VERITAS

Veritas NetBackup Recovery Vault

FAQs

Cloud-based Storage-as-a-Service

This guide is designed to answer frequently asked questions when planning and implementing NetBackup Recovery Vault.

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

Revision History

Version	Date	Changes
1.00	8/31/2022	Initial Version
1.01	10/6/2022	Revised Version

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 de-duplicated data in a secure Veritas tenant hosted in several Cloud Service Providers (CSP). Most STaaS providers have adopted a “shared responsibility model” which makes it clear the providers will not take any action to protect customers’ data.

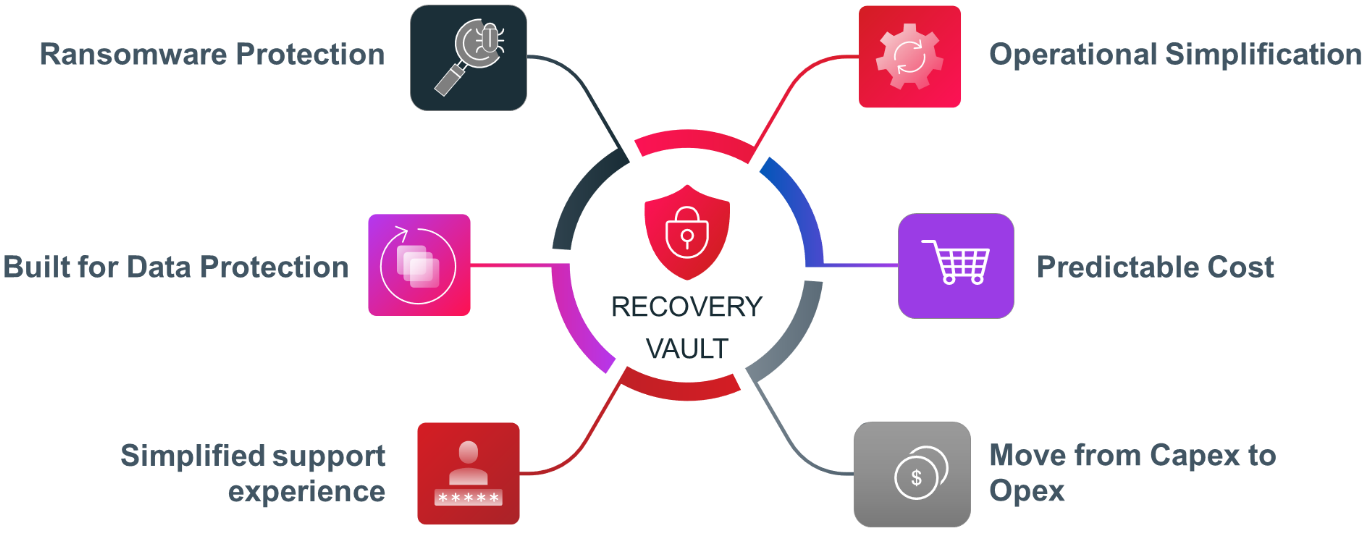
Ransomware Protection
Operational Simplification
Built for Data Protection
RECOVERY
VAULT
Predictable Cost
Simplified support experience
*****
Move from Capex to Opex
$

Figure 1. Why NetBackup Recovery Vault?

TARGET AUDIENCE

This document is targeted at the prospect or customer interested in learning more about NetBackup Recovery Vault.

WHY NETBACKUP RECOVERY VAULT

In a few short years, the adoption of public cloud-based data protection as-a-service has grown significantly. This trend is placing the responsibility on data owners to deliver on data protection SLAs (Service Level Agreements), data sovereignty, security, and ransomware resiliency.

Customers who adopt NetBackup Recovery Vault are seeing the following results: complete backup and recovery of all their application data, fast and flexible data recovery, and secure and flexible provisioning.

NetBackup Recovery Vault provides a fully managed cloud data protection tier that is seamlessly integrated in NetBackup. With NetBackup Recovery Vault, Veritas customers can be confident that their data is secure in the cloud and protected from ransomware, is disaster recovery ready, and able to meet compliance and governance requirements.

NetBackup Recovery Vault is the right technology at the right time. Recovery Vault not only simplifies the process of provisioning new storage in the cloud, but it also reduces risks. All storage as-a-service resources are provisioned and managed

from within NetBackup's locked-down security and role-based authentication policies. Eliminating separate accounts and user interfaces across cloud providers helps ensure that security and compliance policies are in check. And because Recovery Vault is an integral feature of NetBackup, customer cloud storage benefits from all its capabilities.

With NetBackup Recovery Vault you can:

- **Reduce Risks** - Crucial cloud security, retention and compliance managed within NetBackup
- **Scale Limitlessly** – Efficiently manage data growth without compromising manageability
- **Lower TCO (Total Cost of Ownership)** – Predictable as-a-service subscription. Zero hidden costs
- **Automate Resiliency** – Intelligent Cloud Policies and air-gapped multi-cloud isolation protects data from ransomware and other threats

ANSWERS TO COMMONLY ASKED QUESTIONS

What are some of the benefits of Recovery Vault?

1. **Cloud Tiering**. Users require the ability to perform backups in their data center to a local storage pool and tier the data to Recovery Vault for low-cost longer-term retention. Backup infrastructure remains on premises, with data being sent to object storage in cloud.

2. **Backup of cloud-resident workloads**. As workloads are migrated to cloud, the user will deploy NBU in a cloud VM, and send backup data directly to Recovery Vault as a primary backup target and keep it there for LTR (Long Term Retention) storage. In this scenario the production workload might be running in the same public cloud as Recovery Vault, or it could be deployed in another public cloud.

3. **Ransomware protection.** Given the threat landscape for ransomware attacks, many users require that data be stored in a cloud tenant other than their own. Also, it will be important to allow the customer to choose to utilize immutable storage as further protection against ransomware attacks.

4. **Recovery.** Users require the ability to restore an application back to their data center, sending data across the network connection in a deduplicated format. Additionally, users require the ability to restore into a cloud VM, whether on the same cloud as the Recovery Vault storage, or a different cloud platform for migration purposes. The recovery event could be driven by data loss, compliance audit, legal discovery request, or test/dev workflow requirements.

5. **Disaster Recovery.** Users require the ability to orchestrate a large-scale recovery in a location that is physically separate from the production data set. This could mean a different data center, or an IaaS environment.

Why use Recovery Vault in place of a different public cloud service?

- By utilizing Recovery Vault, customers can benefit from more security, compliance, and ransomware protection than any other data protection solution on the market.
- Additionally, customers can take advantage of NetBackup's superior scaling and performance.
- Data protection infrastructure delivered from one vendor.

What's the cost?

- Veritas can reduce overall costs by consolidating and standardizing the protection of a customer's backup data and simplifying the process of integrating cloud storage.
- By standardizing on Recovery Vault, customers can enhance their security, resilience, and protection from ransomware.
- Customers will also avoid ingress and egress fees that other public cloud providers charge, ensuring a predictable cost structure for their organization.

Is Recovery Vault difficult to use?

- Recovery Vault is fully integrated into the NetBackup architecture.
- To get started, customers fill out a simple form, submit it to their Account Manager and the cloud credentials are sent to them. With these credentials, customers will connect to the cloud provider within the NetBackup WebUI and provision the storage buckets.
- Once provisioned, customers can utilize the power of NetBackup to automate backup and recovery, on prem or cloud based, all without intervention.

How does the Recovery Vault licensing work?

- Recovery Vault is licensed by BETB (Back-end TB), in the form of a subscription offering in 1 or 3-year increments. It is on the Veritas Corporate Price List and sold just like other Veritas product offerings.
- It can be sold direct or via the channel and is subject to the same rules and conditions as all other products sold by Veritas.
- Unlike other cloud service providers, there are no ingress or egress fees with Recovery Vault. This greatly enhances the flexibility of our solution vs. other public cloud offerings, allowing customers to use Recovery Vault for test/dev, compliance audits, resiliency, storage tiering, and many other use cases, all without any surprises from a cost perspective.

Which cloud provider(s) will be available?

- Recovery Vault is currently available on either Amazon Web Services (AWS) or Microsoft Azure. Cloud storage will be available across all regions supported by AWS and Azure except mainland China.
- This will eventually be expanded in future phases to support other cloud providers such as Google Cloud Platform (GCP), etc. As we add providers to our list, we will provide customers great flexibility to make cloud storage decisions on an application-by- application basis, all under a single contract.

Is there a way of provisioning the location of your data (e.g., if you are in Germany, can you make sure that your data is in a German DC)?

- Recovery Vault currently supports multiple regions around the world associated with the supported CSPs. Coverage may be expanded into additional regions to support customer data sovereignty as/if needed. Best practices are to generally to choose the region closest to the customer to reduce network latency and optimize transfer speed and support data sovereignty requirement.

Where will Veritas management of the cloud storage take place?

- Majority of management will be U.S. based. 24*7 alerting and monitoring support will be based in India.

Will customers be billed by Veritas or the cloud provider and will they be able to pay in local currency from a local billing entity?

- NetBackup Recovery Vault is a Veritas-provided and Veritas-billed software subscription service. It will be sold like any other product on the Veritas published price list and licensed the same as all software sold, either direct or via the channel.

As a customer scales their amount of data ingested to Recovery Vault, will it scale linearly? How will restore performance look?

- The storage itself scales linearly. The performance of NetBackup as we support more data per MSDP-C node will likely decline, although we are not sure of what the curve will look like. With Cloud Catalyst, we saw performance dropping after 1/2 PB or so. MSDP-C is designed to maintain performance better with a larger bucket.
- The performance of backup and restore will be driven from latency and IOPS provided by the underlying storage which varies from different public cloud providers and different storage classes. The performance should be comparable to BYO (Bring Your Own) in cloud.
- Performance should be the same as native cloud (self-managed) storage. Performance for in-cloud will be much better. Pulling back to on-prem is bottlenecked by bandwidth. For on-prem recovery, we do pull data back in a deduped/compressed format, so that helps. But in general, the customer should architect for local recovery in all cases. 30-90 days of on-prem storage on an NBU appliance. Cloud fetches should be for compliance audits, DR, litigation support, test-dev, etc. If they are using cloud storage for production on-prem recoveries, they have a poor design. In-cloud, on the other hand, should use snaps for fast restore, and NetBackup Recovery Vault where we would normally position our appliances in the data center. There will not be a block-based middle tier target for in-cloud workloads because there is not a performance advantage of block over object in the cloud for our use case.

Can we enable WORM on an existing volume?

- You cannot enable WORM on existing volume instead, you can create another disk volume with WORM.

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

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

If the customer needs to have Immutable Storage (WORM) for Recovery Vault, do they have to upgrade from NBU 9.1.01 to NBU 10?

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

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

- The default value is Unlimited when creating a disk pool and may cause performance issues. Instead, select a value for Maximum I/O streams. Start low and work your way up. Start with 2, and see what performance looks like, and adjust. Once you are saturating your connection, there is no gain to adding more streams.

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

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

To use Recovery Vault immutable storage in Azure, does the appliance software need to be updated to Version 5 in addition to the NBU 10 Software?

- Yes, please review the Veritas NetBackup Recovery Vault Deployment Guide for more information regarding necessary EEBs (Emergency Engineering Binaries) and the Veritas Download Center.
  - https://www.veritas.com/content/support/en_US/doc/NetBackupRecoveryVaultGuide
  - https://www.veritas.com/content/support/en_US/downloads

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

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

Do we have any documents about the service we provide? SLA, performance, ...

- The service description provides an uptime SLA as follows:

  https://www.veritas.com/content/dam/Veritas/docs/policies/NetBackup_Recovery_Vault_Service_Description.pdf

  Veritas' Service Level Agreement 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 login 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.

Do we use a Push model from NBU to Recovery Vault or is it a Pull from RV to NBU over port 443?

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

Does Recovery Vault support instant access?

- No, it is not currently supported.

When a customer receives their Recovery Vault storage account credentials how do they provision storage?

- There are two different methods:
- Through the NetBackup WebUI. Similar to adding an MSDP Disk Pool. (See Recovery Vault Deployment Guide)

  Using an administration tool like Microsoft Azure Storage Explorer or equivalent for their public cloud provider of choice. (See Recovery Vault Deployment Guide.)

Does Recovery Vault contain any type of Role-Based Access Control (RBAC)?

- Yes, 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.

How is Recovery Vault data transmitted from onsite to the cloud provider?

- 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 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 (Federal Information Processing Standards) 140-2 cryptography modules.
- Note: FIPS 140-2 is only supported on Windows.

Does Recovery Vault support immutability/WORM Storage?

- Yes, 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: Two** immutability modes exist:

  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.

How is data deleted from the cloud provider if the service is no longer needed?

- Data is retained until the service is cancelled, terminated, or suspended for non-payment. Unless otherwise prohibited by law or court order, decommissioned 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:

  https://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.

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

How does Recovery Vault connect to the cloud provider? What network changes must be made?

- Recovery Vault uses HTTPS and TLS 1.2 to connect to cloud providers.
- Outbound port 443 must be opened on the customer's firewall.

Do you support Azure Express Route?

- 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 site: https://docs.microsoft.com/en-us/azure/expressroute/expressroute-circuit-peerings

Do you support AWS Direct Connect?

- To use AWS Direct Connect to connect to Recovery Vault store in AWS, customers should use the AWS architecture on how to set up an AWS Direct Connect location over a standard Ethernet fiber-optic cable. More information can be found here:
- https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html

Does Recovery Vault support Locally Redundant Storage (LRS)?

- Yes, by default Veritas uses LRS to protect your data.

Does Recovery Vault support Zone-Redundant Storage (ZRS), Geo-Redundant Storage (GRS), and/or Geo-Zone-Redundant Storage (GZRS)?

- Yes, but on a case-by-case basis. Please contact your Veritas Account Representative to discuss this further.

Does Recovery Vault support Gov Cloud on both AWS and Azure?

- Yes, Recovery Vault supports Gov Cloud for AWS and Azure.

What firewall controls do we have at Veritas subscription/region level?

- Management of the Veritas Azure subscriptions and AWS accounts are restricted to access from Veritas networks only. Veritas team members must either be physically in a Veritas office to join the Veritas network there, or use the Veritas VPN, which requires multifactor authentication (MFA) and only allows users to join the VPN from a Veritas-managed device.

What firewall controls do we have at Customer account level?

- The customer can provide us with a set of public IP ranges (whitelisting) to restrict access to their storage containers / buckets.

Does the provisioning API we have today support IP whitelisting for customer IP addresses and range?

- The Recovery Vault API currently does not have the ability to set IP whitelisting. If a customer were to ask for it, we can at least do it manually right now.

Conclusion

Veritas Recovery Vault not only simplifies the process of provisioning new storage in the cloud, but reduces risk, allows for limitless scalability, lowers TCO and automates resiliency. Through seamless integration with NetBackup, an easy-to-use UI, management and monitoring of cloud storage resources and retention policies, provisioning storage and protecting your data has never been easier.