



Veritas Alta Recovery Vault Azure ExpressRoute Overview Guide

Cloud-based Storage-as-a-Service

This paper is designed to highlight the architecture and steps performed to validate Azure ExpressRoute with Veritas Alta Recovery Vault.

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

TABLE OF CONTENTS

INTRODUCTION	3
EXECUTIVE SUMMARY	3
TARGET AUDIENCE	3
IMPORTANT NOTE REGARDING PUBLIC VS PRIVATE CONFIGURATION	4
WHY VERITAS ALTA RECOVERY VAULT	4
WHY MICROSOFT AZURE EXPRESSROUTE	4
KEY BENEFITS	5
PREREQUISITES	5
CREATING AN EXPRESSROUTE CIRCUIT	5
CONNECTING TO ALTA RECOVERY VAULT STORAGE WITH EXPRESSROUTE	7
PORTS	8
CONNECTION STEPS	8
BACKUP AND RESTORE TESTING	8
BACKUP TESTS:	9
RESTORE TESTS:	10
EXPRESSROUTE BACKUP AND RESTORE SUMMARY	11
CONCLUSION	11
REFERENCES	12

Revision History

Version	Date	Changes	Author
---------	------	---------	--------

1.00	05/23/2023	Initial Version	Neil Glick and Sakshi Nasha
1.01	8/22/2024	Updates	Neil Glick and Sakshi Nasha

Introduction

Executive Summary

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 Alta Recovery Vault, there is no need to build, manage, and protect a physical site to isolate backup data.

Microsoft Azure ExpressRoute is used to create private connections between Azure datacenters and infrastructure on premises or in a colocation environment. ExpressRoute connections do not route through the public internet, and they offer more reliability, faster speed, and lower latency than typical internet connections. In some cases, using ExpressRoute connections to transfer data between on-premises systems and Azure gives you significant cost benefits.

To ensure optimal functionality between Alta Recovery Vault and ExpressRoute, Veritas purchased and configured ExpressRoute to reflect a customer's on-premises NetBackup installation. NetBackup with Alta Recovery Vault was used to backup and restore files over the ExpressRoute to test both functionality and performance. The goal of this guide is to show that once configured, Azure ExpressRoute is transparent to Alta Recovery Vault and NetBackup irrespective of each other.

Target Audience

This document is for customers interested in learning more about how Veritas Alta Recovery Vault and Azure ExpressRoute work together to offer a network connection that is more secure, reliable, and faster than the Internet alone.

Important Note Regarding Public vs Private Configuration

Veritas Alta Recovery Vault is designed as a public internet facing service and as such can only be connected to via a Public Direct Connect configuration / Public VIF. Private Direct Connect peering / Private VIF is not supported.

Why Veritas Alta 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 onus on data owners to deliver on data protection SLAs (Service Level Agreements), data sovereignty, security, and ransomware resiliency.

Traditional approaches to cloud data protection are not keeping pace with IT complexity, growing threats, or economic expectations.

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

Veritas Alta Recovery Vault is the right technology at the right time. Veritas Alta Recovery Vault not only simplifies the process of provisioning new storage in the cloud but 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. Veritas Alta Recovery Vault is an integral feature of NetBackup, customer cloud storage benefits from all its capabilities.

With Veritas Alta 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 Total Cost of Ownership (TCO)** – Predictable as-a-service subscription. Zero hidden costs.
- **Automate Resiliency** – Intelligent cloud policies and air-gapped multi-cloud isolation protect data from ransomware and other threats.

Why Microsoft Azure ExpressRoute

ExpressRoute lets you extend your on-premises network into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Connectivity can be from any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For more information on how to connect your network to Microsoft using ExpressRoute, see [ExpressRoute connectivity models](#).

Key Benefits

- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on.
- Dynamic routing between your network and Microsoft via BGP.
- Built-in redundancy in every peering location for higher reliability.
- Connection uptime [SLA](#).
- QoS support for Skype for Business.

For more information, see the [ExpressRoute FAQ](#).

Prerequisites

[ExpressRoute Prerequisites and Checklist](#), is a Microsoft document that provides the prerequisites that you will need before the ExpressRoute circuit can be created.

Microsoft recommends the following prerequisites:

1. A valid Azure account.
2. An active Microsoft 365 subscription.
3. A connectivity provider.
4. Proper network requirements such as:
 - a. Network redundancy
 - b. Disaster Recovery redundancy
 - c. Proper routing between your onsite and how the provider will connect you to Azure.
 - d. Public IP NAT, no private IP addresses are allowed.
 - e. Follow QoS requirements if any.
 - f. [Network security](#).

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.

Creating an ExpressRoute Circuit

After the pre-requisites have been completed, the ExpressRoute circuit can now be installed. Microsoft provides five different methods listed below:

[Quickstart: Create and modify an ExpressRoute circuit](#) (Create using Azure Portal)

[Quickstart: Create and modify an ExpressRoute circuit using Azure PowerShell](#)

[Quickstart: Create and modify an ExpressRoute circuit using Azure CLI](#)

[Quickstart: Create an ExpressRoute circuit with private peering using Bicep](#)

[Quickstart: Create an ExpressRoute circuit with private peering using an ARM template](#)

Veritas recommends and uses Microsoft Peering to configure Azure ExpressRoute with Alta Recovery Vault storage. 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-peering>

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.

With an ExpressRoute configured for Microsoft Peering, in the past, 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, West US 2, etc.) the customer has chosen for their Alta Recovery Vault Azure storage.

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

<https://learn.microsoft.com/en-us/azure/expressroute/how-to-routefilter-portal>

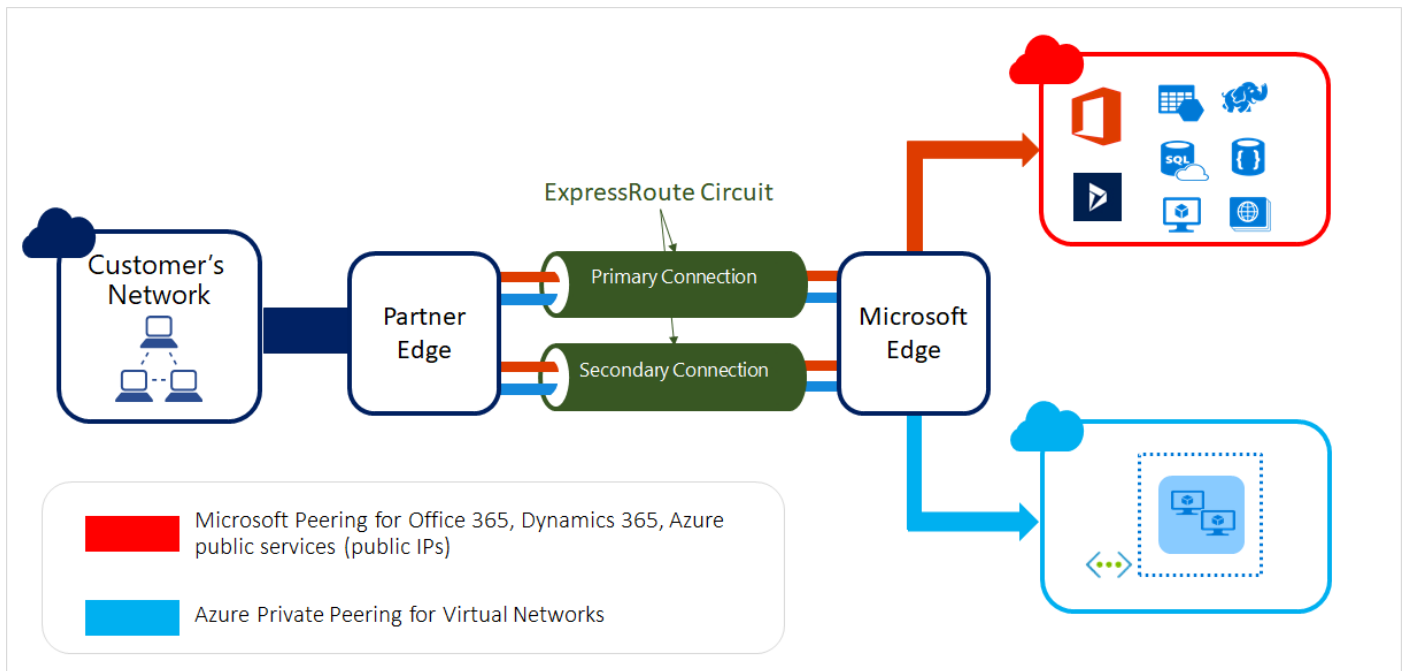


Figure 1. Typical Microsoft ExpressRoute configuration. Using Microsoft / Public Peering with Alta Recovery Vault.

Connecting to Alta Recovery Vault Storage with ExpressRoute

The following is an abbreviated list of steps that are needed to connect to Alta Recovery Vault storage. For an in-depth deployment guide on Alta Recovery Vault, see the [Veritas Alta Recovery Vault Deployment Guide](#).

For an in-depth look at security and best practices for Alta Recovery Vault, see the [Veritas Alta Recovery Vault Security Profile](#).

Note: Once configured, Azure ExpressRoute is transparent to Alta Recovery Vault and NetBackup irrespective of each other.

When requesting storage from Veritas, your 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 data is written in an immutable format.

Immutability gives you the ability to write once, and read many (WORM), to your Alta Recovery Vault storage and 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 Alta Recovery Vault or manipulating the data in any way.

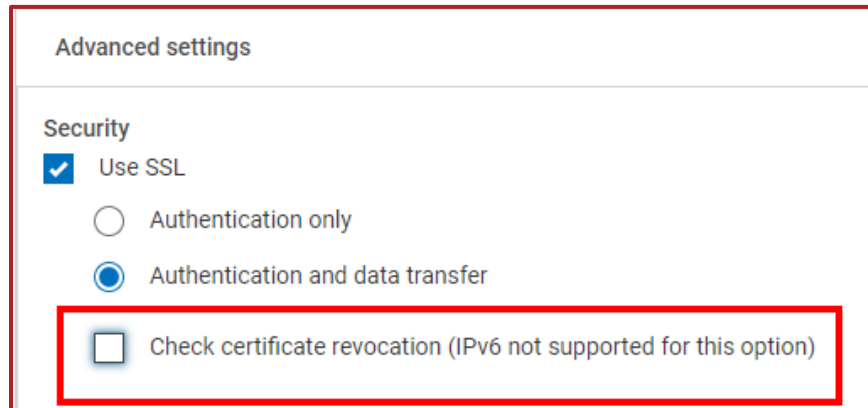
Note: This document is based on NetBackup 10.2 or later, for pre-10.2 steps, see the [Veritas Alta Recovery Vault Deployment Guide](#).

Ports

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. If outbound port 443 cannot be opened for security concerns, a proxy server can be added.

Note: It is a best practice that both DNS and NTP can resolve correctly.

Veritas checks for certificate revocation to ensure the certificates are valid, which means that port 80 needs to be opened outbound on the MSDP-C/storage server unless you do not wish to check for certificate revocation. To remove this certificate validation (not recommended), simply uncheck certificate revocation when creating the disk pool.



The screenshot shows the 'Advanced settings' dialog box with the 'Security' section expanded. It contains three radio buttons: 'Use SSL' (checked), 'Authentication only', and 'Authentication and data transfer'. Below these is a checkbox labeled 'Check certificate revocation (IPv6 not supported for this option)', which is currently unchecked and highlighted by a red rectangular box.

Note: For more information on Alta Recovery Vault security, see the [Alta Recovery Vault Security Profile](#) and [Veritas NetBackup Client Ports](#).

Connection Steps

Connection to your Alta Recovery Vault storage is simple and can be done through the NetBackup WebUI. For complete steps, see the [Alta Recovery Vault Deployment Guide](#)

Backup and Restore Testing

Backup and restore tests were performed with and without the ExpressRoute circuit.

The first test included a non-ExpressRoute virtual machine (VM), which was not part of the ExpressRoute VLAN. After monitoring the network traffic, we could infer that the network routing followed/traversed public Internet and reached the targeted Azure Storage Account, as seen in Figure 2.

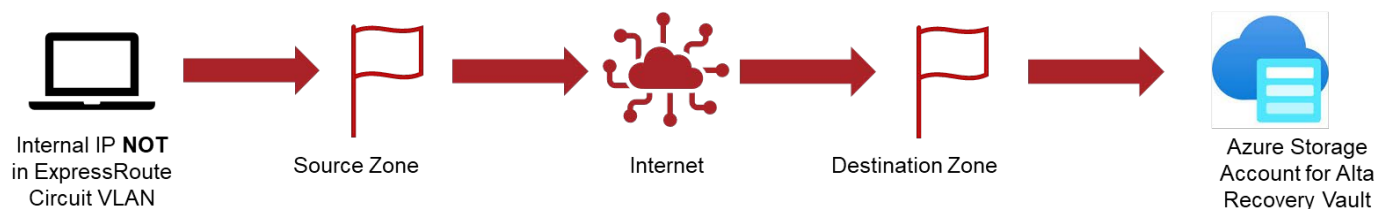


Figure 2: Backup and restore of a VM not in the ExpressRoute VLAN routed over the internet to connect to Azure.

The second test involved the backup and restore of a VM that was within the ExpressRoute VLAN. The network traffic followed the dedicated ExpressRoute channel over the provider's circuit and directly to Azure without traversing the public Internet, as seen in Figure 3.

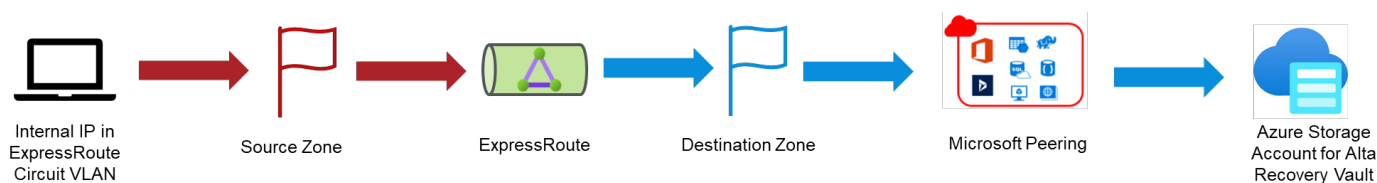


Figure 3: Backup and restore of a VM on the ExpressRoute VLAN that used the ExpressRoute to connect to Azure.

Backup Tests:

The following table shows three backup jobs that were performed on a similar sized file. The following is a summary of the three tests:

- Test Number 1 – Backup of a 3.45GB file using an ExpressRoute circuit of 50 Mbps bandwidth
- Test Number 2 – Backup of a 3.47GB file using the standard public Internet.
- Test Number 3 – Backup of a 3.55GB file using a 500Mbps ExpressRoute circuit.

The tests show the importance of proper bandwidth sizing and potential speed benefits of ExpressRoute.

Note: MBps is Megabyte per sec and Mbps is Megabit per sec. 1 MBps = 8 Mbps

Test Number	Express Route Used	NetBackup Version	File Size	Start	End	Total Time	Transfer Rate	ER Bandwidth
1	Yes	10.2	3.45GB	2:26:44 PM	2:37:20 PM	10 min 37 sec	5.92 MB/sec	50 Mbps
2	No	10.2	3.47GB	1:47:20 PM	1:50:10 PM	2 min 50 sec	64.56 MB/sec	NA
3	Yes	10.2	3.45GB	12:14:26 AM	12:15:45 AM	1 min 19 secs	58.54 MB/sec	500 Mbps

Restore Tests:

The following table shows three restore jobs that were performed on a similar sized file. The following is a summary of the three tests. Your backup and recovery numbers will vary depending on the size of the network pipe(s) and the data that is flowing over them.

- Test Number 1 – Restore of a 3.45GB file using a 50Mbps ExpressRoute circuit.
- Test Number 2 – Restore of a 3.47GB file using the standard public Internet.
- Test Number 3 – Restore of a 3.45GB file using a 500Mbps ExpressRoute circuit.

The tests show the importance of proper bandwidth sizing and potential speed benefits of ExpressRoute.

Test Number	ExpressRoute Used	NetBackup Version	File Size	Start	End	Total Time	Transfer Rate	ER Bandwidth
1	Yes	10.2	3.45GB	4:45:14 PM	5:10:38 PM	25 min 24 sec	2.33 MB/sec	50 Mbps
2	No	10.2	3.47GB	2:09:26 PM	2:11:56 PM	2 min 30 sec	40.2 MB/sec	NA
3	Yes	10.2	3.45GB	12:51:37 AM	12:52:52 AM	1 min 15 secs	51.76 MB/sec	500 Mbps

ExpressRoute Backup and Restore Summary

The speed of your backup and restore jobs, either on an ExpressRoute circuit or not, will depend on the size of the network pipe that the data is flowing over. Typically, larger pipes will provide quicker backup and restore while smaller pipes will become saturated, and the speed will be throttled. The data transfer rate is dependent on numerous factors like bandwidth of the ExpressRoute circuit, latency, frame size, window size, etc.

- Test 1 in both backup and restore shows the importance of proper network sizing. The ExpressRoute circuit is throttled by how much data can be pushed through and backup/restore data transfer rate begins to increase as expected.
- Test 2 in both backup and restore are not the ExpressRoute circuit and shows that with no network throttle, the speeds and feeds will increase dramatically. However, speed and feeds will greatly depend on your non-ExpressRoute circuit.
- Test 3 in both backup and restore depicts how increasing the ExpressRoute circuit bandwidth speeds up the data transfer rate of backup and restore job. As seen in the test the backup and restore finishes quicker than ExpressRoute circuit, due to the point-to-point architecture built into ExpressRoute.

ExpressRoute currently supports bandwidth from 50Mbps to 10Gbps, with the price increasing as bandwidth increases. Careful analysis of your current backup network needs should be considered when purchasing your ExpressRoute circuit. See [Azure ExpressRoute Pricing](#) for more information.

Bandwidth size can be checked in the Azure Portal as seen in Figure 4.

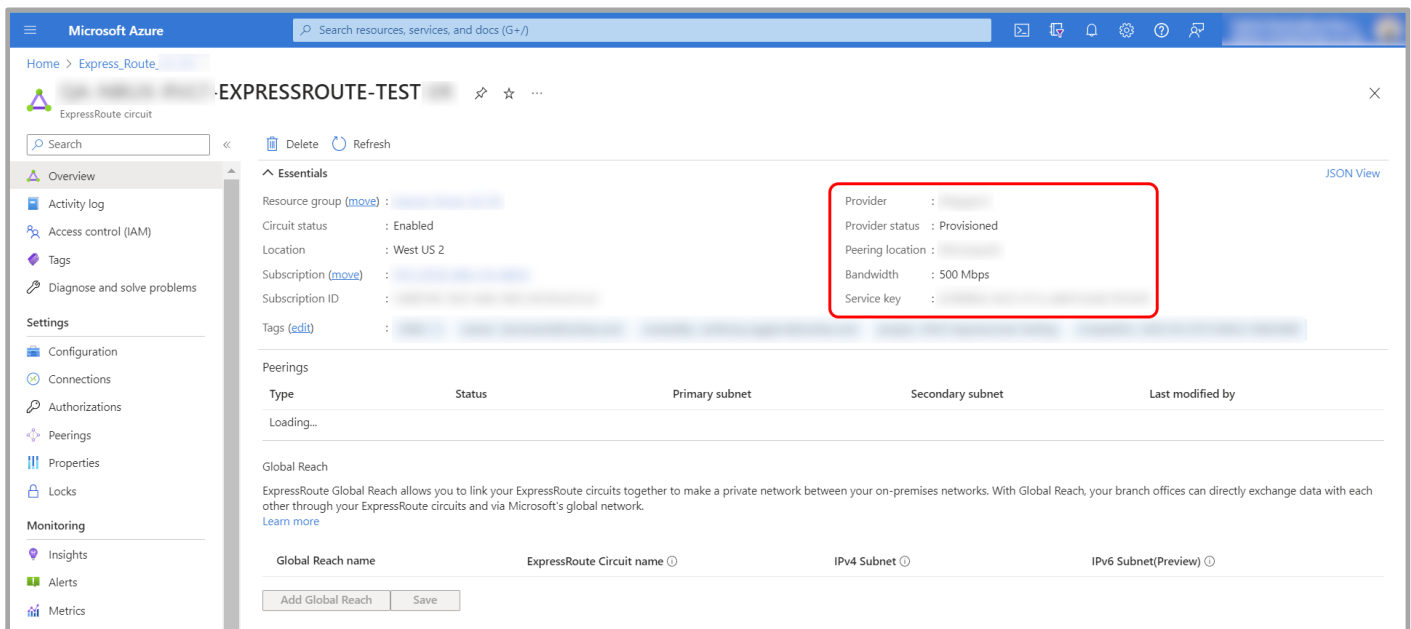


Figure 4: ExpressRoute Circuit with 500Mbps in Azure Portal.

Conclusion

Customers can now choose to use Azure ExpressRoute, which offers more reliability, faster speeds, consistent latencies, and higher security than typical connections over the public Internet or can continue to use standard

TLS (Transport Layer Security) security built into Veritas NetBackup. Either solution is supported and provides excellent connectivity for Veritas Alta Recovery Vault. Alta Recovery Vault not only simplifies the process of provisioning new storage in the cloud, but also reduces risk, allows for limitless scalability, lowers TCO and automates resiliency. Through seamless integration with NetBackup together with 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.

References

[What is Azure ExpressRoute?](#)

[Connect an on-premises network to Azure using ExpressRoute](#)

[ExpressRoute Documentation](#)

[Extend an on-premises network using ExpressRoute](#)

[ExpressRoute connectivity models](#)

[ExpressRoute FAQ](#)

[ExpressRoute Prerequisites and Checklist](#)

[Quickstart: Create and modify an ExpressRoute circuit](#) (Create using Azure Portal)

[Quickstart: Create and modify an ExpressRoute circuit using Azure PowerShell](#)

[Quickstart: Create and modify an ExpressRoute circuit using Azure CLI](#)

[Quickstart: Create an ExpressRoute circuit with private peering using Bicep](#)

[Quickstart: Create an ExpressRoute circuit with private peering using an ARM template](#)

[Veritas Alta Recovery Vault Deployment Guide](#)

[Veritas Alta Recovery Vault Security Profile](#)

[Azure ExpressRoute Pricing](#)

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.

VERITAS™