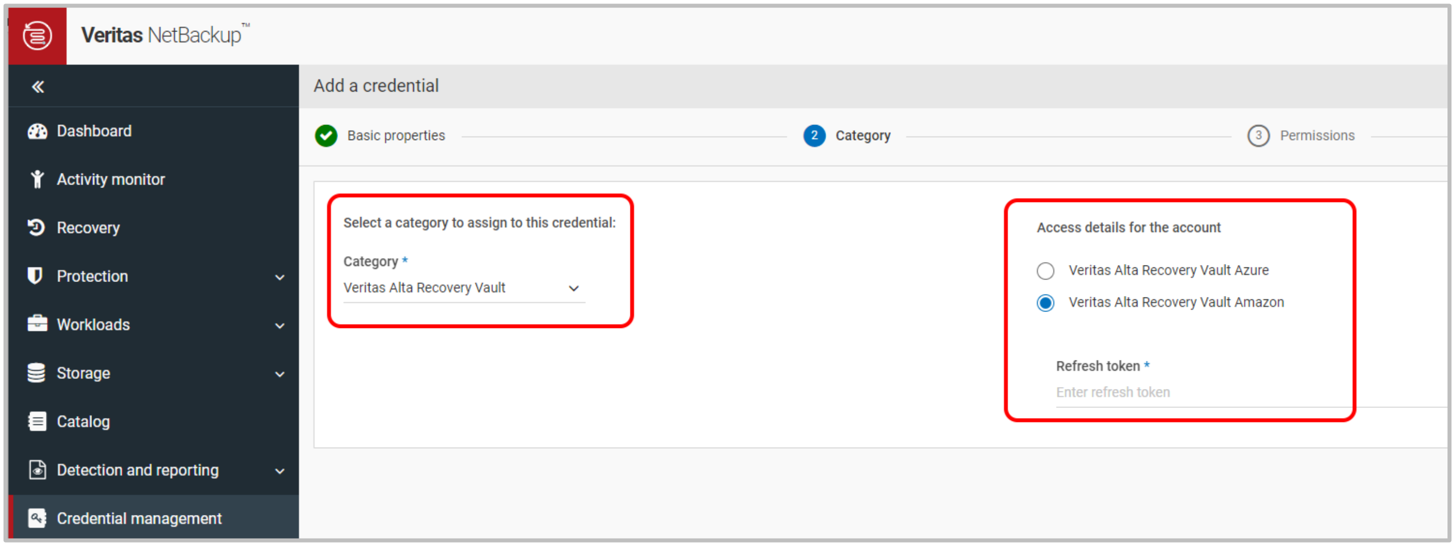
Category *
Veritas Alta Recovery Vault

Access details for the account

Storage account *
Enter storage account name

Refresh token *
Enter refresh token

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.



Add a credential

Basic properties — 2 Category — 3 Permissions

Select a category to assign to this credential:

Category *
Veritas Alta Recovery Vault

Access details for the account

○ Veritas Alta Recovery Vault Azure
● Veritas Alta Recovery Vault Amazon

Refresh token *
Enter refresh token

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 will lead to failures in configurations. 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.

Configuring Image Sharing on Your Primary Server With Veritas Alta Recovery Vault

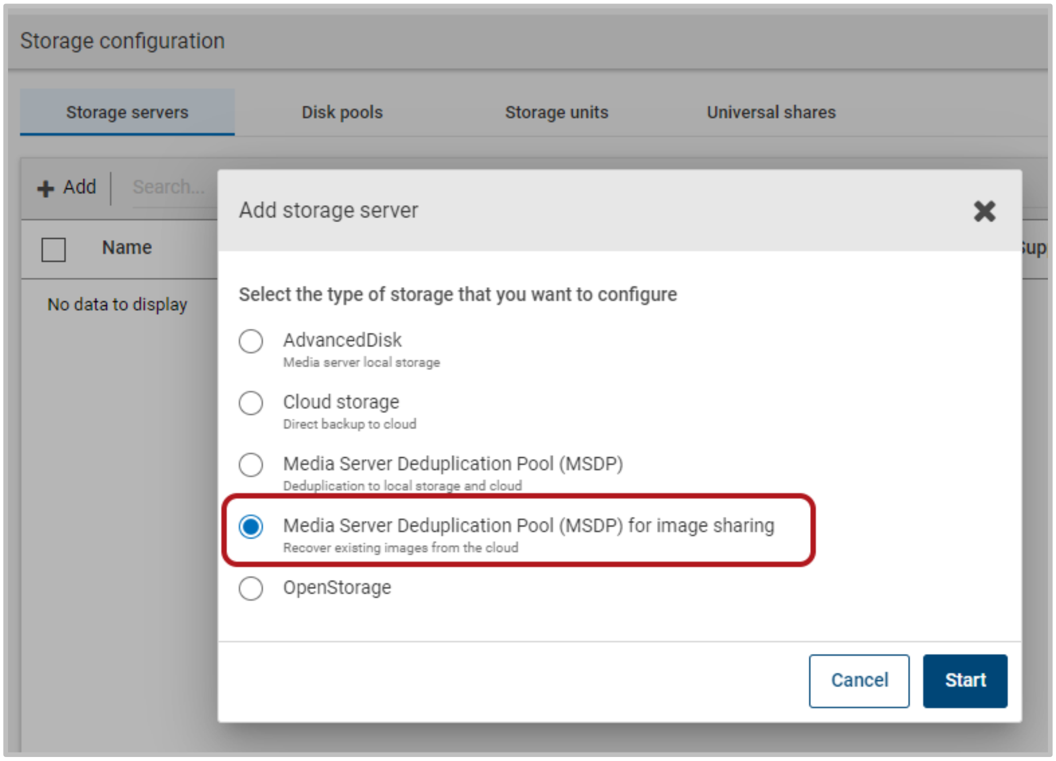
If new to Veritas Alta Recovery Vault, you will need to create a disk pool and storage unit to back up the data you wish to copy to an alternate site. If you are already using Veritas Alta Recovery Vault, backed up data can be imported to an alternate site using Image Sharing. The example used in this document connects to Veritas Alta Recovery Vault in an Azure cloud environment.

Note: To view the steps on how to connect to your Alta Recovery Vault storage, see the Veritas Alta Recovery Vault Deployment Guide.

Note: This document assumes the customer has already connected to their Alta Recovery Vault storage and backups have been sent to the new storage.

1. Log onto the alternate site and create an MSDP with image sharing Storage Server.

   Note: In NetBackup 10.5 and above, an MSDP with image sharing server can be joined to an existing NetBackup domain if you do not wish to create a new domain.



Add storage server

Select the type of storage that you want to configure

○ AdvancedDisk
Media server local storage

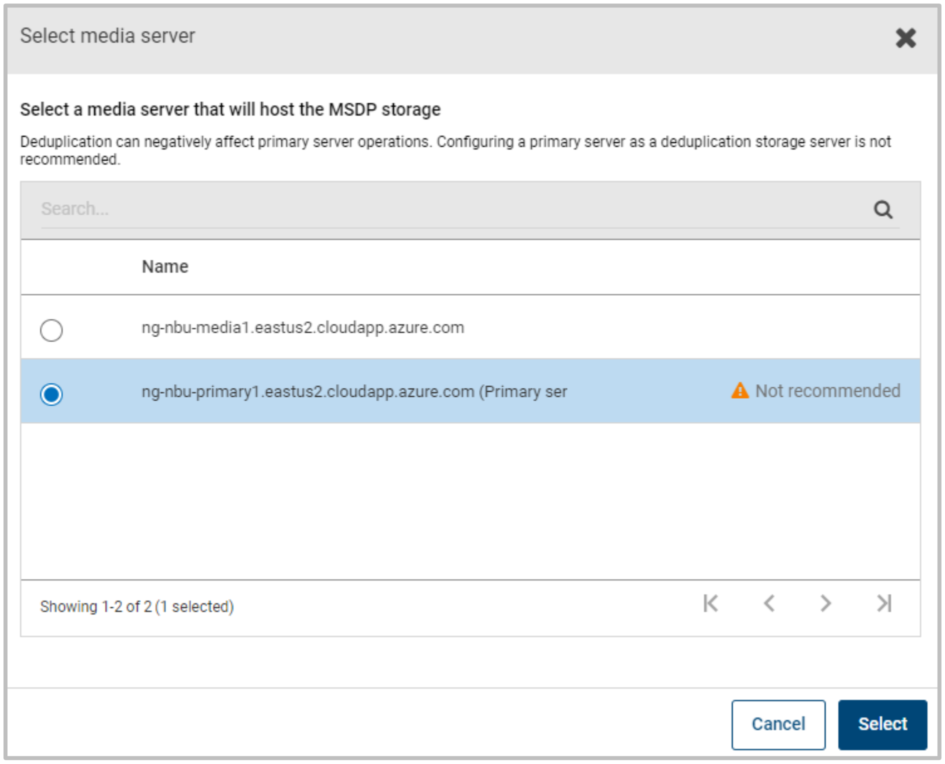
○ Cloud storage
Direct backup to cloud

○ Media Server Deduplication Pool (MSDP)
Deduplication to local storage and cloud

● Media Server Deduplication Pool (MSDP) for image sharing
Recover existing images from the cloud

○ OpenStorage

2. Next choose the alternate Primary server as the media server that will host the MSDP storage. Traditionally this is not a best practice but is mandatory for Image Sharing.



Select media server

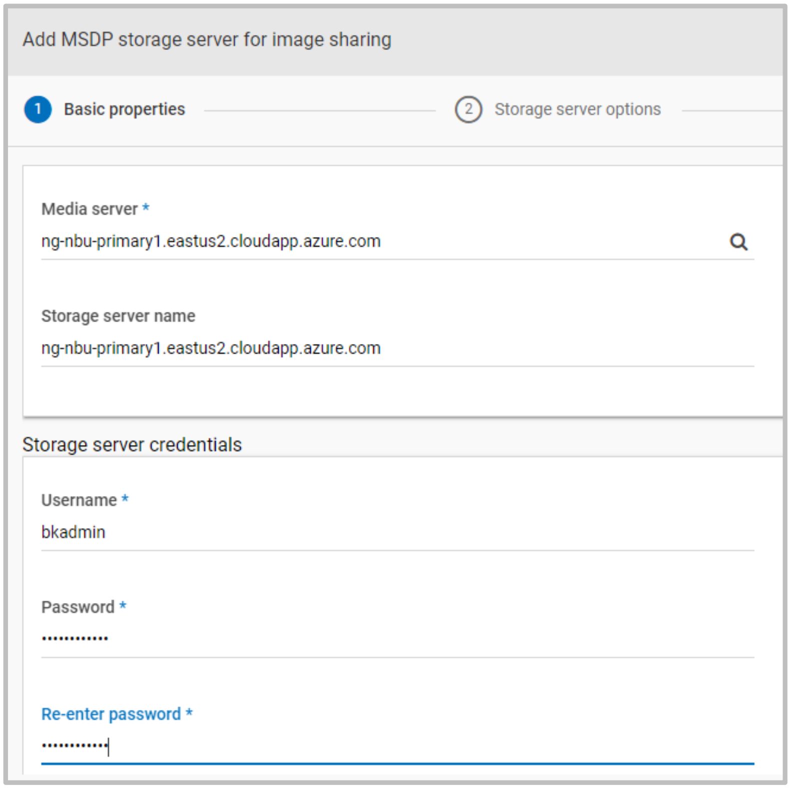
Select a media server that will host the MSDP storage

Deduplication can negatively affect primary server operations. Configuring a primary server as a deduplication storage server is not recommended.

	Name	
○	ng-nbu-media1.eastus2.cloudapp.azure.com	
●	ng-nbu-primary1.eastus2.cloudapp.azure.com (Primary ser	⚠ Not recommended

Showing 1-2 of 2 (1 selected)

3. Enter the username for the alternate primary server.



Add MSDP storage server for image sharing

Media server *
ng-nbu-primary1.eastus2.cloudapp.azure.com

Storage server name
ng-nbu-primary1.eastus2.cloudapp.azure.com

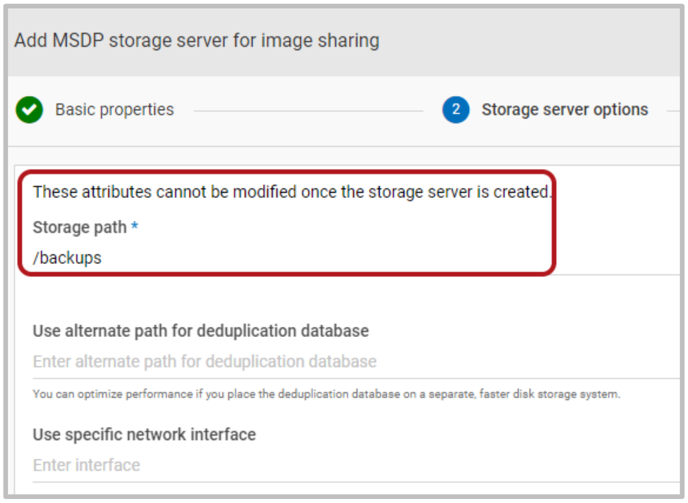
Storage server credentials

Username *
bkadmin

Password *
....

Re-enter password *
....

4. Enter the storage path for the MSDP for image sharing. This does not have to be the same as the MSDP server at the primary site.



Add MSDP storage server for image sharing

These attributes cannot be modified once the storage server is created.

Storage path *

/backups

Use alternate path for deduplication database

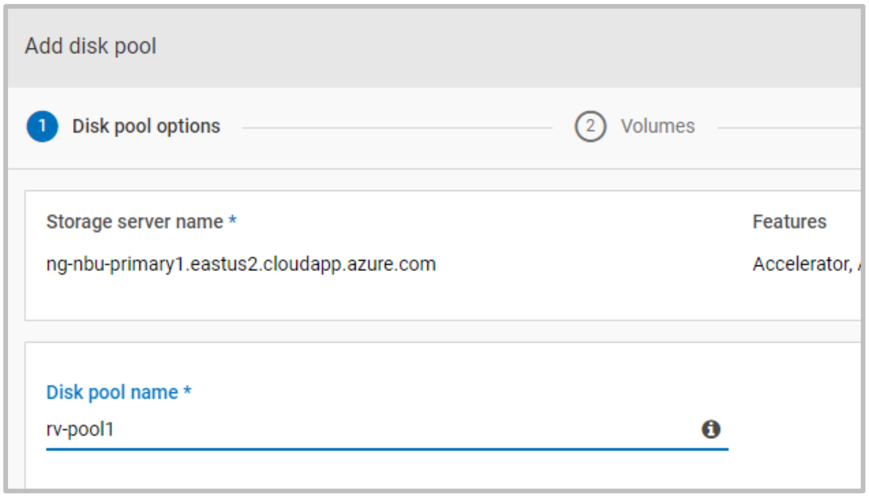
Enter alternate path for deduplication database

You can optimize performance if you place the deduplication database on a separate, faster disk storage system.

Use specific network interface

Enter interface

5. Once the MSDP for image sharing has been created we'll create the disk pool.



Add disk pool

Storage server name *

ng-nbu-primary1.eastus2.cloudapp.azure.com

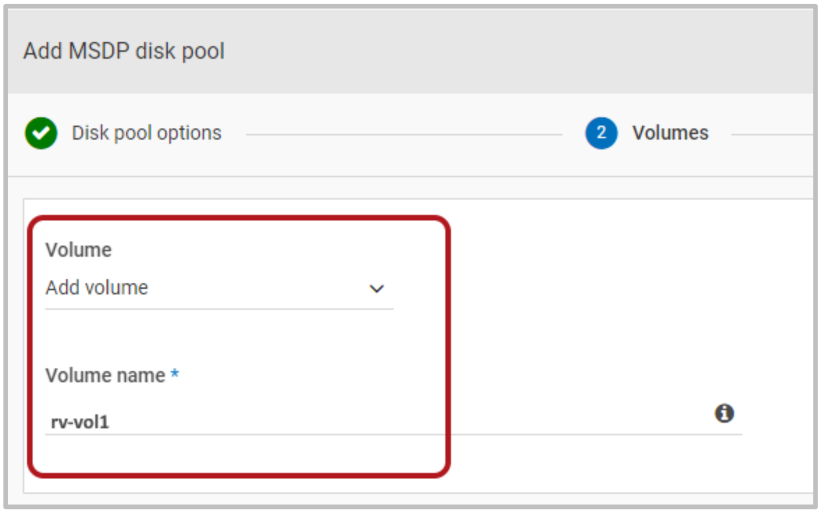
Features

Accelerator, /

Disk pool name *

rv-pool1

6. When creating the volume at the alternate site it is required that its name be the same as the volume at the primary site.



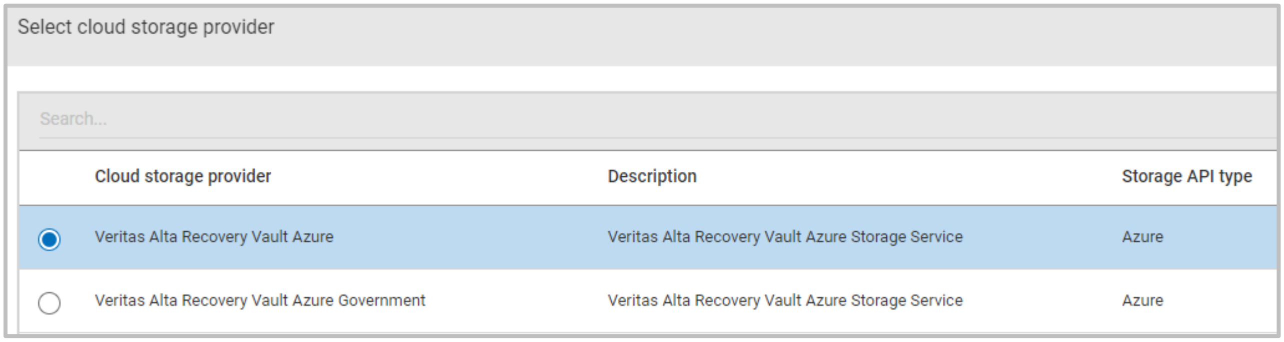
Add MSDP disk pool

✓ Disk pool options — 2 Volumes

Volume: Add volume

Volume name *: rv-vol1

7. Use the same cloud storage provider at the alternate site as you did at the primary site. In this example we’re using Veritas Alta Recovery Vault Azure.

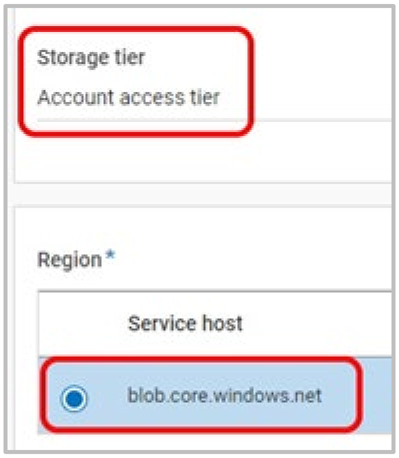


Select cloud storage provider

Search...

	Cloud storage provider	Description	Storage API type
●	Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
○	Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure

8. Leave Storage Tier as the default and select the Region you used at the primary site.

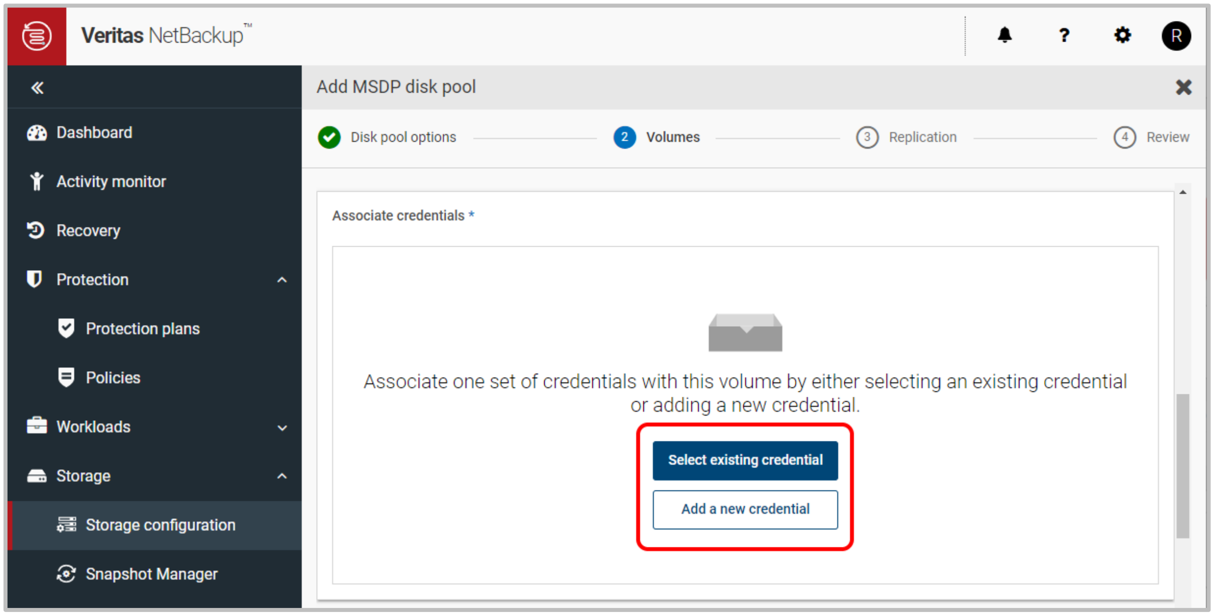


Storage tier: Account access tier

Region *

	Service host
●	blob.core.windows.net

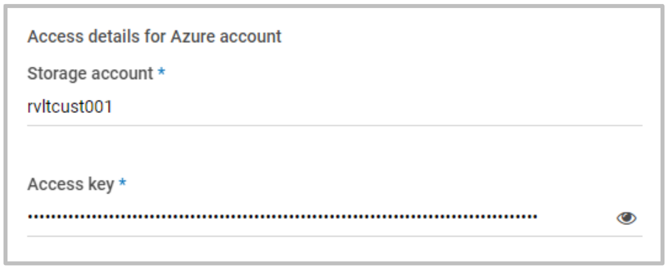
9. Click **Select existing credential** if you've already created your credential from the Short-Lived Token Based Authentication section earlier in this document. If not, click **Add a new credential** and create a **new** credential using the storage account and refresh token given to you by Veritas.



Associate one set of credentials with this volume by either selecting an existing credential or adding a new credential.

If you are using NetBackup 10.1.1 or earlier (Azure) or 10.3.1 or earlier (AWS), enter the storage account and Access key to connect to the storage account.

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

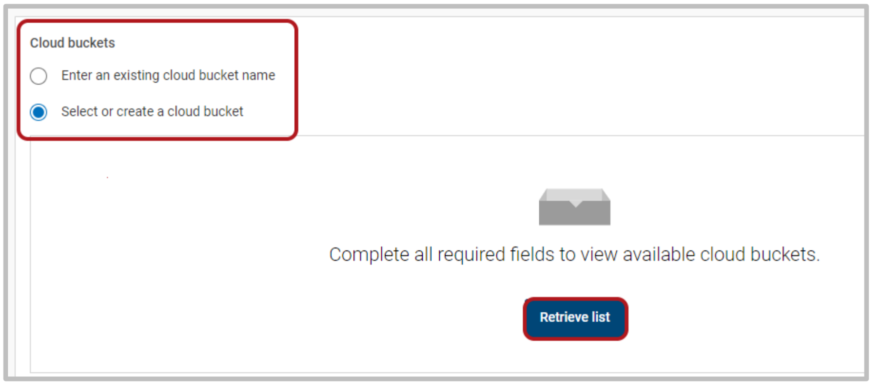


Access details for Azure account

Storage account *
rvltcust001

Access key *
••

10. Once the credentials have been entered, click on Select or create a cloud bucket and Retrieve list to get the list of created storage buckets.



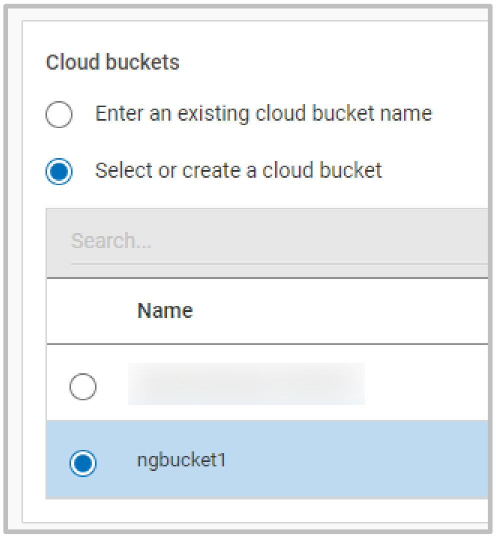
Cloud buckets

○ Enter an existing cloud bucket name

● Select or create a cloud bucket

Complete all required fields to view available cloud buckets.

11. Select the storage bucket that you've been using at the primary site.



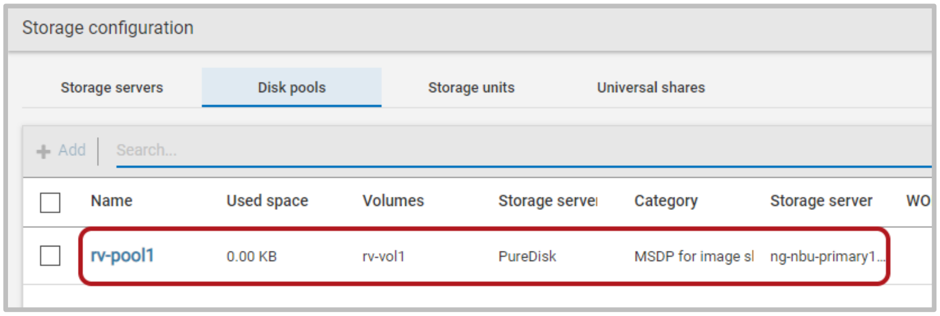
Cloud buckets

○ Enter an existing cloud bucket name

● Select or create a cloud bucket

	Name
○	
●	ngbucket1

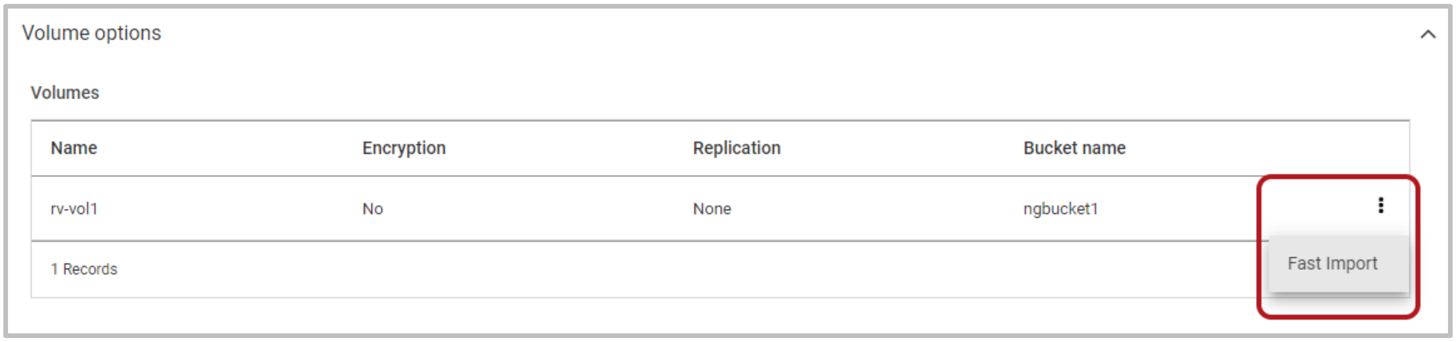
12. After the disk pool has been created, we can now import a backup from NetBackup Recovery Vault into our alternate primary server. Go to Storage Configuration > Disk Pools and click on the disk pool you just created.



Storage configuration

□	Name	Used space	Volumes	Storage serve	Category	Storage server	WO
□	rv-pool1	0.00 KB	rv-vol1	PureDisk	MSDP for image sl	ng-nbu-primary1...	

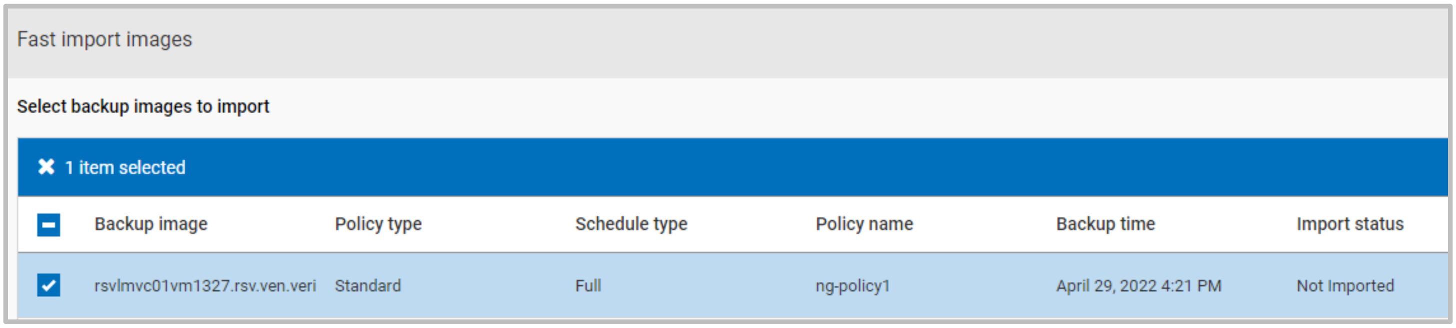
13. Under the Volume Options, click on the three vertical dots and select Fast Import.



Name	Encryption	Replication	Bucket name
rv-vol1	No	None	ngbucket1

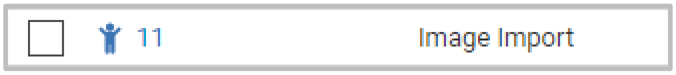
1 Records

14. Select the backup you'd like to import and click on the Import button. (Not shown)



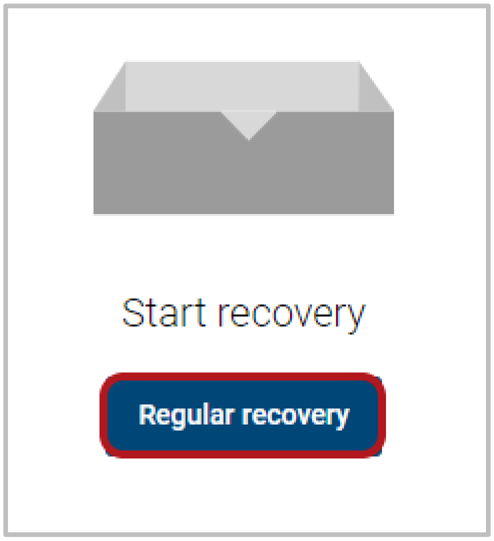
☐	Backup image	Policy type	Schedule type	Policy name	Backup time	Import status
☑	rsvlmvc01vm1327.rsv.ven.veri	Standard	Full	ng-policy1	April 29, 2022 4:21 PM	Not Imported

15. This will import the backup image which can be browsed through recovery allowing for file restores.



☐	11	Image Import

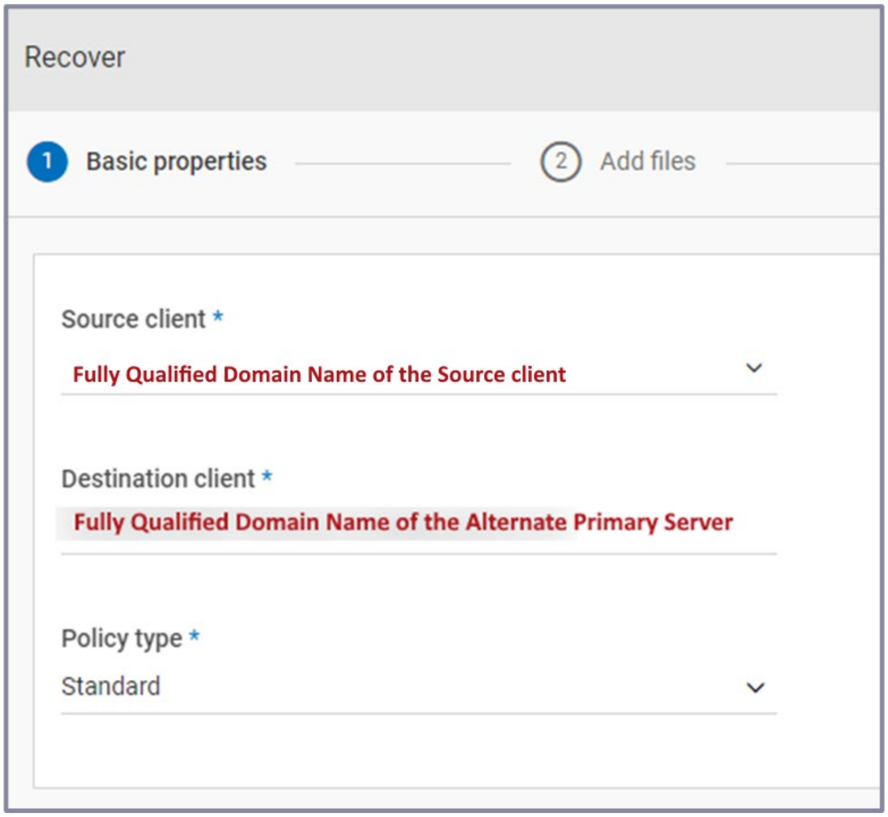
16. Under Recovery, click on the Regular Recovery button.



17. Enter the following information:

   a. Source Client, enter the fully qualified domain name of the primary server.

b. Destination Client, enter the fully qualified domain name of the alternate primary server.
c. Policy Type, select the type that was used to backup the data at the primary server. In this example it's Standard.



Source client *

Fully Qualified Domain Name of the Source client

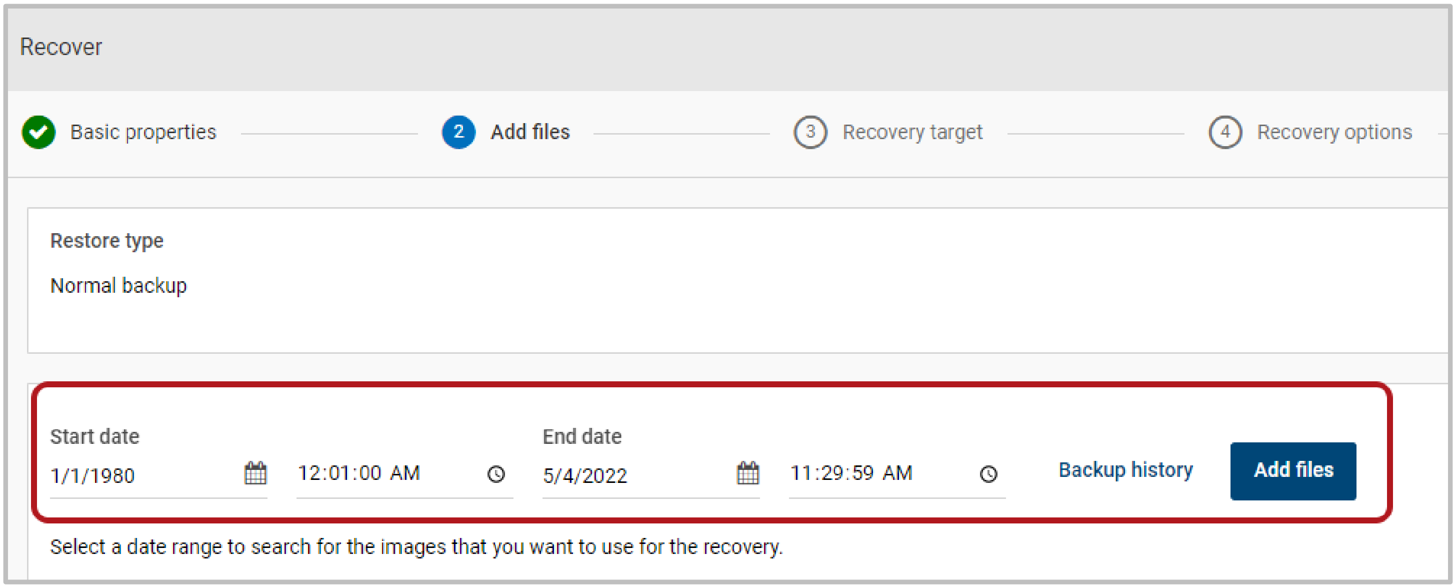
Destination client *

Fully Qualified Domain Name of the Alternate Primary Server

Policy type *

Standard

18. Enter the time and data of the backup and click on Add Files.



Restore type

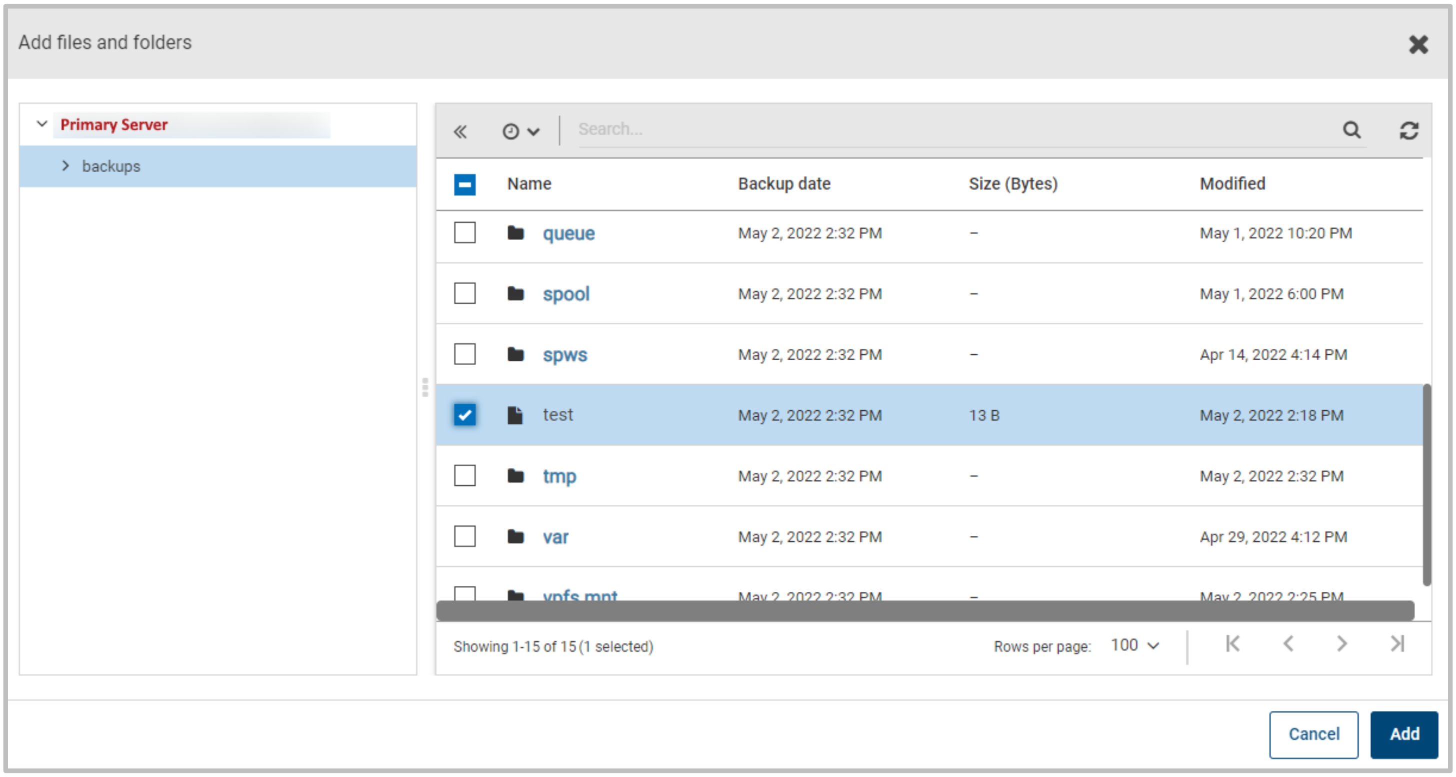
Normal backup

Start date 1/1/1980 12:01:00 AM

End date 5/4/2022 11:29:59 AM

Select a date range to search for the images that you want to use for the recovery.

19. The available backup data will appear. Select what you'd like restored and click on Add.

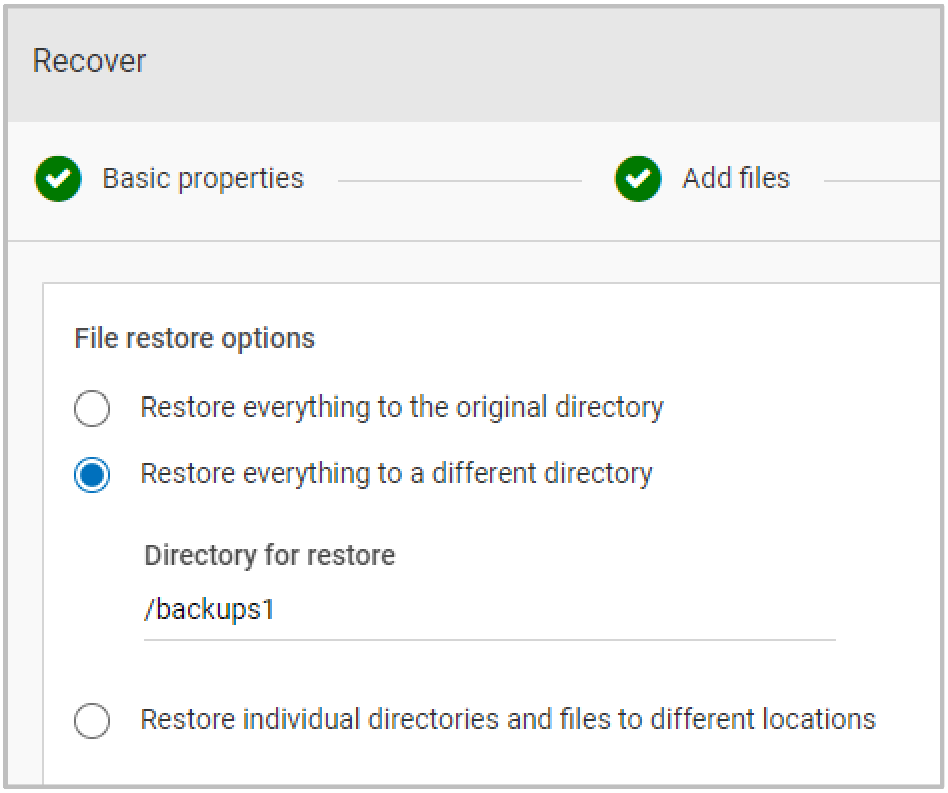


☐	Name	Backup date	Size (Bytes)	Modified
☐	queue	May 2, 2022 2:32 PM	–	May 1, 2022 10:20 PM
☐	spool	May 2, 2022 2:32 PM	–	May 1, 2022 6:00 PM
☐	spws	May 2, 2022 2:32 PM	–	Apr 14, 2022 4:14 PM
☑	test	May 2, 2022 2:32 PM	13 B	May 2, 2022 2:18 PM
☐	tmp	May 2, 2022 2:32 PM	–	May 2, 2022 2:32 PM
☐	var	May 2, 2022 2:32 PM	–	Apr 29, 2022 4:12 PM
☐	vpfs mnt	May 2, 2022 2:32 PM	–	May 2, 2022 2:25 PM

Showing 1-15 of 15 (1 selected)

Rows per page: 100

20. Enter where you'd like to restore the files to. Here we're selecting to restore the file(s) to an alternate location.



File restore options

○ Restore everything to the original directory

● Restore everything to a different directory

Directory for restore

/backups1

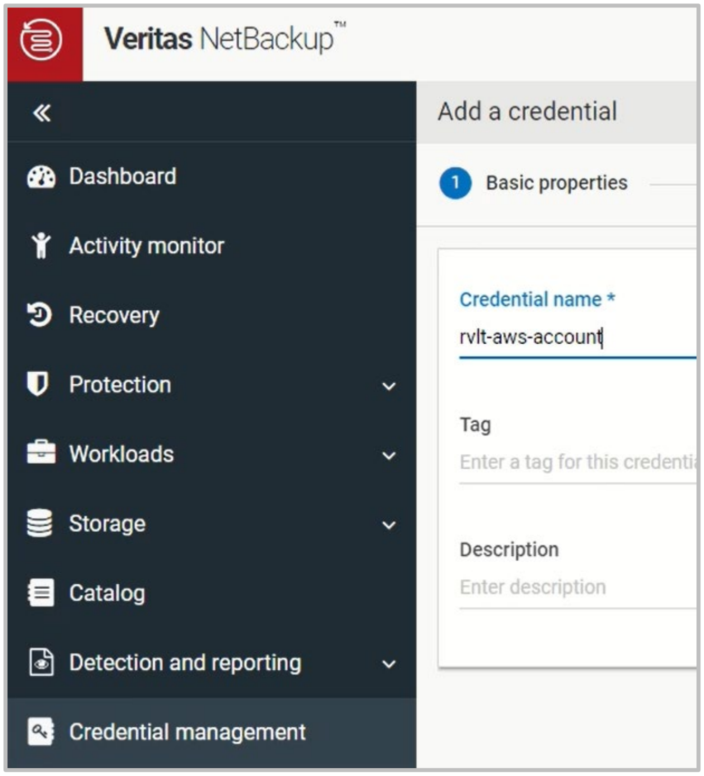
○ Restore individual directories and files to different locations

21. When you’re happy with the restore selections, click on the Start Recovery button to begin the restore.

VMWare conversion on AWS and Azure with Alta Recovery Vault

In versions prior to NetBackup 10.3, when recovering a VMware virtual machine from Alta Recovery Vault, the data store will assume the same accounts, however Alta Recovery Vault did not have the permissions to convert the virtual machine. To accomplish this access to an Azure or AWS account will be used to covert the Alta Recovery Vault backup image and import into. To accomplish the conversion:

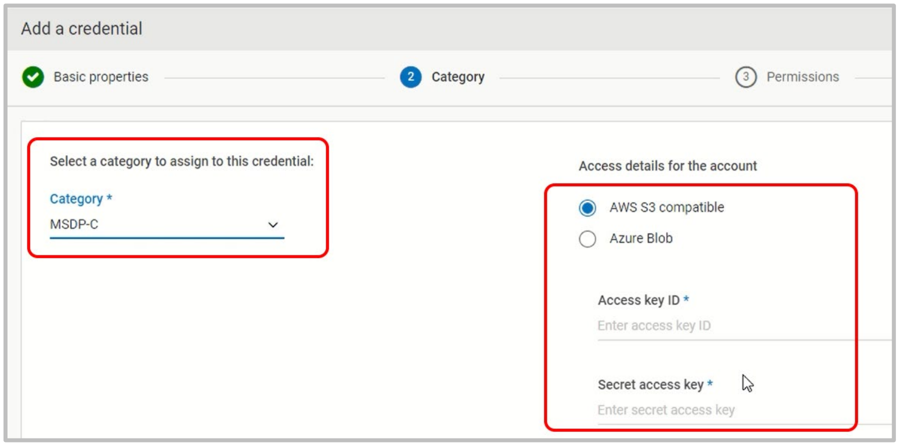
1. Create a secondary primary or a cloud recovery server (CRS) as completed in this document.
2. Create an Alta Recovery Vault credential to your Veritas Azure or AWS storage bucket, ensuring to set the Category as MSDP-C and enter in the credentials for AWS or Azure.



Credential name * rvlt-aws-account

Tag: Enter a tag for this credenti

Description: Enter description


Add a credential

Basic properties — 2 Category — 3 Permissions

Select a category to assign to this credential:

Category *
MSDP-C

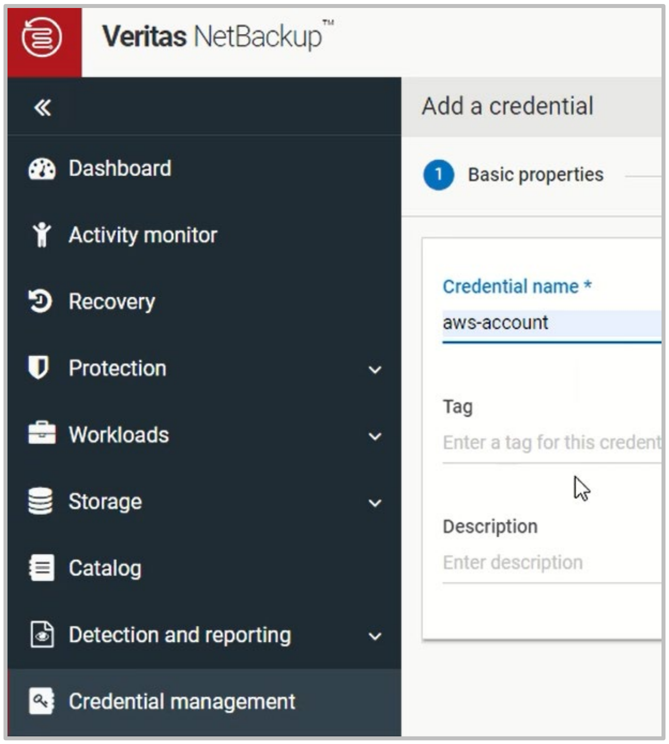
Access details for the account

● AWS S3 compatible
○ Azure Blob

Access key ID *
Enter access key ID

Secret access key *
Enter secret access key

3. Next create another credential, but this time choose your cloud provider that you'd like to import the VMware virtual machine into. Ensure to select MSDP-C as the Category, select your cloud provider and enter in your credentials.



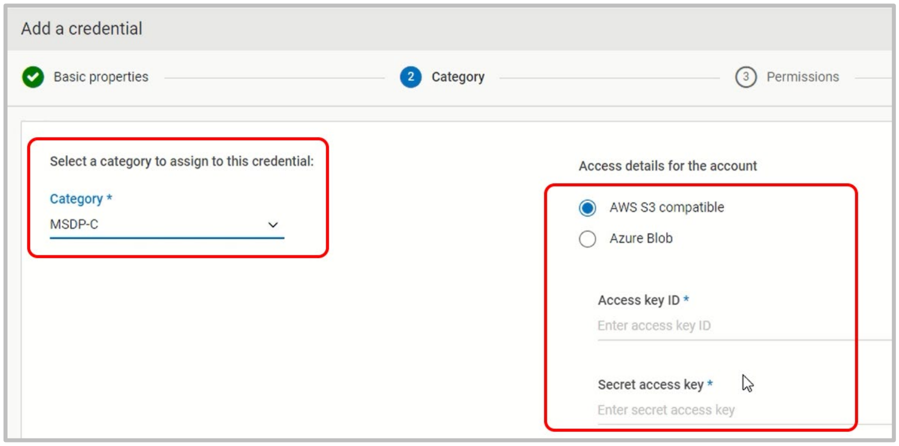
Add a credential

1 Basic properties

Credential name *
aws-account

Tag
Enter a tag for this credent

Description
Enter description



Select a category to assign to this credential:

Category *
MSDP-C

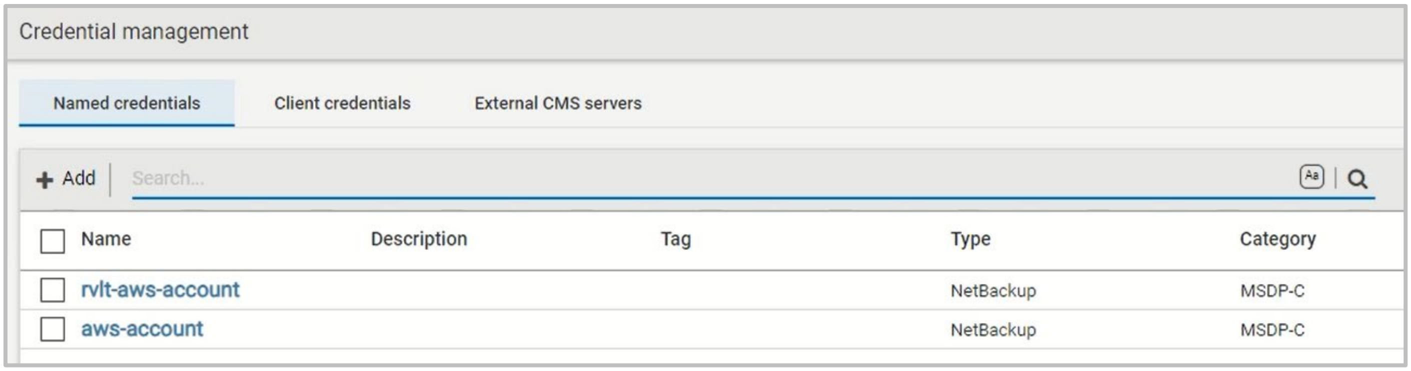
Access details for the account

● AWS S3 compatible
○ Azure Blob

Access key ID *
Enter access key ID

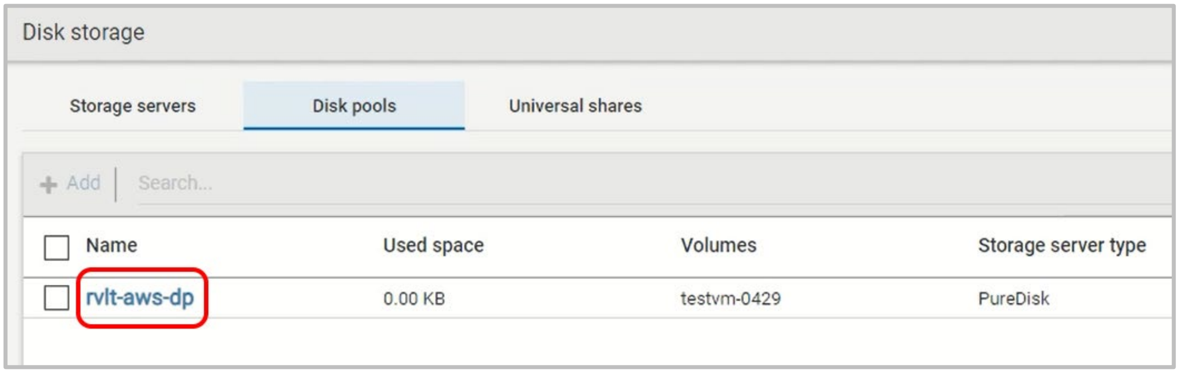
Secret access key *
Enter secret access key

4. You should see something similar with one credential to your Alta Recovery Vault storage that has the backup image of the VMware virtual machine and another where the backup image will be imported into.



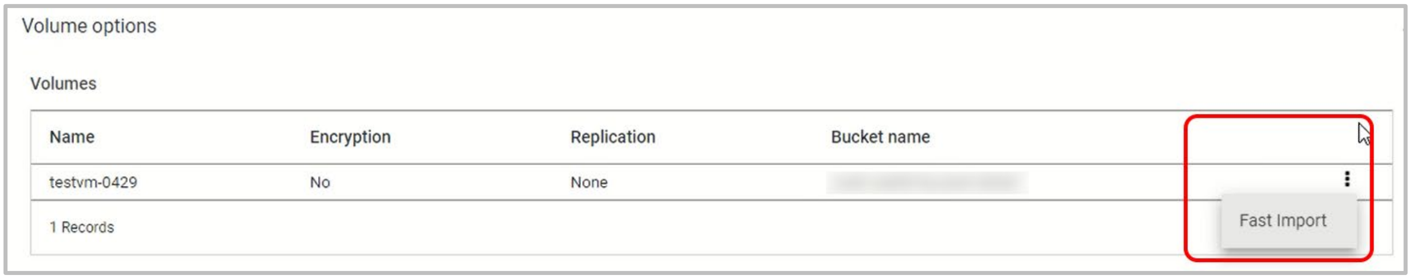
□	Name	Description	Tag	Type	Category
□	rvlt-aws-account			NetBackup	MSDP-C
□	aws-account			NetBackup	MSDP-C

5. Next, connect to the Alta Recovery Vault storage that contains the VMware virtual machine, ensuring that you use the same volume name that was used when first connecting to the storage bucket. As seen in this document.
6. Once the disk pool and volume have been created, click on the disk pool to see its details.



□	Name	Used space	Volumes	Storage server type
□	rvlt-aws-dp	0.00 KB	testvm-0429	PureDisk

7. Find the Volume Options section and click on the three dots and then on Fast Import. This will import the backup image on the Alta Recovery Vault storage.



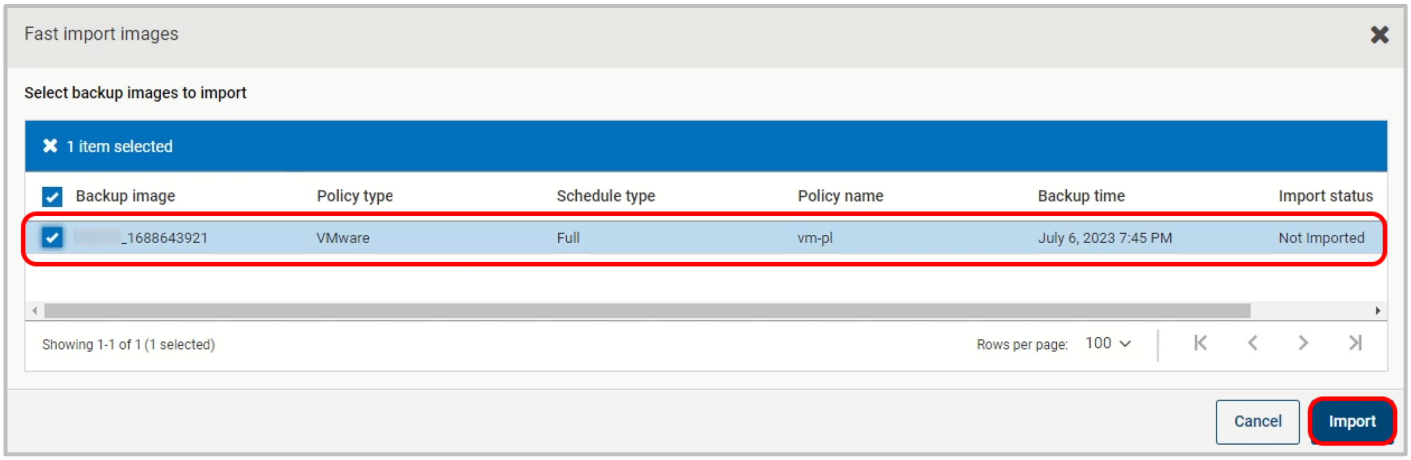
Volume options

Volumes

Name	Encryption	Replication	Bucket name	
testvm-0429	No	None	[redacted]	⋮

1 Records

8. Select the backup image with the VMware virtual machine and click on Import.



Fast import images ✖

Select backup images to import

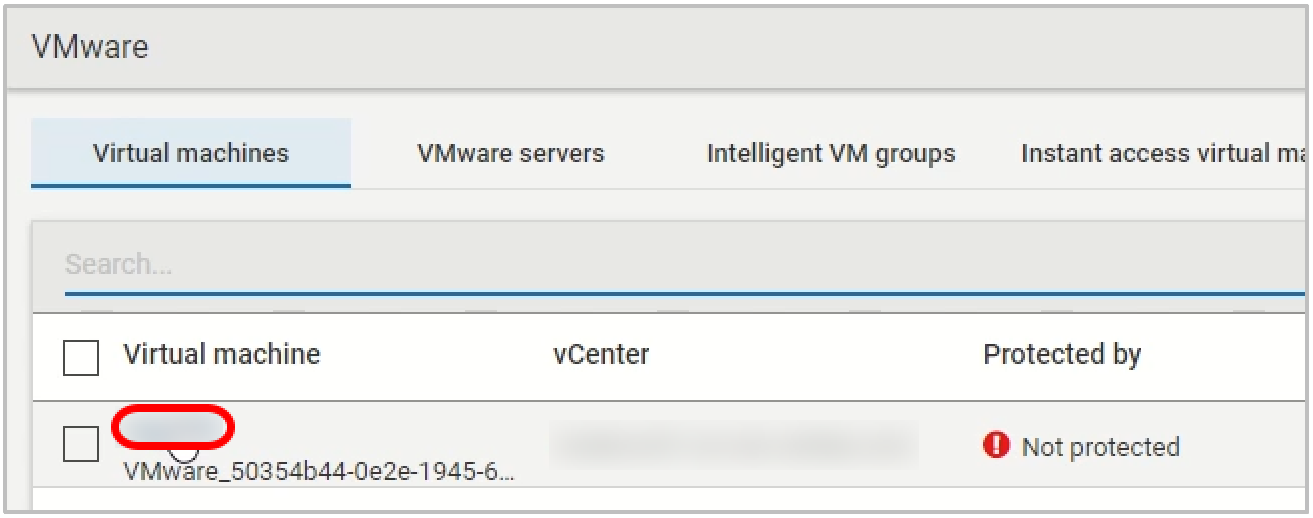
✖ 1 item selected

☑ Backup image	Policy type	Schedule type	Policy name	Backup time	Import status
☑ [redacted]_1688643921	VMware	Full	vm-pl	July 6, 2023 7:45 PM	Not Imported

Showing 1-1 of 1 (1 selected)

Rows per page: 100

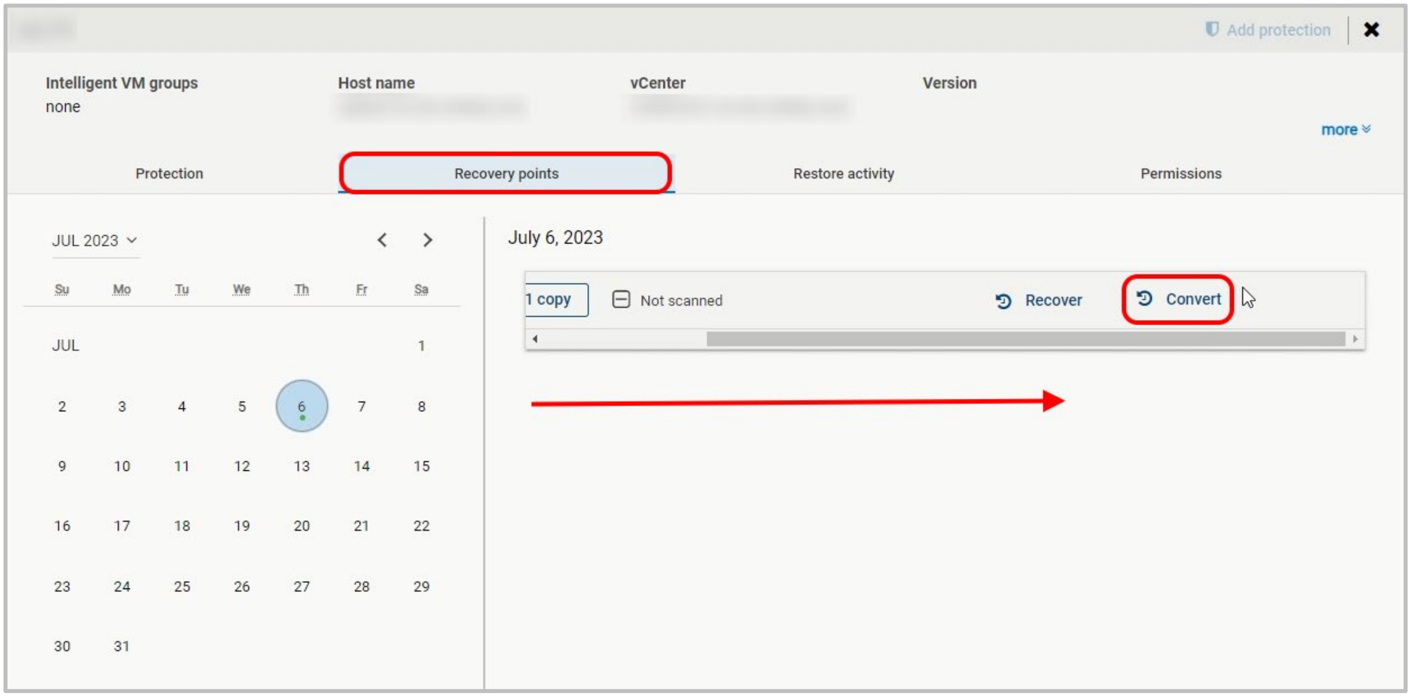
9. Navigate to Workloads -> VMware in the NetBackup WebUI. The virtual machine from the Alta Recovery Vault storage should now appear. Click on the virtual machine.



VMware

□ Virtual machine	vCenter	Protected by
□ [redacted] VMware_50354b44-0e2e-1945-6...	[redacted]	Not protected

10. Click on the Recovery Points tab, select the date and the backup. Scroll to the right and click on the Covert button.



[redacted]

Intelligent VM groups
none

Host name
[redacted]

vCenter
[redacted]

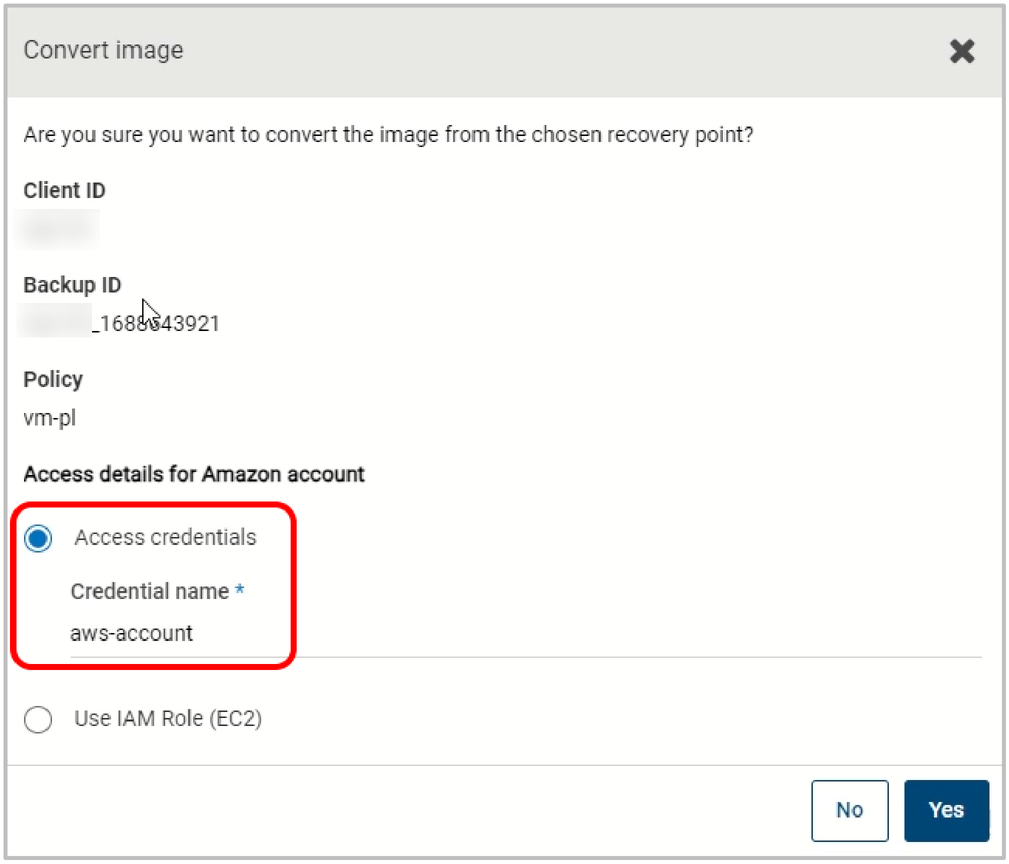
Version

Su	Mo	Tu	We	Th	Fr	Sa
JUL						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

July 6, 2023

1 copy Not scanned

11. Select the credential you created to connect to your cloud service provider, in this example AWS, and click Yes.



Convert image ✖

Are you sure you want to convert the image from the chosen recovery point?

Client ID

[redacted]

Backup ID

[redacted]_1688643921

Policy

vm-pl

Access details for Amazon account

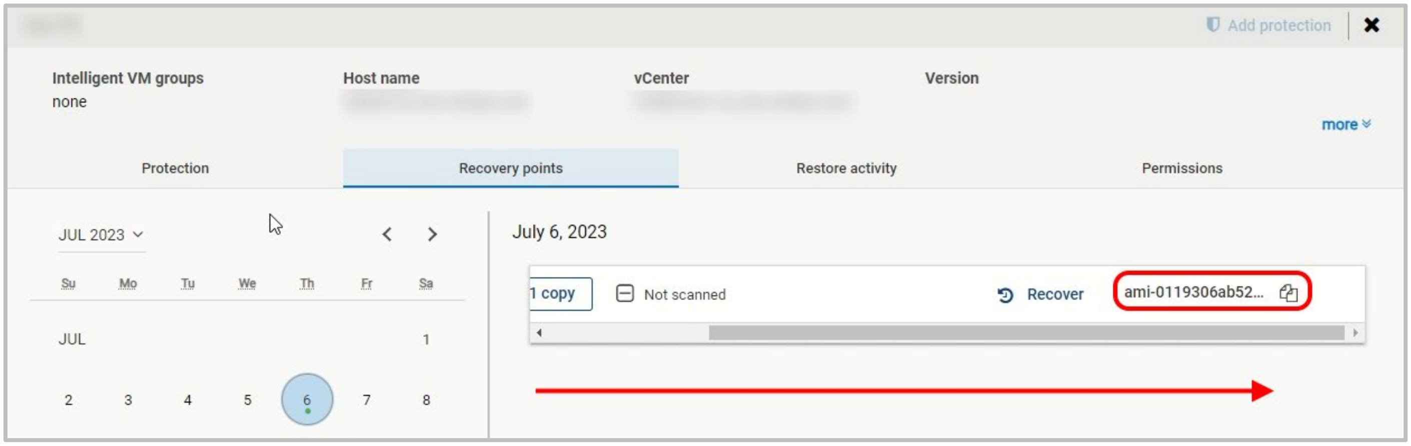
● Access credentials

Credential name *

aws-account

○ Use IAM Role (EC2)

12. Once the restore is complete, go back to Workloads -> VMware from the NetBackup WebUI and click on the virtual machine once again. Click on Recovery Points tab and scroll to the right. You will notice the virtual machine has been given a CSP identifier, in this case AWS.



[redacted]

Intelligent VM groups
none

Host name
[redacted]

vCenter
[redacted]

Version

July 6, 2023

1 copy | Not scanned | Recover | ami-0119306ab52...

The virtual machine will now be present at your CSP.

Conclusion

In these days of rising malware and ransomware attacks, it’s good to know Veritas NetBackup can help secure and quickly restore your data from prior to the attack. Veritas is not just your trusted on-site backup suite, it’s also your one stop shop to backup your cloud resources with simple tools that accomplish difficult tasks. NetBackup enterprise tools makes backing up your data easier and more secure than ever.

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. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

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