VERITAS

In-Cloud Data Recovery with Veritas Alta™ Recovery Vault

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

This paper is designed to highlight the steps customers will need to perform Image Sharing with Veritas Alta Recovery Vault (formerly known as NetBackup Recovery Vault).

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

White Paper | October 2023

VERITAS ALTA™

Contents

Revision History

Version	Date	Changes	Author
1.00	06/2022	Initial Version	Neil Glick
1.01	01/2023	Rebrand	Neil Glick
1.02	09/21/2023	Updates for 10.3	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 toward customers interested in learning about using Veritas Alta Recovery Vault (formerly known as NetBackup™ Recovery Vault) and Image Sharing to backup data from one site and recover it at another.

Why NetBackup Recovery Vault and Image Sharing

Image Sharing is not new to NetBackup, but with the introduction of NetBackup 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 Recovery Vault provides a fully-managed cloud data protection tier that is seamlessly integrated in NetBackup. With NetBackup 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 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 andVeritas Alta Recovery Vault to work together:

1. Image Sharing is supported on 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 a primary and a media server.
4. The Media Server Deduplication Pool (MSDP) for Image Sharing will need to be created at the alternate site.
5. When creating the MSDP storage server, the alternate primary server must be chosen—it cannot be a media server.
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. Current login credentials for AWS.

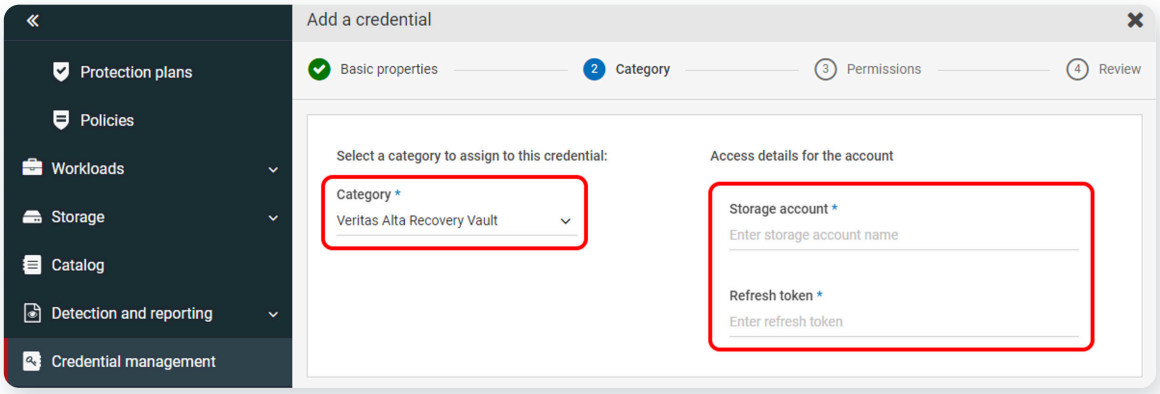
You do not need to make any changes on the primary server as long as the data you wish to copy to the alternate site is located on a Veritas Alta Recovery Vault SaaS MSDP-C disk pool. If you do not have Veritas Alta Recovery Vault, contact your Veritas NetBackup Account Manager for a demonstration and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

Short Lived Token Based Authentication

With NetBackup 10.2 onward, Veritas provides the ability to connect to Veritas Alta Recovery Vault cloud storage in Azure 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. Currently, this feature is only available for Azure users.

Creating the credential at the alternate site is the same process performed at the primary site. The Category and Storage Account will be the same, and a new refresh token will be given to you by the Veritas Provisioning Team.



This credential is then selected when connecting to your Veritas Alta Recovery Vault cloud storage in Azure.

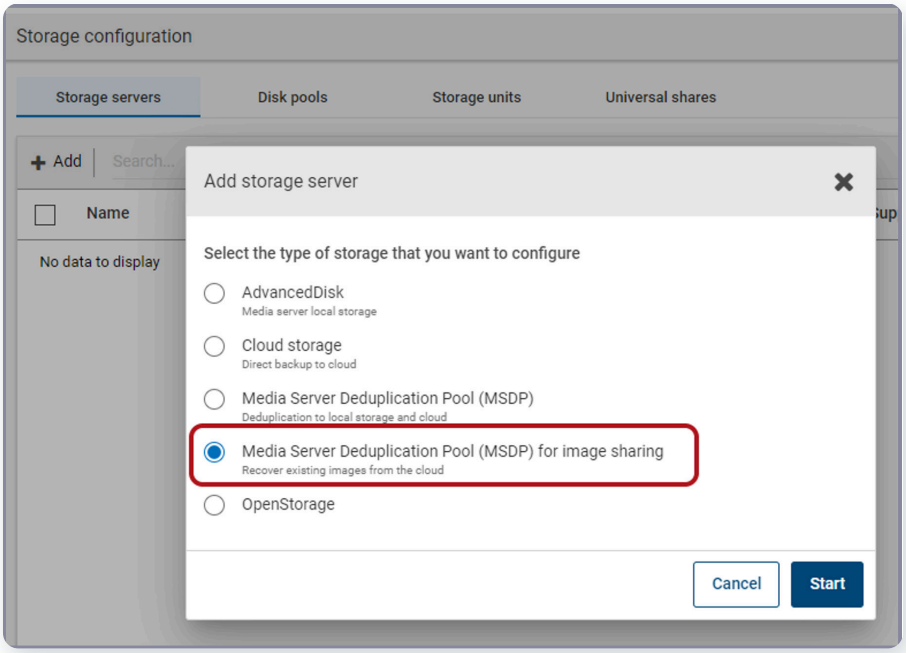
Configuring Image Sharing on Your Primary Server with Veritas Alta Recovery Vault

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 use 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.

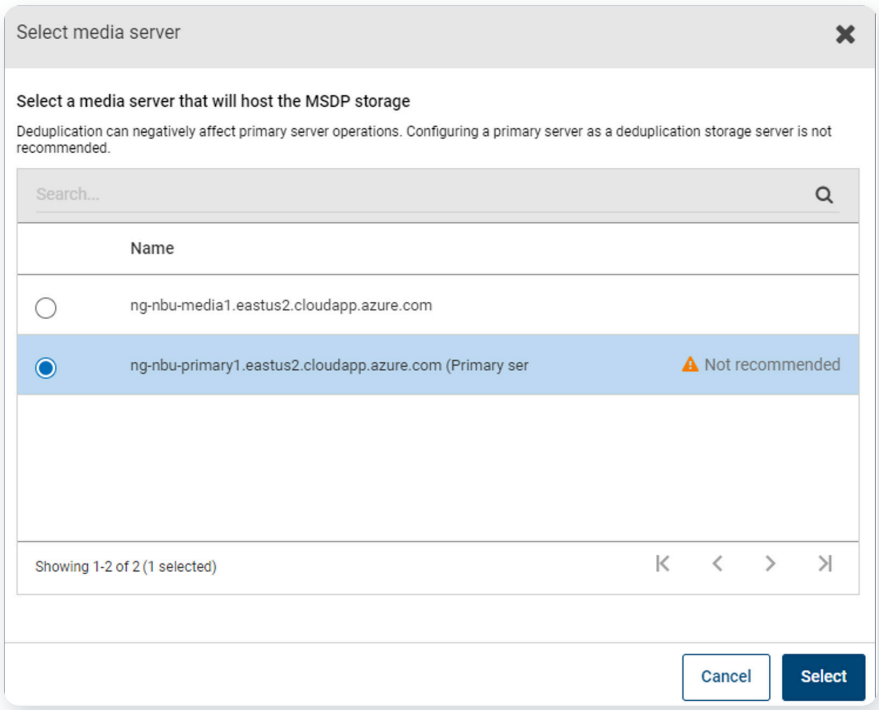
Note: To view the steps on how to connect to your Veritas Alta Recovery Vault storage, see the Veritas Alta Recovery Vault Deployment Guide.

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

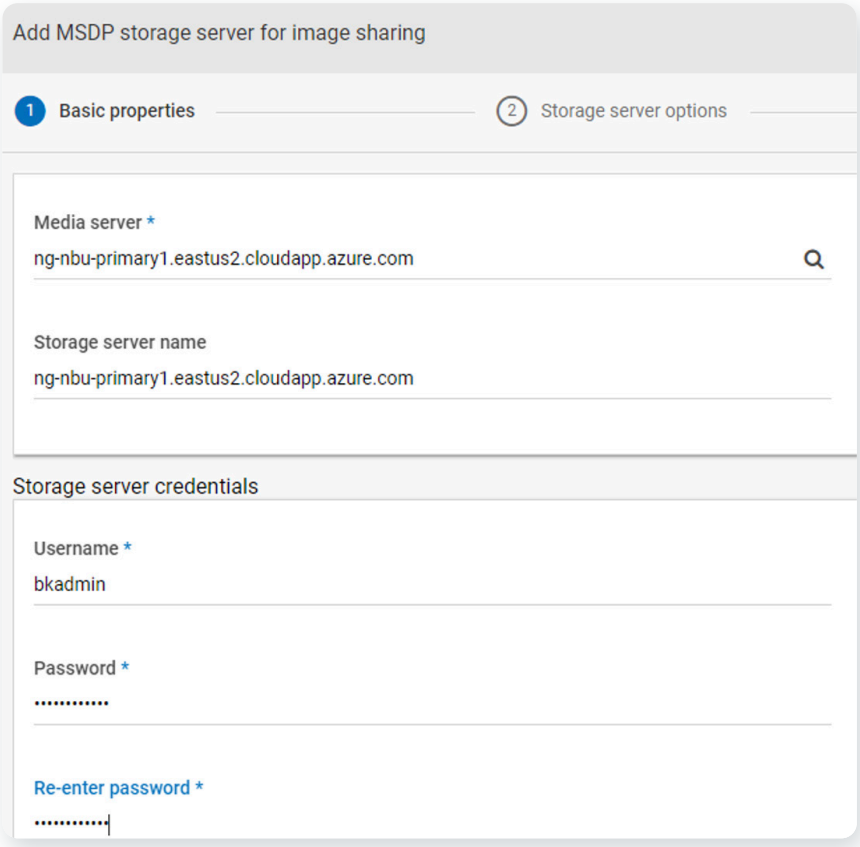
1. Log onto the alternate site and create an MSDP with an Image Sharing Storage Server.



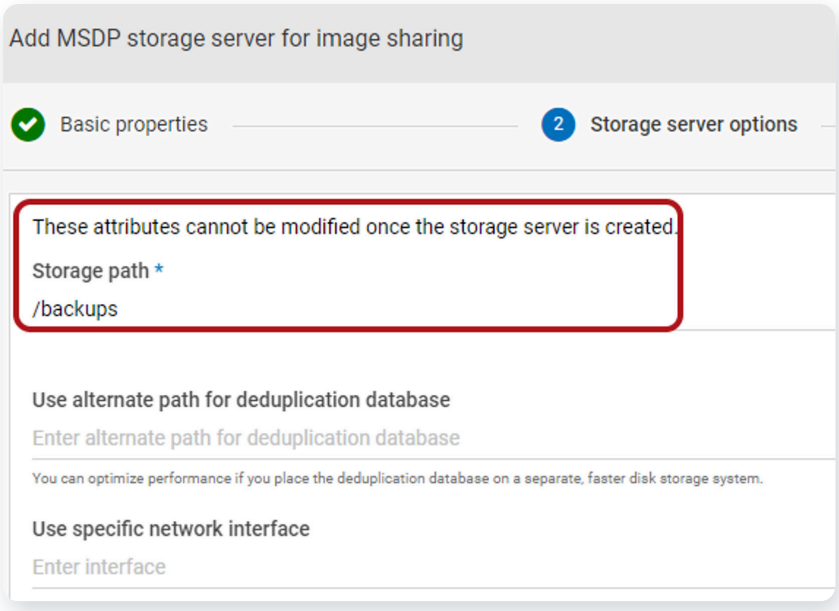
2. Next, choose the alternate primary server as the media server that will host the MSDP storage. Generally, this is not a best practice, but is mandatory for Image Sharing.



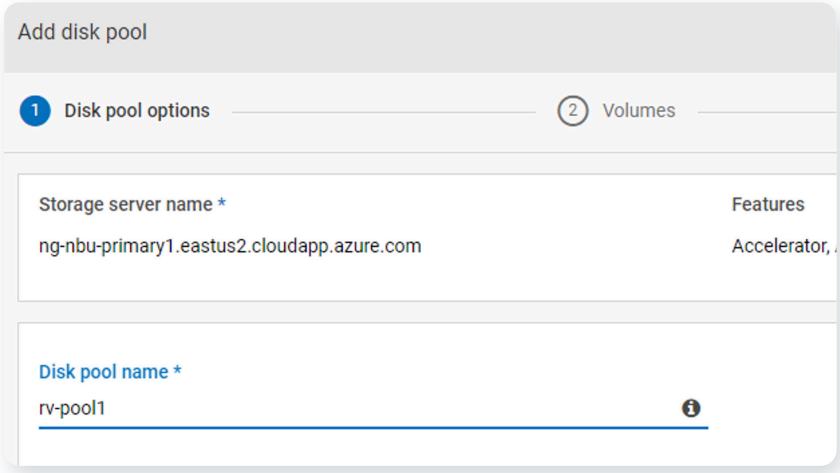
3. Enter the user name for the alternate primary server.



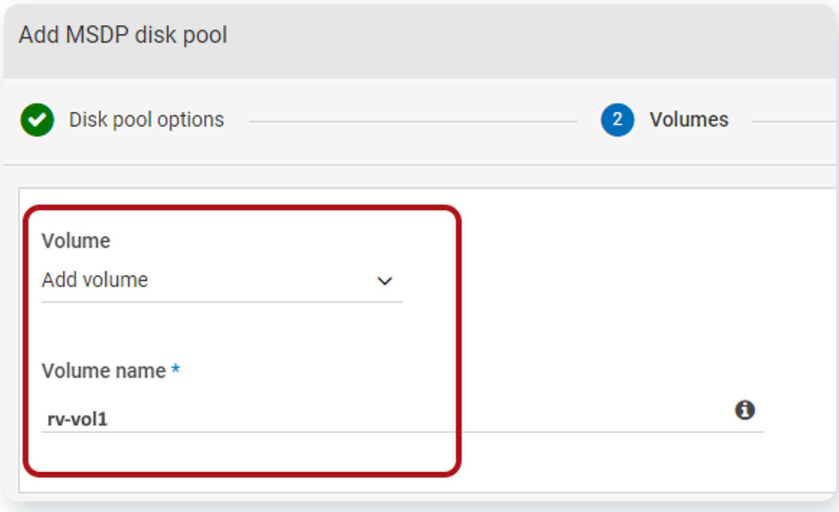
4. Enter the storage path for the MSDP for image sharing. This does not have to be the same as the MSDP server at the primary site.



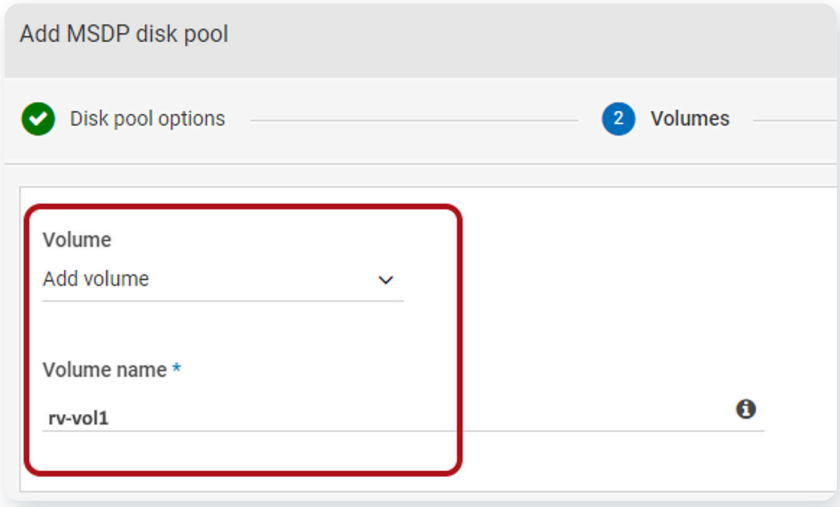
5. Once the MSDP for image sharing has been created we'll create the disk pool.



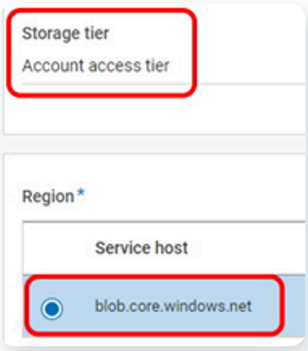
6. When creating the volume at the alternate site, it is required that it's name be the same as the volume at the primary site.



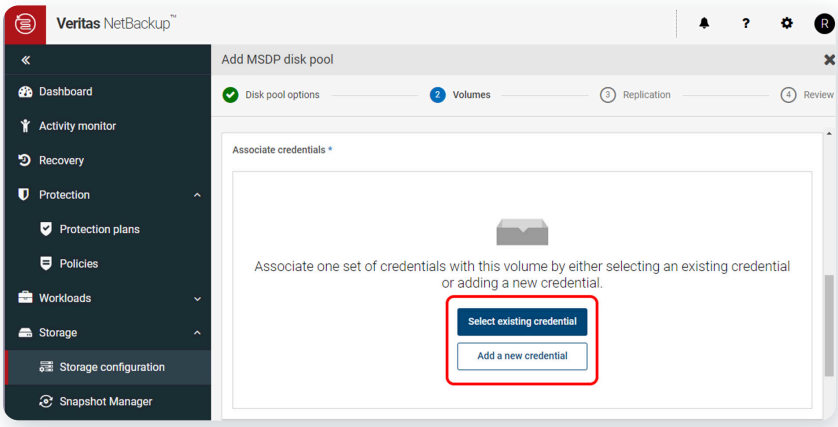
7. Use the same cloud storage provider at the alternate site as you did at the primary site. In this example we're using Veritas Alta Recovery Vault Azure.



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

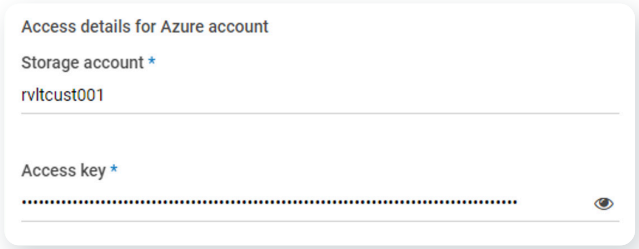


9. Click Select *existing credential* if you've already created your credential from the Short-Lived Token Based Authentication section earlier in this document. If not, click *Add a new credential* and create a new credential using the storage account and refresh token given to you by Veritas.

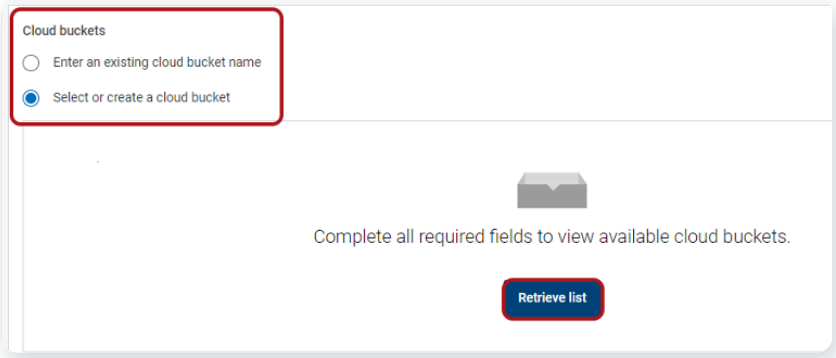


If you are using NetBackup 10.1.1 or earlier, enter the storage account and Access key for Azure.

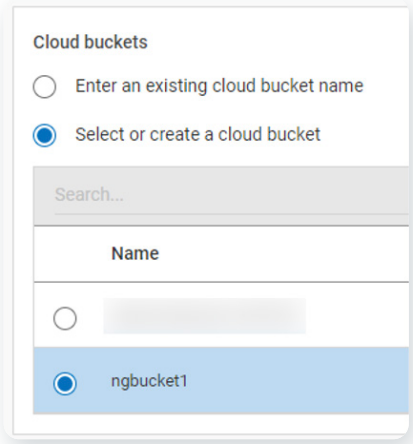
Note: The storage account, short-lived tokens, and access keys are provided by the Veritas Alta Recovery Vault provisioning team.



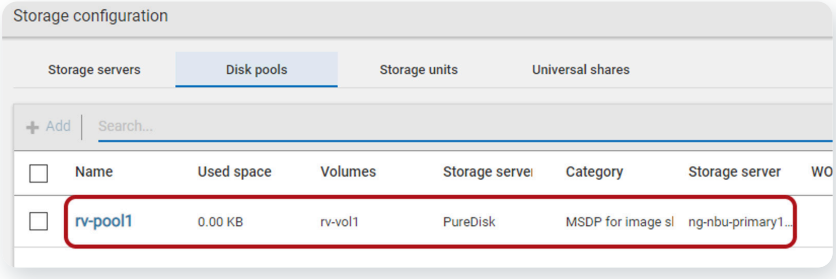
10. Once the credentials have been entered, click on Select or create a cloud bucket and *Retrieve list* to get the list of created storage buckets.



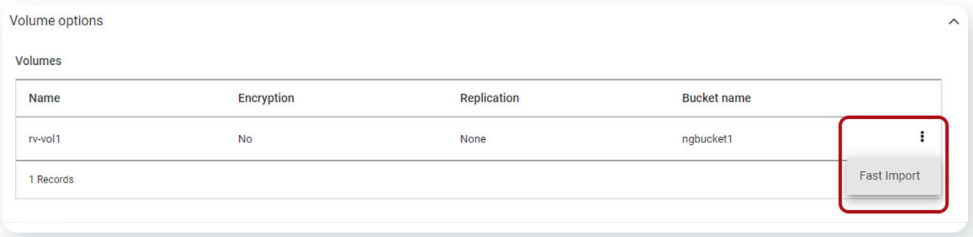
11. Select the storage bucket that you've been using at the primary site.



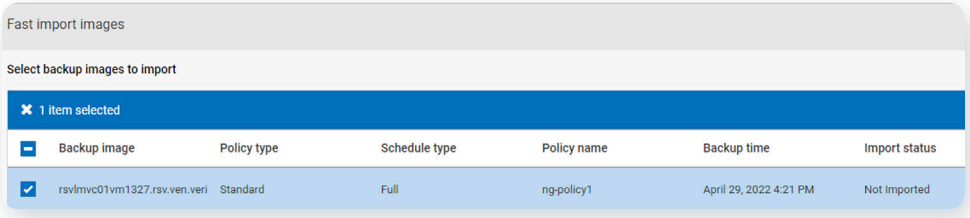
12. After the disk pool has been created, we can now import a backup from NetBackup Recovery Vault into our alternate primary server. Go to Storage Configuration > Disk Pools and click on the disk pool you just created.



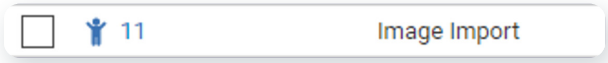
13. Under the *Volume Options*, click on the three vertical dots and select *Fast Import*.



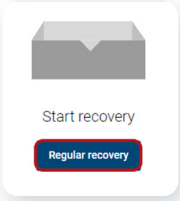
14. Select the backup you'd like to import and click on the *Import* button (not shown).



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



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

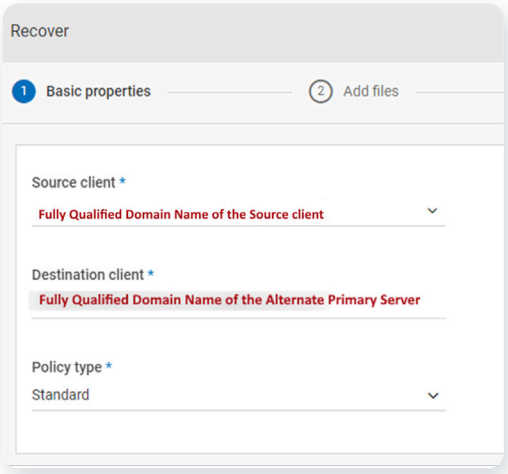


17. Enter the following information:

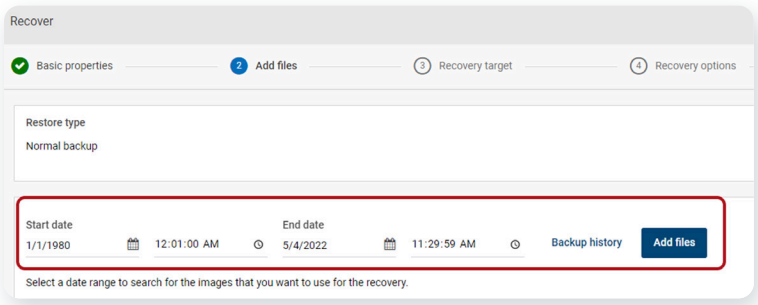
    a. *Source client:* Enter the fully qualified domain name of the primary server.

    b. *Destination client:* Enter the fully qualified domain name of the alternate primary server.

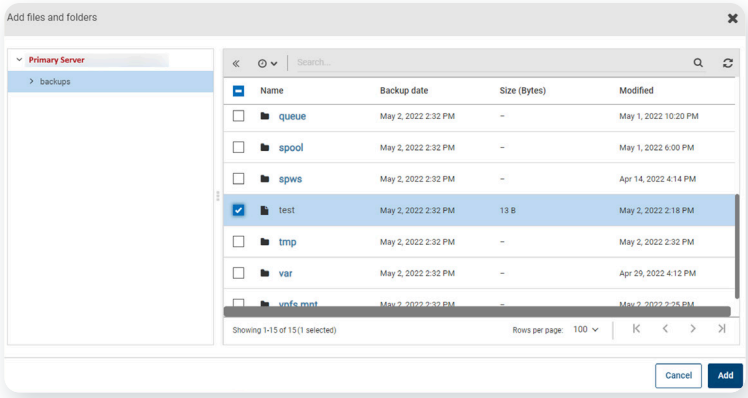
    c. *Policy type:* Select the type that was used to back up the data at the primary server. In this example it is *Standard*.



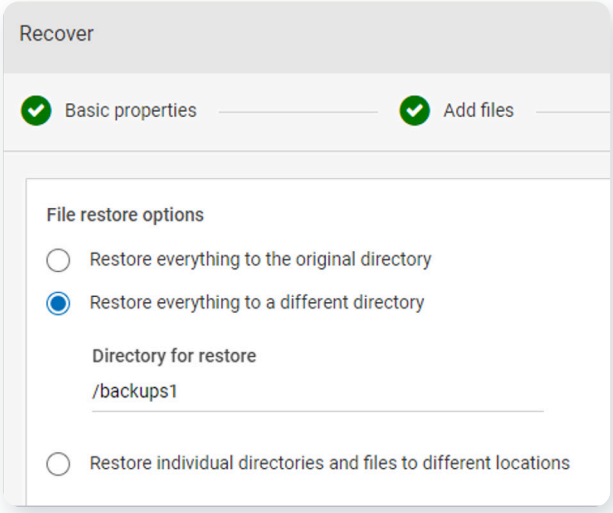
18. Enter the time and data of the backup and click on *Add files*.



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



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



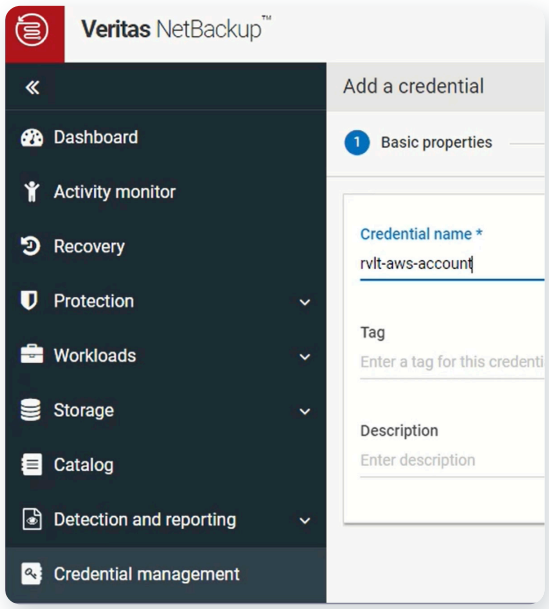
21. When you're happy with the restore selections, click on the *Start recovery* button to begin the restore.

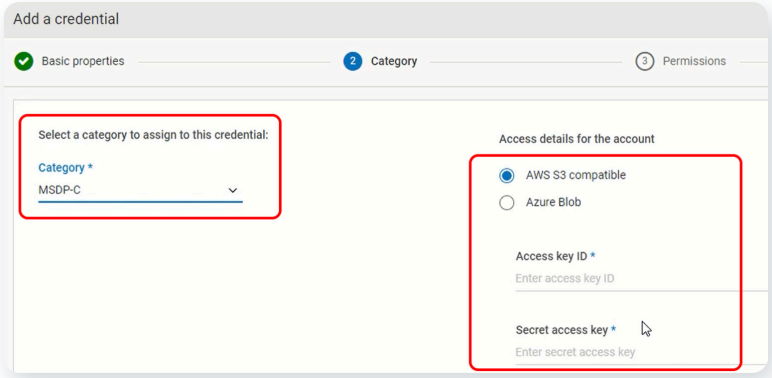
VMWare Conversion on AWS and Azure with Veritas Alta Recovery Vault

In versions prior to NetBackup 10.3, when recovering a VMware virtual machine from Veritas Alta Recovery Vault, the data store will assume the same accounts. However, Veritas 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 convert the Veritas Alta Recovery Vault backup image and import into. To accomplish the conversion:

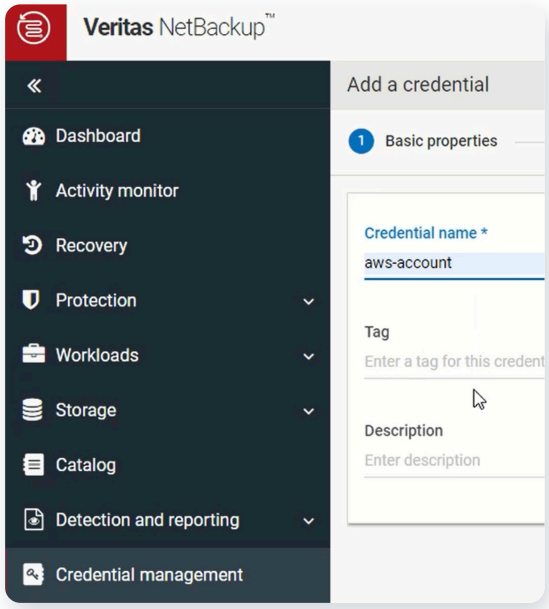
1. Create a secondary primary or a cloud recovery server (CRS) as completed in this document.

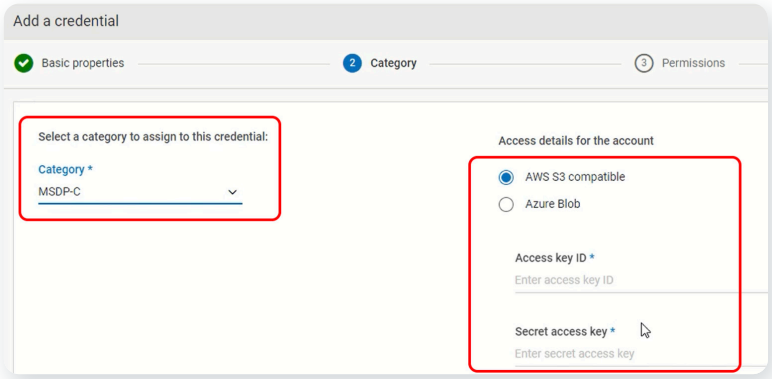
2. Create a Veritas Alta Recovery Vault credential for your Veritas Azure or AWS storage bucket, making sure to set the Category as MSDP-C, and enter in the credentials for AWS or Azure.



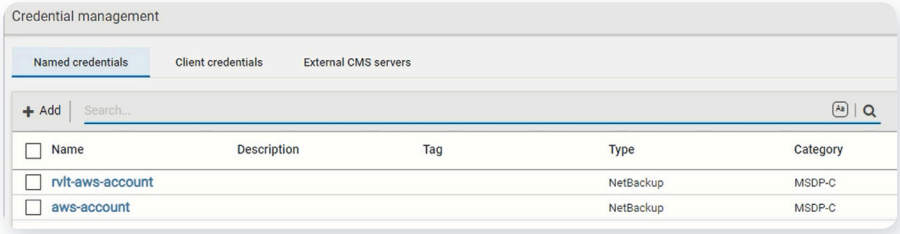


3. Next, create another credential, but this time choose the cloud provider that you'd like to import the VMware virtual machine into. Make sure to select *MSDP-C* as the *Category*, select your cloud provider, and enter your credentials.



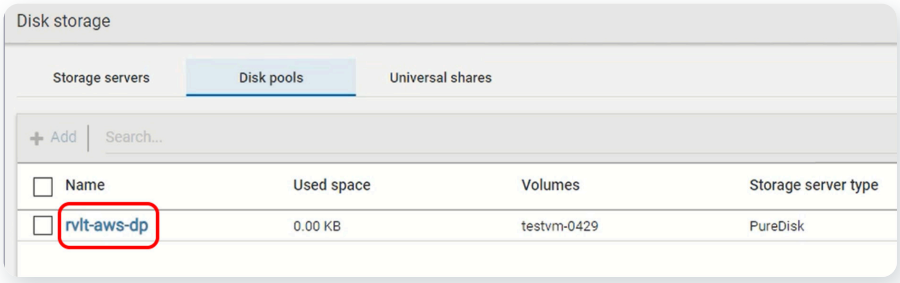


4. You should see something similar with one credential to your Veritas Alta Recovery Vault storage that has the backup image of the VMware virtual machine and another where the backup image will be imported into.

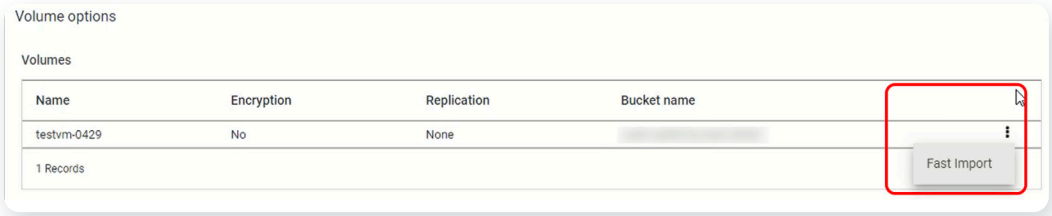


5. Next, connect to the Veritas Alta Recovery Vault storage that contains the VMware virtual machine, ensuring that you use the same volume name that was used when first connecting to the storage bucket (as seen in this document).

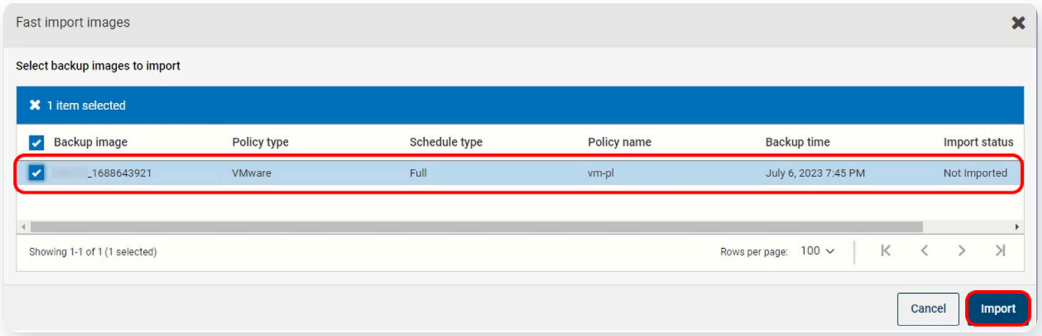
6. Once the disk pool and volume have been created, click on the disk pool to see its details.



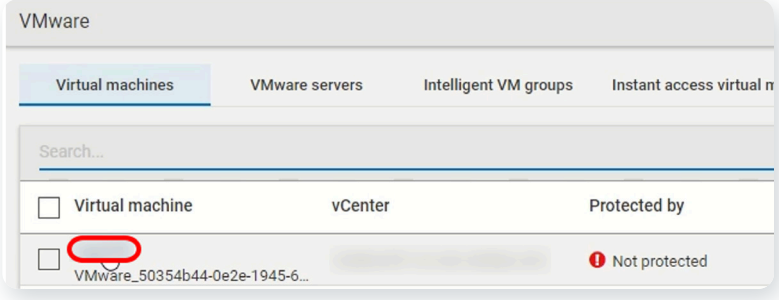
7. Find the *Volume Options* section and click on the three dots. Then on *Fast Import*. This will import the backup image on the Veritas Alta Recovery Vault storage.



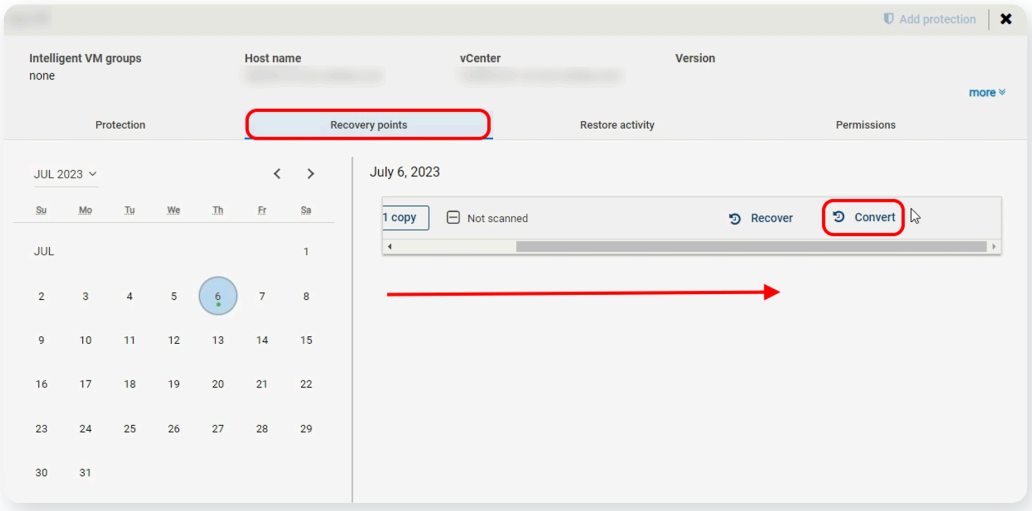
8. Select the backup image with the VMware virtual machine and click on *Import*.



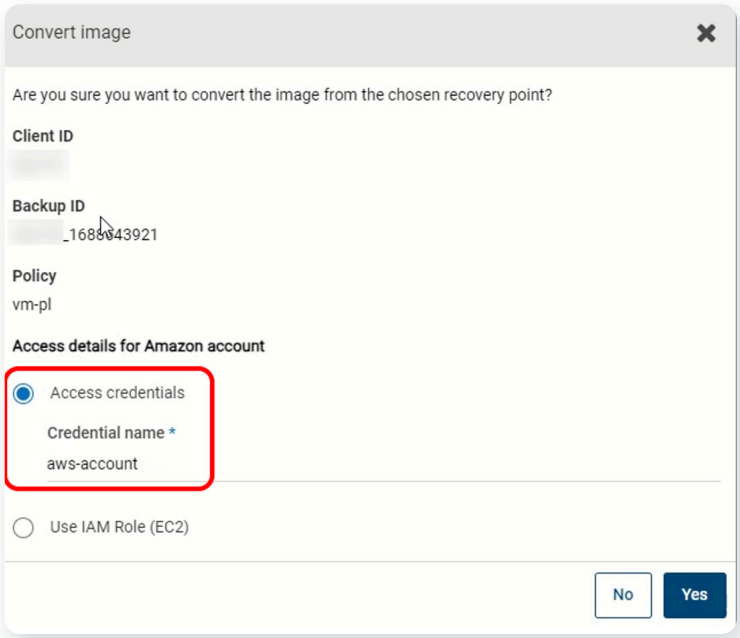
9. Navigate to *Workloads* > *VMware* in the NetBackup WebUI. The virtual machine from the Veritas Alta Recovery Vault storage should now appear. Click on the virtual machine.



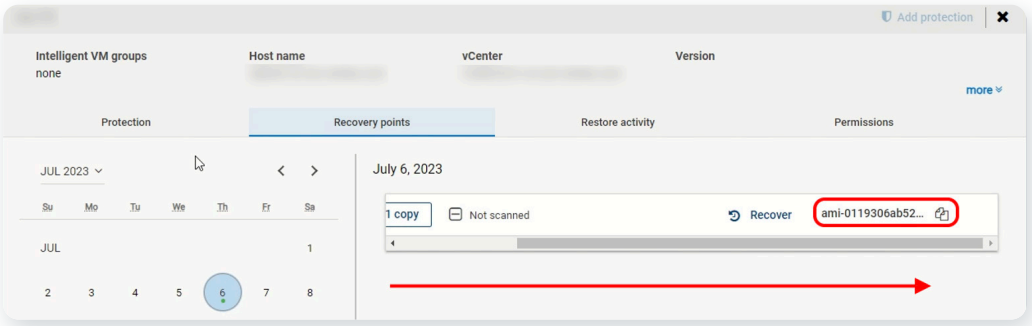
10. Click on the *Recovery Points* tab, select the date and the backup. Scroll to the right and click on the *Convert* button.



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



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



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 that 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 back up your cloud resources, with simple tools that accomplish difficult tasks. NetBackup enterprise tools make 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 www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

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

For global contact information visit:
veritas.com/company/contact

V1573 10/23