VERITAS

# Veritas Alta Recovery Vault Security Profile

## Cloud-based Storage-as-a-Service

*This guide is designed to highlight the security features built into Veritas Alta Recovery Vault.*

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

September 2024

## TABLE OF CONTENTS



## Revision History

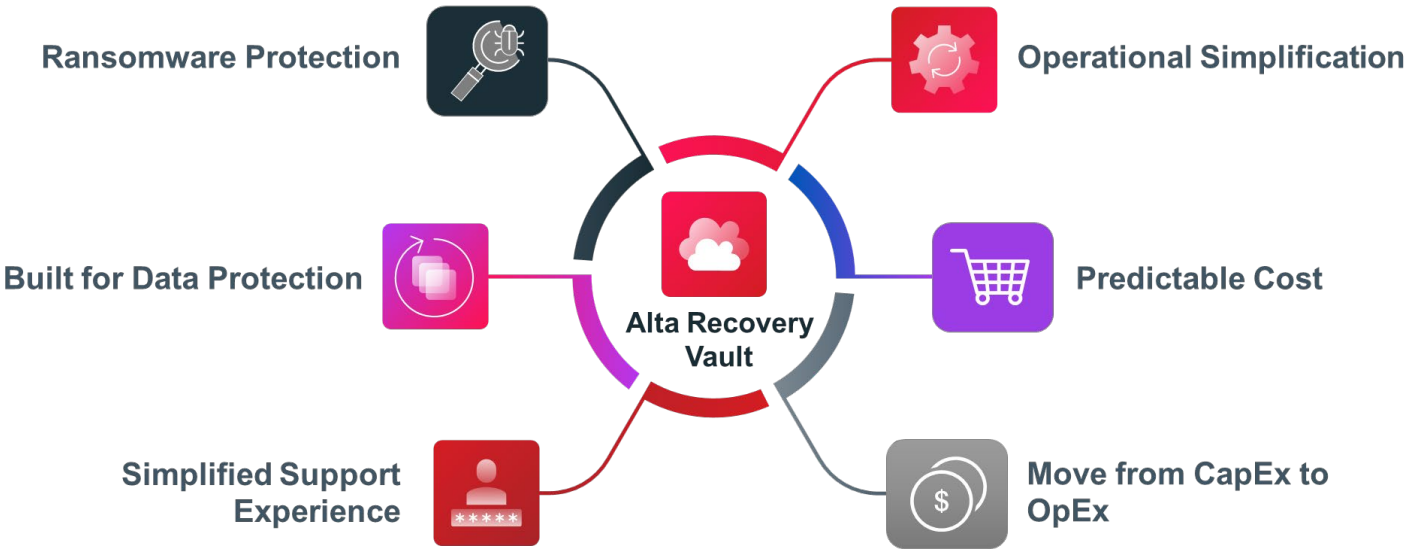
| Version | Date | Changes |
|---|---|---|
| 1.00 | 8/29/2022 | Initial Version |
| 1.01 | 12/16/2022 | Rebrand |
| 1.02 | 5/16/2023 | Azure ExpressRoute Added |
| 1.03 | 11/29/2023 | Tokens, AWS Direct Connect, updates added. |
| 1.04 | 2/1/2024 | GDPR Section Added. |
| 1.05 | 3/1/2024 | Updates for 10.4 |
| 1.06 | 8/27/2025 | Updates for 10.5 |

## Introduction

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, or protect a physical site to isolate backup data.

Veritas Alta Recovery Vault customers can protect their NetBackup™ compressed and deduplicated data in a secure Veritas tenant hosted by several cloud service providers (CSPs). Most storage as a service (STaaS) providers have adopted a shared responsibility model, which makes it clear that providers will not take any action to protect customer data. The job of protecting the data in the CSP is completely the responsibility of the customer. Customers who adopt Veritas Alta Recovery Vault benefit from the following results: • Complete backup and recovery of all application data • Fast and flexible data recovery • Secure and flexible provisioning.

Why Veritas Alta Recovery Vault?




**NECESSARY INFORMATION**

The first step to your journey to STaaS is to contact your NetBackup account manager. Your account manager will collect the necessary information needed to provision your Veritas Alta Recovery Vault storage account. Following are examples of the information you might provide to Veritas:

- Cloud provider(s)

- Data center region
- Number of buckets
- Size of the buckets
- Veritas account representative
- Veritas partner name
- Immutability support

  **Note:** Non-immutable storage is not available in Veritas Alta Recovery Vault.

## IMMUTABILITY/WORM

Immutability/WORM gives you the ability to write once, and read many, to your Veritas Alta Recovery Vault storage, and to select how long you would like the images to be retained. In the event of a threat actor/malware compromise, immutability prevents the threat actor from expiring your backup images in Veritas Alta Recovery Vault or manipulating the data in any way.

Veritas Alta Recovery Vault currently supports Governance mode (also known as Enterprise mode). Governance immutability gives users special permissions to disable the retention lock and then delete the image.

Governance mode allows users to accelerate the expiration of images, compliance mode does not allow this. Alta Recovery Vault is closer to compliance mode because no users have the ability to shorten a lock duration since the customer is not the cloud tenant for the storage.

**Note**: Only the cloud administrator user can disable the retention lock and then delete the image if required. For Veritas Alta Recovery Vault, Veritas is the cloud administrator.

When requesting storage from Veritas, your Veritas Alta Recovery Vault storage buckets, created by Veritas, will have immutability enabled. All NetBackup cloud storage units must be created with Governance mode immutability enabled to ensure that data is written in an immutable format.

**Note**: For more information about immutability and the msdpcldutil command, refer to these NetBackup Deduplication Guide resources:

veritas.com/support/en_US/doc/25074086-159245004-0/v152917675-159245004

VERITAS.COM/SUPPORT/EN_US/DOC/25074086-149019166-0/V149102641-149019166

## SHORT-LIVED TOKEN-BASED AUTHENTICATION

With NetBackup 10.2 and later for Azure and 10.4 and later for AWS, 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.

Azure users are given their storage account and a refresh token to connect to their Veritas Alta Recovery Vault storage. Once this new information has been provided, you can create a credential in Credential Management.

## ROLE-BASED ACCESS CONTROL (RBAC)

Veritas Alta Recovery Vault is built right into NetBackup, with the ability to apply RBAC in your environment. Use RBAC to provide access for users who do not currently have access to NetBackup. Or, for current NetBackup users with administrator access, you can provide limited access and permissions based on their role in your organization.

The following are relevant roles included with NetBackup for Veritas Alta Recovery Vault:

1. **Administrator**
    a. **This role has permissions to perform all actions within the NetBackup Web UI.**
2. **Default Security Administrator**
    a. This role has permissions to manage NetBackup security, including RBAC, certificates, hosts, identity providers and domains, global security settings, and other permissions. This role can also view settings and assets in most areas of NetBackup, including workloads, storage, licensing, and other areas.
3. **Default Storage Administrator**
    a. This role has permissions to configure and manage disk-based storage and cloud storage.

Either the Storage Administration or the Administrator must perform the modifications to the MSDP storage to add a cloud tier. The Security Administrator may also be involved if a new media server is involved as part of the preparation of the environment to add Veritas Alta Recovery Vault. Security Administrators do not have permissions to see or modify storage configurations.

## HOW VERITAS ALTA RECOVERY VAULT COMMUNICATES IN NETBACKUP

NetBackup primary server, media servers, and clients communicate with each other using TLS architecture that conforms to the X.509 Public Key Infrastructure (PKI) standard in the form of certificates, either managed by the primary server or by an external certificate authority. This is a common form of endpoint verification on the web. Cloud providers will also have their own certificates for TLS encrypted communication. Communication and data transmission between the NetBackup deduplication engine and the cloud tier leverages this same trust of the cloud vendor certificates. Our Cloud Provider package reflects the cloud solutions currently supported.

Ensure secure communication with the media server hosting MSDP, according to the procedures in the NetBackup Security & Encryption Guide. Communication to AWS or Azure for Veritas Alta Recovery Vault is handled by the Cloud Provider package, where the certificates are already trusted by NetBackup. The version of the Cloud Provider package is aligned to the version of NetBackup.

When setting up the cloud tier for MSDP, after the storage account information has been added, additional security settings are available in the Advanced section. By default, SSL is enabled, and this is also where to toggle immutability using object lock.

**Note:** In NetBackup version 10.2 and above, the primary server communicates with the Veritas Alta Recovery Vault webserver over port 443, and the media server communicates with the cloud service provider (Azure or AWS) over port 443 and uses port 80 for certificate revocation listing (CRL). If you do not wish to open port 443 on the primary server, a proxy server can be used.

Pre NetBackup 10.2, only the media server communicates to the CSP over ports 443 and 80 for CRL. If you do not wish to open port 443 from the media server, a proxy server can be used.

**Note:** Azure ExpressRoute and AWS Direct Connect can also be used and are discussed in this paper.

**Note:** Veritas Alta Recovery Vault is designed as a public internet facing service and as such can only be connected to via a Public ExpressRoute configuration / Microsoft Peering or Public Peering. Private ExpressRoute peering / Private Peering is not supported.

## VERITAS ALTA RECOVERY VAULT SECURITY FUNDAMENTALS AND ARCHITECTURE

Veritas Alta Recovery Vault uses media server deduplication pool cloud tier (MSDP-C) to directly write deduplicated data to cloud object storage from memory.

Unlike traditional MSDP-C, Veritas manages cloud object storage, and each customer has their own storage account and keys (Azure), access key id/secret key(token), and IAM roles for MSDP-C in AWS(token). In

addition, a customer may choose to set IP restrictions on their object storage access. Communication to the external storage bucket requires port 443 to be opened outbound so the NetBackup API can communicate with the cloud provider's storage bucket through HTTPS.

The Veritas Alta Recovery Vault underlying cloud storage is provided by third parties, such as Microsoft Azure and Amazon Web Services (AWS). When provisioning Veritas Alta Recovery Vault, customers select the cloud data center locations/regions where the backup data is hosted. Veritas does not make copies or replicate your data.

## DATA SECURITY

Your data's security is paramount to Veritas. Customer data is categorized as *Highly Confidential* and always encrypted in transit. The service transmits using TLSv1.2 and stores all encrypted data in Azure blob or AWS storage using AES 256 cipher modules.

Any credentials stored within the NetBackup database are hashed and can also be stored using FIPS 140-2 cryptographic modules.

Note: FIPS 140-2 is only supported on Windows.

Available in 10.1 and later, customers can scan the stored Veritas Alta Recovery Vault backups for malware using the NetBackup Malware Scanner or third-party malware scanner integrations using customer-provided Microsoft Defender or Symantec's Protection Engine. When a customer wishes to perform a recovery, NetBackup users can visually see in the backup history if the data being restored was identified as infected with malware, prompting several alerts as an effort to prevent reinfection.

### DATA IN TRANSIT

Data Channel in Transit Encryption (DTE) is an option within the NetBackup boundaries to negotiate TLS-encrypted paths for the data channel. The data is not modified in this scenario, and there is no impact to deduplication rates. This feature requires NetBackup clients to have version 9.1 or higher. By default, this feature is off, but can be configured with global options, or for specific clients.

- **Preferred Off (default)**: Specifies that the data in transit encryption is disabled in the NetBackup domain. This setting can be overridden by the NetBackup client setting.
- **Preferred On**: Specifies that the data in transit encryption is enabled only for NetBackup 9.1 and later clients. Configuring data in transit encryption (DTE) 363 enables the global data in transit encryption setting. This setting can be overridden by the NetBackup client setting.

- **Enforced**: Specifies that the data in transit encryption is enforced if the NetBackup client setting is either *Automatic* or *On*. With this option selected, jobs fail for the NetBackup clients that have the data in transit encryption set to *Off*, and for hosts prior to NetBackup version 9.1.

DTE is supported for MSDP storage, and *Use SSL* is a default and recommended option for the blob or bucket.

The data path between the customer's NetBackup installation of MSDP and the CSP should utilize the endpoints according to the desired transmission route, with considerations to name resolution and firewall ports to allow NetBackup deduplication traffic. For more information, see the NetBackup Network Ports Reference Guide. Additional security concerns for this segment of communication are outside the Veritas span of control.

**DATA AT REST**

NetBackup data stored in Veritas Alta Recovery Vault is storage-optimized using MSDP deduplication and uses a combination of data encryption keys wrapped with key encryption keys. The key encryption keys can be provisioned within NetBackup's built-in key management service (KMS), or from an external KMS that supports the key management interoperability protocol (KMIP). NetBackup uses AES 256-bit encryption and also supports FIPS 140-2 cryptographic modules when writing the data to Veritas Alta Recovery Vault object storage (backed by Azure). Stored Azure blob data is also encrypted with Microsoft Azure's Storage encryption with Microsoft-managed keys. Because of this, the data is encrypted twice at rest.

Note: FIPS 140-2 is currently only supported on Windows.

Using KMS with MSDP is set at the time of storage server creation; adding KMS to an existing storage server is not supported.

NetBackup encryption keys can be rotated as needed, while external KMS vendor solutions offer their own controls to rotate keys. NetBackup KMS can be operated in the FIPS mode, wherein the encryption keys that you create are always FIPS 140-2 approved.

Enabling encryption using the pd.conf file is not recommended. Use the contentrouter.cfg for these configuration changes.

Enable encryption on the storage server at the time of creation, or configure this option in the configuration file:

```
[storage location]/etc/puredisk/contentrouter.cfg
```

Edit with the following:

```
ServerOptions=verify_so_references,fast,encrypt
```

Authentication with an external KMS server uses security certificates. During each operation, NetBackup presents the certificate to the external KMS. eKMS validates the certificate and performs that operation if the user has the required permissions.

Data stored at rest in Azure is encrypted using Azure's Storage encryption with Microsoft-managed keys. In AWS, data at rest is encrypted with Amazon S3-managed keys (SSE-S3).

**DATA DELETION**

Data is retained until the service is canceled, terminated, or suspended for non-payment.

Unless otherwise prohibited by law or court order, decommissioned Veritas Alta Recovery Vault customer data will be deleted in accordance with Veritas standard deletion practices within thirty (30) days of the applicable data decommissioning event above and is irretrievable thereafter.

Customer data is stored in Azure or AWS. The customer manages their own data and performs deletes themselves. When data is deleted, Azure or AWS performs erasure and disposal according to their standards:

**Azure:** Data deletion is discussed on page 21 in the *Data Protection in Azure* document:

go.microsoft.com/fwlink/p/?LinkID=2114156&clcid=0x409&culture=en-us&country=US

**AWS:** *How do I delete Amazon S3 Objects and Buckets?* Discusses the various methods to delete data located in AWS S3 buckets:

aws.amazon.com/premiumsupport/knowledge-center/s3-delete-objects-and-buckets

## DATA HANDLING

Veritas has a policy that details how information is classified with appropriate controls. The Veritas Information Classification and Handling Method specifies the requirements for classifying, labeling, and protecting data. Information is classified by its value, legal requirements, sensitivity, criticality to the organization, and information handling protocol for the different types of information classification. Veritas data is classified *Public*, *Confidential*, or *Highly Confidential* based on the above factors.

Customer data is treated as Highly Confidential and restricted to a subset of employees and contractors handling customer data following the least privilege rule. The least privilege rule means all access is denied

except that which is specifically granted by management. Access is granted to individual user accounts performing roles that have limited responsibilities to perform their jobs.

All parties who contractually provide services on behalf of Veritas are required to meet security policy standards of Veritas. *Veritas Provider Security Requirements* describes the security controls and compliance placed on third-party providers, such as MS Azure, in the contracting process. The contractual terms are also made available to all interested parties at veritas.com/company/privacy under the *Data Processing Terms for Providers (Subcontractors)* tab:

veritas.com/content/dam/Veritas/docs/policies/DATA%20PROCESSING%20TERMS%20FOR%20PROVIDERS%20(with%20new%20SCCs).pdf'

## General Data Protection Regulation (GDPR)

Veritas Alta Recovery Vault utilizes storage from AWS that has passed the GDPR readiness audit: https://aws.amazon.com/compliance/gdpr-center/, and from Azure that is committed to be compliant to GDPR as well: https://www.microsoft.com/en-us/trust-center/privacy. All Veritas management activities related to the Alta Recovery Vault Service are provided as out-of-band, meaning that the data path for a customer's backup data is directly from the customer's NetBackup server(s) to native AWS or Azure storage in the Veritas tenant. The storage will be provisioned in the region as designated by the customer and will remain in that region unless the customer requests or makes a change. Also, the customer has sole responsibility for maintaining encryption keys for the data, meaning that Veritas does not have the ability to read any data stored within Recovery Vault.

## NETWORK/HARDWARE REQUIREMENTS

NetBackup writes to Veritas Alta Recovery Vault using a NetBackup MSDP-C server. Hardware requirements for the MSDP role on the media server are:

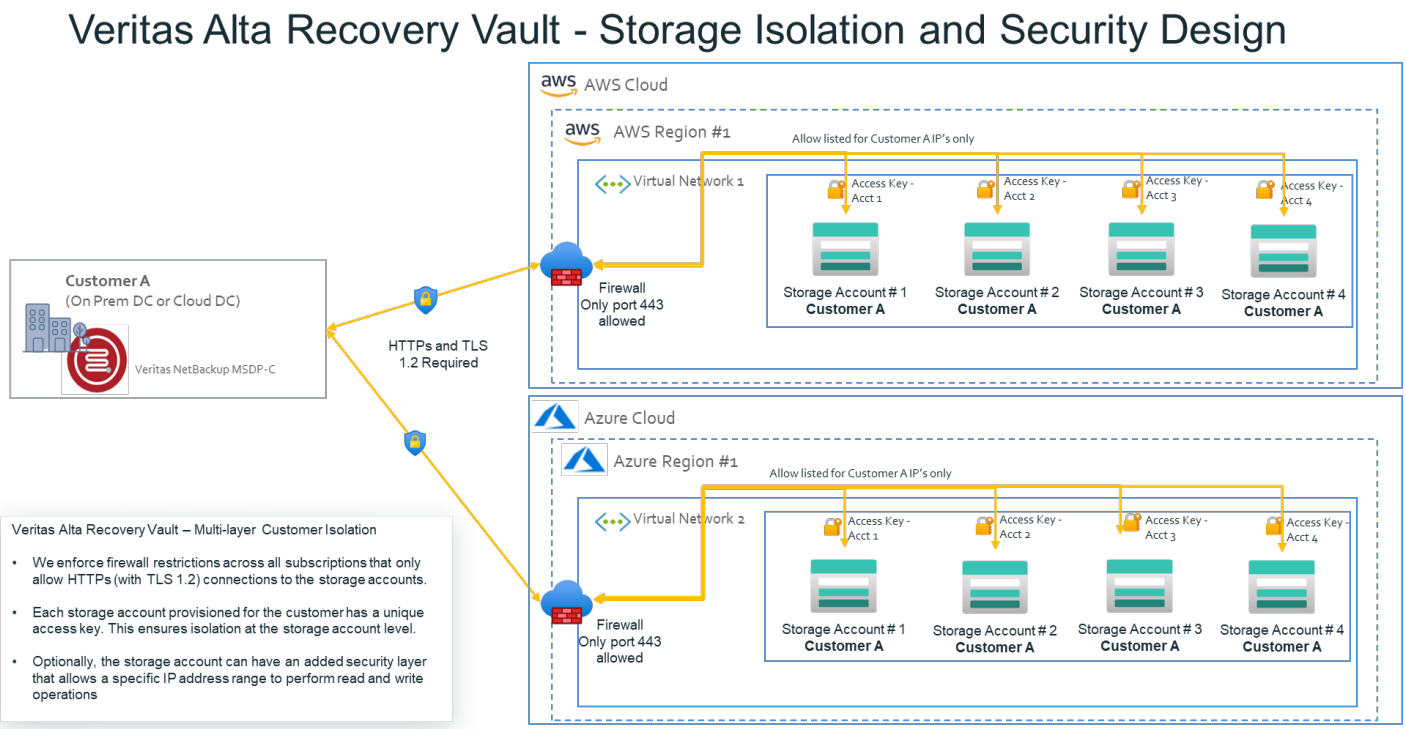
- Hardware requirements for block storage only MSDP pool: No change from NetBackup 8.2 MSDP guidance. Max capacity is 960 TB for the NetBackup appliance, and 400 TB for BYO MSDP.

- Hardware requirements for object storage only pool: Max capacity of 1 PB and 196 GB of memory. The default is 1 TB of available local storage per cloud logical storage unit (LSU), and the overall file system utilization should not exceed 90%.

- Hardware requirements for mixed object and block storage: Similar hardware requirements as local storage only pool. Total max capacity is 1.2 PB.

- Operating system: Cloud LSUs can be configured on the storage servers running on Red Hat Linux Enterprise or CentOS platforms. No platform limitations for clients and load-balancing servers.

The Veritas Alta Recovery Vault network capacity will depend greatly on the amount of data that is sent off-site and the speed at which it needs to arrive at the cloud provider. Veritas Alta Recovery vault does require port 443 to be opened outbound so it can communicate through HTTPS to the cloud provider.




**AZURE AND AWS IP RANGES**

For customers that want to whitelist the AWS and/or Azure IP ranges to connect to Microsoft and/or Amazon, please refer to the following sites:

Azure: [microsoft.com/en-us/download/confirmation.aspx?id=56519](microsoft.com/en-us/download/confirmation.aspx?id=56519)

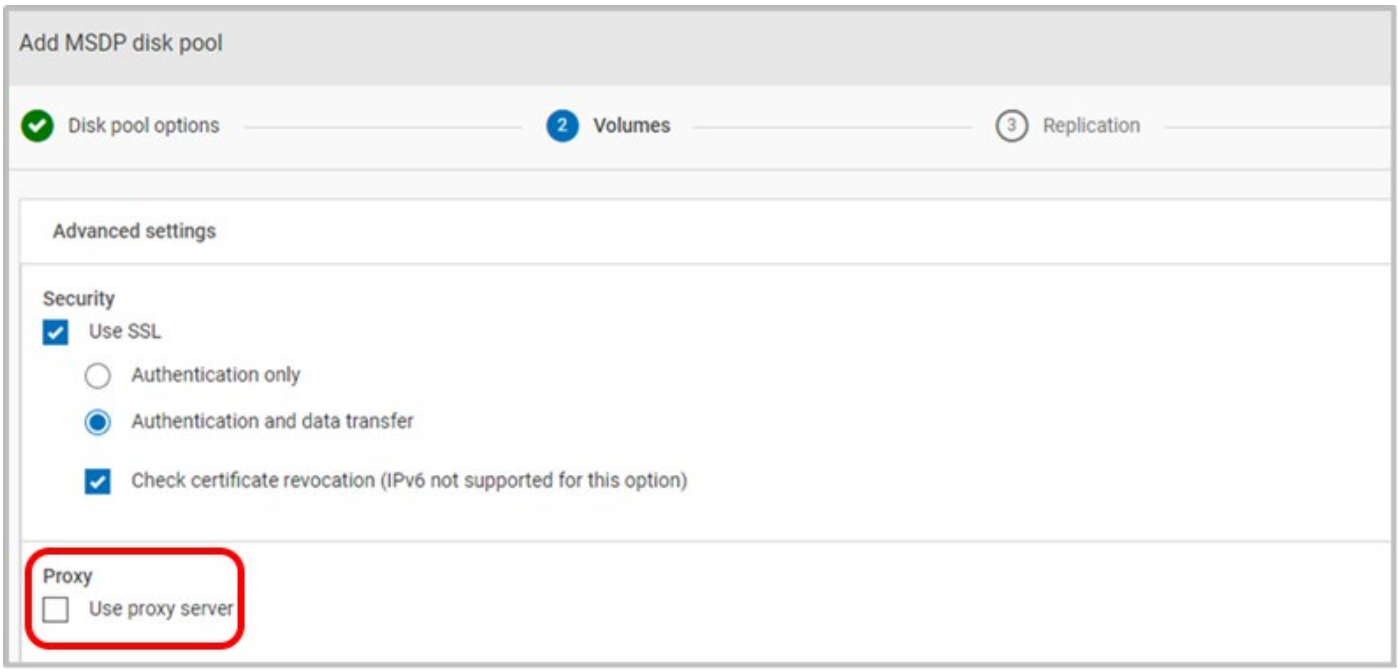
AWS: docs.aws.amazon.com/general/latest/gr/aws-ip-ranges.html

**ALTERNATE NETWORK CONNECTIONS**

Veritas is aware that standard connectivity methods may not meet every customer's requirements. Veritas supports the following alternative connection methods (other than HTTPS with outbound port 443).

## PROXY SERVER

A proxy server can be used if ports 443 and 80 cannot be opened. For more information, see the NetBackup Deduplication Guide.




## AZURE EXPRESSROUTE WITH MICROSOFT / PUBLIC PEERING

To use Azure ExpressRoute to connect to Veritas Alta Recovery Vault storage in Azure, customers should use Azure ExpressRoute *Microsoft Peering*, and not Azure *Private Peering*. The differences are described on Microsoft's site: docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings

In the past, with an ExpressRoute configured for Microsoft Peering, Microsoft used to send all the prefixes for public IPs. Now, customers should configure a route filter first—which is a border gateway protocol (BGP)

community value for the prefixes you want to receive—to the storage region (such as East US or West US 2) the customer has chosen for their Veritas Alta Recovery Vault Azure storage.

Please review Microsoft's guide on setting up a route filter for the prefixes the customer wants to receive:

learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal

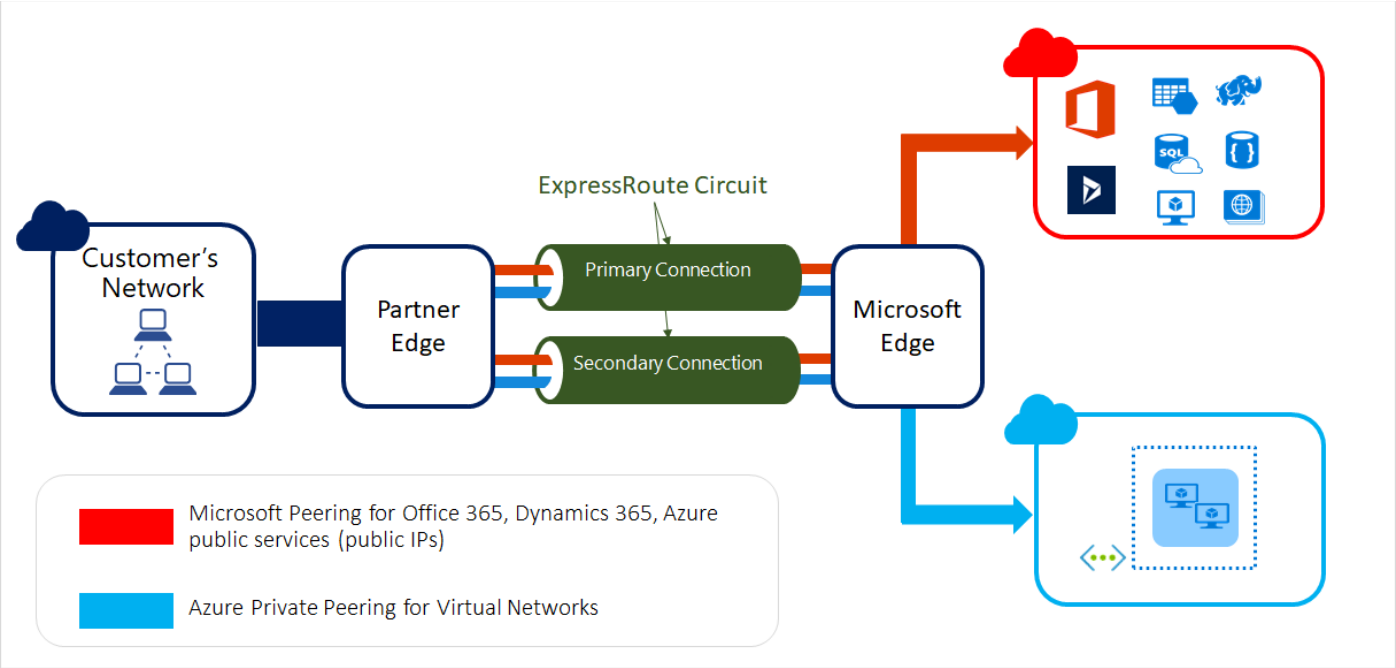



*Figure 1. Microsoft ExpressRoute configuration compatible with Veritas Alta Recovery Vault*

For more information about our testing with AWS Direct Connect, see the Veritas Alta Recovery Vault ExpressRoute Overview Guide.

## MICROSOFT VIRTUAL NETWORK PEERING

Veritas does not recommend using Microsoft virtual network peering for Veritas Alta Recovery Vault. Virtual network peering is cost prohibitive if used for backup and restore purposes. The least expensive vVirtual network peering is within the same region, at $0.01 per GB for inbound or outbound traffic, and charged at both

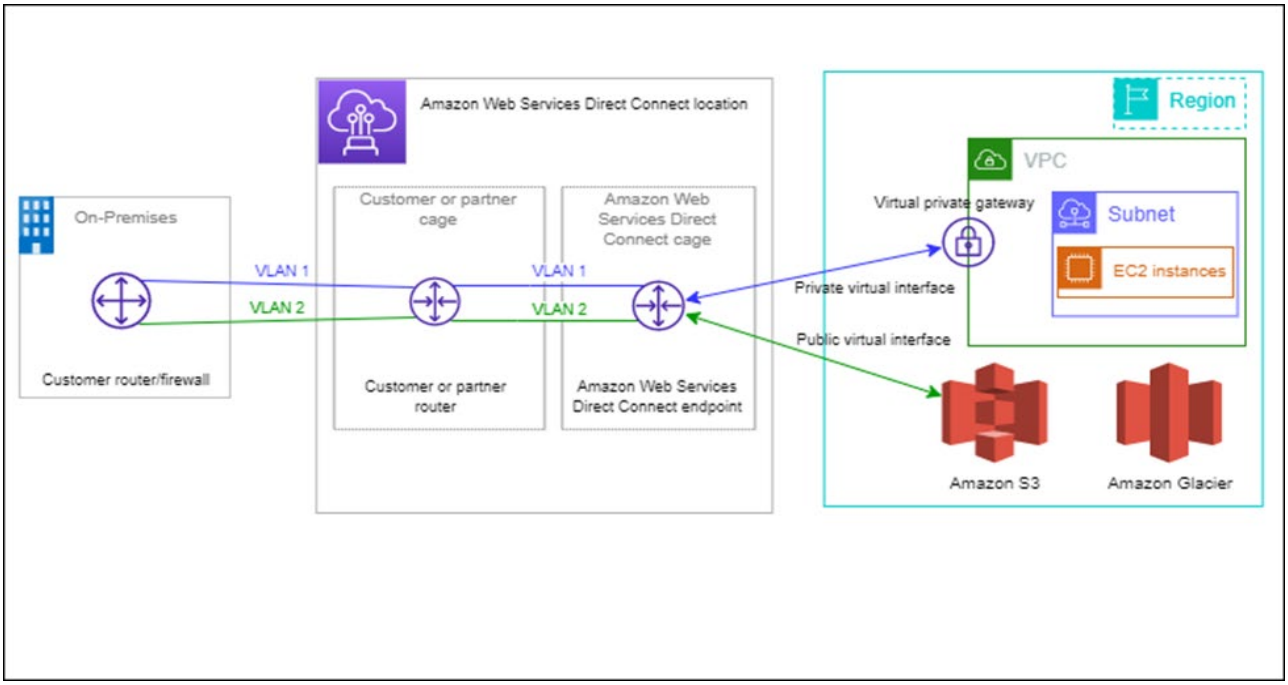
ends of the peered networks. Veritas and the end user would incur costs which will lead to transfers out of the same region that are 3.5x to 16x more expensive, depending on the regions used.

Virtual network peering also requires non-overlapping IP addresses, and Veritas Alta Recovery Vault is a multi-tenant environment. As multiple customers are connecting to their storage in the same Veritas Azure subscription, there could be overlap with IP ranges with future customers, and we would not be able to support future customer requests.

## AWS DIRECT CONNECT HOSTED CONNECTION

Veritas Alta Recovery Vault has been tested and certified to use AWS Direct Connect using a hosted connection. AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to public AWS services (such as Amazon S3) or to Amazon VPC, bypassing internet service providers in your network path. An AWS Direct Connect location provides access to AWS in the region with which it is associated. You can use a single connection in a public region or AWS GovCloud (US) to access public AWS services in all other public regions.

While in transit, your network traffic remains on the AWS global network and never touches the public internet. This reduces the chance of hitting bottlenecks or unexpected increases in latency. When creating a new connection, you can choose a hosted connection provided by an AWS Direct Connect delivery partner or choose a dedicated connection from AWS — and deploy at more than 100 AWS Direct Connect locations around the globe. For more information, visit aws.amazon.com/directconnect.
The following diagram shows a high-level overview of how AWS Direct Connect interfaces with your network.




For more information about our testing with AWS Direct Connect, see the Veritas Alta Recovery Vault Direct Connect Overview Guide.

## HELPFUL FAQS

Q - Can we enable WORM on an existing volume?

A - You can't enable WORM on an existing volume. Instead, you can create another disk volume with WORM. Veritas Alta Recovery Vault only supports WORM.

Q - Beyond creating a new volume, do we need anything else from the Veritas provisioning team to support WORM?

A - To configure WORM, you will need WORM-enabled credentials from the provisioning team.

Q - If the customer needs to have immutable storage (WORM) for Veritas Alta Recovery Vault, do they have to upgrade from NetBackup 9.1.01 to NetBackup 10?

A - For Azure, yes, the customer needs to upgrade to NetBackup 10 to get WORM. For AWS, they can work with 9.X.

Q - In the Veritas Alta Recovery Vault technote *Recovery Vault for NetBackup* (veritas.com/support/en_US/article.100051821) there is a caution to not leave I/O streams unlimited. Is there any guidance on what limit to set?

A - If *Limit I/O streams* is left cleared, the default value is *Unlimited* and may cause performance issues. Start low and work your way up. Start with 2, see what performance looks like, and adjust. Once you saturate your connection, there is no gain to adding more streams.

Q - Does Veritas Alta Recovery Vault provide network bandwidth for replication of data?

A - NetBackup utilizes MSDP-C to write to Veritas Alta Recovery Vault. The customer would have the same network options as they would with any other MSDP-C target.

Q - To use Veritas Alta Recovery Vault immutable storage in Azure, does the appliance software need to be updated to Version 5 in addition to the NetBackup 10 software?

A – Yes, please review the Veritas Alta Recovery Vault Deployment Guide and the Veritas Download Center for more information regarding necessary EEBs:

- veritas.com/support/en_US/doc/VeritasAltaRecoveryVaultGuide

- veritas.com/content/support/en_US/downloads

Q - Can Veritas Alta Recovery Vault be integrated into the existing environment without major changes?

A – Yes. You should be able to tier data to Veritas Alta Recovery Vault without disrupting the current environment.

Q – Are there any documents regarding service we provide? SLA, performance, etc.?

A - The service description provides an uptime SLA as follows:

The Veritas SLA shall provide 99.9% or higher uptime for the service.

Uptime is defined as the time during which a customer can access the service, as reported by the Veritas incident management system. Access is defined as a customer being able to successfully log in and use the service functionality, as outlined in this service description.

Uptime is measured every calendar month as a percentage value. The monthly uptime percentage is the total number of minutes of uptime achieved in a calendar month, divided by the total number of minutes in a calendar month.

We use native Azure and AWS storage, and users can expect performance as such. Our management of the storage is out of band and doesn't impose overhead.

Q - Do we use a *Push* model from NetBackup to Veritas Alta Recovery Vault, or is it a *Pull* from Veritas Alta Recovery Vault to NetBackup over port 443?

A - All data movement is driven by native NetBackup operations. Veritas Alta Recovery Vault is a standard object storage target from the perspective of NetBackup.

## CONCLUSION

Veritas Alta Recovery Vault offers a single, flexible, and secure offsite repository for all your data sources. Through its seamless integration with NetBackup, Veritas Alta Recovery Vault simplifies cloud storage as a service, delivering limitless scale without compromising security or compliance.

## SOURCES


Veritas Alta Recovery Vault for NetBackup TechNote

NetBackup Security and Encryption Guide

NetBackup Deduplication Guide

NetBackup Backup Planning and Performance Tuning Guide

Azure Locations

ExpressRoute Circuits and Peering

Download Azure IP Ranges and Service Tags

Virtual Network Pricing

ExpressRoute or Virtual Network VPN – What's right for me?

AWS Locations

AWS IP Address Ranges

What is AWS Direct Connect

Veritas Alta Recovery Vault Deployment Guide

Announcing Default Encryption for Azure Blobs, Files, Table and Queue Storage

Veritas Download Center

## 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 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.