

Veritas NetBackup on AWS PrivateLink for Amazon S3 Deployment Guide

Securing NetBackup Data Between
on Premises and AWS S3

Table of Contents

Introduction.....	4
Why Would I Want It?	4
How it Works – The Short Version.....	4
The Architecture.....	5
In AWS:.....	5
In NetBackup:	5
On Premise VPN:.....	6
How it Works – The Long Version	7
Create the AWS PrivateLink Architecture Components.....	7
Use NetBackup to Connect to AWS Using PrivateLink.....	16
Conclusion.....	27

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

Veritas NetBackup on AWS PrivateLink for Amazon S3

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 an 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
```

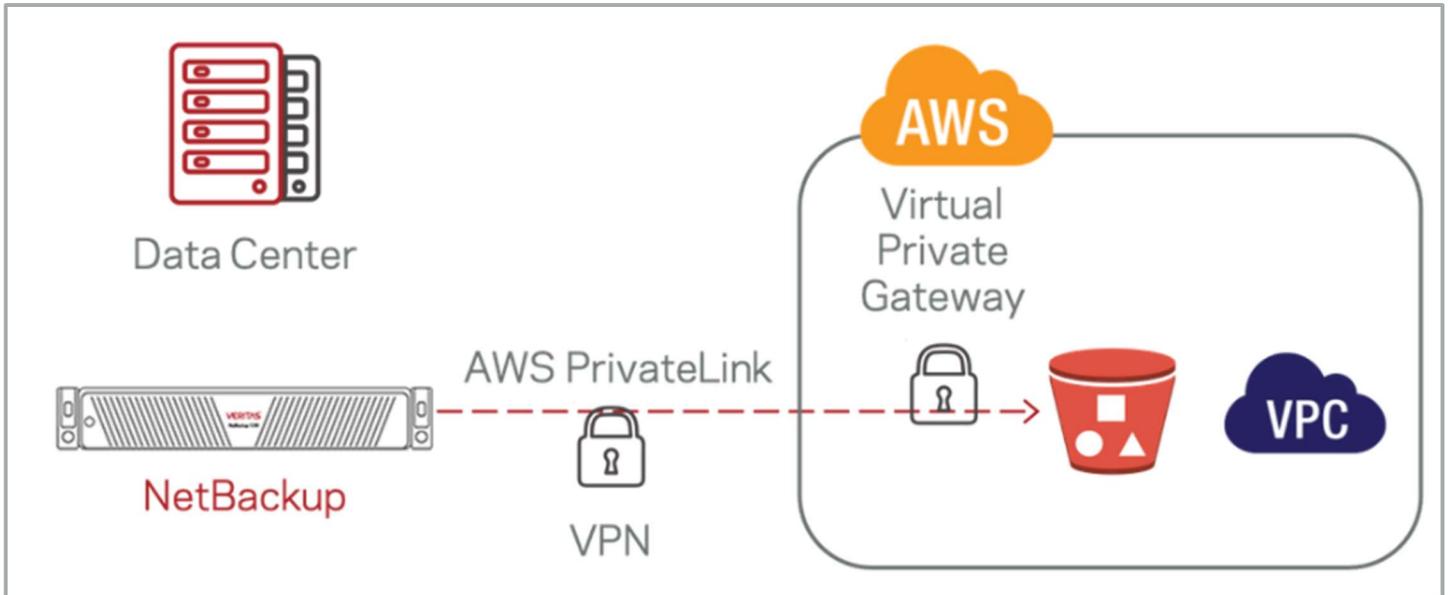
5. Add the PrivateLink Region Name, Location Constraint, Endpoint/Service URL and HTTP/HTTPS ports.



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:

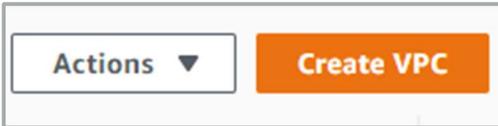
<https://docs.aws.amazon.com/vpc/latest/privatelink/vpce-interface.html>

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.

A screenshot of the 'Create VPC' configuration page in the AWS console. The page title is 'Create VPC' with an 'Info' link. Below the title is a descriptive sentence: 'A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.' The main content is divided into two sections: 'VPC settings' and 'Tags'.
VPC settings:
- 'Name tag - optional': A text input field containing 'AWS_PrivateLink_VPC', which is highlighted with a red box.
- 'IPv4 CIDR block': Two radio buttons are present. The first, 'IPv4 CIDR manual input', is selected. The second is 'IPAM-allocated IPv4 CIDR block - new'.
- 'IPv4 CIDR': A text input field containing '10.240.0.0/24', highlighted with a red box.
- 'IPv6 CIDR block': Four radio buttons are present. The first, 'No IPv6 CIDR block', is selected. The others are 'IPAM-allocated IPv6 CIDR block - new', 'Amazon-provided IPv6 CIDR block', and 'IPv6 CIDR owned by me'.
- 'Tenancy': A dropdown menu set to 'Default'.
Tags:
- A section titled 'Tags' with a descriptive sentence: 'A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.'
- Two input fields are shown: 'Key' with 'Name' and 'Value - optional' with 'AWS_PrivateLink_VPC'. Both fields have a search icon and a close icon. A 'Remove' button is to the right.
- An 'Add new tag' button is below the input fields.
- A note at the bottom of the tags section says 'You can add 49 more tags.'
At the bottom right of the form are 'Cancel' and 'Create VPC' buttons.

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.

Subnets (1) Info

Filter subnets

Subnet ID: subnet-01cd512451c5cedb6 X Clear filters

<input type="checkbox"/>	Name	Subnet ID	State
<input type="checkbox"/>	AWS_PrivateLink_S2S	subnet-01cd512451c5cedb6	Available

4. Create a subnet within the newly created VPC.

VIRTUAL PRIVATE NETWORK (VPN)

- Customer Gateways
- Virtual Private Gateways**
- Site-to-Site VPN Connections
- Client VPN Endpoints

You do not have any Virtual Private Gateways in this region

Click the Create Virtual Private Gateway button to create your first Virtual Private Gateway

[Create Virtual Private Gateway](#)

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

Create Virtual Private Gateway

A virtual private gateway is the router on the Amazon side of the VPN tunnel.

Name tag ⓘ

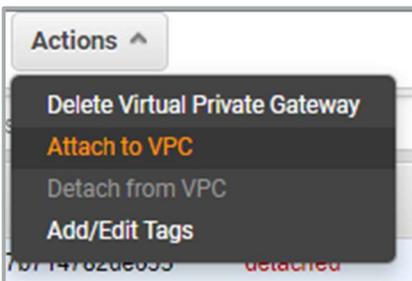
ASN Amazon default ASN ⓘ
 Custom ASN

* Required Cancel **Create Virtual Private Gateway**

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

Create Virtual Private Gateway		Actions ▾	
Filter by tags and attributes or search by keyword			
<input type="checkbox"/>	Name ▾	ID ▲	State
<input checked="" type="checkbox"/>	AWS_Private...	vgw-0e687b714782de653	detached

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.

Create Virtual Private Gateway		Actions
Filter by tags and attributes or search by keyword		
Name	ID	State
AWS_Private...	vgw-0e687b714782de653	attached

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

Create Customer Gateway

Specify the IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).

VPNs can use either Pre-Shared Keys or Certificates for authentication. When using Certificate authentication, an IP address is optional. To use Certificate authentication, specify a Certificate ARN when you create your Customer Gateway. To use Pre-Shared Keys, only an IP address is required.

Name:

Routing: Static Dynamic

IP Address:

Certificate ARN:

Device:

* Required Cancel

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.

Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (2)				
<input type="text" value="Filter routes"/>				
Destination			Target	
CIDR Block Given by IT			vgw-0e687b714782de653	
10.240.0.0/24			local	

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.

sg-09db3a17f5d2d8d00 - default									
Details	Inbound rules	Outbound rules	Tags						
Inbound rules (1/1)									
<input type="text" value="Filter security group rules"/>									
<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source		
<input checked="" type="checkbox"/>	-	sgr-07eadea191593d4c5	IPv4	HTTPS	TCP	443	CIDR Block Given by IT		

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

Create Endpoint

A VPC endpoint enables you to securely connect your VPC to another service. There are three types of VPC endpoints – Interface endpoints, Gateway Load Balancer endpoints, and gateway endpoints. Interface endpoints and Gateway Load Balancer endpoints are powered by AWS PrivateLink, and use an elastic network interface (ENI) as an entry point for traffic destined to the service. Interface endpoints are typically accessed using the public or private DNS name associated with the service, while gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Service category

- AWS services
- Find service by name
- Your AWS Marketplace services

Service Name com.amazonaws.us-east-2.s3 ⓘ

Add filter

	Service Name	Owner	Type
<input type="radio"/>	com.amazonaws.us-east-2.s3	amazon	Gateway
<input checked="" type="radio"/>	com.amazonaws.us-east-2.s3	amazon	Interface

VPC* vpc-0754e76a68009ec0e ⓘ

Subnets subnet-01cd512451c5cedb6 ⓘ

Availability Zone	Subnet ID
<input checked="" type="checkbox"/> us-east-2a (use2-az1)	subnet-01cd512451c5cedb6 (AWS_PrivateLink_S2S)
<input type="checkbox"/> us-east-2b (use2-az2)	No subnet available
<input type="checkbox"/> us-east-2c (use2-az3)	No subnet available

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.

Enable DNS name Not supported by service

Security group sg-09db3a17f5d2d8d00 [Create a new security group](#) ⓘ

Select security groups ▲

Filter by tags and attributes or search by keyword 1 to 1 of 1

<input type="checkbox"/>	Group ID	Group Name	VPC ID		Description	Owner ID
<input checked="" type="checkbox"/>	sg-09db3a17f...	default	vpc-0754e76...	EC2-VPC	default VPC s...	678113565301

[Close](#)

Policy* Full Access - Allow access by any user or service within the VPC using credentials from any Amazon Web Services accounts to any resources in this Amazon Web Services service. All policies — IAM user policies, VPC endpoint policies, and Amazon Web Services service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed. ⓘ

Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

```

{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

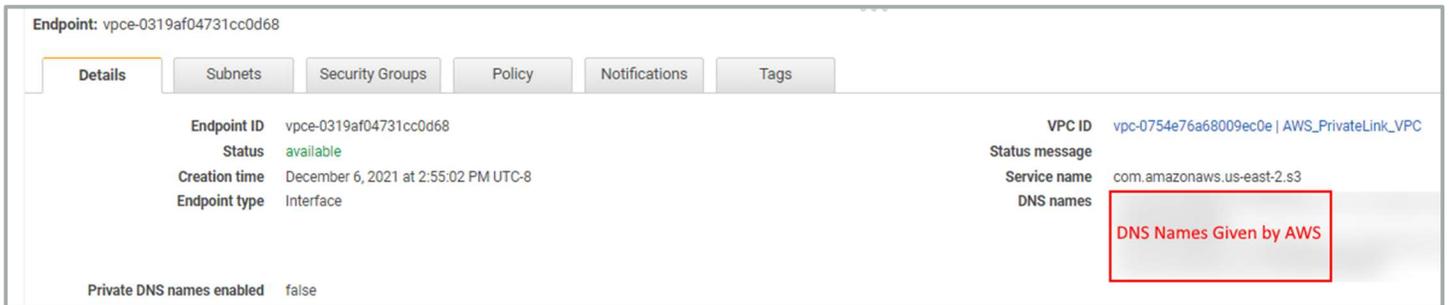
14. Endpoint Part 2.

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

Key <small>(128 characters maximum)</small>	Value <small>(256 characters maximum)</small>
<i>This resource currently has no tags</i>	
Add Tag 50 remaining <small>(Up to 50 tags maximum)</small>	
Cancel Create endpoint	

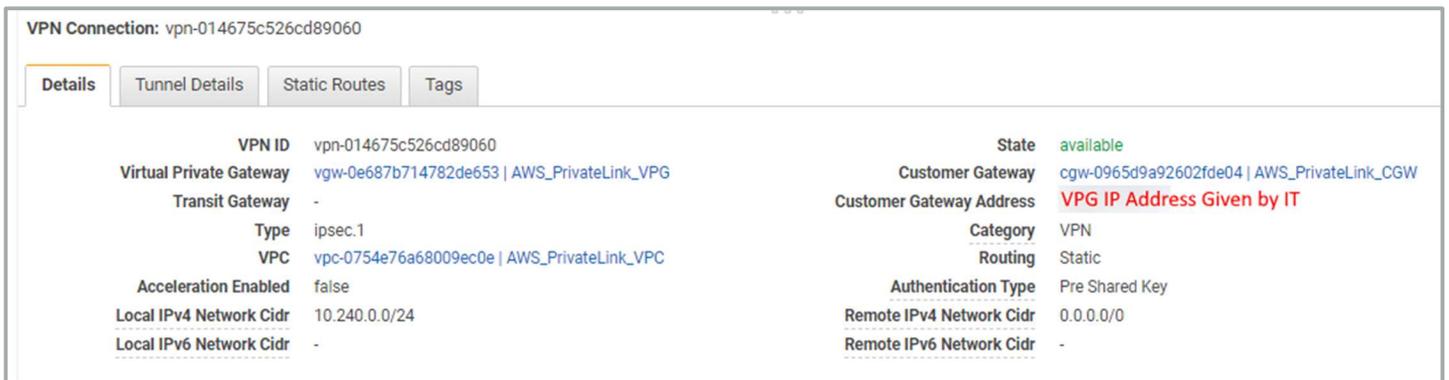
15. Endpoint Part 3.

- Add any necessary Tags and click on Create Endpoint.

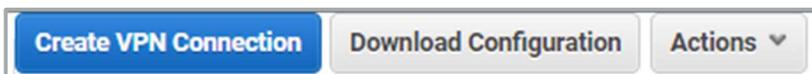


16. Endpoint Part 4.

- 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:

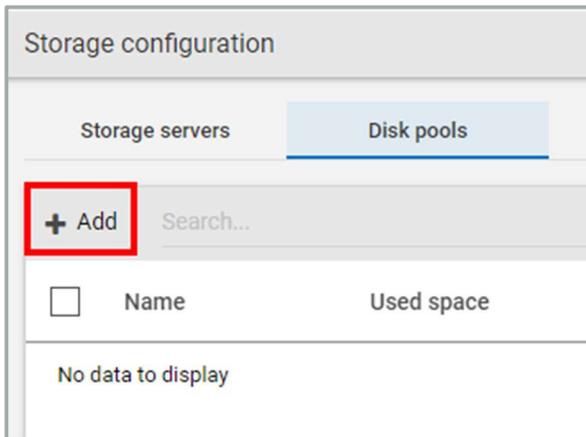
Veritas NetBackup on AWS PrivateLink for Amazon S3

```
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.

Add disk pool

1 Disk pool options 2 Volumes

Storage server name *
MSDP Storage Server

Disk pool name *
AWS_DiskPool1 ⓘ

Description
Enter description

Limit I/O streams
Concurrent read and write jobs affect disk performance. Limit I/O streams to prevent disk overload.

The following options do not apply if you select a cloud MSDP disk volume in the next step.

High water mark
98 %

Low water mark
80 %

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

Add MSDP disk pool

✓ Disk pool options ————— 2 Volumes

Volume

Select volume

Add volume

	Name	Available space	Total size	Encryption
<input checked="" type="radio"/>	PureDiskVolume	452.43 GB	470.99 GB	No

Showing 1-1 of 1 (1 selected)

3. Next click on Add volume.

Volume
Add volume ▼

Volume name *
AWS_Volume1 ⓘ

Cloud storage provider * **Storage API type**
Select cloud storage provider -

4. Add Volume Part 1.

- Give The volume a name.
- Click on Cloud Storage Provider.

Select cloud storage provider

✕ 1 item selected

Cloud storage provider	Description	Storage API type
<input checked="" type="radio"/> Amazon	Simple Storage Service	S3
<input type="radio"/> Amazon GovCloud	Simple Storage Service	S3

Veritas NetBackup on AWS PrivateLink for Amazon S3

Select cloud storage provider

Search...

Cloud storage provider	Description	Storage API type
<input type="radio"/> Veritas Alta Recovery Vault Azure	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input type="radio"/> Veritas Alta Recovery Vault Azure Government	Veritas Alta Recovery Vault Azure Storage Service	Azure
<input checked="" type="radio"/> Veritas Alta Recovery Vault Amazon	Veritas Alta Recovery Vault Amazon Storage Service	S3
<input type="radio"/> Veritas Alta Recovery Vault Amazon Government	Veritas Alta Recovery Vault Amazon Storage Service	S3

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.

Add a region ✕

Region name *
US East (Ohio)

Location constraint *
us-east-2

Service URL *
bucket.the_dns_name_given_by_AWS_under_endpoints

Endpoint access style
Virtual hosted style

HTTP port *
80

HTTPS port *
443

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.

Region *

Service host	Region name	Region identifier
<input checked="" type="radio"/> bucket.the_dns_name_given_by_AWS_under_endpoints	US East (Ohio)	us-east-2
<input type="radio"/> s3-fips.us-east-1.amazonaws.com	US East (N. Virginia)	us-east-1
<input type="radio"/> s3-fips.us-east-2.amazonaws.com	US East (Ohio)	us-east-2
<input type="radio"/> s3-fips.us-west-1.amazonaws.com	US West (Northern California)	us-west-1

Access details for Amazon account

Access credentials

Access key ID *

Secret access key *

Use IAM Role (EC2)
NetBackup retrieves the AWS IAM Role name and credentials that are associated with the EC2 instance. Ensure that the selected media server is hosted on the EC2 instance.

7. Add Volume Part 4.

- Select the newly created Region.
- Enter in the AWS Access Credentials and Secret Access Key.

Advanced settings

Security

Use SSL

Authentication only

Authentication and data transfer

Check certificate revocation (IPv6 not supported for this option)

Enable server-side encryption

Proxy

Use proxy server

WORM

Use object lock

NetBackup retrieves the Object Lock information from Cloud storage. Ensure that the targeting bucket is created, and the Object Lock mode is set. Refer to the NetBackup Deduplication Guide for more details.

8. Add Volume Part 5.

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

Cloud buckets

Enter an existing cloud bucket name

Select or create a cloud bucket

Complete all required fields to view available cloud buckets.

Retrieve list

Compression and Encryption

✓ MSDP compression is automatically enabled

✗ MSDP KMS encryption is not enabled

9. Add Volume Part 6.

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

Cloud buckets

Enter an existing cloud bucket name

Select or create a cloud bucket

+ Add

Search...

Name	Region
<input type="radio"/> cp-nbu-vid	us-west-1
<input checked="" type="radio"/> ngawsbucket1	us-east-2

Compression and Encryption

✓ MSDP compression is automatically enabled

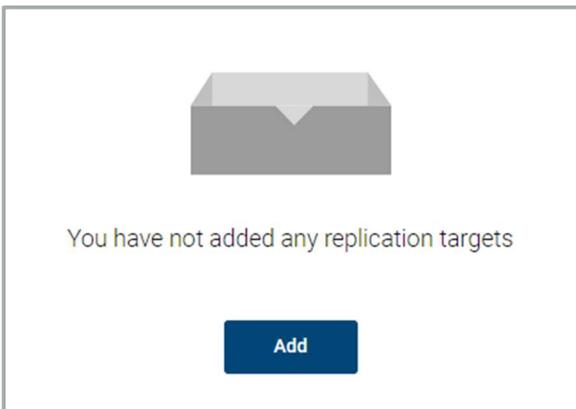
✗ MSDP KMS encryption is not enabled

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.
 - o Review what will be created and click Finish.

Storage configuration

Storage servers | **Disk pools** | Storage units | Universal shares

+ Add | Search...

<input type="checkbox"/>	Name	Used space	Volumes	Storage server type	Category	Storage server
<input type="checkbox"/>	AWS_Diskpool1	0.00 KB	AWS_Volume1	PureDisk	MSDP	

- 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.

Storage configuration

Storage servers | Disk pools | **Storage units**

+ Add | Search...

<input type="checkbox"/>	Name ^	Media servers	Category
No data to display			

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

The screenshot shows a dialog box titled "Add storage unit" with a close button (X) in the top right corner. Below the title bar, the text "Select the type of storage that you want to configure" is displayed. There are four radio button options: "AdvancedDisk" (Media server local storage), "Cloud storage" (Direct backup to cloud), "Media Server Deduplication Pool (MSDP)" (Deduplication to local storage and cloud), and "OpenStorage". The "Media Server Deduplication Pool (MSDP)" option is selected and highlighted with a red rectangular box. At the bottom right of the dialog, there are two buttons: "Cancel" and "Start".

15. Select MSDP and click Start.

The screenshot shows a configuration screen titled "Add MSDP storage unit". It has a tab labeled "1 Basic properties". Below the tab, there is a "Name *" field with the text "AWS_Storage_Unit1" entered, which is highlighted with a red rectangular box. Below this, there are two dropdown menus: "Maximum concurrent jobs" set to "1" and "Maximum fragment size" set to "51200" with "MB" as a unit. The "Maximum fragment size" dropdown also has a small arrow icon next to it.

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

Select a disk pool

Search...

Name	Used space	Volumes	Storage type	Storage server	Replication
<input checked="" type="radio"/> AWS_Diskpool1	0.00 KB of 8.00 PI	AWS_Volume1	PureDisk		None

Showing 1-1 of 1 (1 selected)

17. Select the disk pool recently created.

Select media server

Allow NetBackup to automatically select

Manually select

Name	NetBackup version	OS platform
<input checked="" type="checkbox"/>	9.1.0.1	Linux

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](https://twitter.com/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.

VERITAS™