VERITAS

Veritas NetBackup on AWS PrivateLink for Amazon S3 Deployment Guide

Securing NetBackup data between on-premises and AWS S3.

Deployment Guide | January 2022

Contents

Revision History

Version	Date	Changes	Author
1.00	12/2/2021	Initial Version	Neil Glick

Introduction

Amazon Web Services (AWS) PrivateLink provides private network connectivity between Amazon Simple Storage Service (S3) and on-premises resources that use private IP addressing from your virtual network. This approach eliminates the need to deploy proxy servers that typically constrain performance, add single points of failure, and increase operational complexity.

With AWS PrivateLink you can now access S3 directly as a private endpoint using your secure, virtual network, which leverages a new interface endpoint within your Virtual Private Cloud (VPC). This feature extends functionality for existing gateway endpoints by enabling users to access S3 using private IP addresses. The Veritas NetBackup™ API and secure HTTP requests to S3 can now be automatically directed through interface endpoints that connect to S3 securely and privately via PrivateLink. (See Figure 1.)

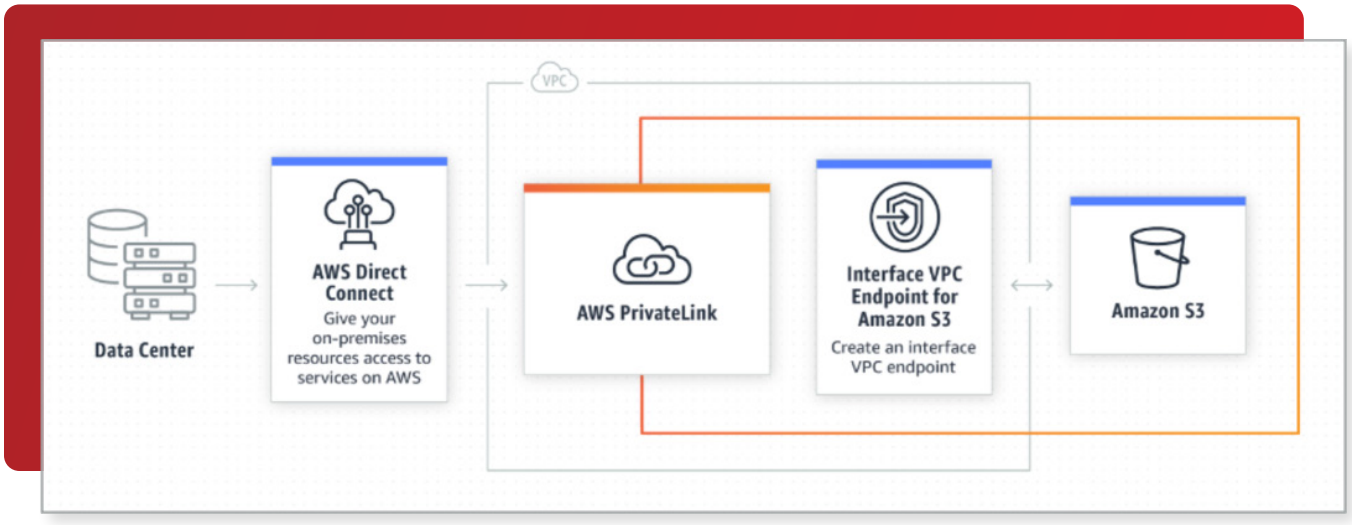


Figure 1. AWS PrivateLink provides a secure connection from an organization's network to Amazon S3.

Why use NetBackup with AWS PrivateLink?

Interface endpoints simplify the NetBackup network architecture when connecting to S3 by eliminating the need to deploy an Internet gateway or configure firewall rules. With this setup, you also gain additional visibility into your network traffic plus the ability to capture and monitor flow logs within your VPC. Finally, you can take additional security measures with your interface endpoints by creating security groups and enabling access control policies.

An Overview: How NetBackup Works with AWS PrivateLink

The AWS Shared Responsibility Model defines the distribution of security responsibilities between AWS and its customers. One of the biggest concerns that influences cloud adoption is security. In the context of data protection to the cloud, transport remains an area of concern for many organizations that are subject to data regulatory and/or compliance requirements. NetBackup users can now safely transfer data to and from the AWS cloud without the risk of exposing sensitive data to visibility, tampering, or theft. Veritas has thoroughly tested NetBackup with AWS PrivateLink to send backup data as well as recover to and from AWS S3. We are also proud to announce that NetBackup provides day-zero support for AWS PrivateLink.

The Architecture

Figure 2 shows an sample environment with NetBackup and AWS PrivateLink S3. This architecture uses the AWS VPN approach. You will need to complete the following steps to perform backups to S3 using AWS PrivateLink:

In AWS

1. Create a Virtual Private Cloud (VPC) if one doesn't exist.
2. Configure the VPC IP range specific to the private network being deployed.
3. Add an S3 interface endpoint to the VPC. This is the actual PrivateLink.
4. Create a Virtual Private Gateway (VPG) and attach it to the VPC.
5. Create a site-to-site VPN used to connect from on-premises to AWS.
6. Add the subnet for the on-premises server to the VPN and VPC subnet routing tables.
7. Create an AWS Customer Gateway (CGW).
8. Download the CGW configuration file for the router model being used and configure the VPN.
9. Configure the CGW with the IP from the VPN configuration.
10. Add the on-premises IP CIDR to the VPN routing table.

In NetBackup

1. Create or use an existing media server deduplication pool (MSDP) storage server for the S3 backups.
2. Connect to the AWS S3 endpoint from the on-premises server.
3. Create a new disk pool. (Completed in NetBackup.)
4. Create a new volume.
5. Connect Amazon S3 for the cloud storage provider.
6. Add the PrivateLink Region Name, Location Constraint, Endpoint/Service URL, and HTTP/HTTPS ports.
7. Supply the Access Key ID.
8. Supply the Secret Access Key.
9. Retrieve the List of Cloud Buckets; if none exists, create one.
10. Create a storage unit and connect to the new MSDP storage.

On-Premises VPN

- Submit the CGW configuration file to the on-premises networking team to configure the VPN.

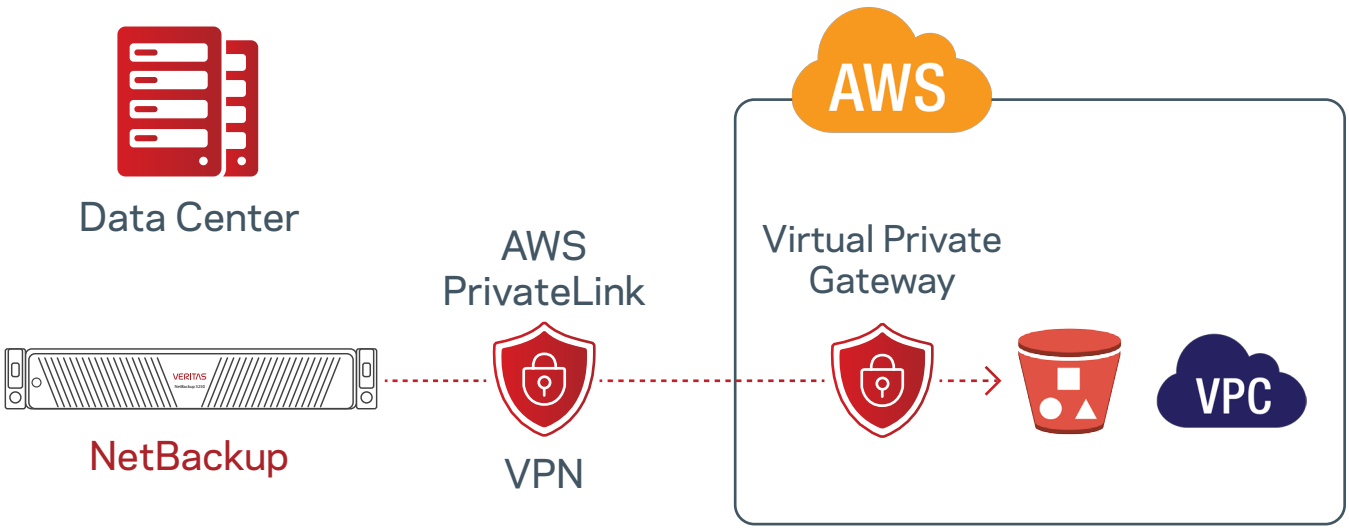


Figure 2. A sample environment using NetBackup and AWS PrivateLink to Amazon S3.

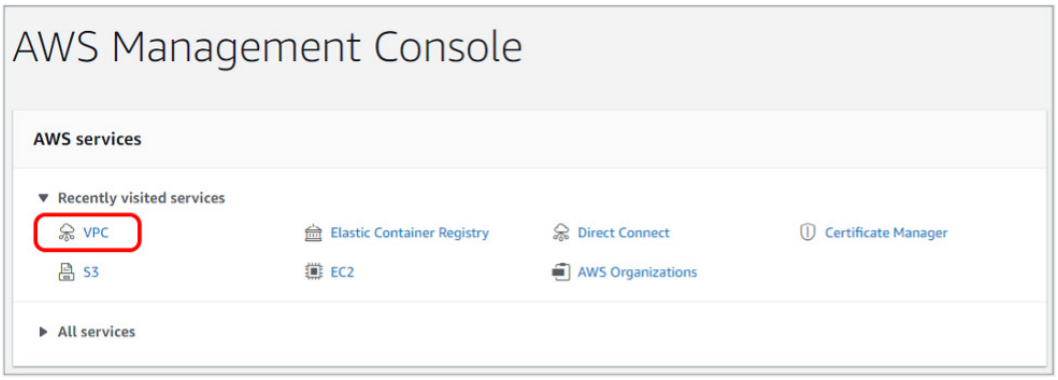
Configuring AWS PrivateLink for Use with NetBackup

Your AWS PrivateLink will be unique to your environment, but you can use the following architecture to set up an environment like the one shown in Figure 2. For in-depth information about AWS PrivateLink technology and how to customize it for your environment, visit https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html.

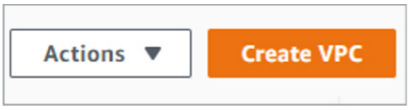
Create the AWS PrivateLink Architecture Components

From within AWS, select the region in which you will create the new VPC. In this example, we have used US East 2 or Ohio.

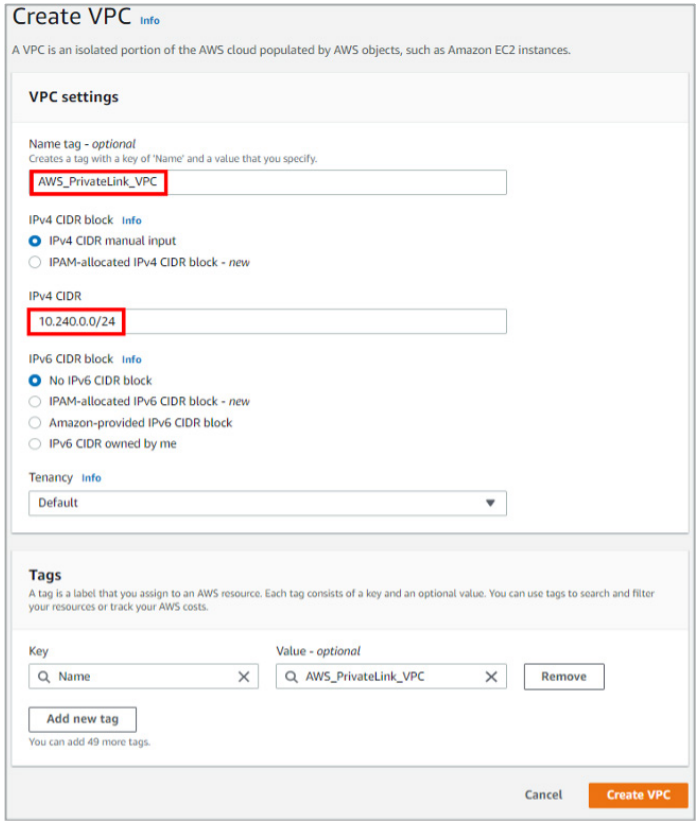
1. In the AWS Management Console, click the **VPC** service.



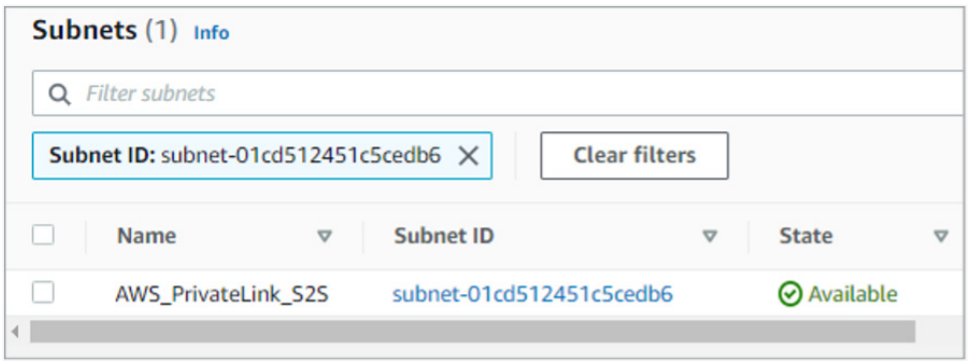
2. Next, select **Create VPC** from the upper right corner.



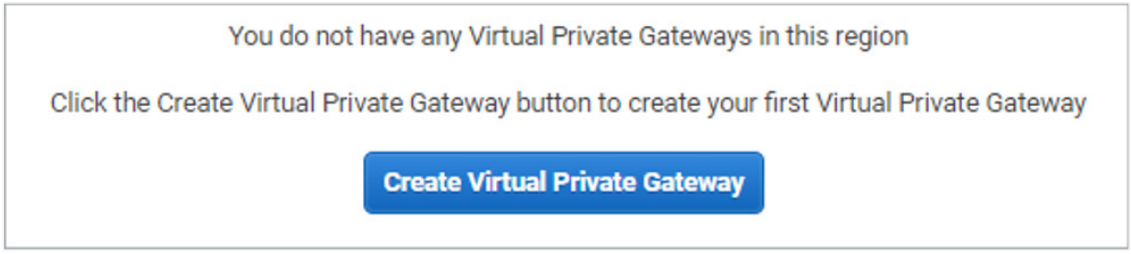
3. Give your VPC a name and define the network size of the new CIDR block range. In this example, we have used IPv4.



4. Create a subnet within the newly created VPC.

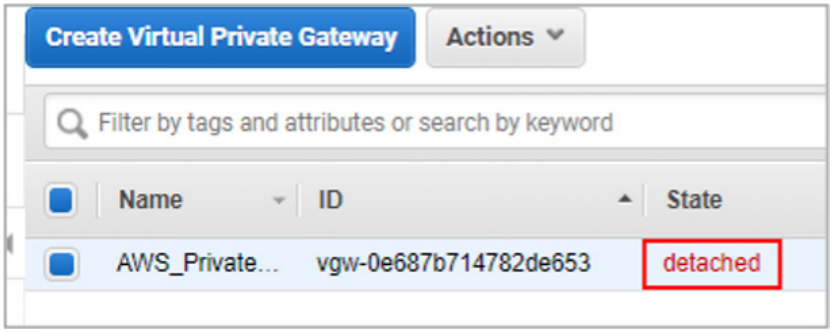


5. Next, create a Virtual Private Gateway (VPG).

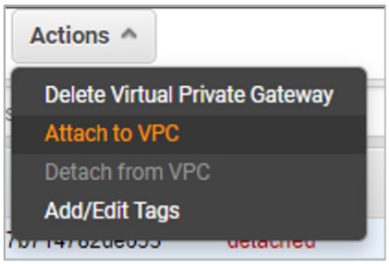


6. Give the VPG a name and click on **Create Virtual Private Gateway**.

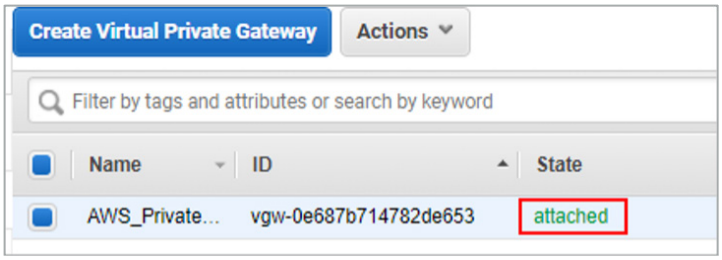
7. The VPG you just created will be in a detached state. You need to attach the VPG to the VPC you created earlier.



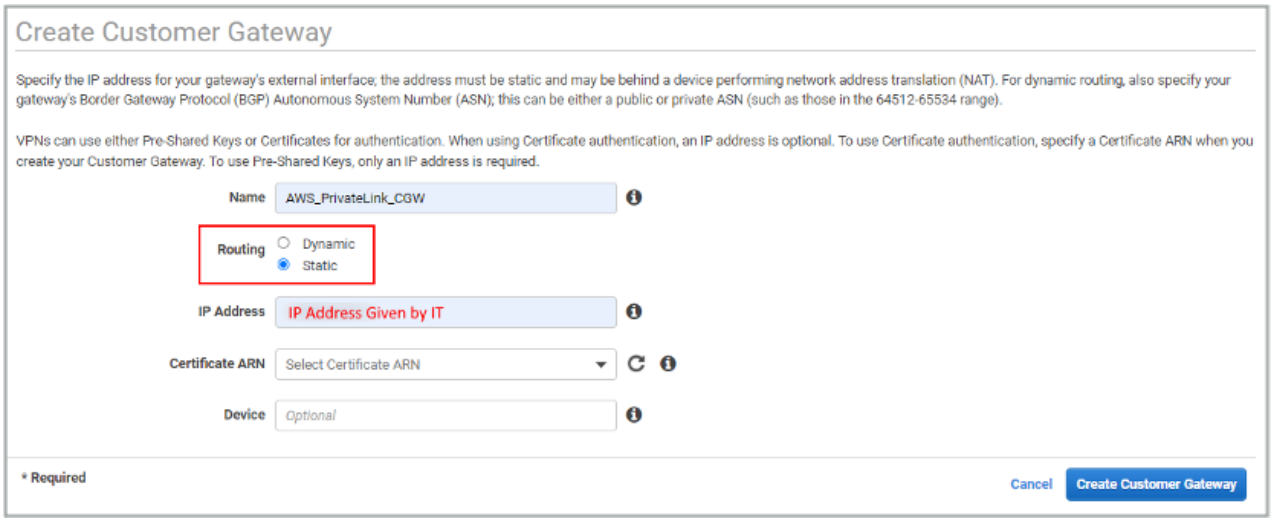
8. Click on the **Actions** button, select **Attach to VPC**, and select the VPC you created earlier.



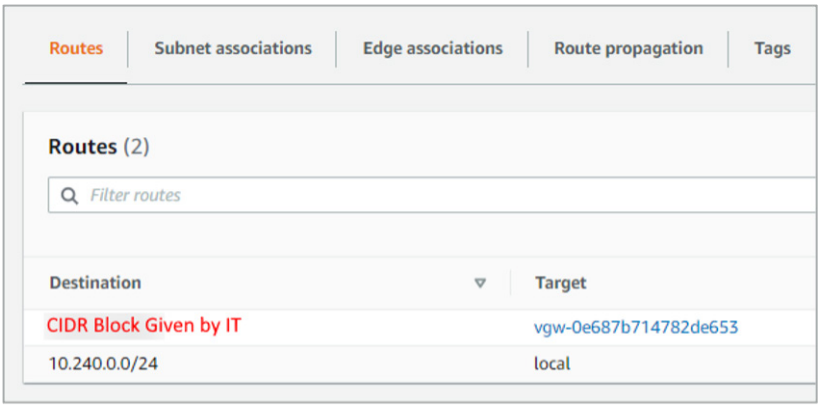
9. After attaching the VPG to the VPC, the **State** should change to "attached."



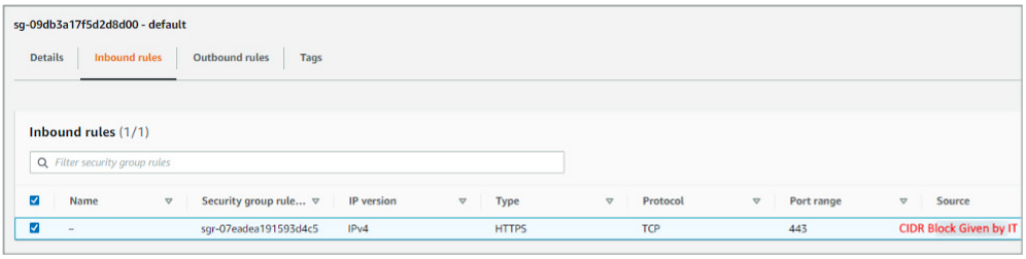
10. Next, create a Customer Gateway (CGW). Give it a name, select **Static Routing**, and enter the public IP address given by your IT department. Click **Create Customer Gateway**.



11. Add your on-premises IP CIDR block to the VPC route table with the VPG as the target. This CIDR block is usually the subnet with the NetBackup on-premises infrastructure.

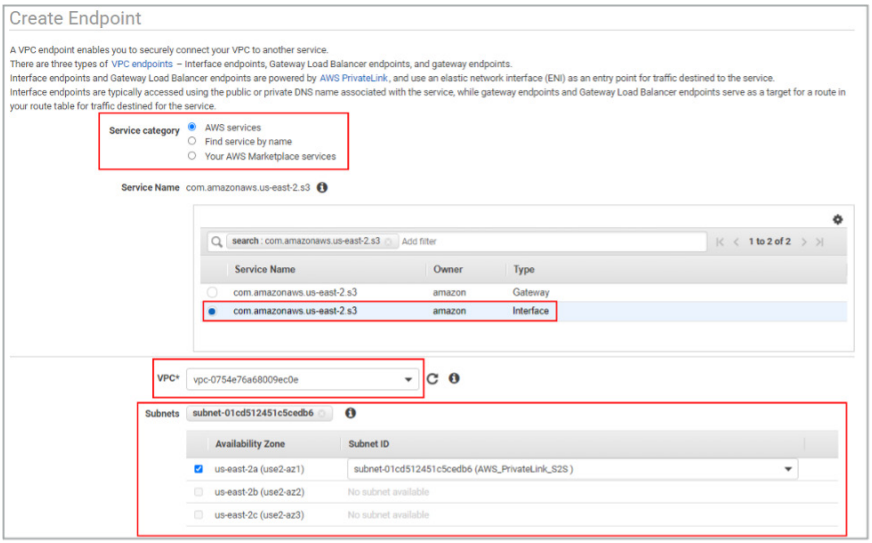


12. Next, add an inbound HTTPS rule with the CIDR block you used in step 11 to the VPC security group.

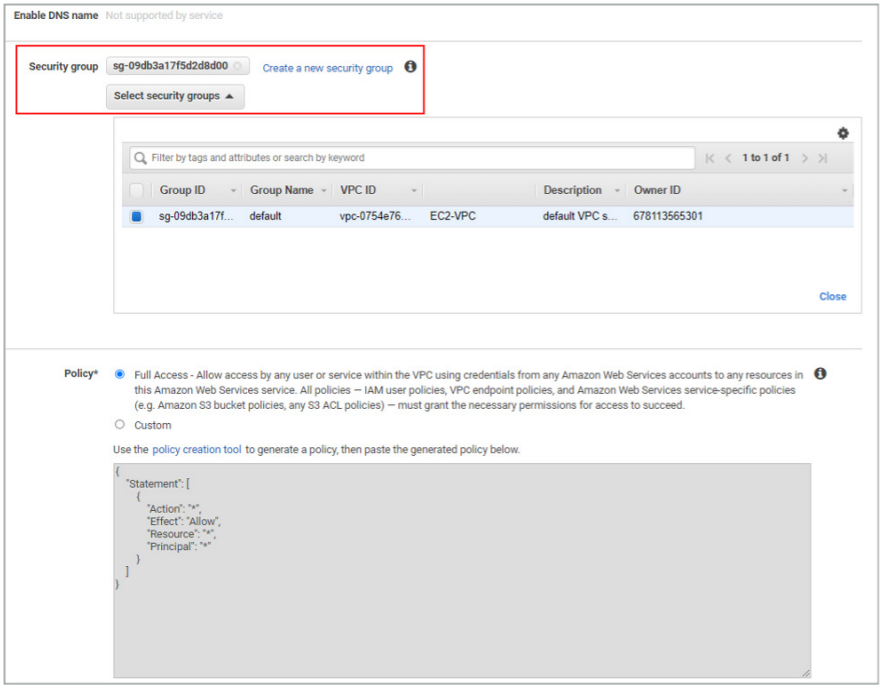


13. Creating the endpoint is a multi-step process:

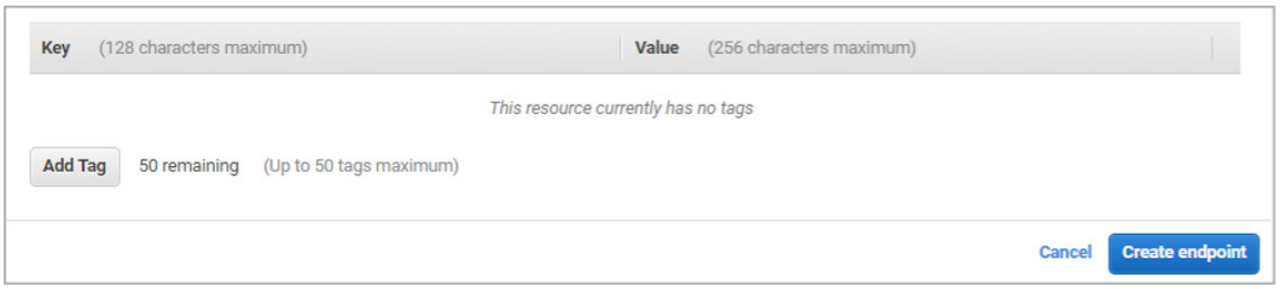
- First, define the Service category as **AWS services** and the Service Name. The Service Name will depend on the region in which your PrivateLink is deployed. In this example, we are using com.amazonaws.us-east-2.s3 with the type as "Interface."



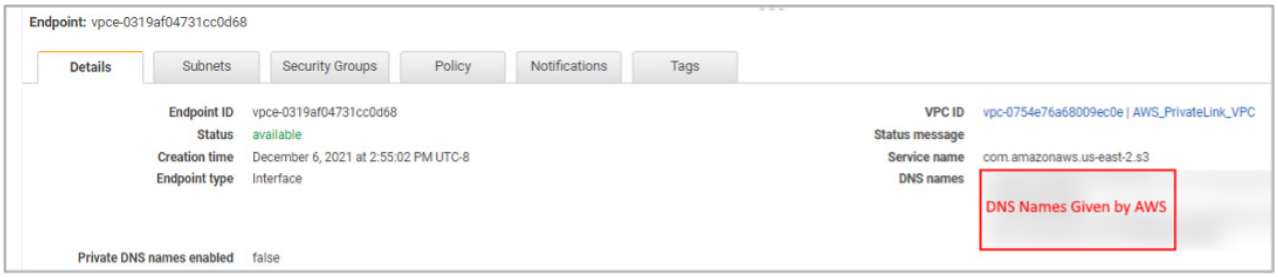
- Next, select the security group for this VPC. If you would like to add specific (custom) access, you can enter that here.



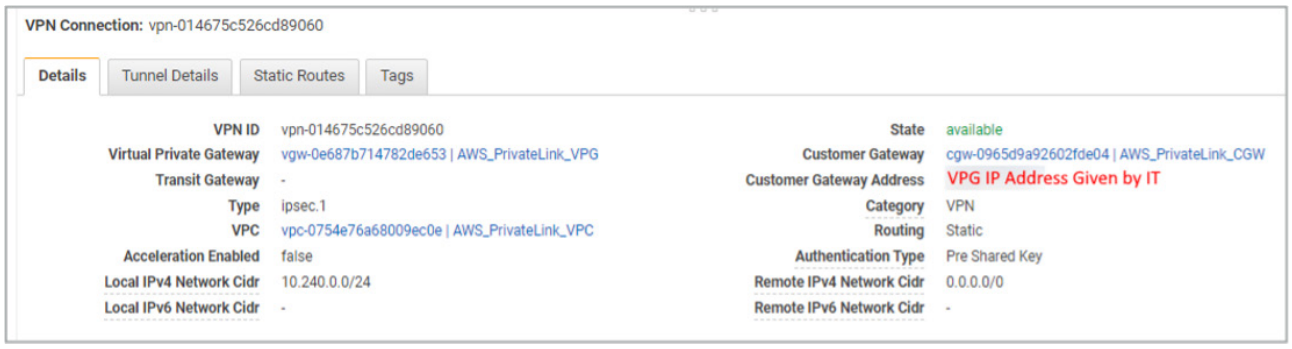
- Add any necessary tags and click on **Create endpoint**.



14. Finally, be sure to note the DNS Names given by AWS because you will need them to connect from your NetBackup infrastructure.



15. Now you will create a site-to-site VPN connection. To do so, you will need the VPC CIDR block, the VPG given by your IT department, and the on-premises CIDR block on which your NetBackup infrastructure is located. (Although not shown here, the on-premises CIDR block will also require configuration. We've used **Static Routing** in this example.)

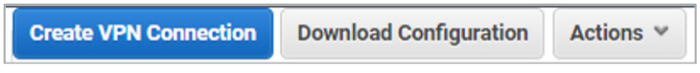


16. The next step is to click on **Download Configuration** and share the downloaded file with your IT/Security department. It should contain most of the information needed to build the on-premises rules required for PrivateLink.

    Once the on-premises configurations are complete, it's time to validate PrivateLink works correctly. Type in the following command from the terminal of the NetBackup Primary server:

    openssl s_client -showcerts -connect bucket.The_DNS_Name_AWS_Gave:443

    If everything is configured correctly, the connection should be successful and a list of SSL certificates will be shown.

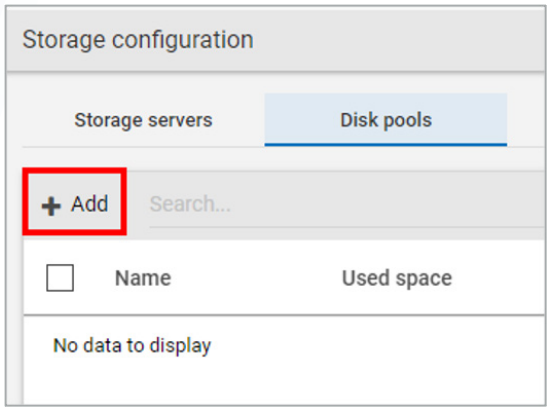


Use NetBackup to Connect to AWS Using PrivateLink

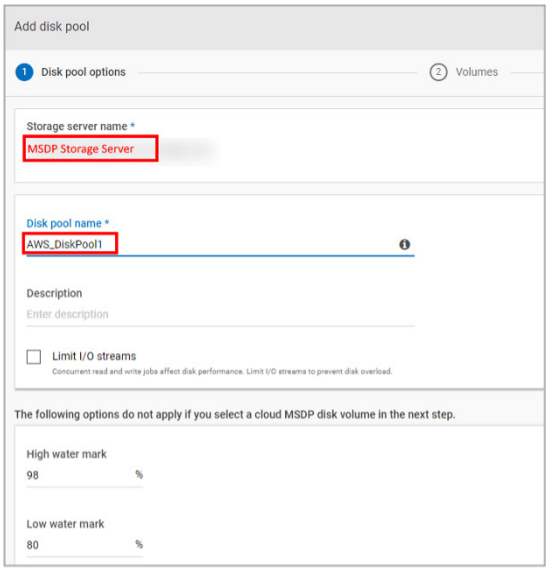
To connect to the newly created AWS PrivateLink, log into the NetBackup Primary server and navigate to Storage > Storage Configuration. You will need to add an MSDP storage server or use an existing one. This guide assumes one has already been created.

To add an MSDP storage server, refer to https://www.veritas.com/content/support/en_US/doc/25074086-149019166-0/v149102574-149019166.

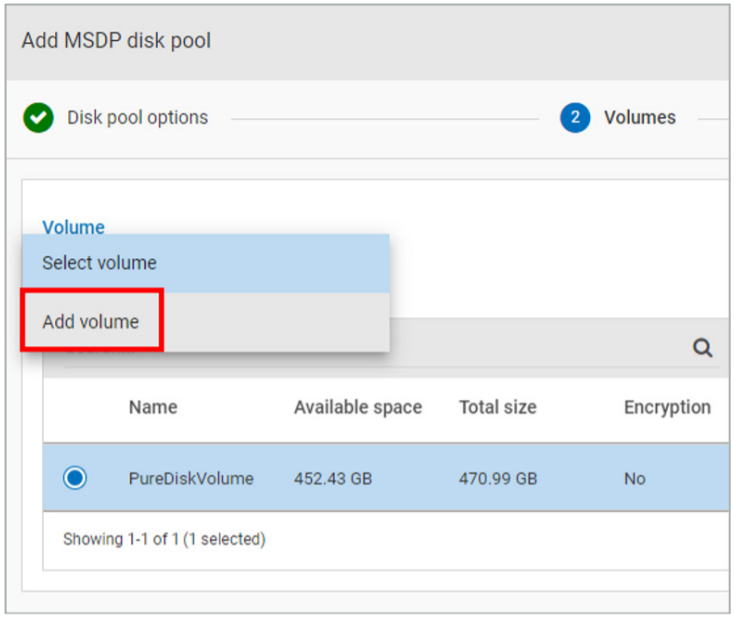
1. From Storage configuration, click on **Disk pools** and **+Add** to create a new disk pool and volume.



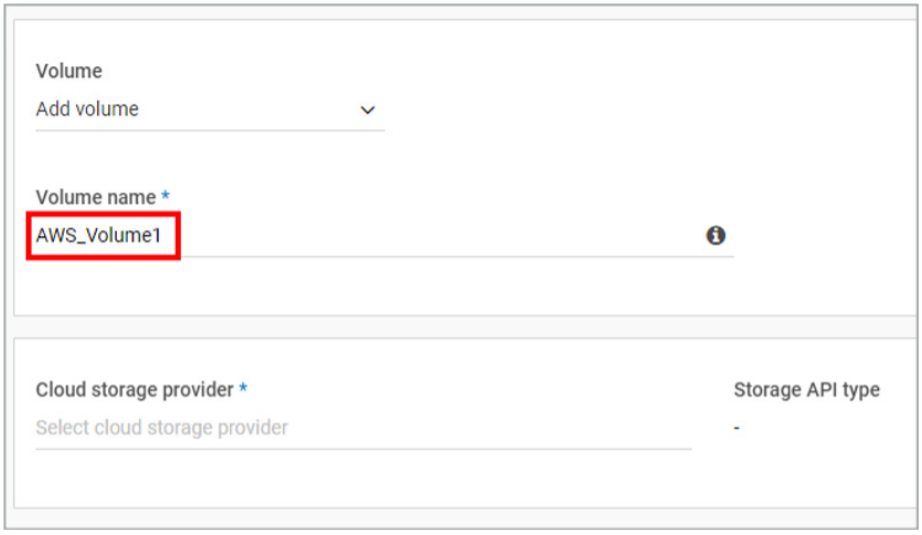
2. Select the MSDP server that will be used and give the new disk pool a name. Click **Next** to continue.



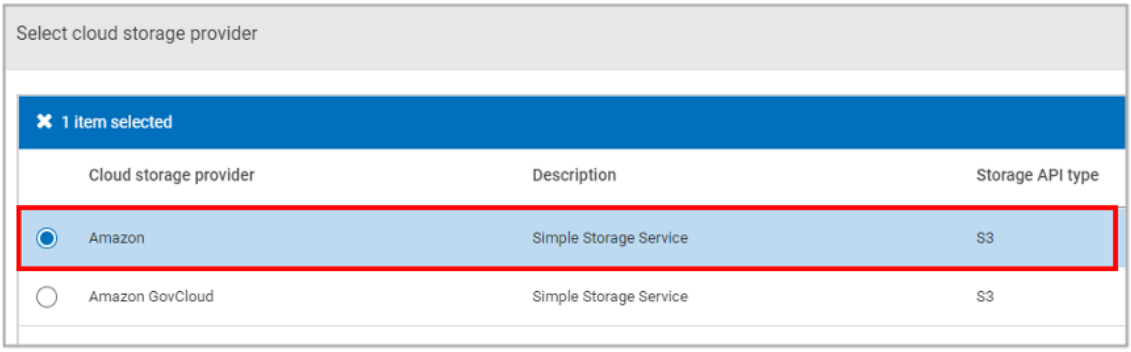
3. Next, you will add a volume. Click on **Add volume** from the drop-down.



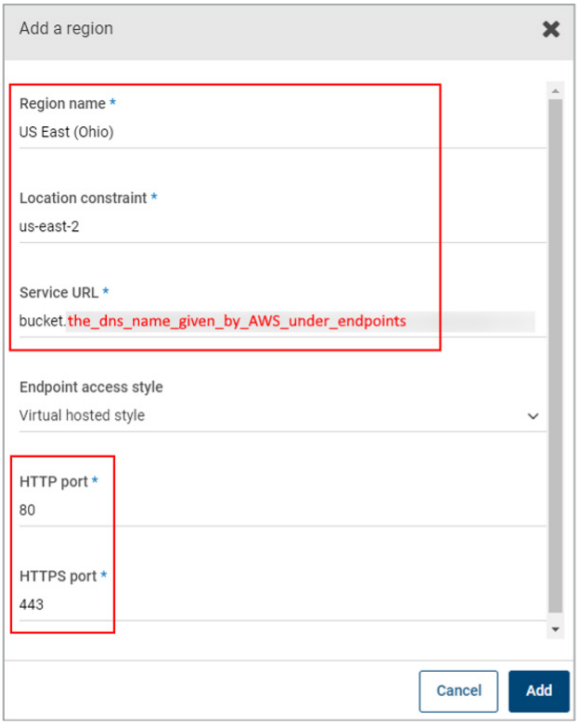
- Give the volume a name and then click on **Cloud storage provider**.



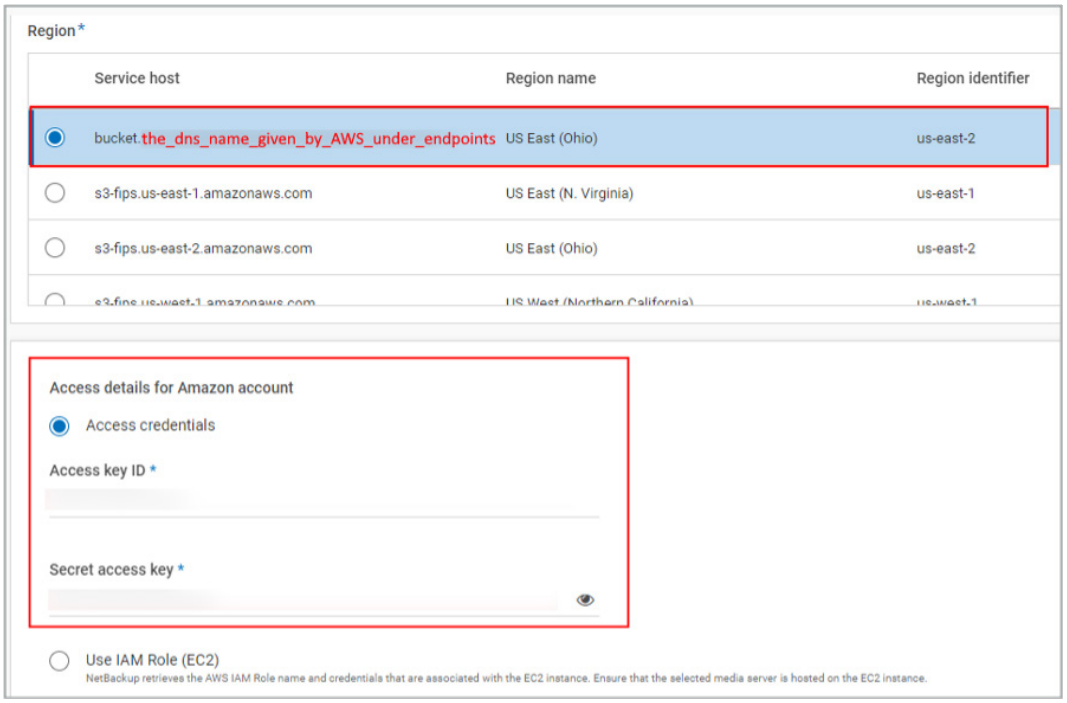
- Select **Amazon** as the cloud storage provider.



4. Now you will add a region and define the cloud bucket as follows:
   - Give the region a name.
   - Enter the **Location constraint**.
   - Add the **Service URL**, which is the DNS name given by AWS under Endpoints with the prefix "bucket." attached.
   - Change or keep the defaults for the HTTP/ HTTPS ports.
   - Click on **Add**.

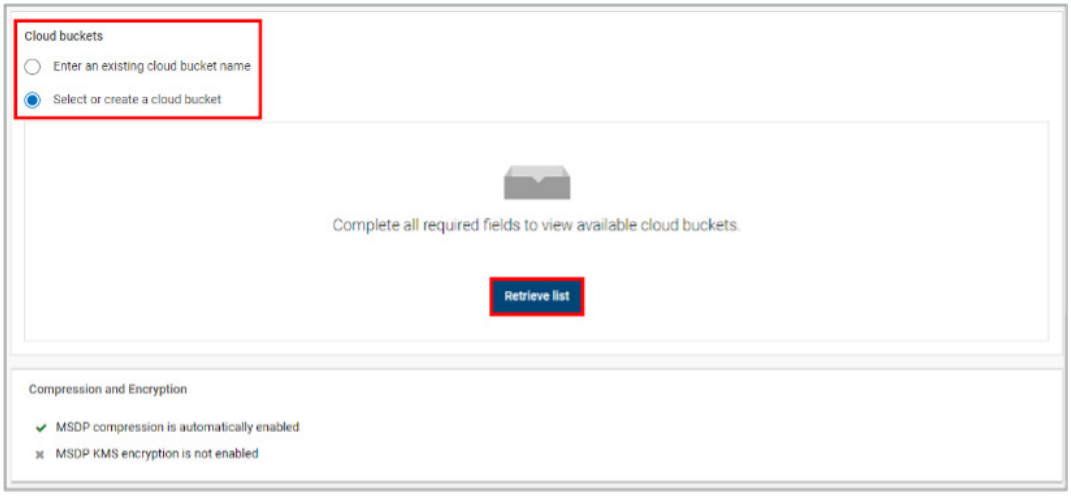


- Select the newly created region and enter your AWS **access credentials** and **secret access key**.

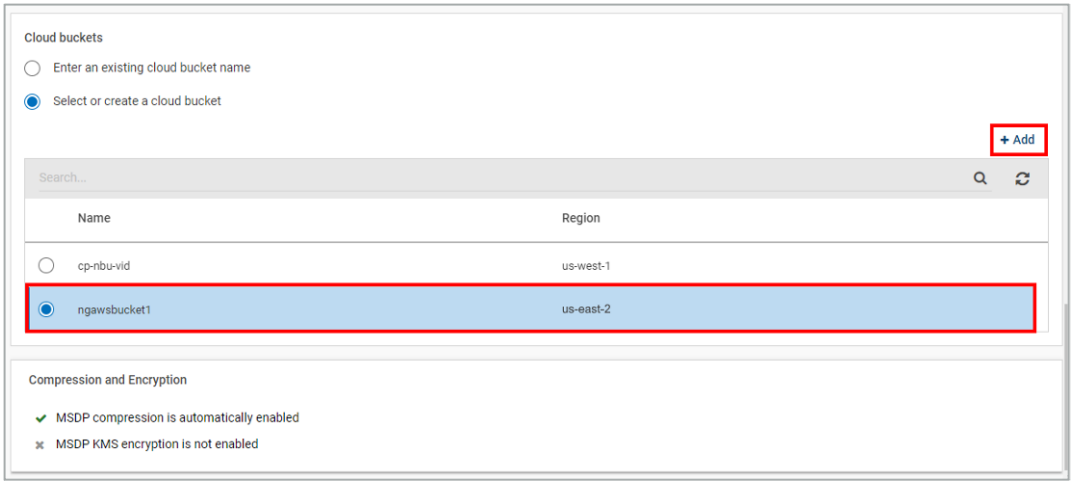


- Select if you would like to change any of the default security settings.

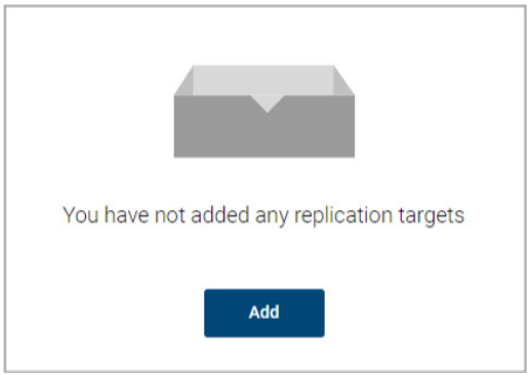
- Choose **Select or create a cloud bucket**. Click on **Retrieve list** to connect to AWS.



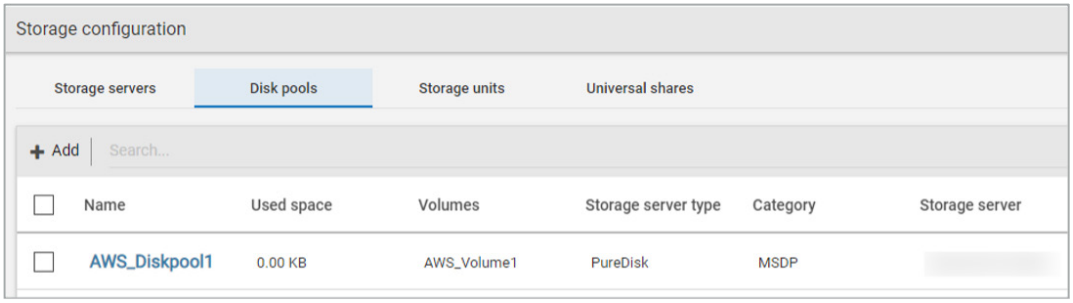
- After connecting to AWS, either select a pre-created bucket or click on the **+Add** button to create a new bucket. Click **Next** to continue.
- Add any replication targets, if required, by clicking **Add**.



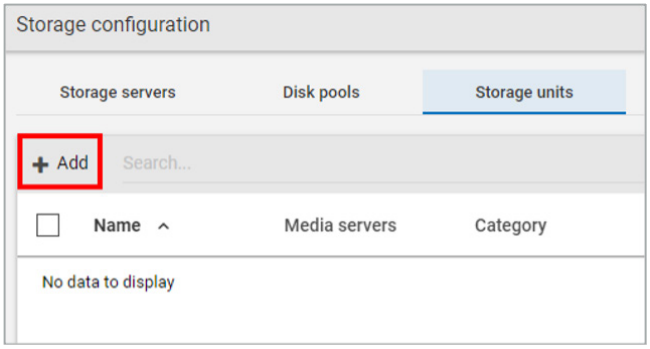
- Finally, review what will be created and click **Finish**.



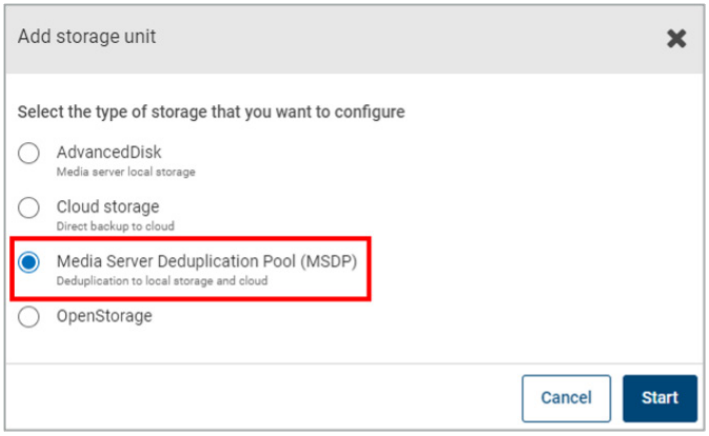
5. The disk pool has been created. The next step is to add a storage unit so backups can use the new AWS PrivateLink.



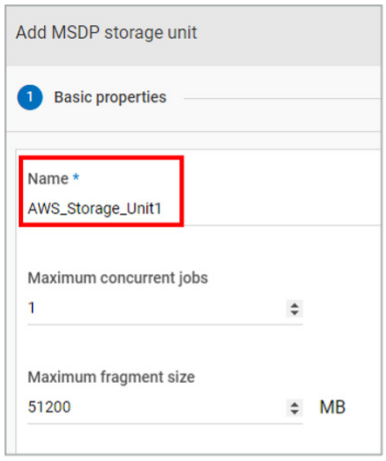
6. Click on the **Storage units** tab and then click on **+Add**.



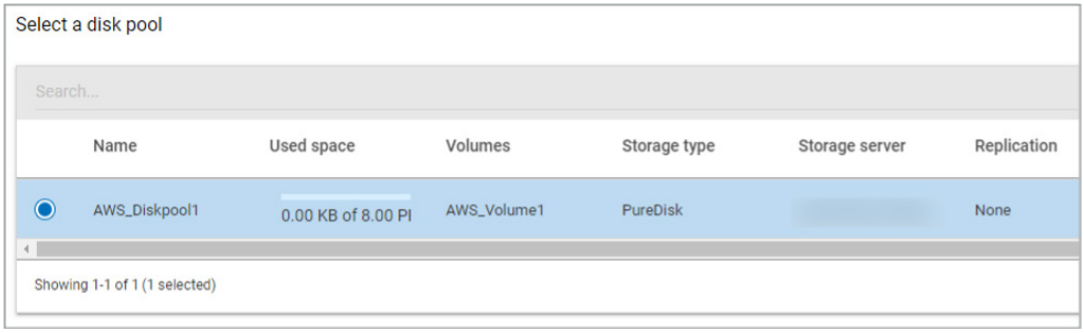
7. Select MSDP and click **Start**.



8. Name the MSDP storage unit and click on **Next**.



9. Select the disk pool you recently created.



10. Select the media server you'd like to use and click **Save**.

The storage configuration is now complete, and you may now use the new media to perform backups.

Conclusion

With Veritas NetBackup and AWS PrivateLink, you can now access your S3 directly as a private endpoint using a new VPC interface and safely transfer data to and from the AWS cloud without risk of exposing sensitive data to visibility, tampering, or theft.

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

V1495 01/22