VERITAS

In-Cloud Data Recovery with NetBackup Recovery Vault

Disaster Recovery for Storage-as-a-Service.

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

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

White Paper | June 2022

Contents

Revision History

Version	Date	Changes	Author
1.00	06/2022	Initial Version	Neil Glick

Introduction

Executive Summary

NetBackup™ Recovery Vault is a cloud-based storage-as-a-service offering that provides a seamless, fully managed secondary storage option for NetBackup customers. Seamlessly integrated with NetBackup, it provides an easy-to-use UI that simplifies provisioning, management, and monitoring of cloud storage resources and retention policies. Most NetBackup Recovery Vault customers will want to use Image Sharing, which is a feature in NetBackup that packages a minimal set of metadata with all backup data to make it self-describing. This allows backup data to be restored from a primary location onto a NetBackup primary server in an alternate domain or cloud environment to meet data compliance and governance requirements.

Target Audience

This document is targeted at customers interested in learning about using NetBackup Recovery Vault and Image Sharing to backup data from one site and recover it at another.

Why NetBackup Recovery Vault and Image Sharing

NetBackup Recovery Vault provides a fully managed cloud data protection tier that is seamlessly integrated with NetBackup to scale protection across any cloud model, while controlling costs. NetBackup Recovery Vault can use NetBackup Image Sharing to copy data from a primary site to an alternate site in a different domain or in the cloud. With NetBackup Recovery Vault and Image Sharing, you can copy your mission-critical data and restore it using a completely autonomous primary server located off-site. In the event the primary server is compromised, your mission-critical data can be converted to the alternate site to continue to meet data compliance and governance requirements.

Image Sharing and Recovery Vault Prerequisites and Requirements

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

1. 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.
2. The Media Server Deduplication Pool (MSDP) for Image Sharing will need to be created at the alternate site.
3. When creating the MSDP storage server, the alternate primary server must be chosen, which cannot be a media server.
4. The name of the backup volume used at the alternate site must match the name of the volume at the primary site.
5. The NetBackup Recovery Vault cloud bucket used for primary backups will need to be used at the alternate site.
6. NetBackup Recovery Vault account credentials will need to be available or already in use.

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 NetBackup Recovery Vault SaaS MSDP-C disk pool. If you do not have NetBackup Recovery Vault, contact your Veritas NetBackup Account Manager for a demonstration and additional documentation on the benefits of the SaaS offering.

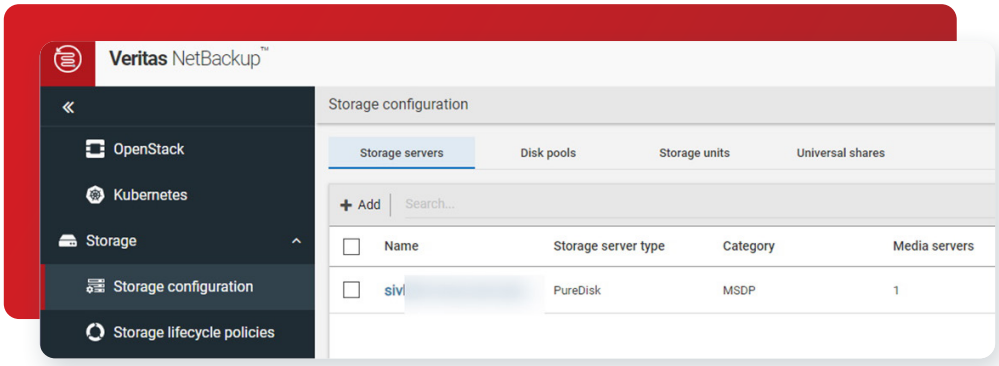
Configuring Image Sharing on Your Primary Server With Netbackup Recovery Vault

If new to NetBackup 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 NetBackup Recovery Vault, backed up data can be imported to an alternate site using Image Sharing. The example used in this document connects to NetBackup Recovery Vault in an Azure cloud environment. This document assumes the customer already has an MSDP storage server created at the primary site. For more information on how to add a storage

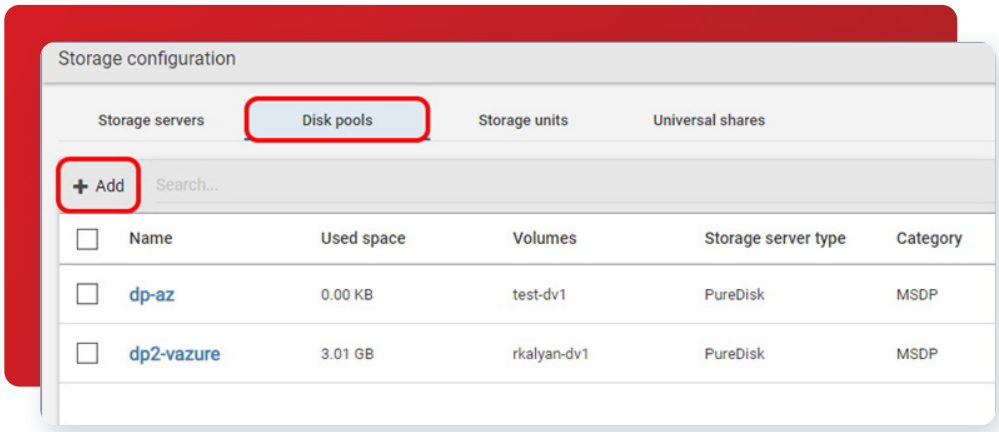
server, see the NetBackup Deduplication Guide:
https://www.veritas.com/content/support/en_US/doc/25074086-146020141-0/v24630236-14602014.

1. To get started, from within your NetBackup primary server web UI, navigate to **Storage > Storage configuration**.

   You should see your storage server(s) listed.



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



3. From this screen you will set the disk pool options:

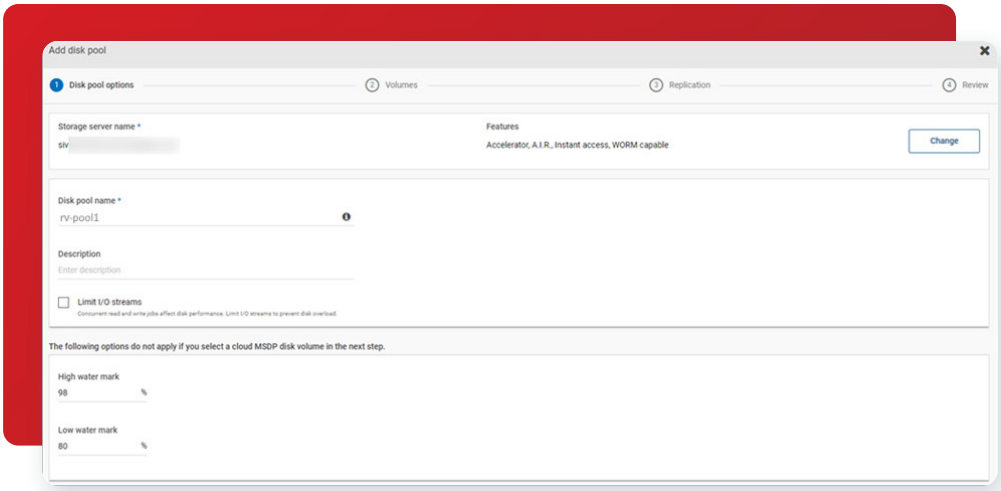
   a. Select the **Storage server name** where this disk pool will reside. In this example, we've chosen the storage server listed on the first screen.

   b. Provide a name for the disk pool. We've named it: **"rv-pool1"**.

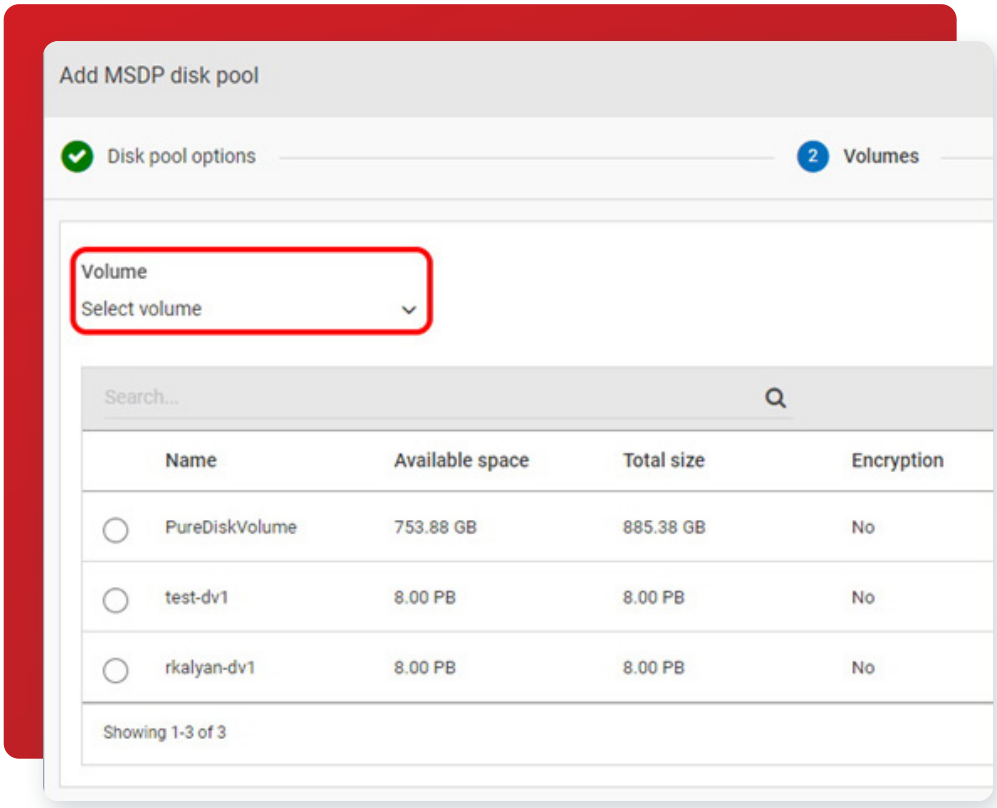
   c. Provide a description of the pool, if needed.

   d. Select **Limit I/O** streams, if desired. This option could help limit disk I/O contention.

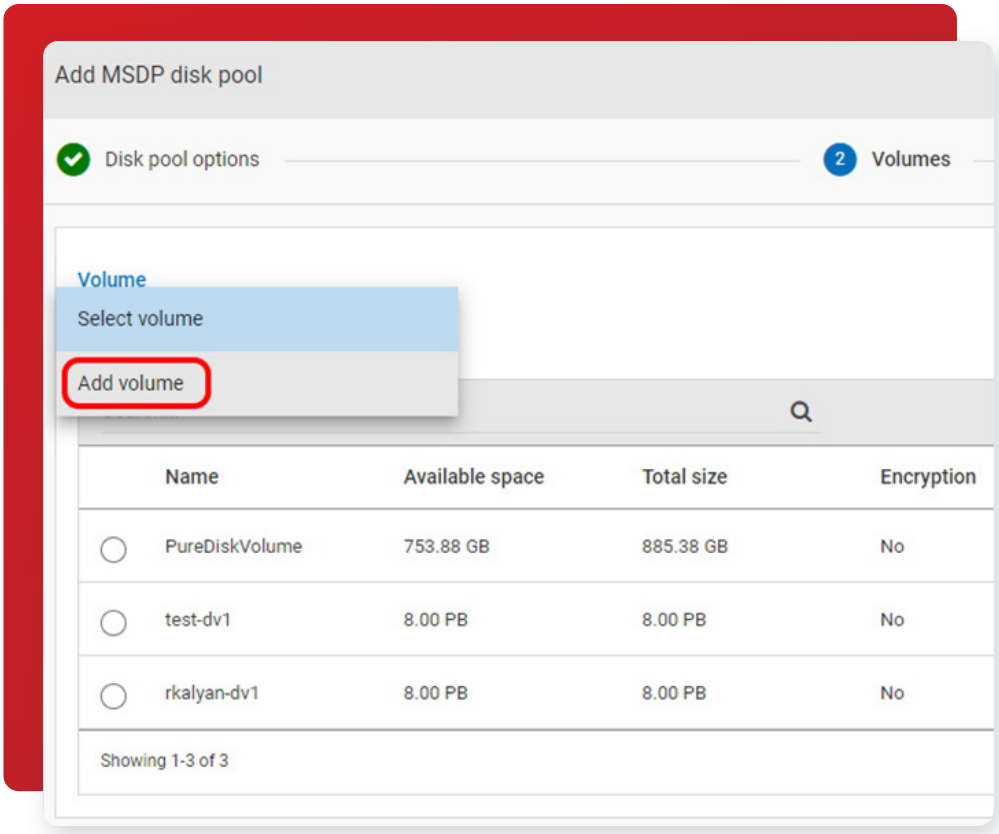
   e. Click **Next** at the bottom of the page to continue.



4. Next, you will need to define a new volume. From the Volumes page, you may already have volumes created (in the example screen below, there are three), but you will want to add a new one for NetBackup Recovery Vault, so click **Volume> Select volume**.

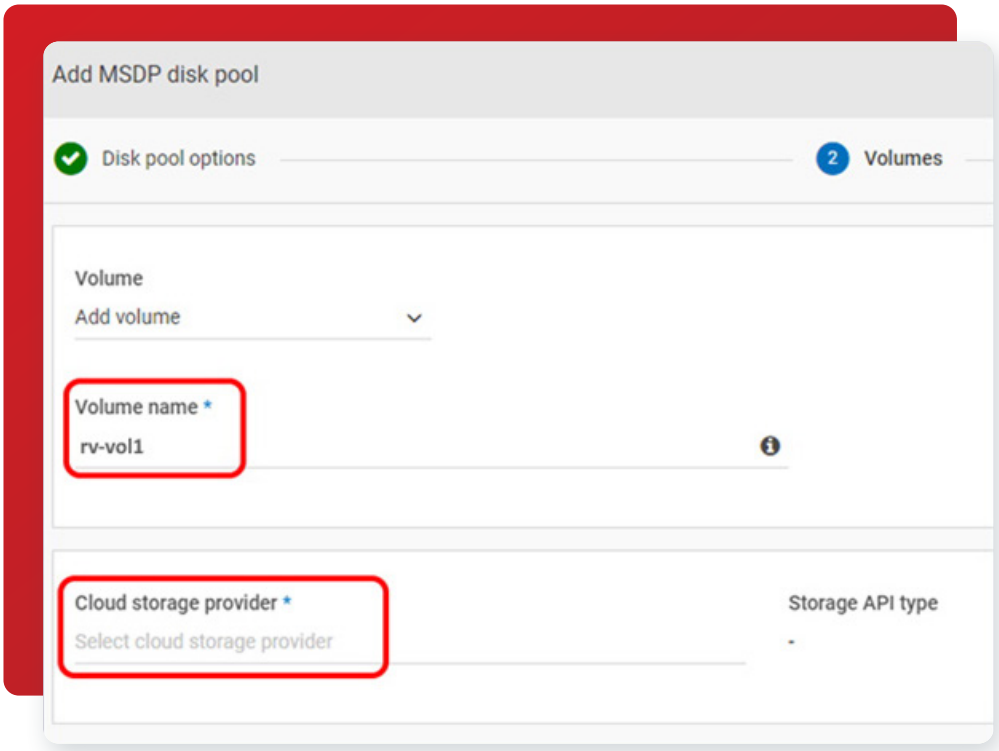


5. Click **Add volume** to begin the process.

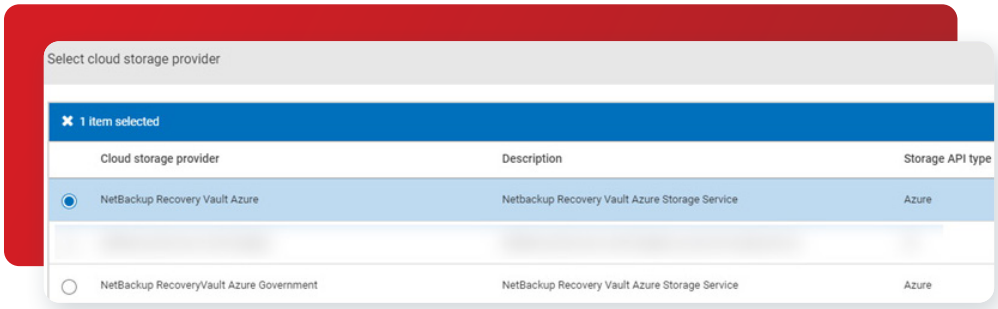


6. Provide a **Volume name** for the new volume and then click **Cloud storage provider**.

Note: The volume name at the primary site and the volume name at the alternate site must be the same.

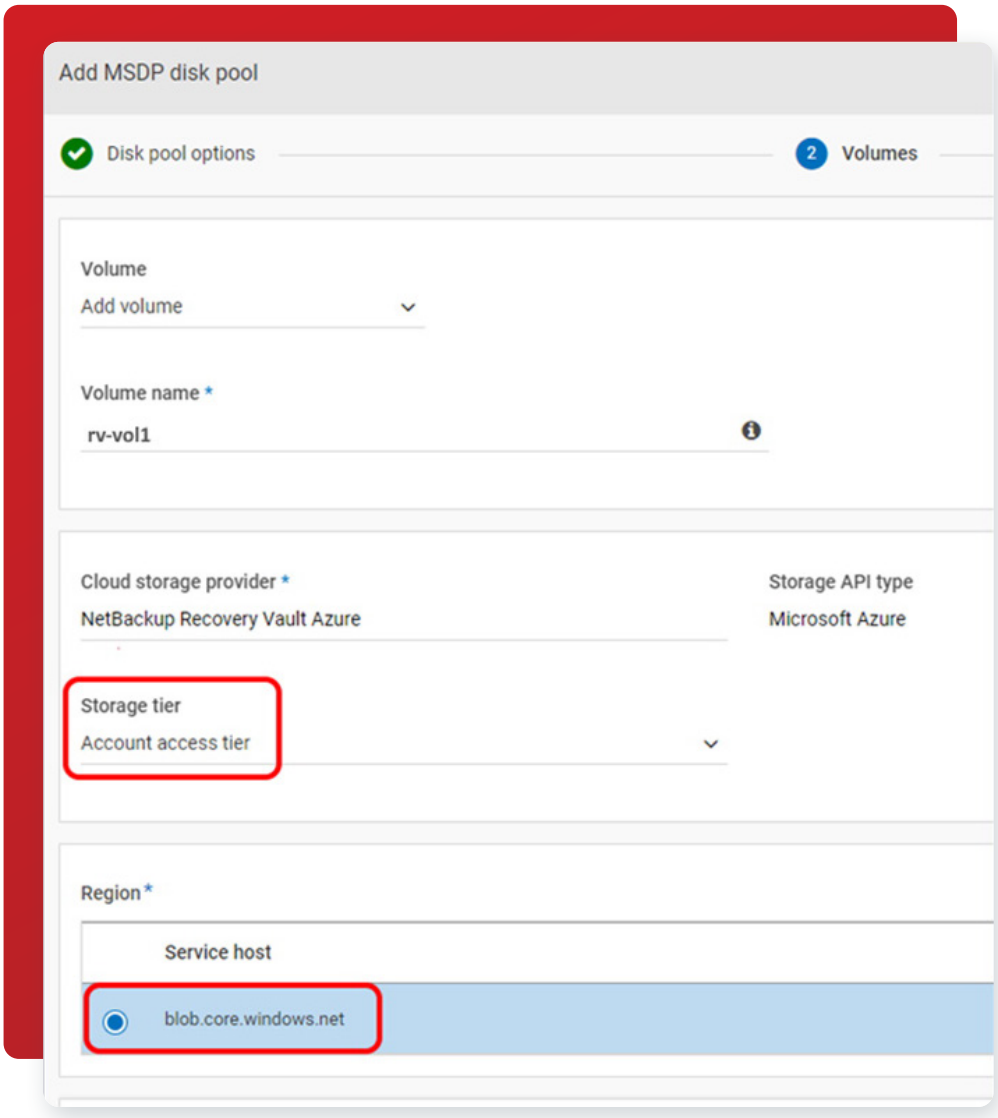


7. Search for **"Netbackup Recovery Vault."** In this example, we will choose **NetBackup Recovery Vault Azure**.



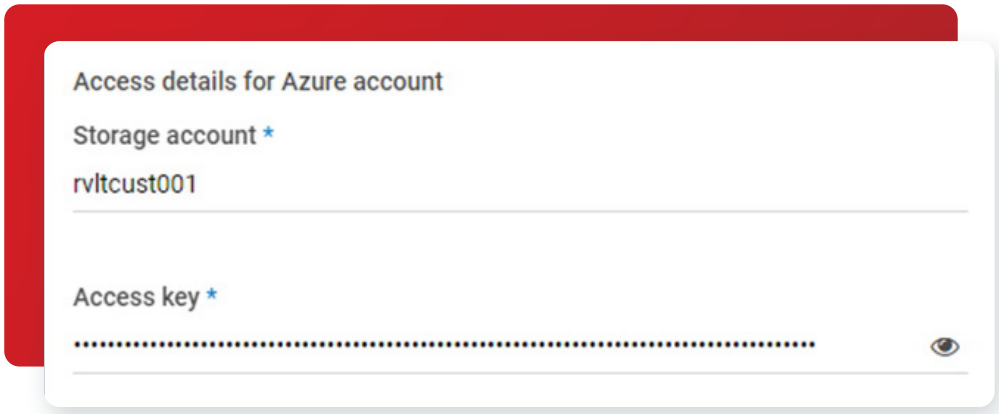
8. On the **Add MSDP disk pool** screen, select the appropriate **Storage tier** and **Region** to be used.

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

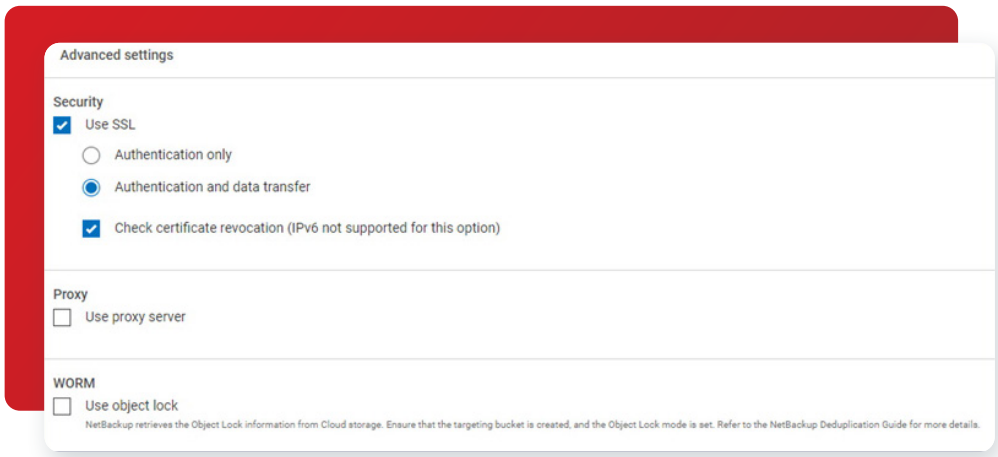


9. Next, enter the **Storage account** and **Access key**.

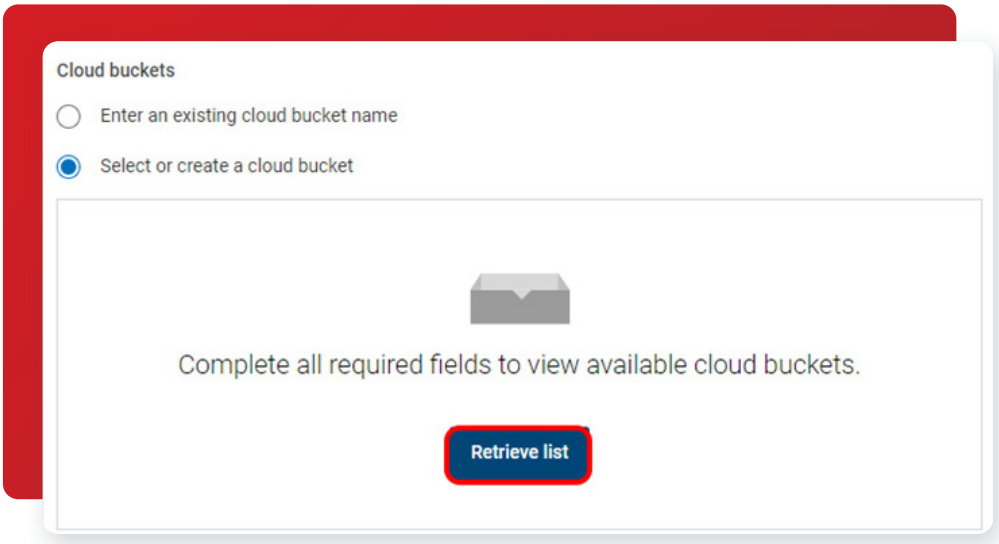
Note: The Veritas Recovery Vault Provisioning Team will provide these.



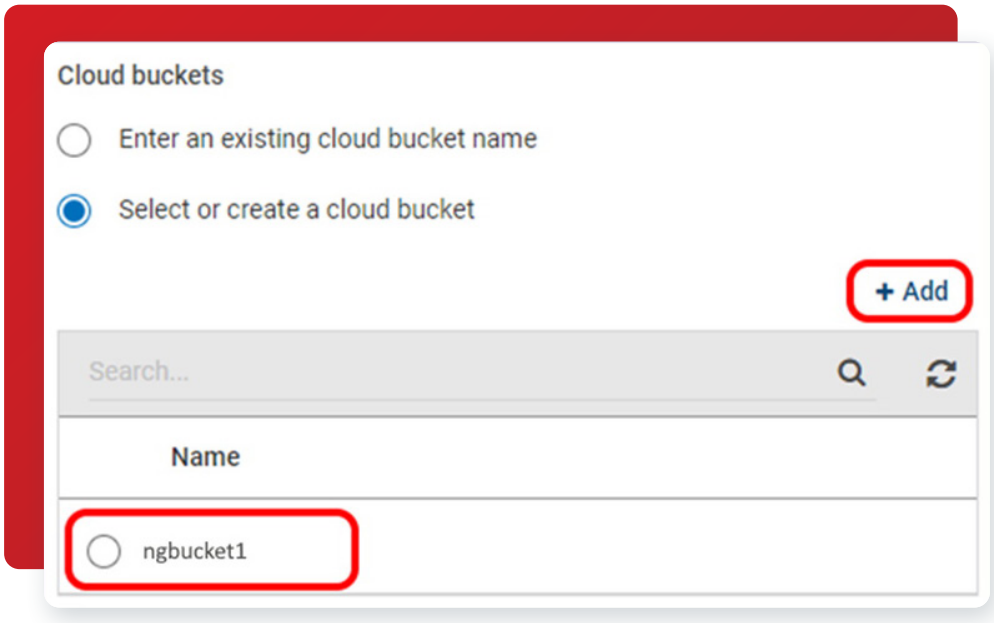
10. Next, enter the required **Security**, **Proxy**, or **WORM** advanced settings preferences. Below are the default settings:



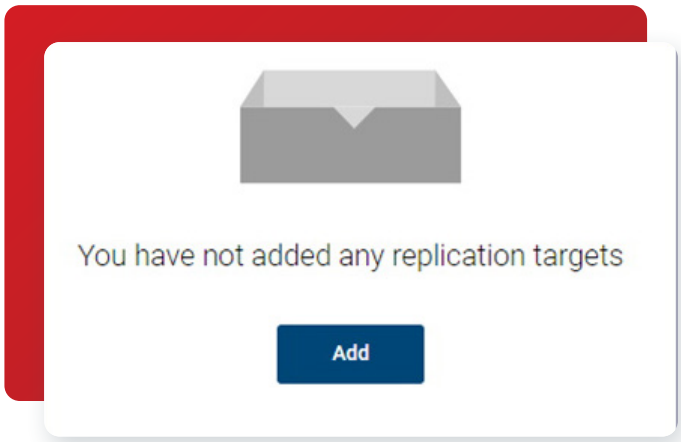
11. Click **Select or create a cloud bucket** and then click **Retrieve list**. This process logs into your cloud storage provider (in this case Azure) using the credentials entered earlier and displays the new cloud bucket you created (with Microsoft Azure Storage Explorer or equivalent).



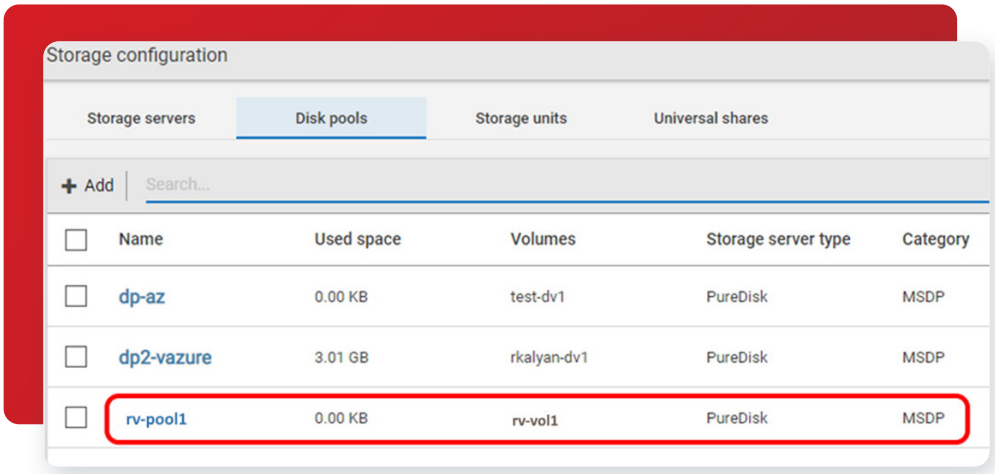
12. Select the new cloud storage bucket you created (with Microsoft Azure Storage Explorer or equivalent) from the list retrieved by NetBackup. You can also create a new bucket using the **+ Add** button after connecting to the new storage account. In our example, we are going to select **"ngbucket1"**. Of course, the name of your cloud bucket will be different, the one below is for reference only.



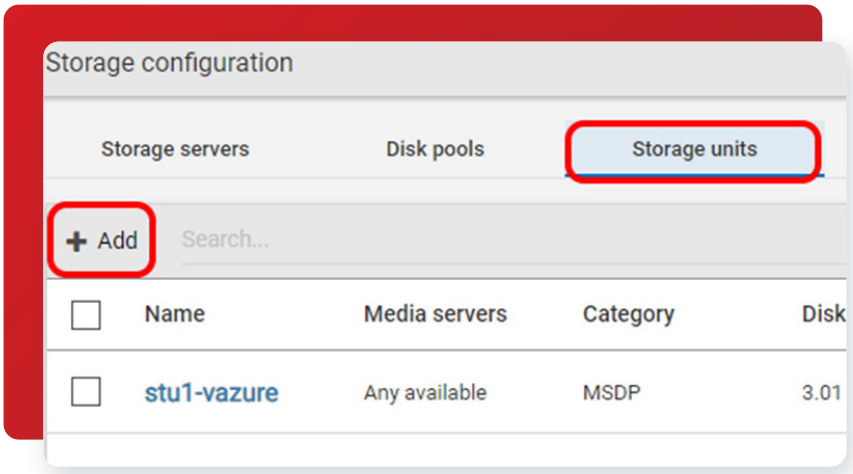
13. If you would like to set up replication targets, you can do that now. Otherwise, click Next (not shown in image below).



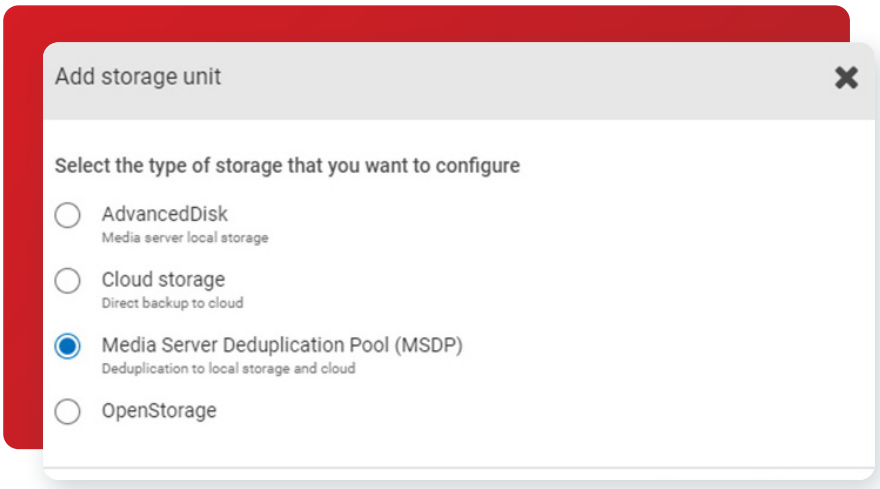
14. This brings you to the summary page. If everything looks good, you can create the new disk pool. In this example, we created the new **"rv-pool1"**.



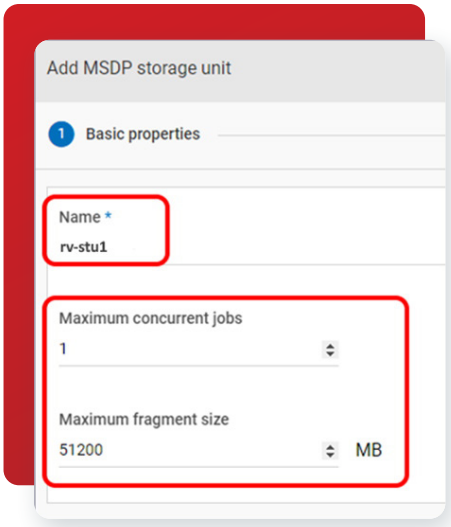
15. Next, you will need to add a storage unit, so you can use your new NetBackup Recovery Vault storage. Click the **Storage Units** tab and click **+ Add**.



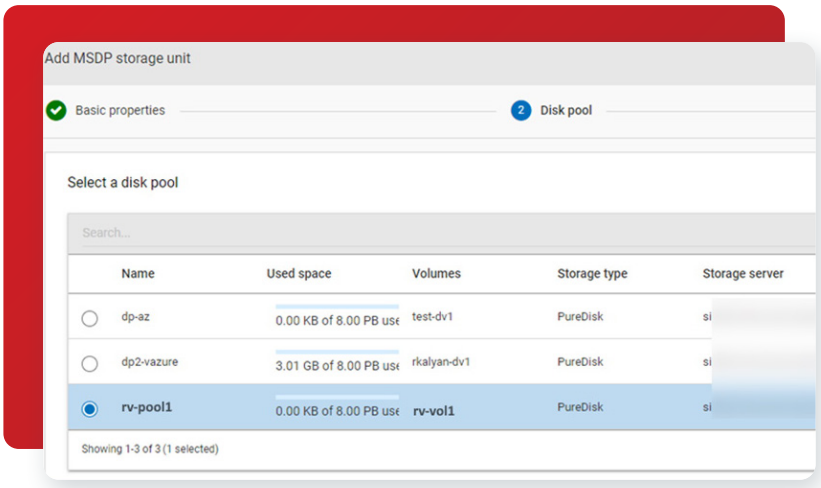
16. Select **Media Server Deduplication Pool (MSDP)** and click **Start**.



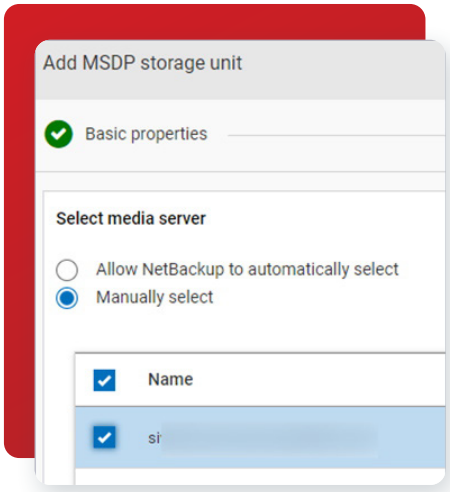
17. Provide the new MSDP storage unit a **Name** and select the **Maximum concurrent jobs** and **Maximum fragment size** you want. Click **Next** to continue.



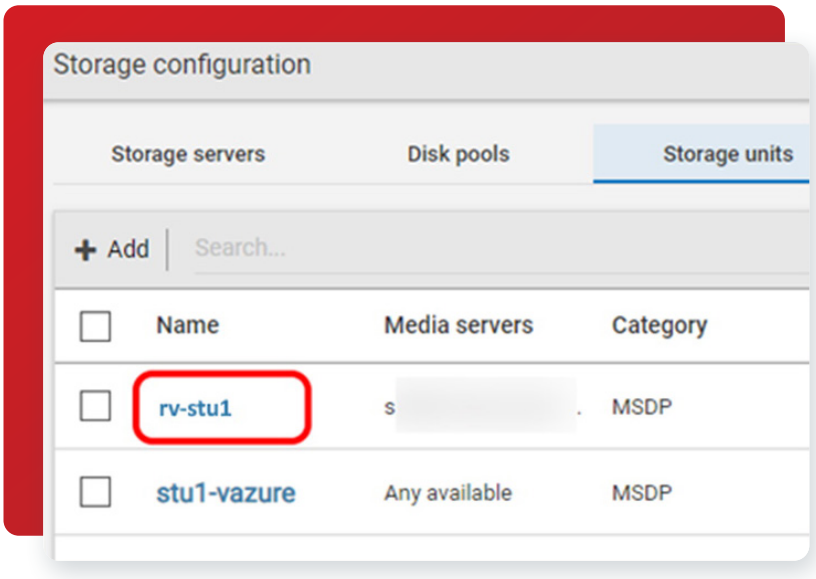
18. Select the NetBackup Recovery Vault volume you created earlier and then click **Next** to continue.



19. Select the media server you wish to use and then click **Next** to continue.



20. As shown, you can see the new **"rv-stu1"** storage unit was successfully created.



21. Next, you will need to create a backup policy so Image Sharing will have data that needs to be sent to your alternate site. Located under **Protection > Policies** you will **Create policy**:

    a. Name the policy.

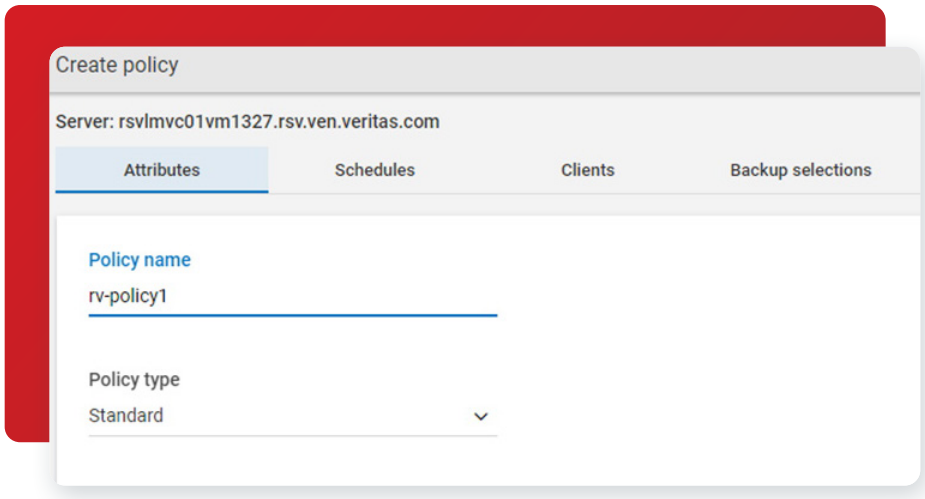
    b. Choose the policy type.

    c. Create a schedule.

    d. Select the client(s) to be backed up.

    e. Choose what should be backed up on the clients.

    f. Click on Create when ready. (Not shown)

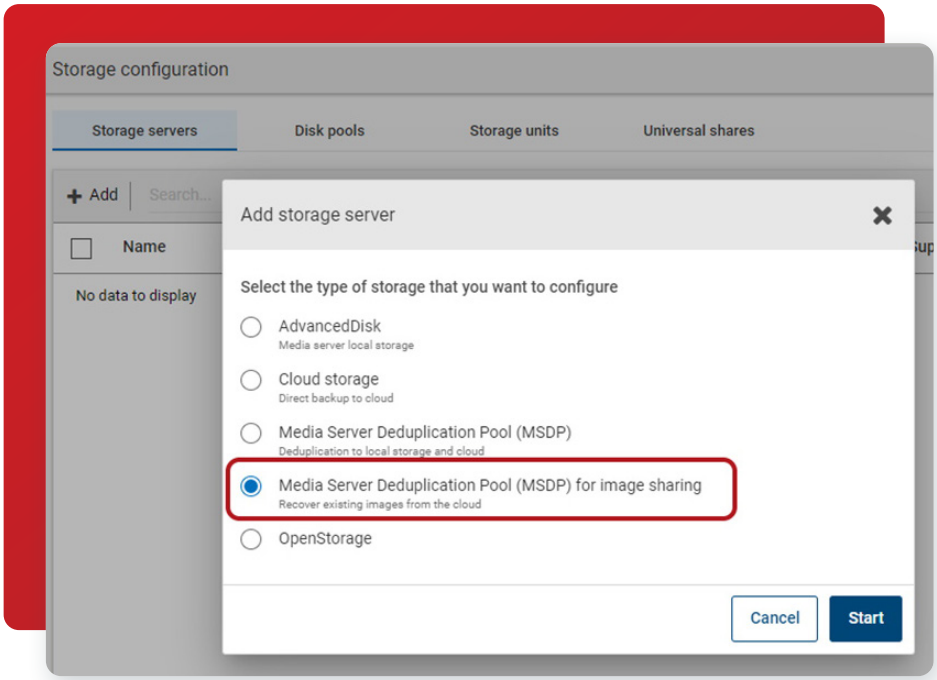


Running a Manual Backup in NetBackup Recovery Vault With Image Sharing

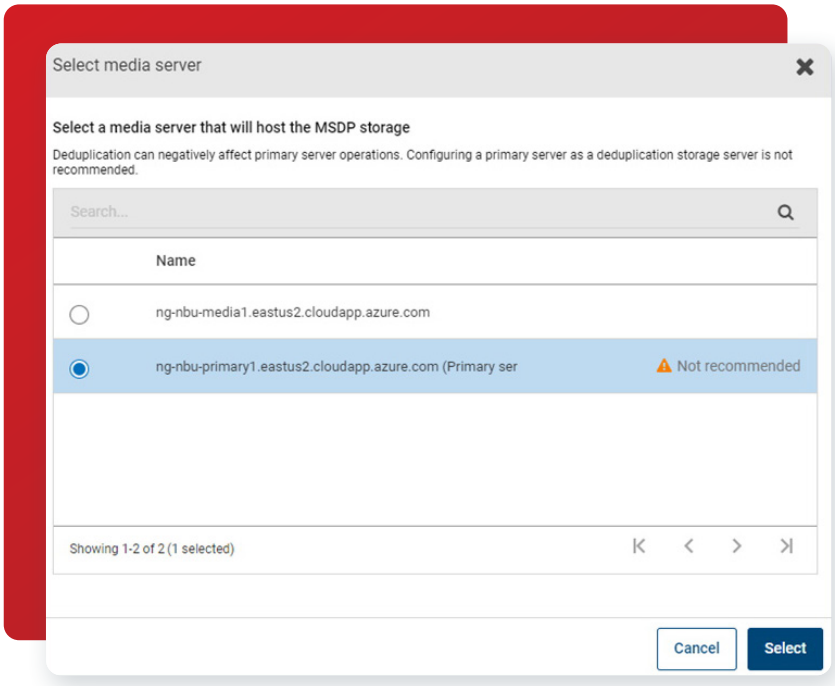
The next step is to take a manual backup to populate NetBackup Recovery Vault with the data you would like to copy to your alternate site. If you've already been using NetBackup Recovery Vault and have data backed up, this step is unnecessary.

Once the backup has run, the backup can be imported to the alternate site using Image Sharing. To do this:

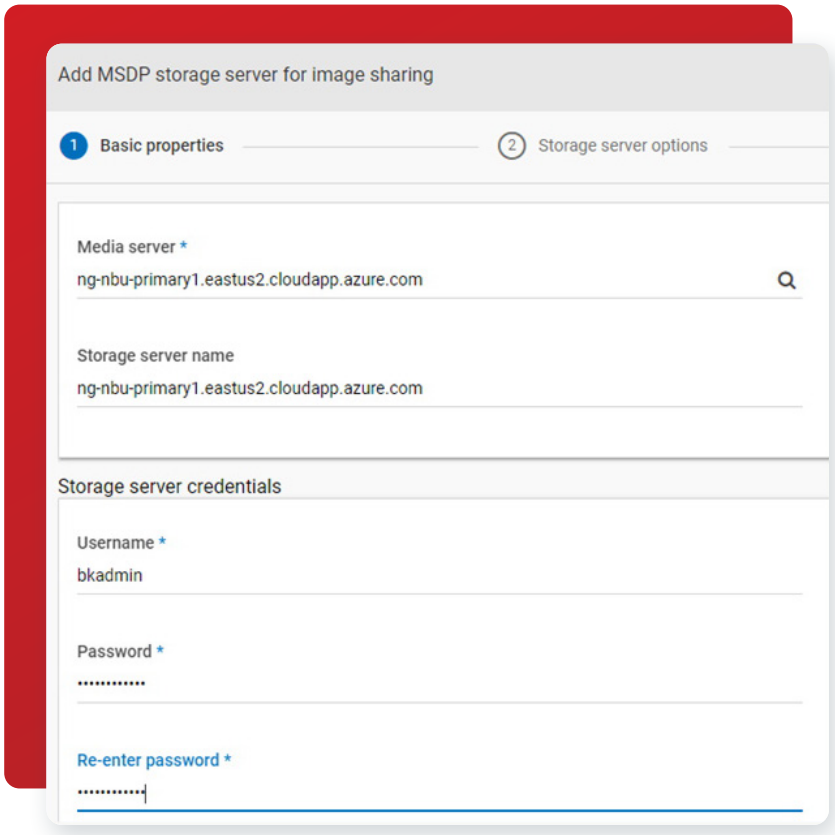
1. Log onto the alternate site and create an MSDP with an Image Sharing storage server. Select **Media Server Deduplication Pool (MSDP) for image sharing** and click **Start**.



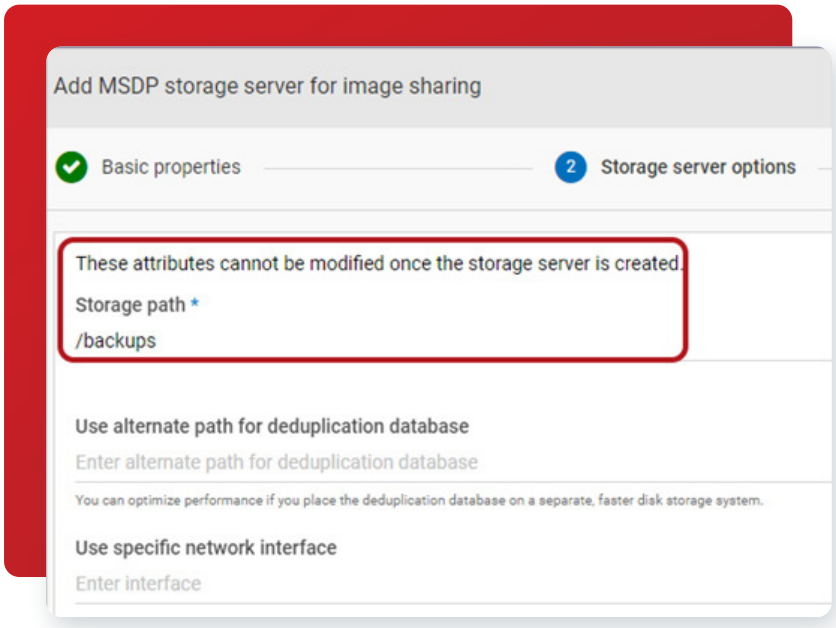
2. Next, selectthe **media server that will host the MSDP storage**. Traditionally, this is not a best practice but is mandatory for Image Sharing.



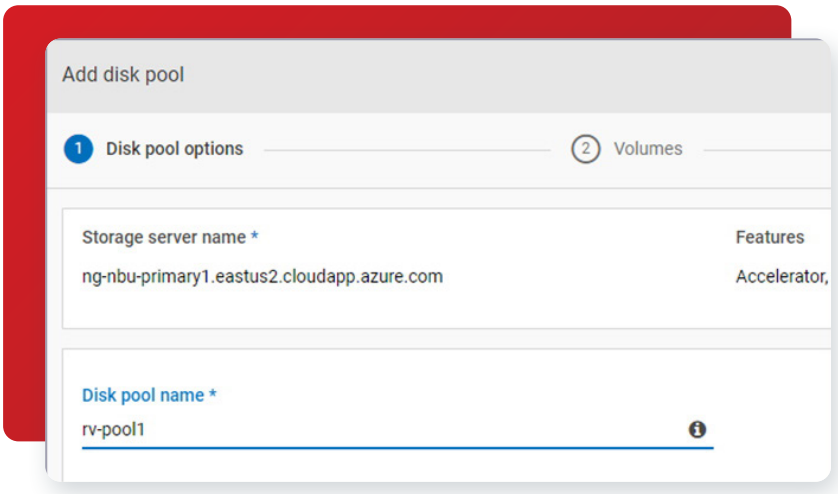
3. Enter the **Storage server credentials**: **Username** and **Password**.



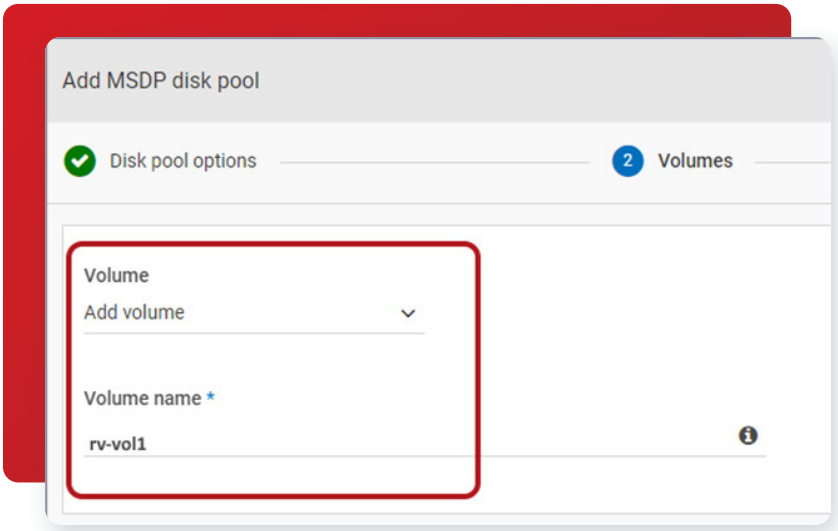
4. Enter the storage path for the MSDP for Image Sharing. This does not have to be the same as the MSDP server at the primary site.



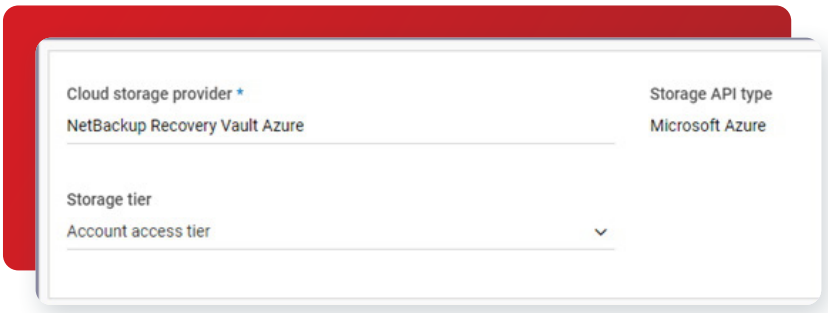
5. Once the MSDP for image sharing has been created you will need to create the disk pool.



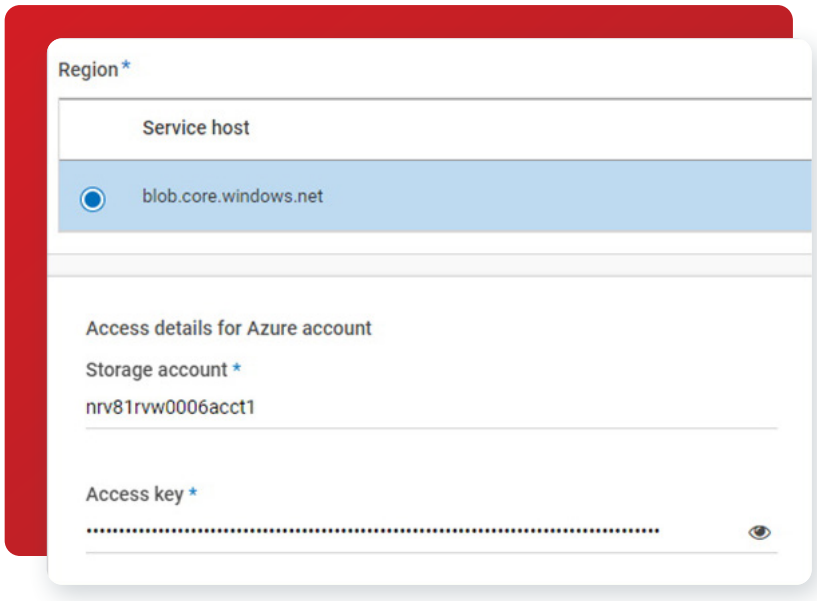
6. Remember, when creating the volume at the alternate site, it must be the same name as the volume at the primary site.



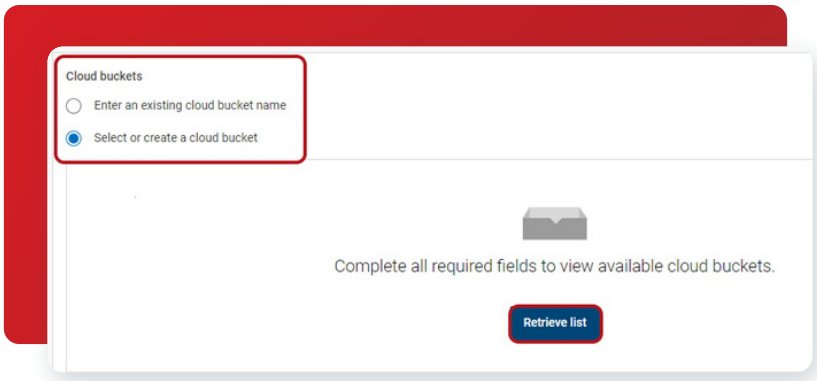
7. Use the same **cloud storage provider** at the alternate site as you did at the primary site. In this example, we're using NetBackup Recovery Vault Azure.



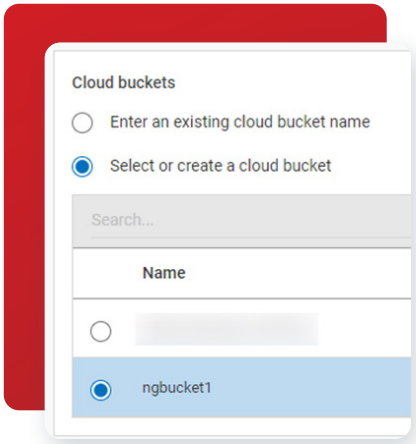
8. Use the same information you used at the primary site for Region and Account details.



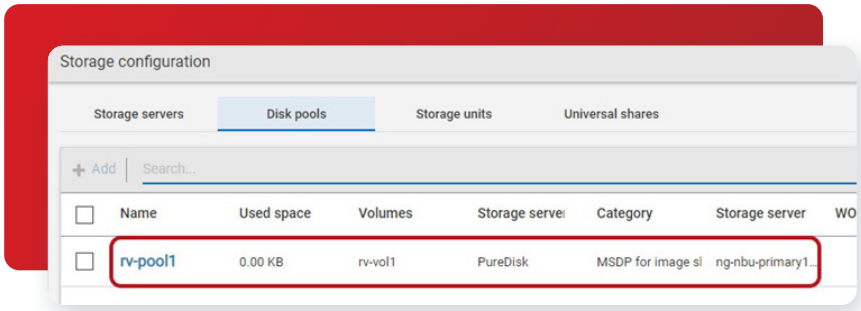
9. Once the credentials have been entered, click on **Select or create a cloud bucket** and **Retrieve list** to get the list of storage buckets you have created.



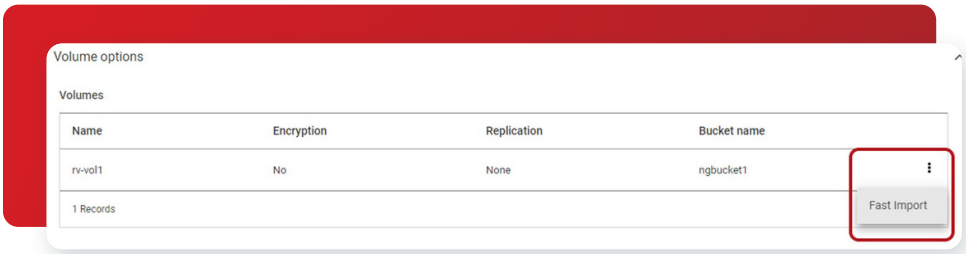
10. Select the storage bucket that you've been using at the primary site.



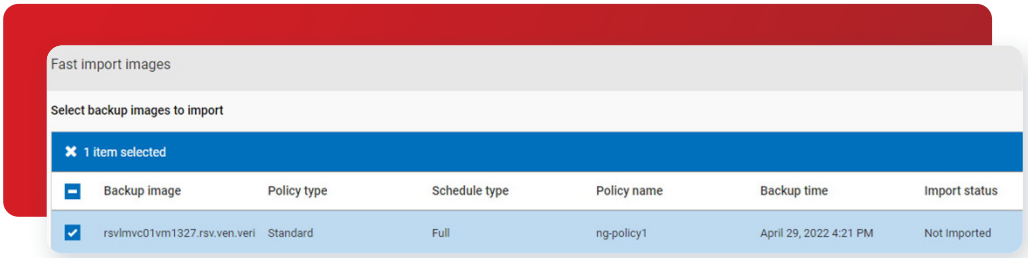
11. After the disk pool has been created, you can now import a backup from NetBackup Recovery Vault into your alternate primary server. Go to **Storage Configuration > Disk Pools** and click on the disk pool you just created.



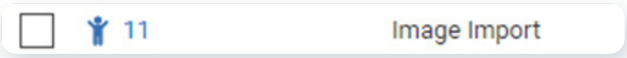
12. Under the **Volume options**, click on the three vertical dots and select **Fast Import**.



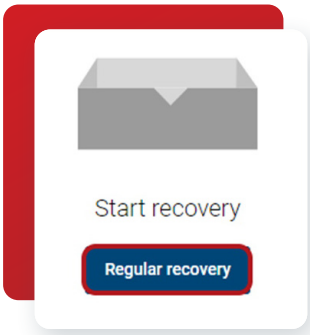
13. Select the backup you'd like to import and click on the Import button.



14. This will import the backup image, which can be browsed through NetBackup Recovery Vault to allow for file restores.



15. Under **Start recovery**, click on the **Regular recovery** button.

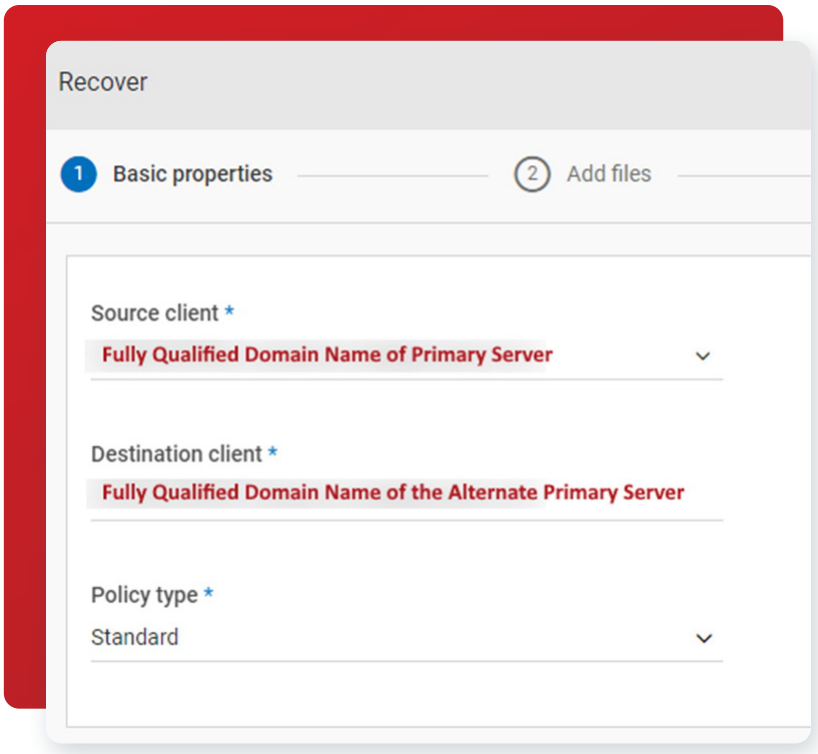


16. Then, enter the following information:

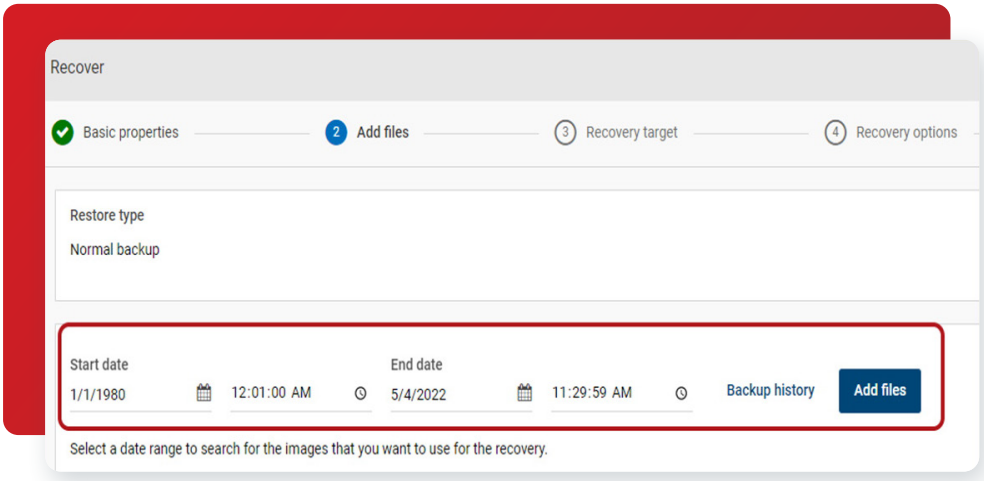
    a. Source Client - enter the fully qualified domain name of the primary server.

    b. Destination Client - enter the fully qualified domain name of the alternate primary server.

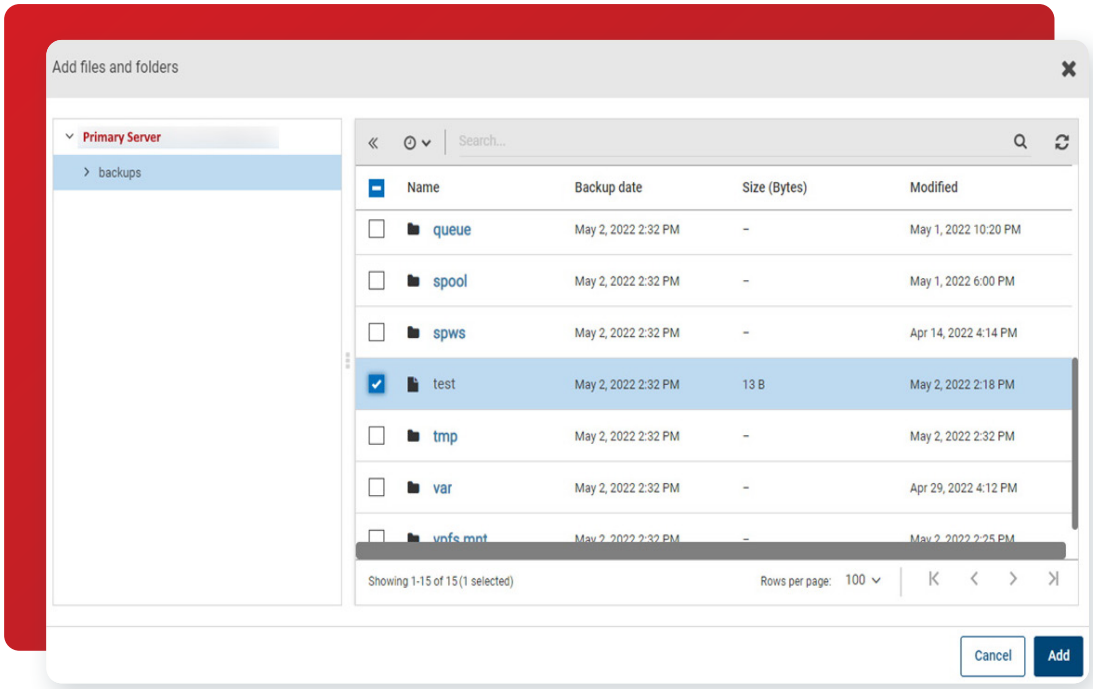
    c. Policy Type - select the policy type that was used to backup the data at the primary server. For this example, it's Standard.



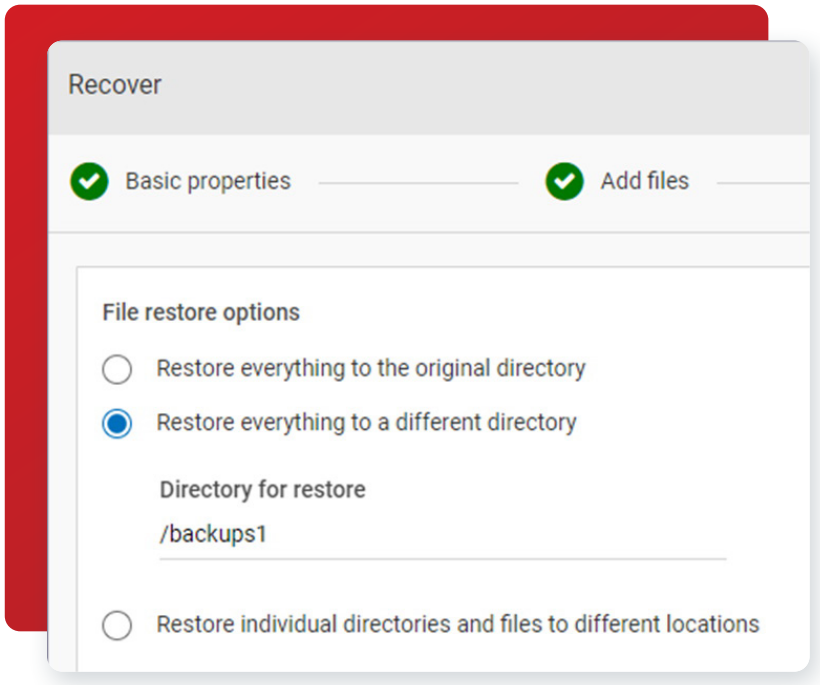
17. Enter the **Start** and **End date** and time of the backup. Then, click **Add files**.



18. The screen will display the backup data that's available. You can select what you'd like restored and click **Add**.



19. Enter where you'd like to restore the files. In this example, we're restoring the file(s) to an alternate location.



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

Conclusion

NetBackup Recovery Vault with Image Sharing simplifies the process of provisioning new storage in the cloud, reducing risk, enabling limitless scalability, lowering TCO, automating resiliency, and allowing for simple restores of critical data to an alternate NetBackup. With the easy-to-use UI, the management and monitoring of your cloud storage resources and retention policies, not to mention the provisioning of your storage and the protection of your data has never been easier.

Disclaimer

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. 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 06/22