VERITAS

NetBackup Recovery Vault

Security Profile.

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

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

White Paper | September 2022

Contents

Introduction 4

Necessary Information 4

Role-Based Access Control (RBAC) 5

How Recovery Vault Communicates In NetBackup 5

Recovery Vault Security Fundamentals and Architecture 5

Data Security 6

Data-in-Transit 6

Data-at-Rest 6

Immutability/Write Once, Read Many (WORM) Storage 7

Data Deletion 7

Data Handling 8

Network/Hardware Requirements 8

Azure and AWS IP Ranges 9

Alternate Network Connections 9

Azure ExpressRoute with Microsoft Peering 9

Microsoft vNet Peering 10

AWS 10

FAQs 11

Conclusion 13

Sources 13

Revision History

Version	Date	Changes	Author
1.00	8/29/2022	Initial Version	Neil Glick

Introduction

NetBackup Recovery Vault is a cloud-based secondary storage platform for enterprise organizations to centrally manage cloud storage.

NetBackup Recovery Vault customers can protect their NetBackup compressed and deduplicated data in a secure Veritas tenant hosted in several cloud service providers (CSPs). Most storage-as-a-service (STaaS) providers have adopted a shared responsibility model, which makes it clear that the providers are not obligated to take any action to protect customer data. The job of protecting data in the CSP is completely the responsibility of the customer. Customers who adopt NetBackup Recovery Vault see the following results:

- Complete backup and recovery of all their application data
- Fast and flexible data recovery
- Secure and flexible provisioning

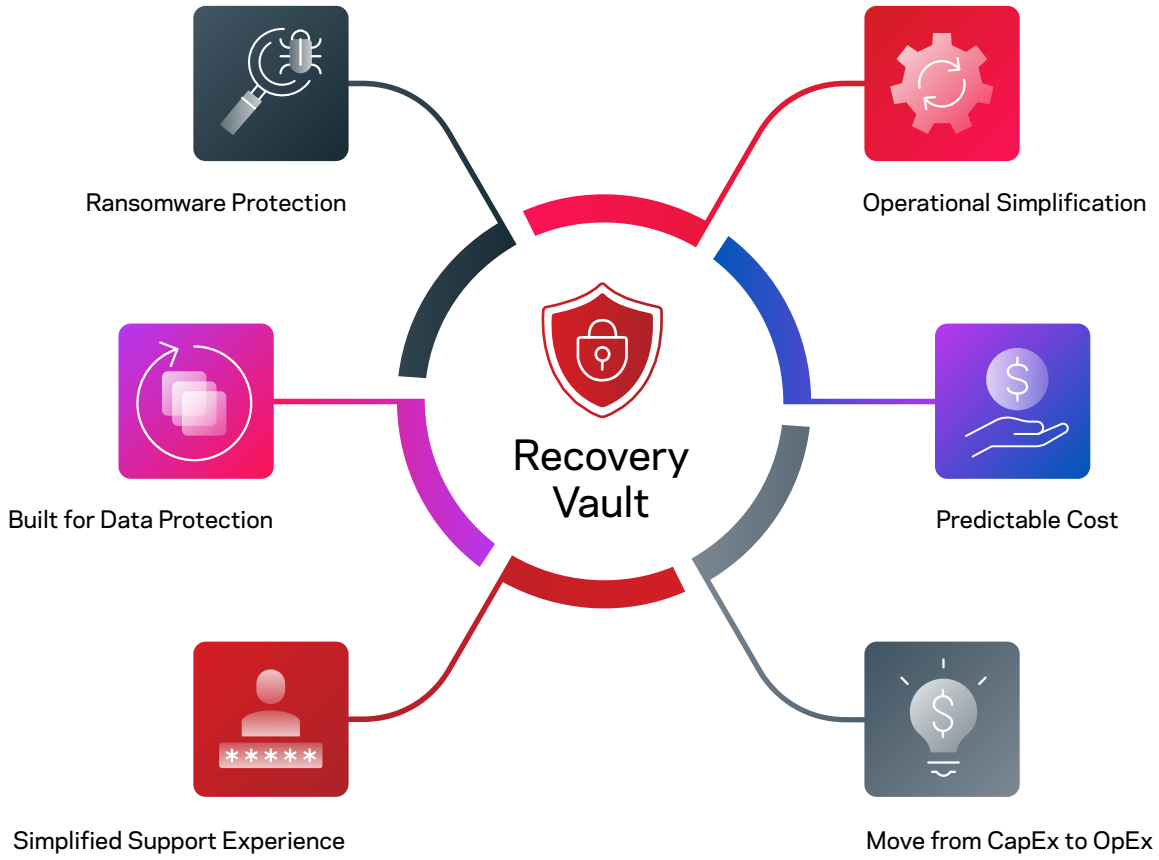

Figure 1. Why NetBackup Recovery Vault?

Necessary Information

The first step on your journey to storage-as-a-service is to contact your Veritas NetBackup Account Manager. Your account manager will collect the necessary information needed to provision your Recovery Vault storage account. Following are examples of the information you might provide to Veritas:

1. Cloud provider(s)
2. Data center region
3. Number of buckets
4. Size of the buckets (1.2PB per disk volume)
5. Veritas account representative
6. Veritas Partner Name
7. Immutability support (yes/no)

Role-Based Access Control (RBAC)

Recovery Vault is built right into NetBackup and NetBackup provides the ability to apply role-based access control (RBAC) in your environment. Use RBAC to provide access for the users that 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 Recovery Vault:

1. **Administrator**: This role has permissions to perform all actions within the NetBackup Web UI.
2. **Default Security Administrator**: 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**: This role has permissions to configure and manage disk-based storage and cloud storage.

Either the Storage Administrator or the Administrator must perform the modifications to the media server deduplication pool (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 Recovery Vault. Security administrators do not have permissions to see or modify storage configurations.

How Recovery Vault Communicates in NetBackup

NetBackup Primary server, NetBackup 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, managed by the primary server or an External Certificate Authority. This is a common form of endpoint verification on the web, as well. 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 currently supported cloud solutions.

Ensure secure communication with the media server hosting MSDP, according to the procedures in the NetBackup Security and Encryption Guide. Communication to AWS or Azure for 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. This is also where you will toggle immutability using object lock.

Recovery Vault Security Fundamentals and Architecture

NetBackup 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, and identity and access management (IAM) roles for MSDP-C in AWS. 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 open outbound so the NetBackup API can communicate with the storage bucket through HTTPS.

The Recovery Vault underlying cloud storage is provided by third parties, such as Microsoft Azure and Amazon Web Services (AWS). When provisioning 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 encrypted at all times in transit. The service transmits using TLSv1.2 and stores all customers' 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 cryptography modules.

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

Available in 10.1 and later, customers can scan the stored 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, the 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 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 Configure 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 the hosts earlier than 9.1

DTE is supported for MSDP storage. Use SSL is a default and is the 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 span of control provided by Veritas.

Data-at-Rest

NetBackup data stored in Recovery Vault is storage-optimized using MSDP deduplication, using a combination of data encryption keys wrapped with the 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 cryptography modules when writing the data to Recovery Vault Object storage (backed by Azure). Stored Azure blob data is also encrypted with Microsoft's Azure Storage Service 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 else 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 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 Service Encryption with Microsoft-managed keys. In AWS, data at rest is encrypted with Amazon S3-managed keys (SSE-S3)

Immutability/Write Once, Read Many (WORM) Storage

Immutability/WORM (Write Once Read Many) storage is supported in NetBackup Recovery Vault. If immutability is required, Veritas needs to enable the function at the cloud provider before immutable disk pools can be created. Please inform your account representative that you wish to use immutability during the provisioning process. In addition, immutability needs to be enabled on the media server that will be the MSDP-C storage server.

Note: For more information on immutability, refer to the NetBackup Deduplication Guide:
https://www.veritas.com/support/en_US/doc/25074086-149019166-0/v149102641-149019166

Note the following regarding Compliance versus Governance modes:

Compliance Mode:

Users cannot overwrite or delete the data that is protected using the compliance mode for the defined retention period. After you set a retention period for the data storage, you can extend it, but you cannot shorten it.

Governance Mode (Also Known as Enterprise Mode):

Users require special permissions to disable the retention lock and then delete the image. Only the cloud administrator user can disable the retention lock and then delete the image if required. You can use the governance mode to test the retention period behavior before you use the compliance mode.

Note: If immutability has not been setup on both the cloud provider (Veritas responsibility) and at the command line, the web UI will error if you attempt to create an immutable disk pool.

For further instructions on how to set immutability in Recovery Vault, see the Veritas NetBackup Recovery Vault Deployment Guide.
https://www.veritas.com/content/support/en_US/doc/NetBackupRecoveryVaultGuide

Data Deletion

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

AWS: The various methods to delete data located in AWS S3 buckets is discussed in How do I delete Amazon S3 objects and buckets?.
https://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 which is specifically granted by management. Access is granted to individual user accounts performing roles which have limited responsibilities to perform their jobs

All parties who contractually provide services on behalf of Veritas are required to meet Veritas security policy standards. Veritas Provider Security Requirements describes the security controls and compliance placed on third-party providers, such as Microsoft Azure, in the contracting process. The contractual terms are also available here:

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

Network/Hardware Requirements

NetBackup writes to 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. Maximum capacity is 960 TB for the NetBackup Appliance, and 400 TB for BYO MSDP.
- Hardware requirements for object storage only pool: Maximum 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 percent full.
- Hardware requirements for mixed object and block storage: Similar hardware requirements as local storage only pool. Total maximum 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 Recovery Vault network capacity will depend greatly on the amount of data that is being sent offsite and the speed at which it needs to arrive at the cloud provider. Recovery Vault does require port 443 to be opened outbound so it can communicate through HTTPS to the cloud provider.

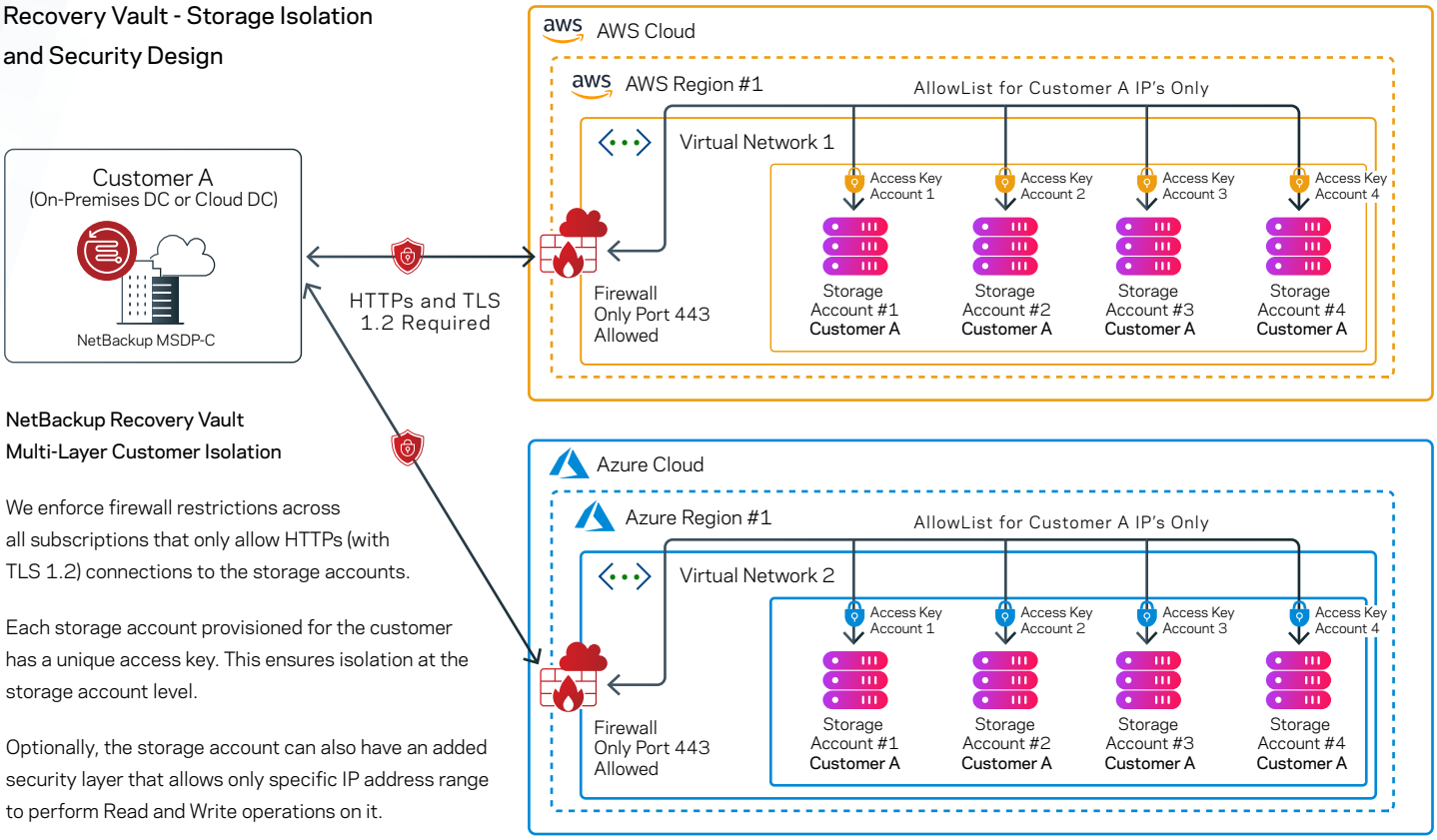

Figure 2. Recovery Vault – Storage Isolation and Security Design

Azure and AWS IP Ranges

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

Azure: https://www.microsoft.com/en-us/download/confirmation.aspx?id=56519

AWS: https://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, and supports the following alternative connection methods to HTTPS with outbound port 443:

Azure ExpressRoute With Microsoft Peering

In order to use Azure ExpressRoute to connect to Recovery Vault storage in Azure, customers should use Azure ExpressRoute "Microsoft Peering", and not Azure "Private Peering". The differences are described on Microsoft's website: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings

In the past, Microsoft used to send all the prefixes for public IPs with an ExpressRoute configured for Microsoft Peering. 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 Recovery Vault Azure storage.

Please review Microsoft's guide on setting up a route filter for the prefixes the customer wants to receive: docs.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal

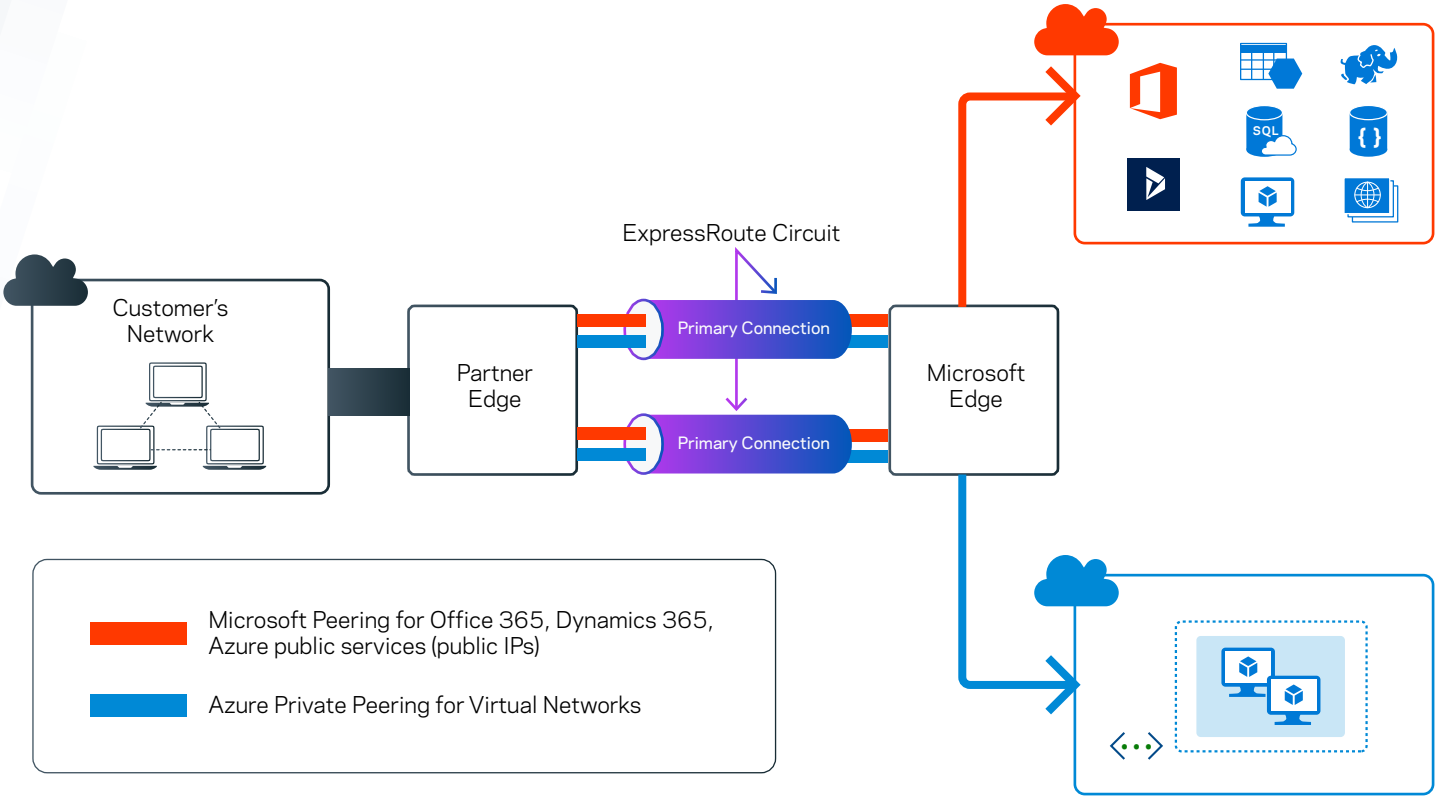

Figure 3. Microsoft ExpressRoute Configuration Compatible with Recovery Vault

Microsoft vNet Peering

Veritas does not recommend using Microsoft vNet Peering for Recovery Vault. vNet Peering is cost prohibitive if used for backup and restore purposes. The least expensive vNet 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 leading to transfers out of the same region that are 3.5–16 times more expensive, depending on the regions used.

vNet Peering also requires non-overlapping IP addresses, and Recovery Vault is a multi-tenant environment. As multiple customers connect 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 requests.

AWS

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.

Please review the AWS guide on setting up a route filter for prefixes:
https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

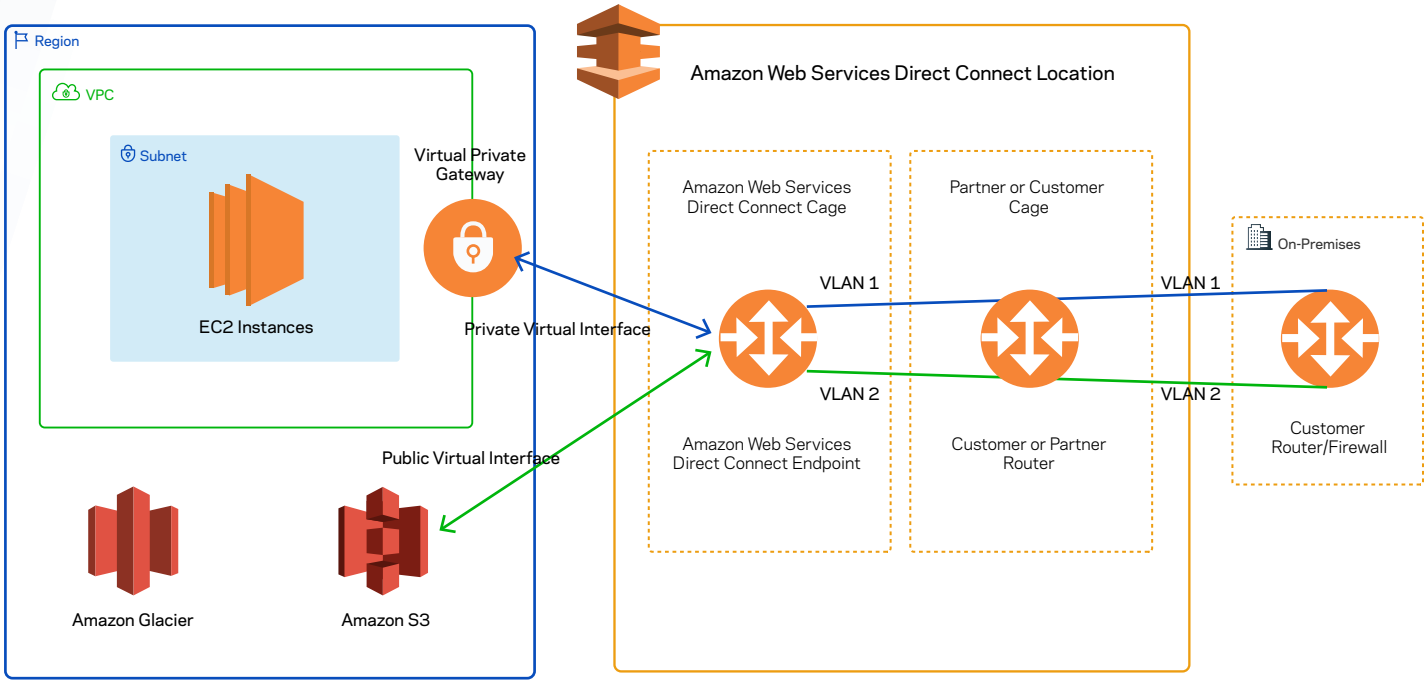

Figure 4. AWS Direct Connect Compatible with Recovery Vault

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.

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 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 Recovery Vault technote 'Recovery Vault for NetBackup (veritas.com) there is a caution to not leave I/O streams unlimited, is there any guidance on what limit to set? https://www.veritas.com/support/en_US/article.100051821

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 are saturating your connection, there is nothing gained by adding more streams.

Q - Does NetBackup Recovery Vault provide network bandwidth for replication of data to Recovery Vault?

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

Q - To use 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 NetBackup Recovery Vault Deployment Guide and the Veritas Download Center for more information regarding necessary EEBs.

- https://www.veritas.com/content/support/en_US/doc/NetBackupRecoveryVaultGuide
- https://www.veritas.com/content/support/en_US/downloads

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

A – Yes. You should be able to tier data to Recovery Vault without disrupting the current environment. MSDP-C does not require a lot of local disk.

Q - Is there any documentation about the service you provide?

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

Veritas' Service Level Agreement shall provide 99.9 percent 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 does not impose overhead.

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

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

Conclusion

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

Sources

- 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 NetBackup Recovery Vault Deployment Guide
- Announcing Default Encryption for Azure Blobs, Files, Table and Queue Storage
- Veritas Download Center

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 95 percent of the Fortune 100—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

V1537 09/22