VERITAS

Veritas NetBackup on AWS PrivateLink for Amazon S3 Deployment Guide

Securing NetBackup Data Between on Premises and AWS S3

Table of Contents

Revision History

Version	Date	Changes	Author
1.00	12/2/2021	Initial Version	Neil Glick
1.01	11/25/2024	Included Veritas Alta Recovery Vault Support for AWS PrivateLink	Sakshi Nasha

Introduction

AWS PrivateLink provides private network connectivity between Amazon Simple Storage Service (S3) and on-premises resources which use private IP addressing from your virtual network. This eliminates the need to deploy proxy servers which 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 new feature extends functionality for existing gateway endpoints by enabling users to access S3 using private IP addresses. 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.

Why Would I Want It?

Interface endpoints simplify the NetBackup network architecture when connecting to S3 by eliminating the need to deploy an internet gateway or configure firewall rules. Additional visibility with your network traffic can now be realized with 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.

How it Works – The Short Version

The AWS Shared Responsibility Model defines the distribution of security responsibilities between AWS and its customers. One of the biggest concerns that influence cloud adoption is security. In the context of data protection to the cloud the 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

The high-level diagram illustrated below shows an example environment with NetBackup and AWS PrivateLink S3. The below architecture uses the AWS VPN approach. The following steps will need to be completed to perform backups to S3 using the AWS PrivateLink:

In AWS:

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

In NetBackup:

1. Create or use an existing 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 Access Key ID
8. Supply Secret Access Key
9. Retrieve List of Cloud Buckets if none exist create one.

10. Create a Storage Unit and connect to the new MSDP storage.

In NetBackup for Alta Recovery Vault:

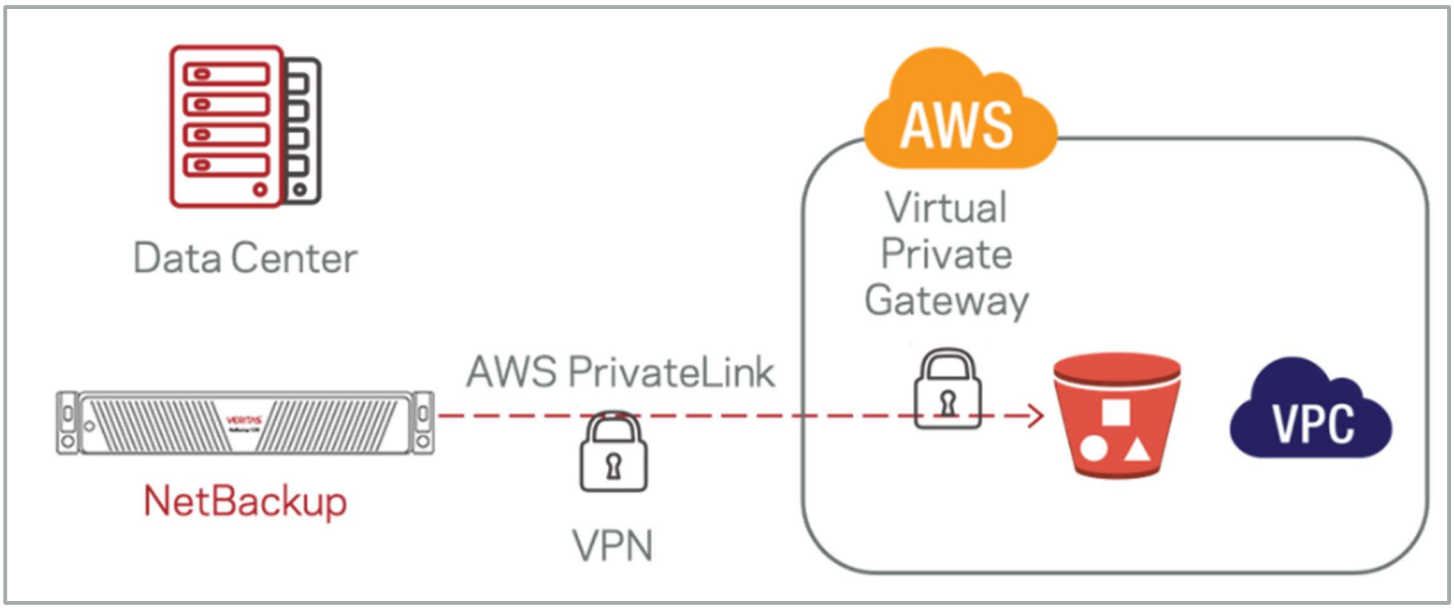
1. Create or use and existing MSDP Storage Server. For more information on how to add a storage server, see the NetBackup Deduplication Guide: **https://www.veritas.com/content/support/en_US/doc/25074086-159245004-0/v24332600-159245004**
2. Create a new Disk Pool.
3. Create a new Volume. Search for “Veritas Alta Recovery Vault Amazon” and the following Cloud storage providers appear. For this example, you will choose Veritas Alta Recovery Vault Amazon.
4. Before adding the PrivateLink Region you can check by curling the AWS PrivateLInk from the VM to check if network connections are well established:

   curl -v https://bucket.vpce-<endpoint-id>.s3.<region>.vpce.amazonaws.com
5. Add the PrivateLink Region Name, Location Constraint, Endpoint/Service URL and HTTP/HTTPS ports.

6. Add the credentials of the Alta Recovery Vault AWS Bucket
7. Retrieve List of Cloud Buckets if none exist create one.
8. Create a Storage Unit and connect to the new MSDP storage.
9. For more information on Alta Recovery Vault: https://www.veritas.com/content/support/en_US/doc/VeritasAltaRecoveryVaultGuide

On Premises VPN:

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



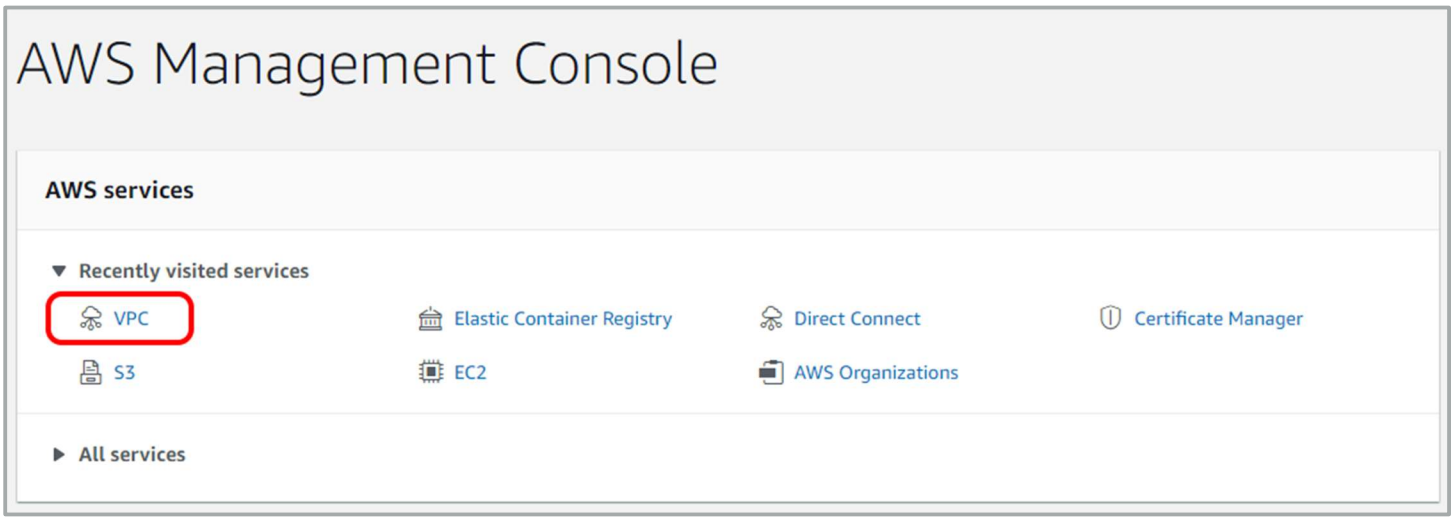
How it Works – The Long Version

Your AWS PrivateLink will be unique to your environment, but the following architecture can be used to set up an environment similar to the diagram shown above. For more in depth understanding of AWS PrivateLink technology and how to customize it for your environment, visit:

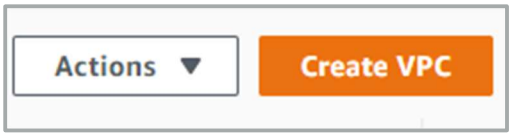
https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html

Create the AWS PrivateLink Architecture Components

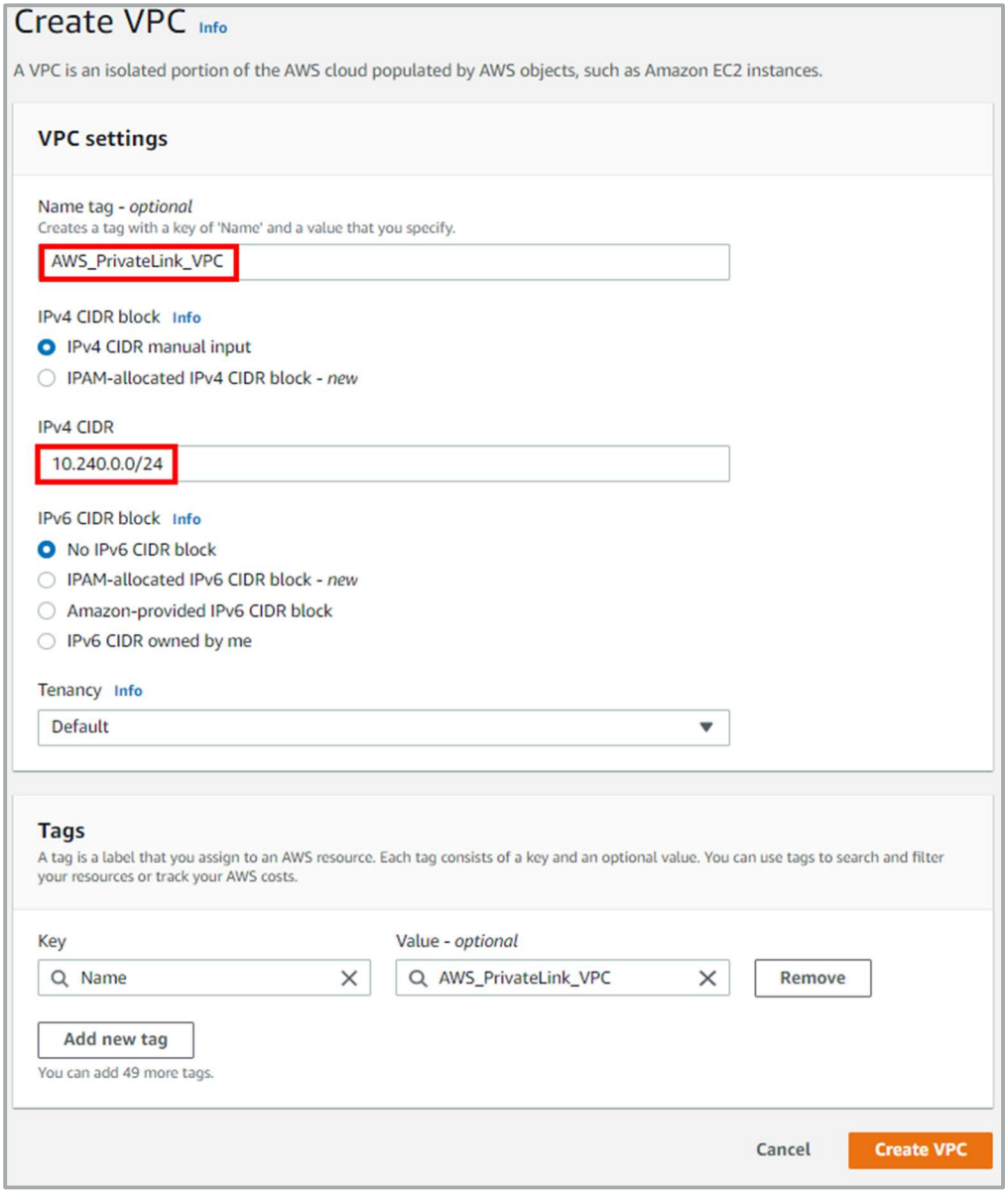
From within AWS select the region the new VPC will be created in. In this example US East 2 or Ohio is used.



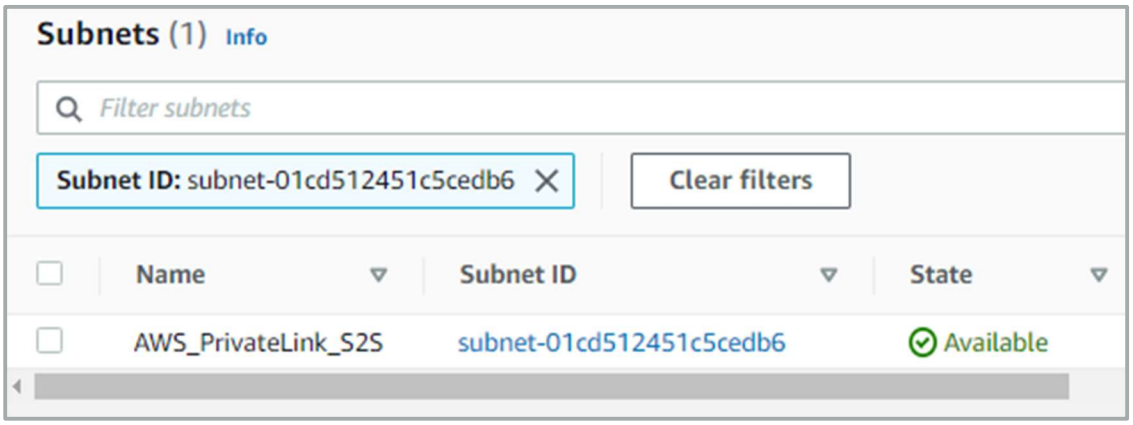
1. In the AWS Management Console click on VPC.



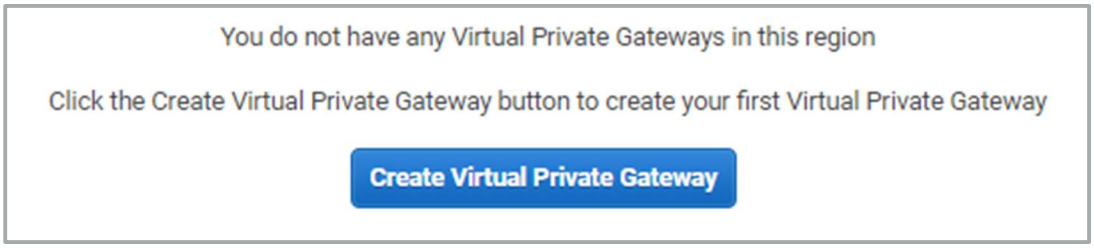
2. Next, select Create VPC from the upper right corner.



3. Give your VPC a name, and what the network size of the new CIDR block range should be. In the following example IPV4 will be used and not IPV6.

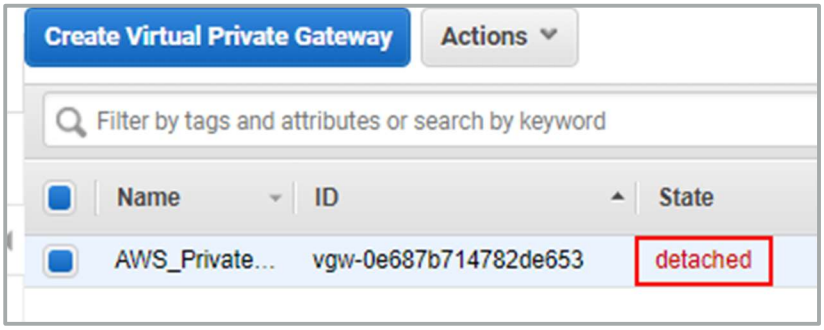


4. Create a subnet within the newly created VPC.

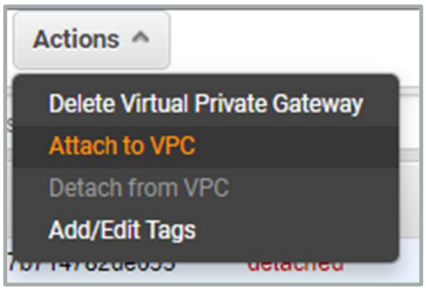


5. The next step is to create a Virtual Private Gateway.

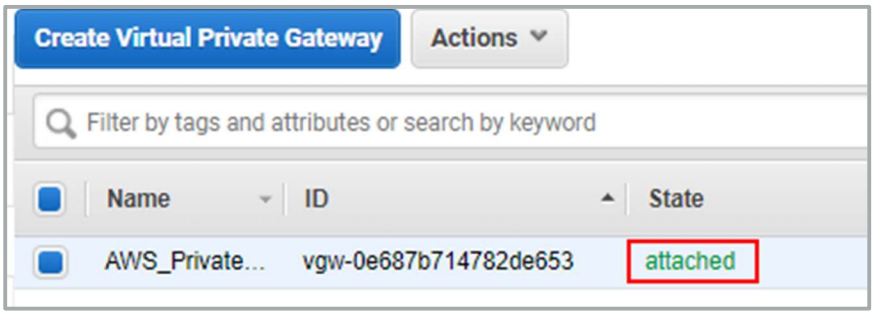
6. Give the VPG a name and click on Create Virtual Private Gateway.



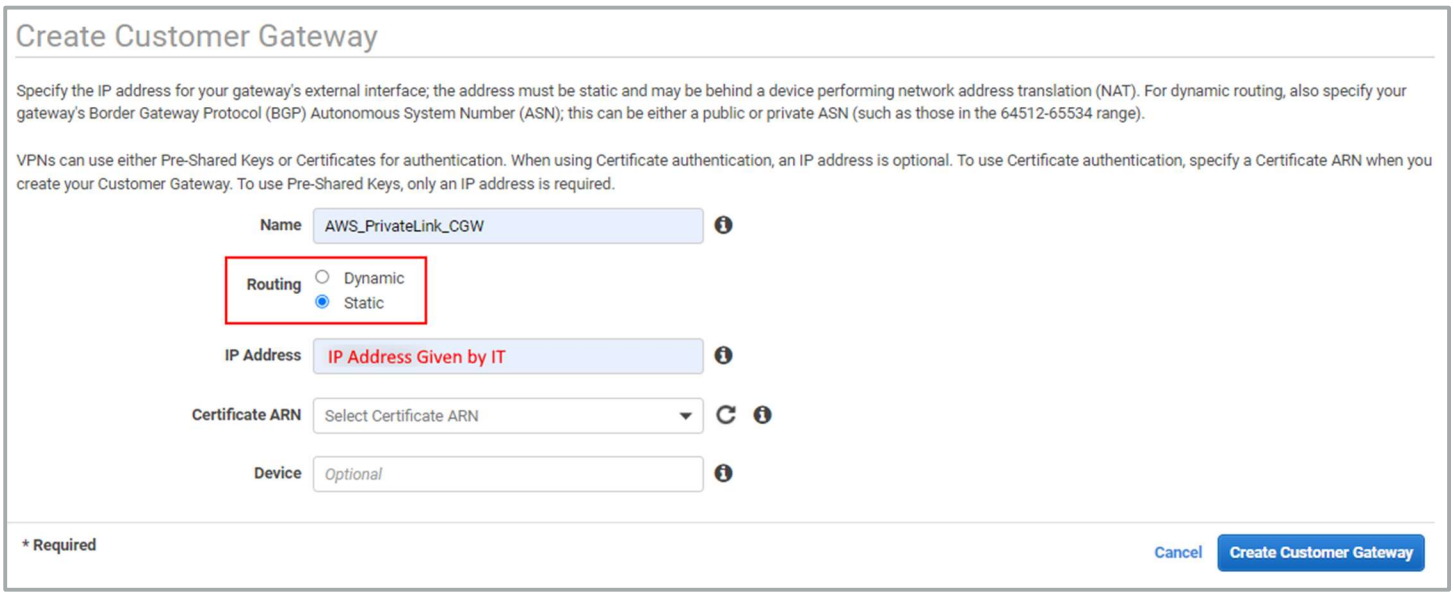
7. The VPG has been created but will be in a detached state. We need to attach the VPG to the VPC created earlier.



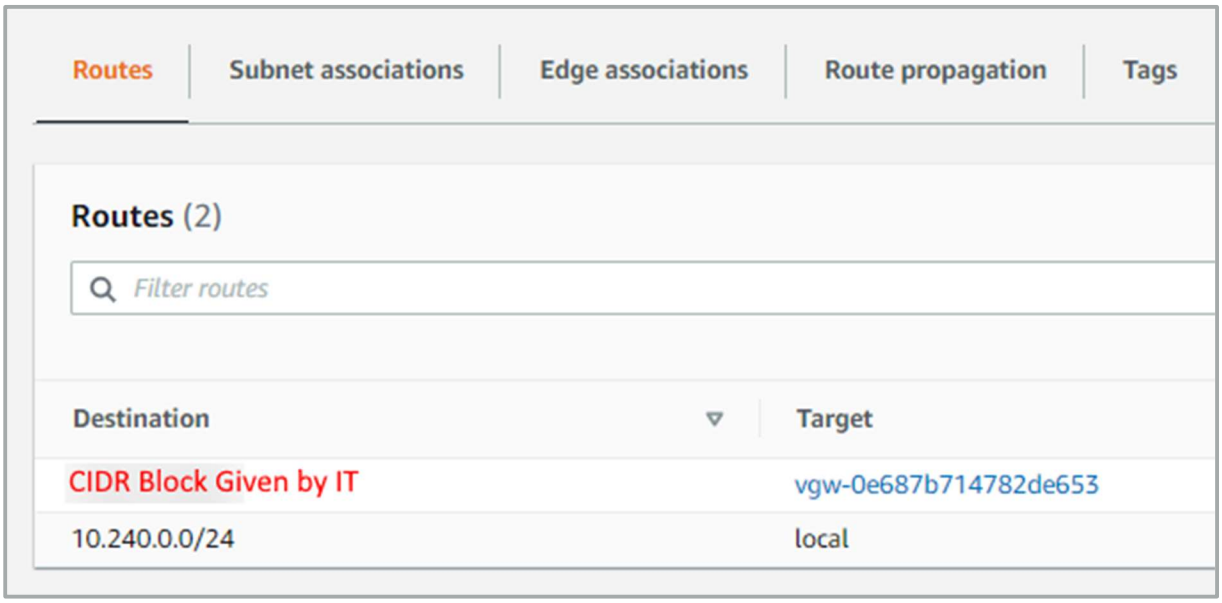
8. Click on the Actions button and select Attach to VPC and select the VPC created earlier.



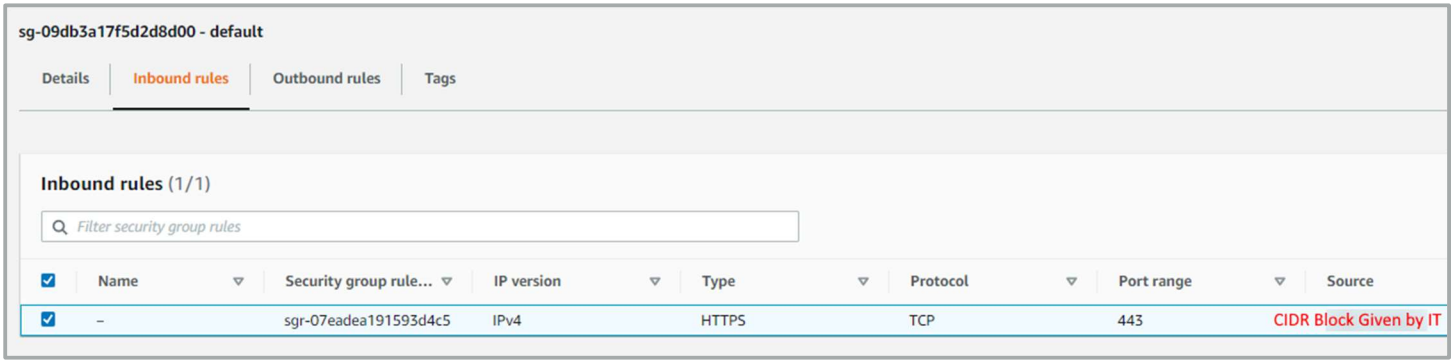
9. After attaching the VPG to the VPC the state should change to attached.



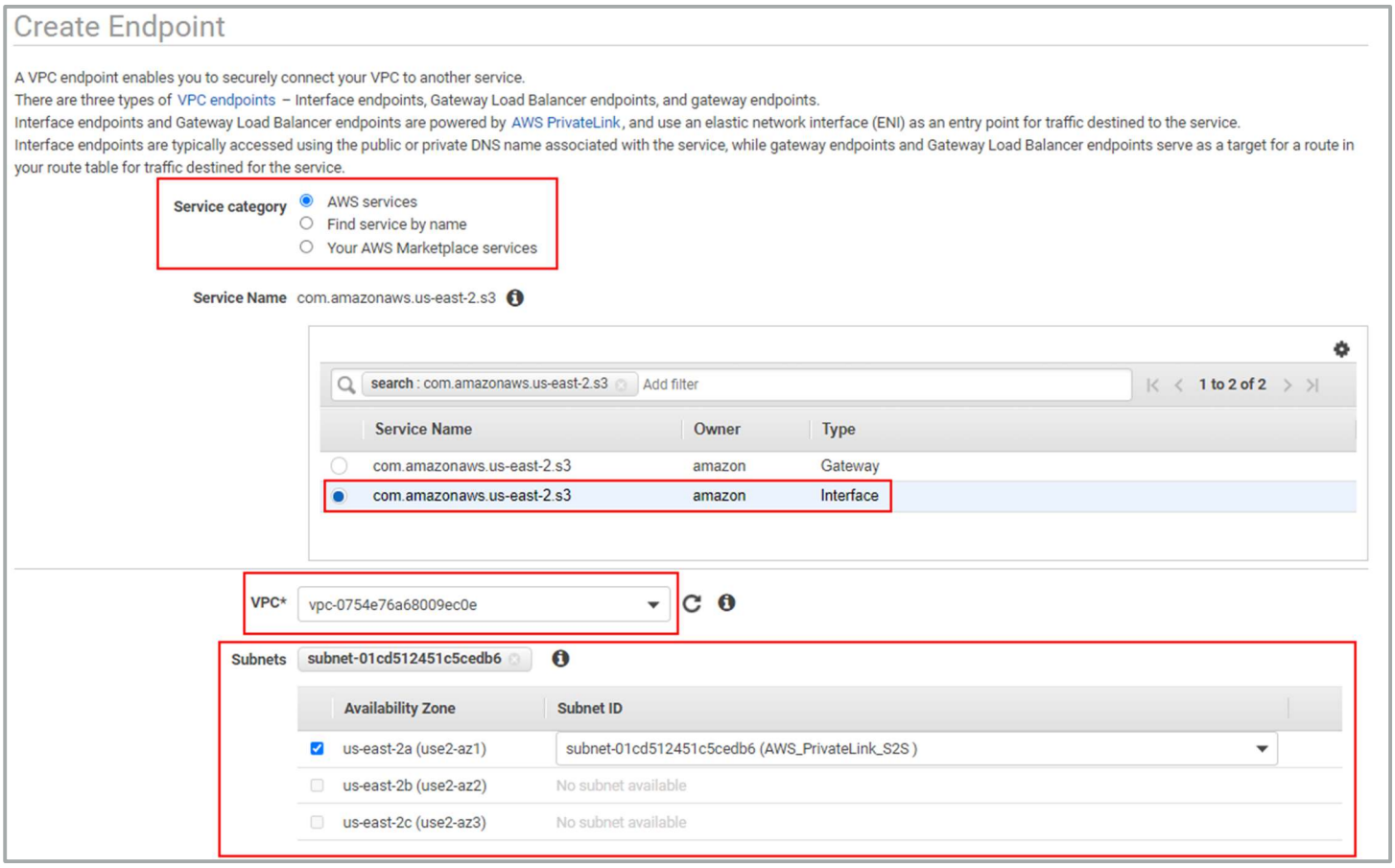
10. Next create a Customer Gateway. Give it a name, select Static Routing and enter in the public IP address given by your IT department.



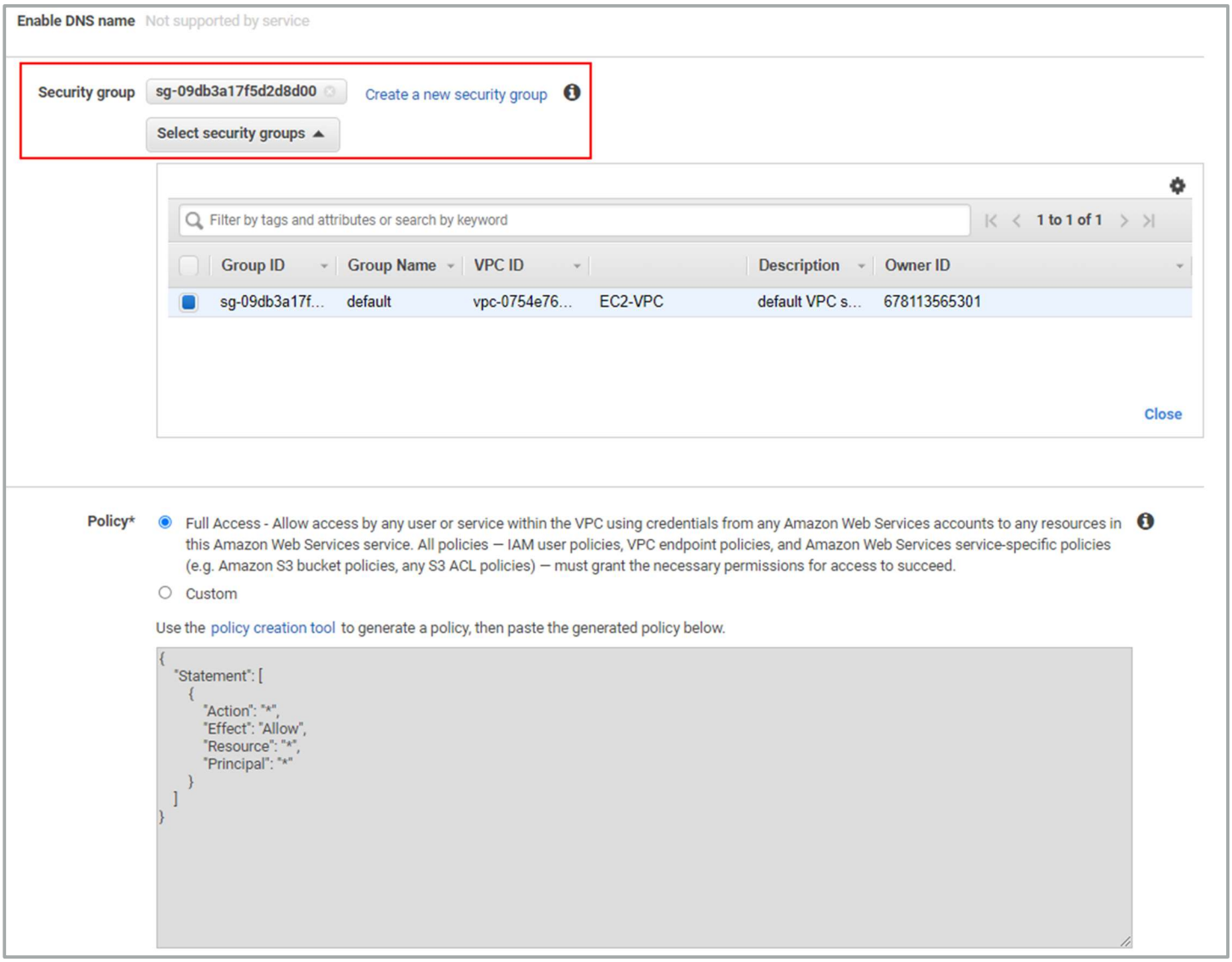
11. Add your on-premises IP CIDR block to the VPC route table with the VPG as the target. This CIDR block is usually the subnet that the NetBackup on-premises infrastructure is on.



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

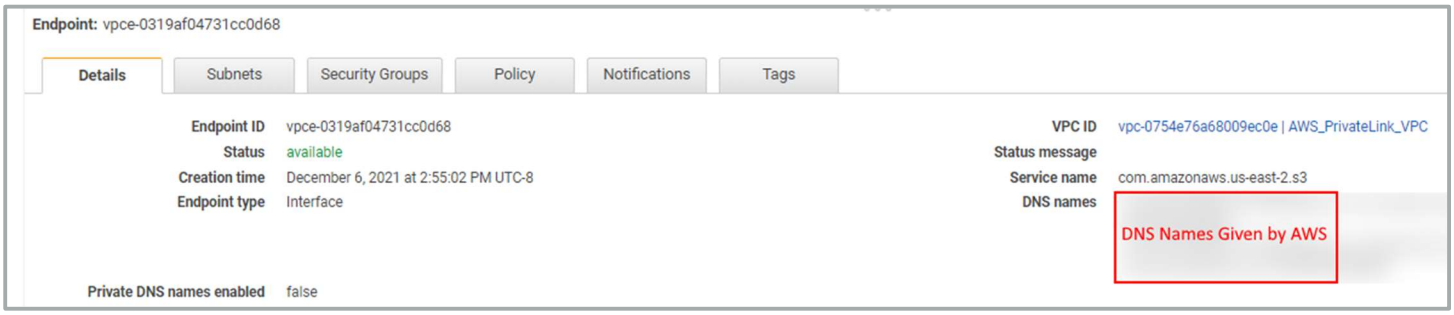


13. The next step is to create the Endpoint. (Part 1)
    - Service Category – AWS Services
    - Service name will depend on the region your PrivateLink is deployed in. In this example we are using com.amazonaws.us-east-2.s3 with type as Interface.

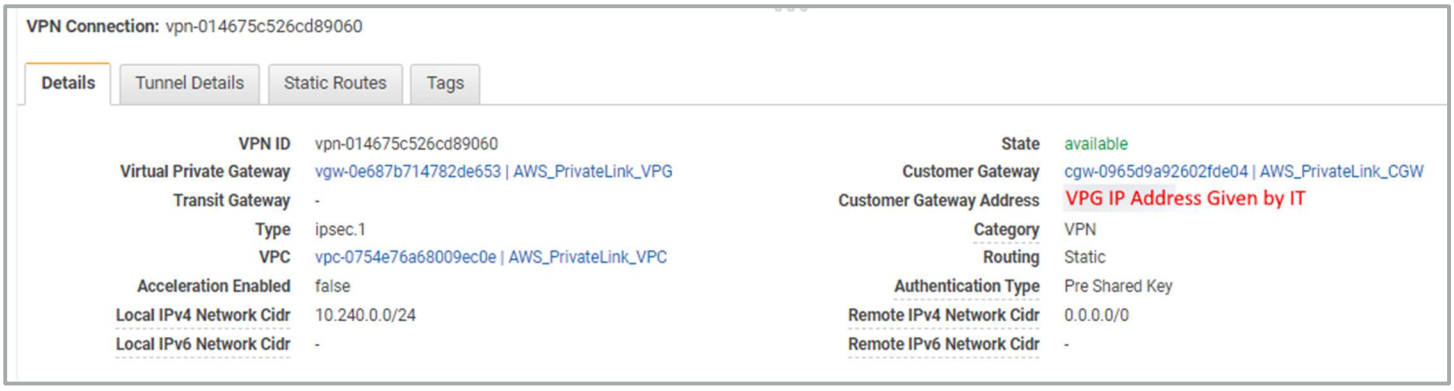


14. Endpoint Part 2.
    - Select the Security Group for this VPC.
    - If you would like to add specific access it can be entered here.

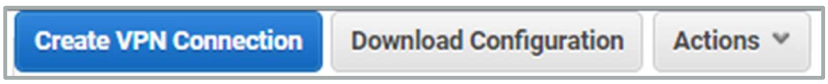
15. Endpoint Part 3.
    - Add any necessary Tags and click on Create Endpoint.



16. Endpoint Part 4.
    - Copy down the DNS Names given by AWS, you will need these to connect from your NetBackup infrastructure.



17. Create a Site to Site VPN connection. You will need the VPC CIDR Block, VPG given by your IT department and the on-premise CIDR block that your NetBackup infrastructure is located on. (The on-prem CIDR block is not show in this image. Static routing is used in this example.)



18. 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 needed for PrivateLink.

19. Once the on-premises configurations are complete, it's time to validate the PrivateLink works correctly.

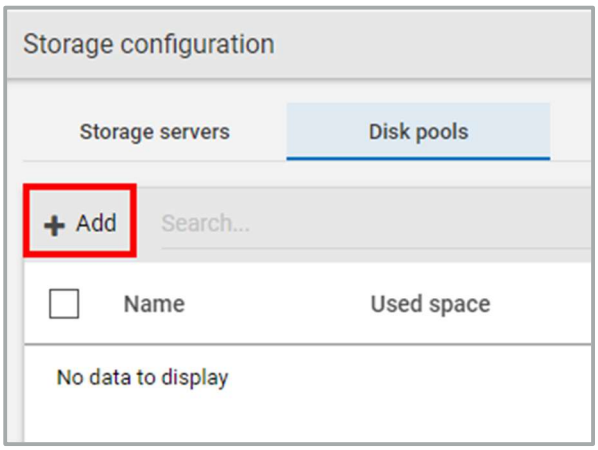
    From the terminal of the Primary NetBackup server type the following command:

```
openssl s_client -showcerts -connect bucket.The_DNS_Name_AWS_Gave:443
```

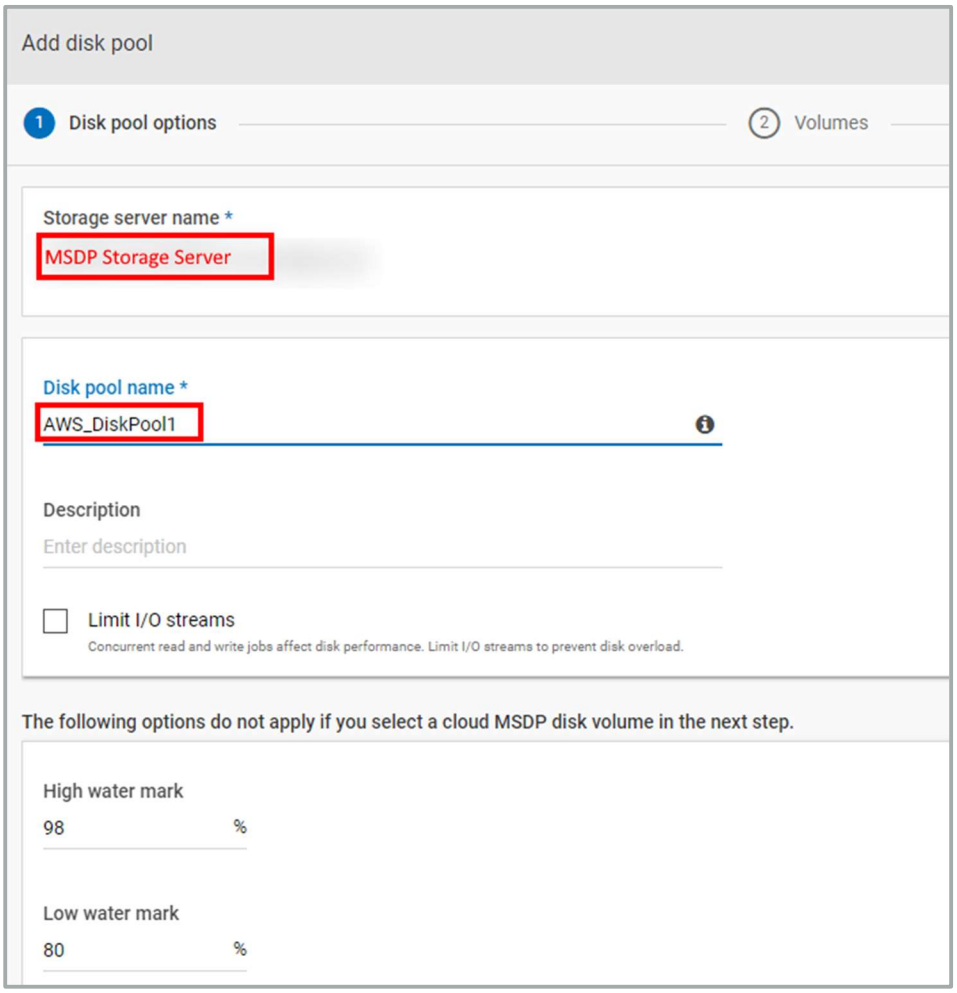
If everything is configured correctly, the connection should be successful, and a list of SSL certificates will be shown.

Use NetBackup to Connect to AWS Using PrivateLink

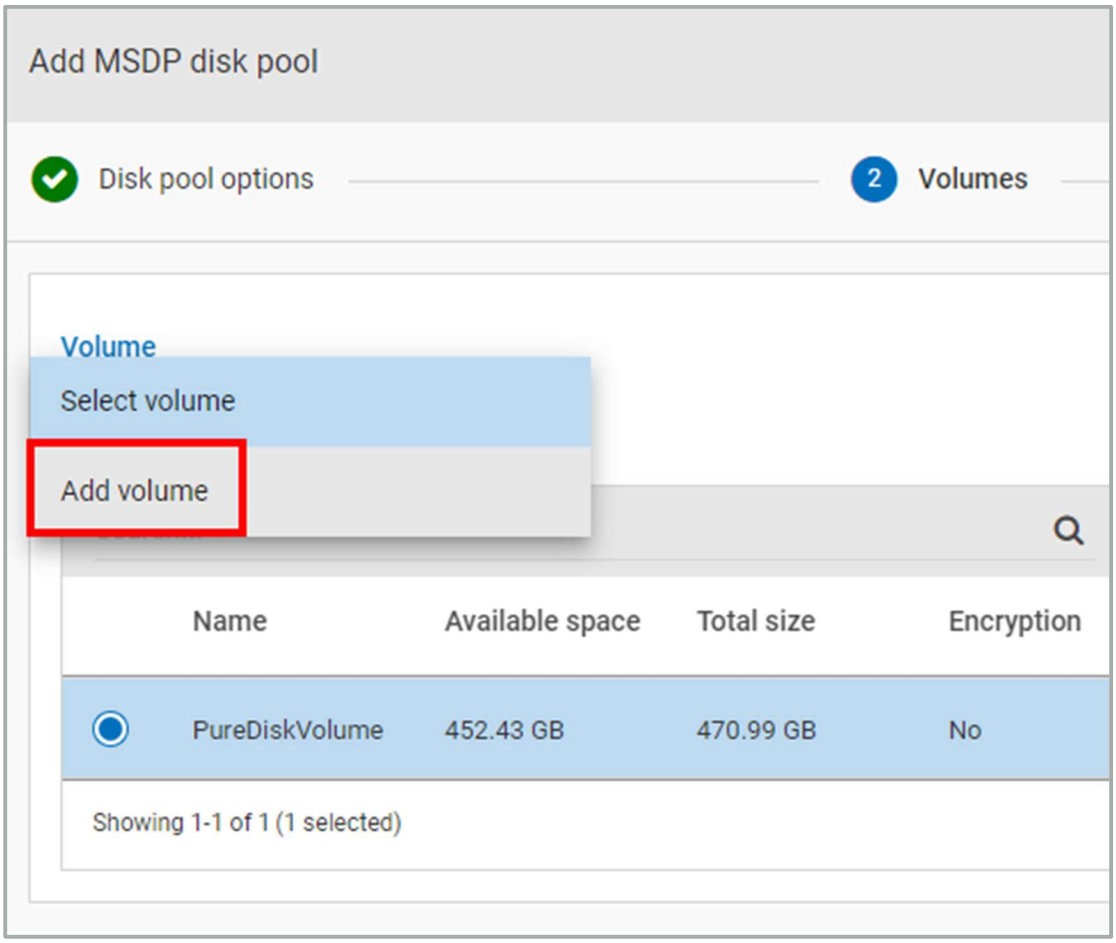
To connect to the newly created AWS PrivateLink, log into the NetBackup Primary server and navigate to Storage > Storage Configuration. An MSDP Storage Server will need to be added or an existing one can be used. This document assumes one has already been created.



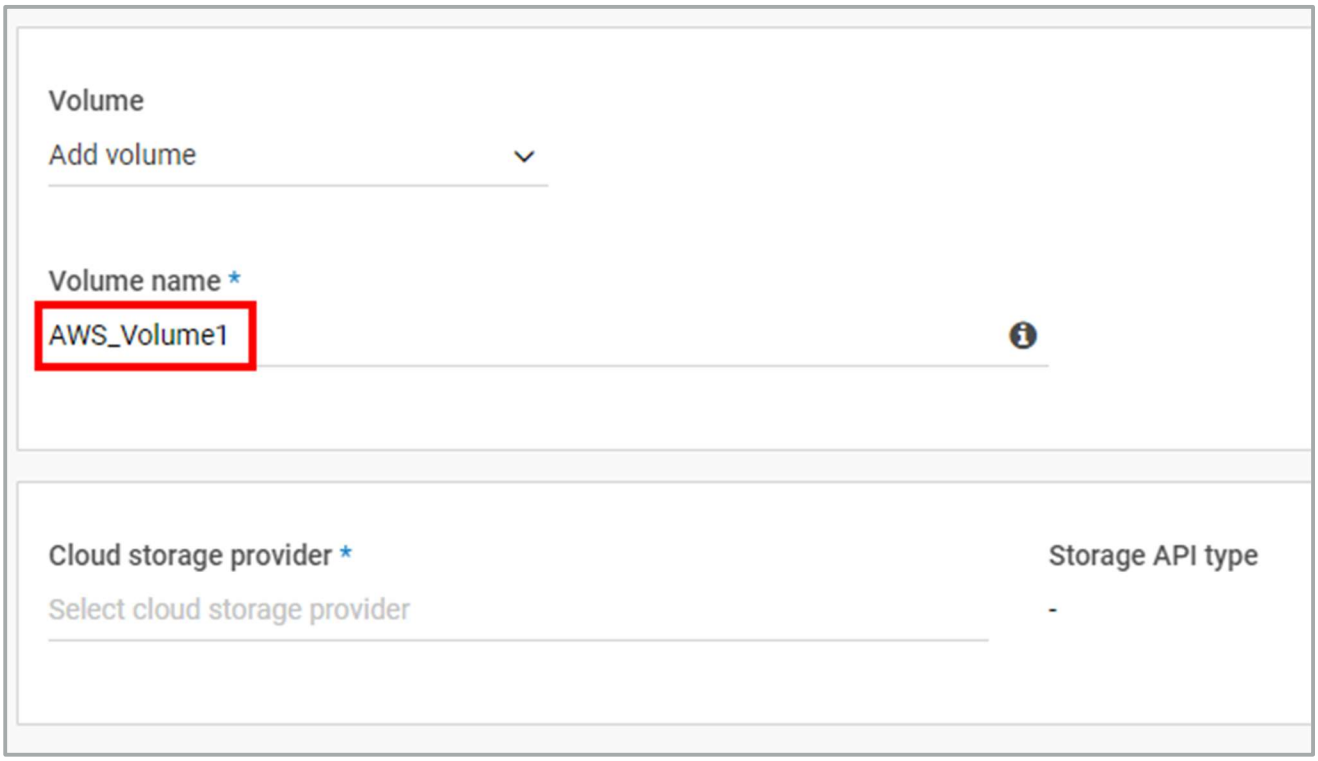
1. From Storage Configuration, click on Disk Pools and +Add to create a new Disk Pool and Volume.



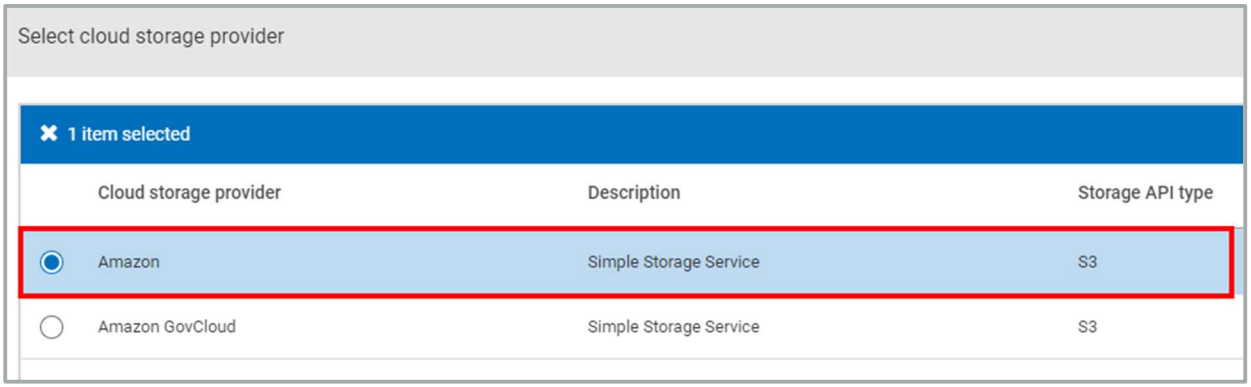
2. Select the MSDP server that will be used and give the new Disk Pool a name. Click Next to continue.

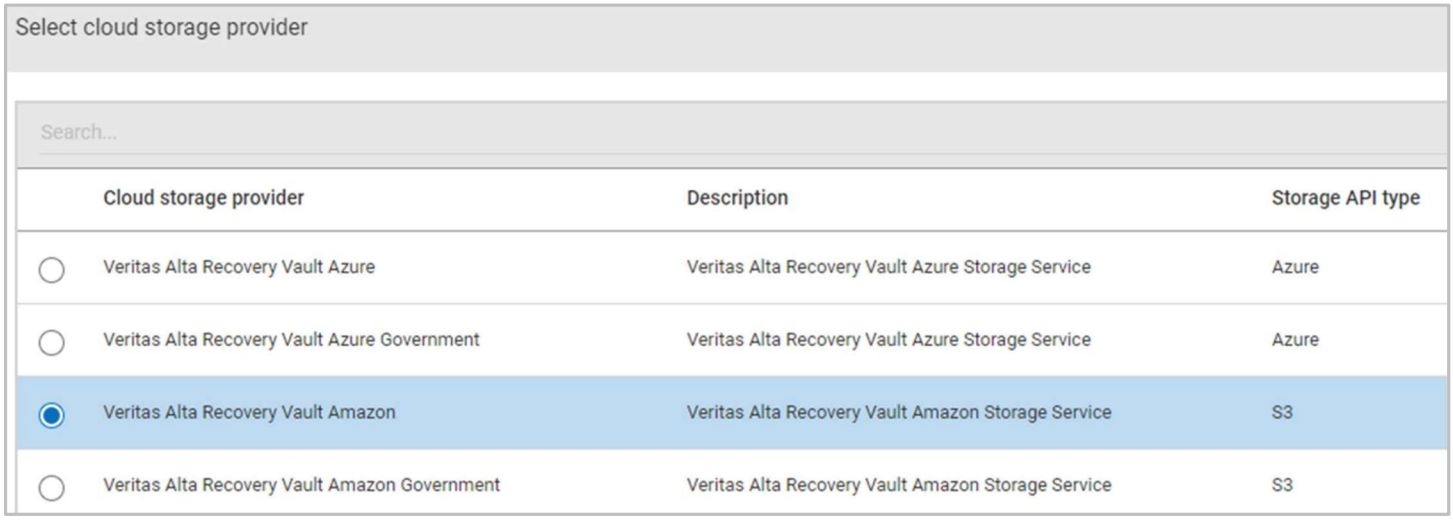


3. Next click on Add volume.



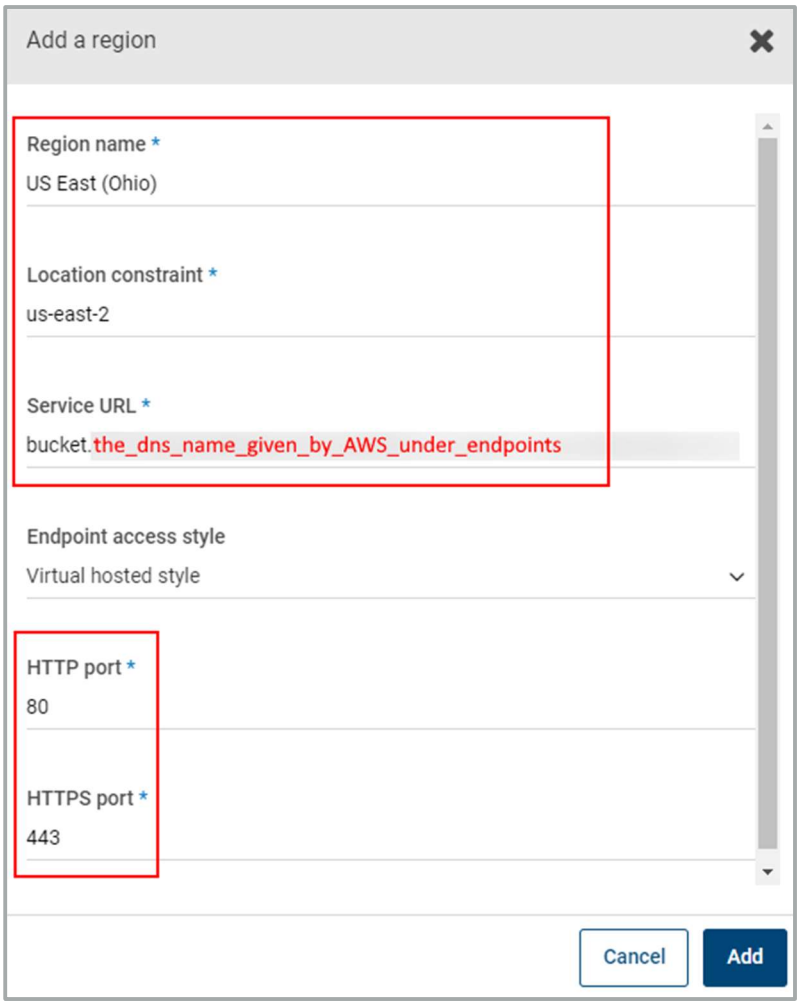
4. Add Volume Part 1.
    - Give The volume a name.
    - Click on Cloud Storage Provider.



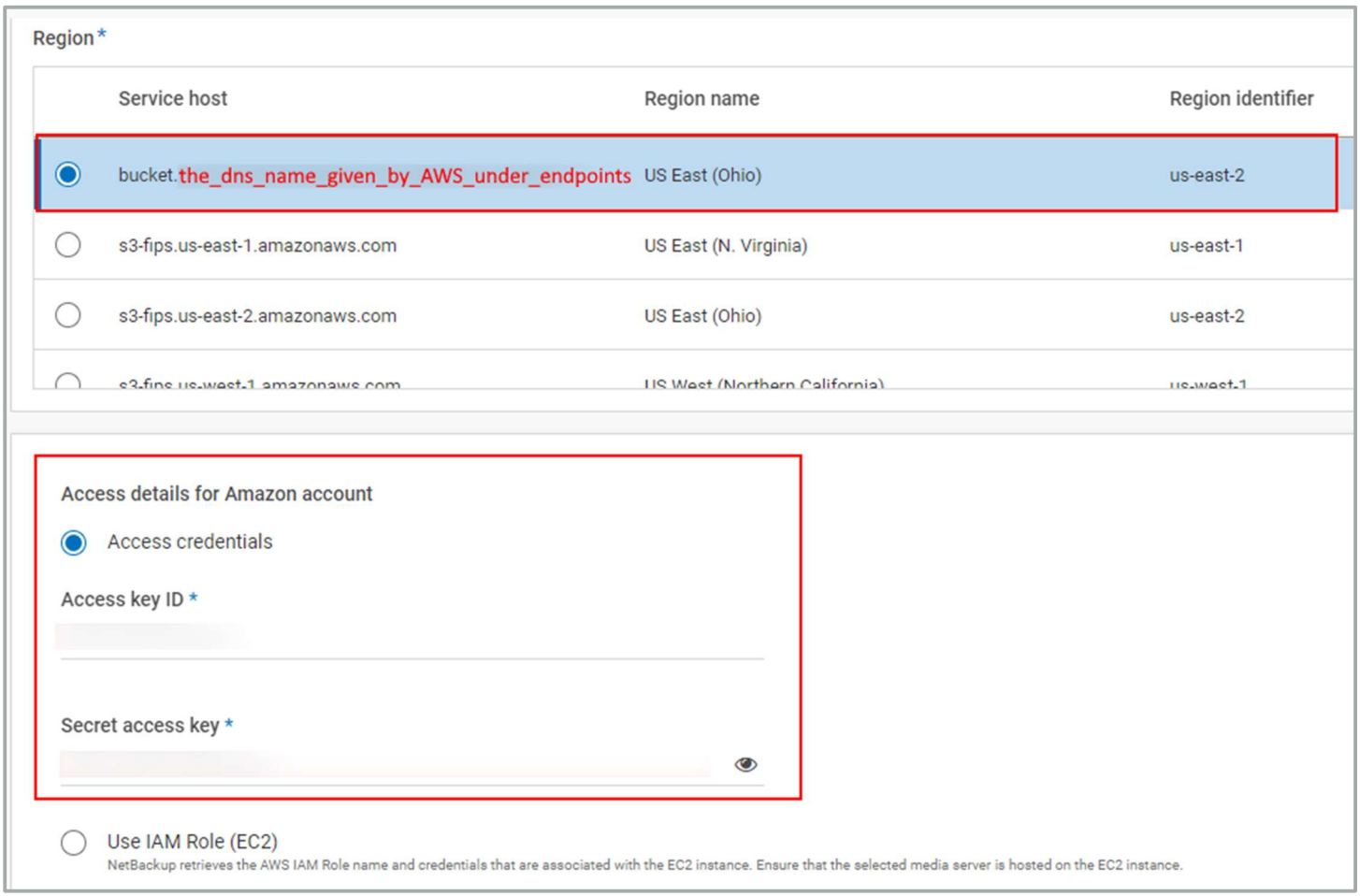


5. Add Volume Part 2.

- Click on Amazon and click select.
- For Alta Recovery Vault Amazon Bucket : 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.

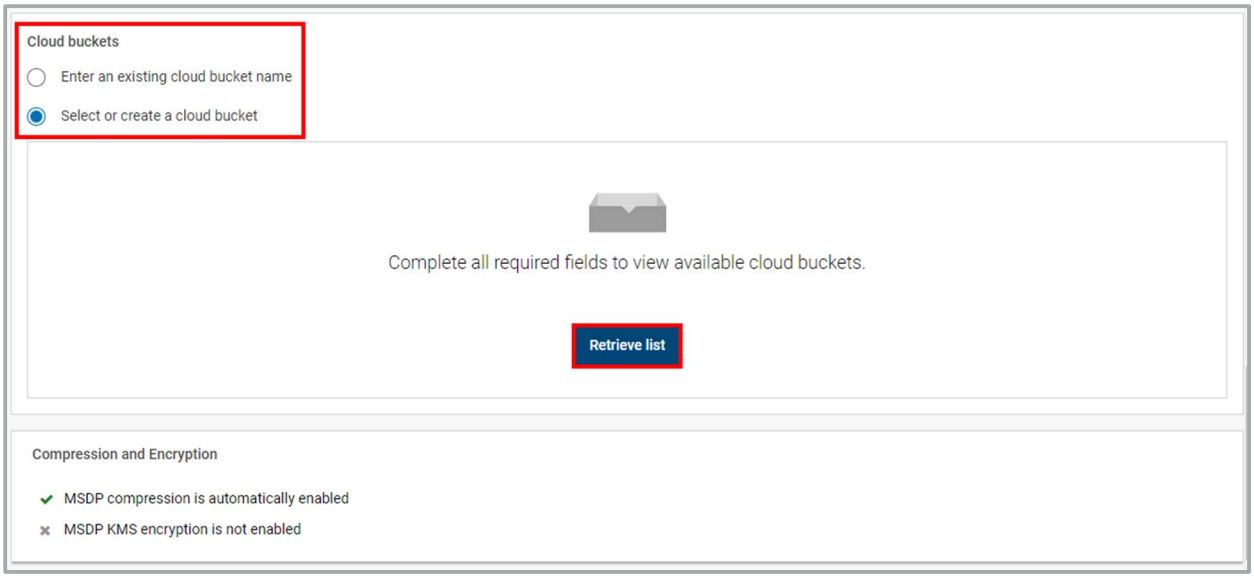


6. Add Volume Part 3.
    - Give the region a name.
    - Enter the Location Constraint.
    - Add the Service URL which is the DNS name given by AWS under Endpoints with the prefix “bucket.” attached.
    - Change or keep the defaults for HTTP/HTTPS ports.
    - Click on Add.

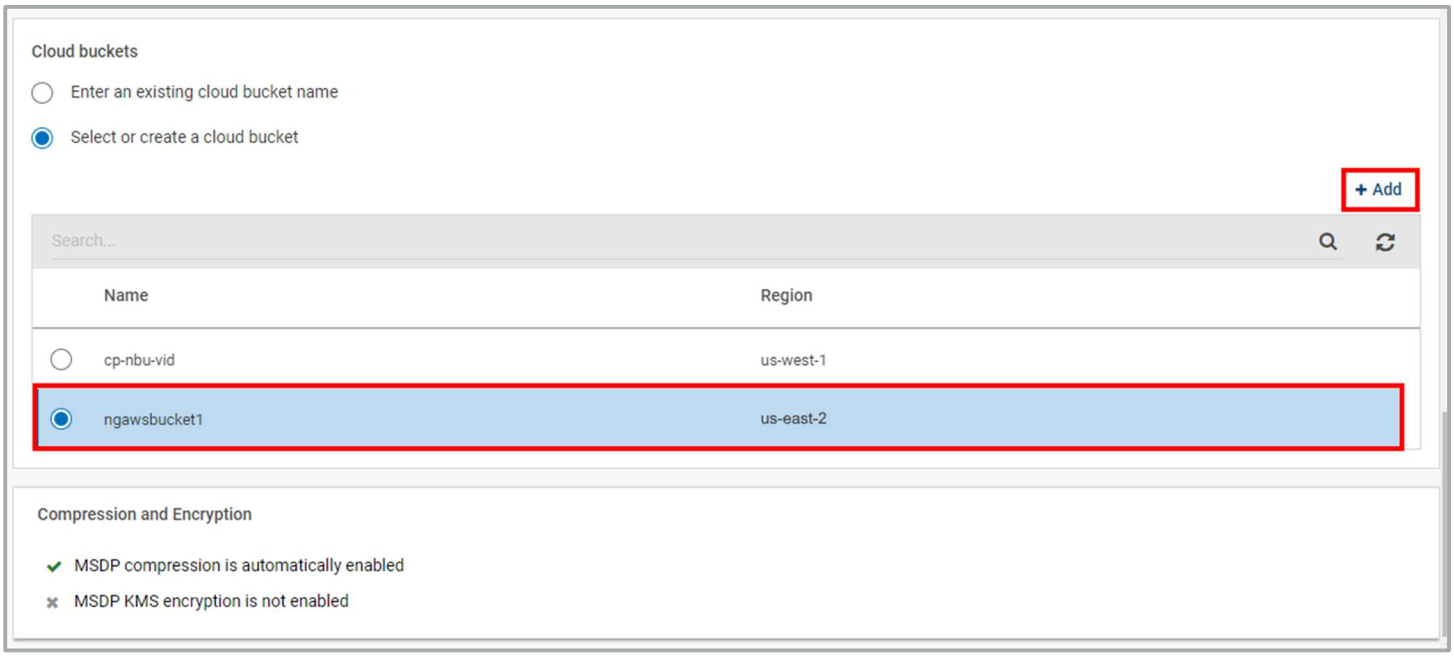


7. Add Volume Part 4.
    - Select the newly created Region.
    - Enter in the AWS Access Credentials and Secret Access Key.

8. Add Volume Part 5.
    - Select if you would like to change any of the default security settings.

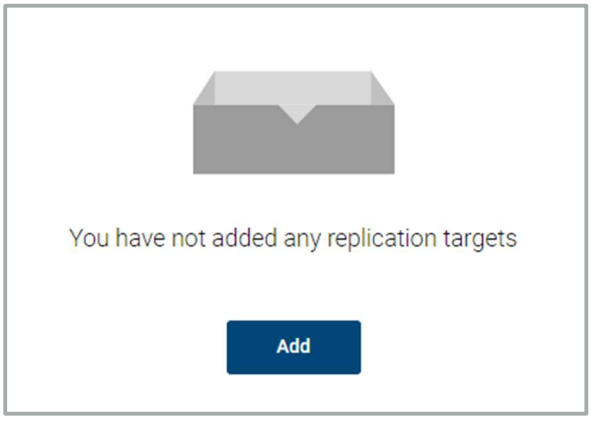


9. Add Volume Part 6.
    - Choose Select or create a cloud bucket.
    - Click on Retrieve List to connect to AWS.

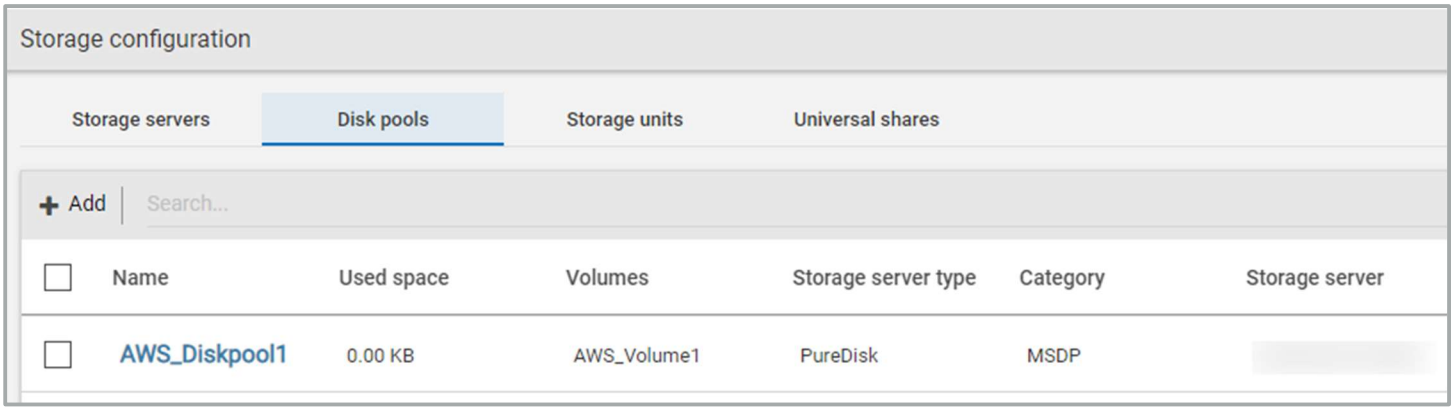


10. Add Volume Part 7.
    - After connecting to AWS, either select a pre-created bucket or click on the +Add button to create a new bucket.
    - Click Next to continue.

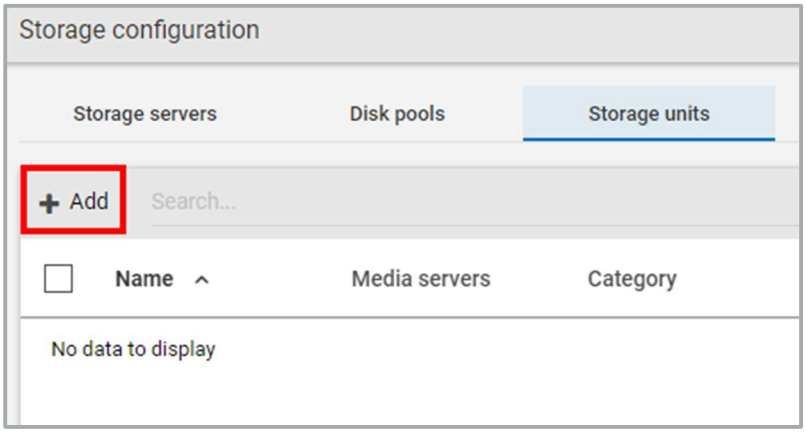
11. Add volume Part 8.
    - Add any replication targets if required.



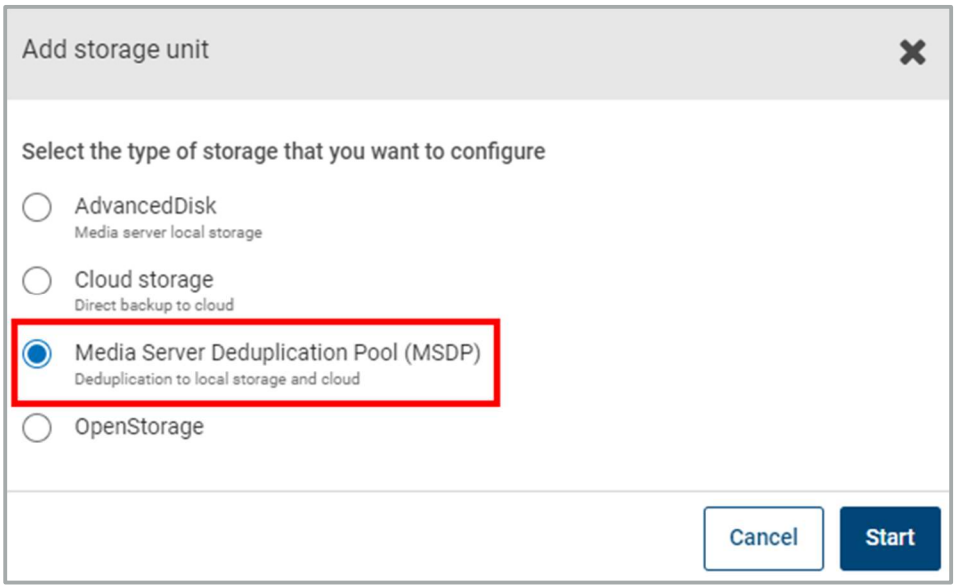
12. Add Volume Part 9.
    - Review what will be created and click Finish.



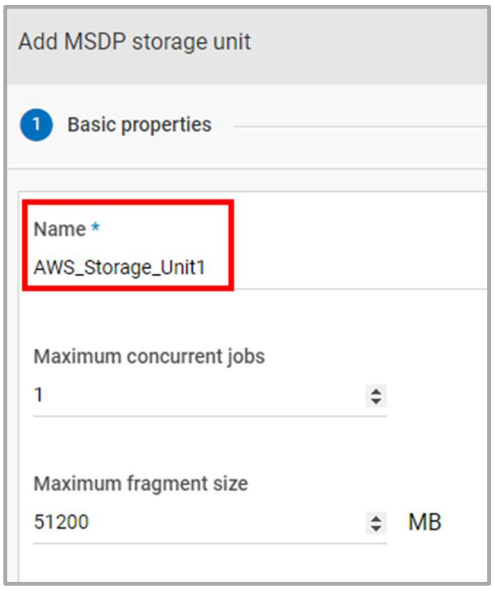
13. The Disk Pool has been created and the next step is to add a Storage Unit so backups can use the new AWS PrivateLink.



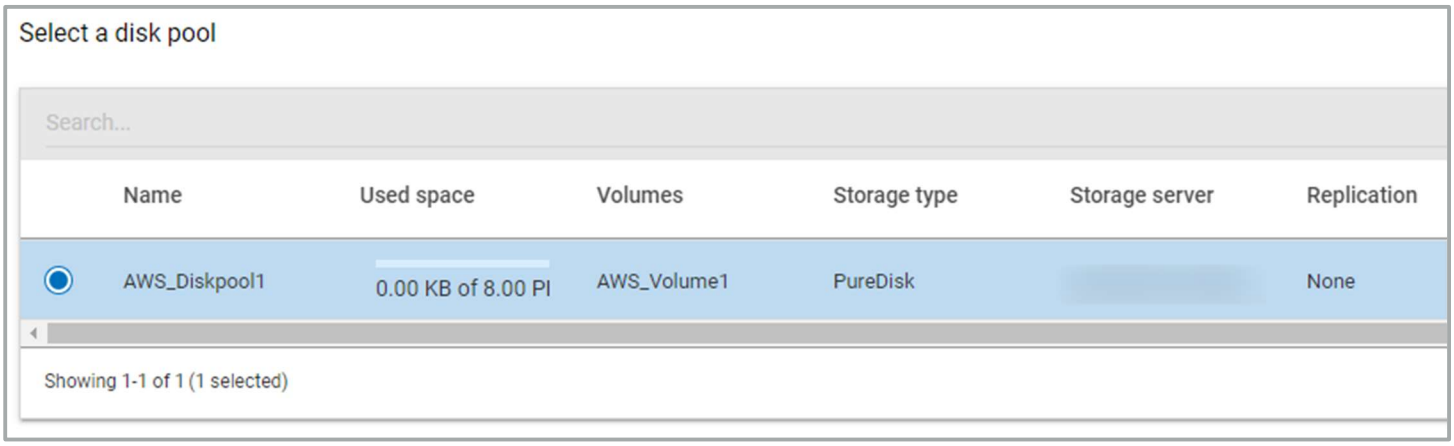
14. Click on the Storage Units tab and click on +Add.



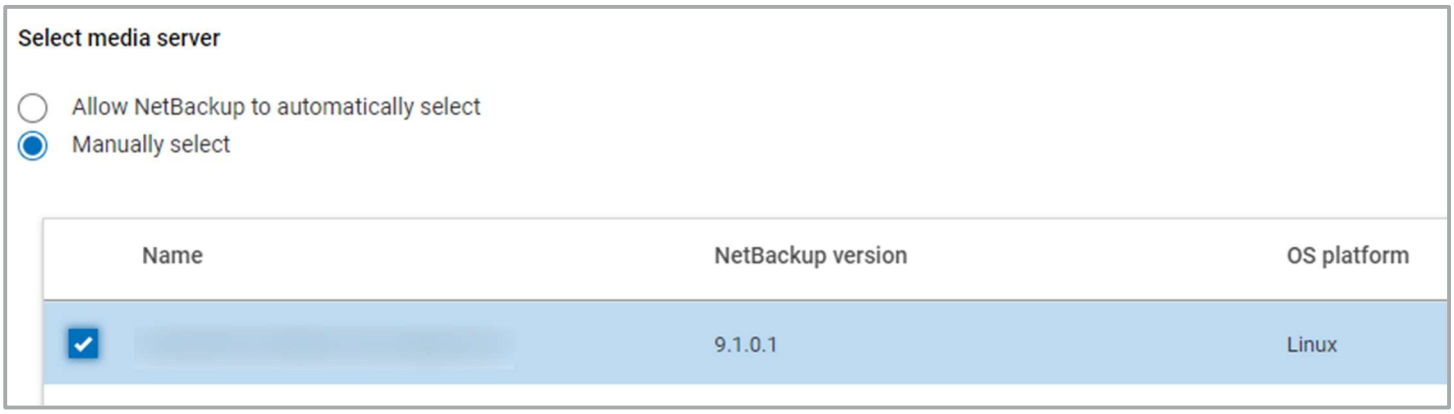
15. Select MSDP and click Start.



16. Name the MSDP Storage Unit and click on Next.



17. Select the disk pool recently created.



18. Select Media Server you'd like to use.
19. When the desired selections have been made, click on Save.
20. The storage configuration is complete, and the new media can be used to perform backups.

Conclusion

With Veritas NetBackup, Veritas Alta Recovery Vault and AWS PrivateLink, users can now safely transfer data to and from the AWS cloud without the risk of exposing sensitive data to visibility, tampering or theft. Users can now access S3 directly as a private endpoint using a secure, virtual network which leverages a new interface endpoint within your Virtual Private Cloud (VPC).

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.

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

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