VERITAS

Veritas Alta™ Recovery Vault AWS Direct Connect Overview Guide

Cloud-based Storage-as-a-Service

This paper is designed to highlight the architecture and steps performed to validate AWS Direct Connect with Veritas Alta Recovery Vault

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

White Paper | October 2023

VERITAS ALTA™

Revision History

Version	Date	Changes	Author
1.00	8/14/2023	Initial Version	Neil Glick and Sakshi Nasha

Contents

Introduction 4

Executive Summary 4

Target Audience 4

Why Veritas Alta Recovery Vault 4

Why AWS Direct Connect 5

How it Works 5

AWS Direct Connect Components 6

AWS Direct Connect Pricing 7

How to Configure AWS Direct Connect 7

Prerequisites to Configure AWS Direct Connect. 7

Steps to Set Up AWS Direct Connect 8

Connecting to Veritas Alta Recovery Vault Storage with AWS Direct Connect 9

Ports 9

Connection Steps 10

Backup and Restore Testing 10

Backup Tests 11

Restore Tests 11

Direct Connect Backup and Restore Summary 12

Conclusion 12

References. 13

Introduction

Executive Summary

Veritas Alta Recovery Vault is cloud-based storage as a service that provides a seamless, fully-managed secondary storage option for NetBackup™ users. With Veritas Alta Recovery Vault, protecting critical data in the cloud has never been easier. Seamlessly integrated with NetBackup, an easy-to-use UI simplifies provisioning, management, and monitoring of cloud storage resources and retention policies. Veritas Alta Recovery Vault offers a single, flexible repository for all your data sources—from on-premises to your public cloud workloads. Veritas Alta Recovery Vault safely stores anything that NetBackup can protect.

The AWS Direct Connect cloud service is the shortest path to your AWS resources. It is a networking service that provides an alternative to the internet for connecting to AWS. Using AWS Direct Connect, data that would have previously been transported over the internet is delivered through a private network connection between your facilities and AWS. AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to one or more virtual private clouds (VPCs).

To ensure optimal functionality between Veritas Alta Recovery Vault and AWS Direct Connect, Veritas configured and tested Direct Connect with on-premises NetBackup. NetBackup with Veritas Alta Recovery Vault was used to back up and restore files over Direct Connect to test functionality and performance. The goal of this guide is to show that once configured, AWS Direct Connect is transparent to Veritas 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 AWS Direct Connect work together to offer a network connection that is more secure, reliable, and faster than the internet alone.

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 service level agreements (SLAs), data sovereignty, security, and ransomware resiliency.

Traditional approaches to cloud data protection cannot keep 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, protected from ransomware, disaster recovery ready, and can meet compliance and governance requirements.

Veritas Alta Recovery Vault is the right technology at the right time. It 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 are 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 AWS Direct Connect

AWS Direct Connect is a networking service that provides an alternative to using the internet to connect to AWS. Using AWS Direct Connect, data that would have previously been transported over the internet is delivered through a private network connection between your facilities and AWS. AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to one or more VPCs. AWS Direct Connect can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections. The AWS Direct Connect cloud service is the shortest path to your AWS resources. All AWS services, including Amazon Elastic Compute Cloud (EC2), Amazon Virtual Private Cloud (VPC), Amazon Simple Storage Service (S3), and Amazon DynamoDB can be used with AWS Direct Connect.

Following are some of the major reasons for choosing AWS Direct Connect:

1. AWS Direct Connect makes it easy to establish a dedicated connection from an on-premises network to one or more VPCs.
2. 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, thus improving application performance.
3. It is highly secure, as you can use multiple encryption options while the data moves between your network and AWS.
4. It can reduce your networking costs, with low data transfer rates out of AWS, and with higher bandwidth throughput.
5. It provides a more consistent network experience than internet-based connections.
6. It uses industry-standard 802.1Q VLANs to connect to Amazon VPC using private IP addresses. The VLANs are configured using virtual interfaces (VIFs), and you can configure three different types of VIFs: Public Virtual interface, Private Virtual Interface, and Transit Virtual Interface.
7. Dedicated connectivity also gives you much more flexibility. Multiple connection speeds and delivery options are available in order to support a wide range of scenarios.

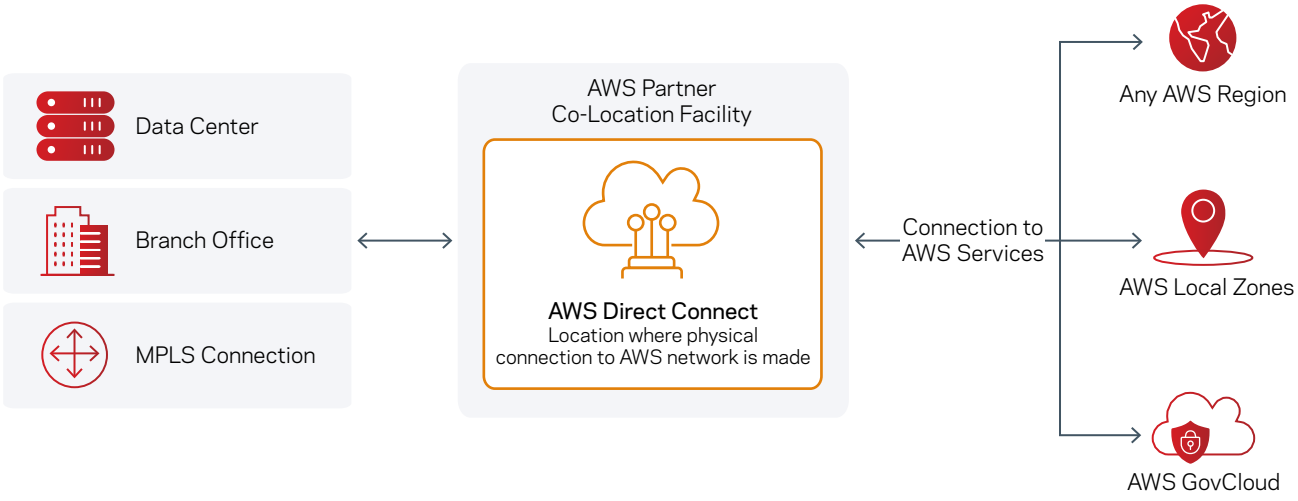


Figure 1. AWS Direct Connect Overview

How it Works

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 (for example, to 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 dDelivery pPartner, or choose a dedicated connection from AWS—and deploy at more thanover 100 AWS Direct Connect locations around the globe. For more information about AWS Direct Connect, please visit: aws.amazon.com/directconnect/ https://aws.amazon.com/directconnect.

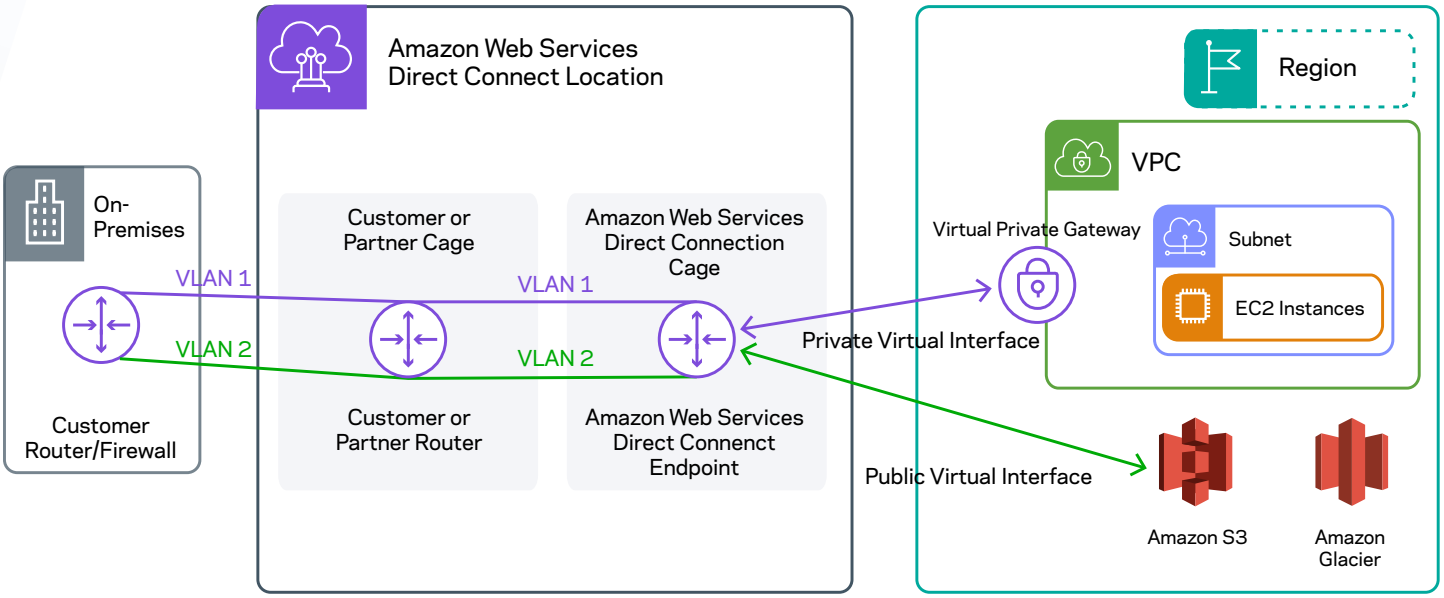


Figure 2. High-level overview of how AWS Direct Connect interfaces with your network

AWS Direct Connect Components

AWS Direct Connect has two main components:

1. **Connections:**

You need to create a connection in an AWS Direct Connect location to establish a network connection from your premises to an AWS Region. There are two types of connections:

a. **Dedicated Connection:** A physical Ethernet connection associated with a single customer. Customers can request a dedicated connection through the AWS Direct Connect console, the CLI, or the API.

For more information, see docs.aws.amazon.com/directconnect/latest/UserGuide/dedicated_connection.html.

b. **Hosted Connection:** A physical Ethernet connection that an AWS Direct Connect Partner provisions on behalf of a customer. Customers request a hosted connection by contacting a partner in the AWS Direct Connect Partner Program. The partner then provisions the connection.

For more information, see docs.aws.amazon.com/directconnect/latest/UserGuide/hosted_connection.html.

2. **Virtual Interfaces:**

You must create one of the following virtual interfaces to begin using your AWS Direct Connect connection:

a. **Private Virtual Interface:** A private virtual interface should be used to access an Amazon VPC using private IP addresses.

b. **Public Virtual Interface:** A public virtual interface can access all AWS public services using public IP addresses.

c. **Transit Virtual Interface:** A transit virtual interface should be used to access one or more Amazon VPC Transit Gateways associated with Direct Connect gateways. You can use transit virtual interfaces with any AWS Direct Connect dedicated or hosted connection of any speed.

For information about Direct Connect gateway configurations, see docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html.

For more information about virtual interfaces, see docs.aws.amazon.com/directconnect/latest/UserGuideWorkingWithVirtualInterfaces.html.

AWS Direct Connect Pricing

AWS Direct Connect has three major factors that determine pricing:

1) Capacity: The maximum rate that data can be transferred through a network connection. The capacity of AWS Direct Connect connections are measured in megabits per second (Mbps) or gigabits per second (Gbps). One gigabit per second, or 1 Gbps, is equal to 1,000 megabits per second (1,000 Mbps).

2) Port Hours: The time that a port is provisioned for your use with AWS, or an AWS Direct Connect Delivery Partner's networking equipment inside an AWS Direct Connect location. Even when no data is passing through the port, you are charged for port hours. Port hour pricing is determined by the connection type (dedicated or hosted).

a) Dedicated connections are physical connections between your network port and an AWS network port inside an AWS Direct Connect location. Dedicated port hours are billed as long as that port is provisioned for your use. You request a dedicated connection through the AWS Direct Connect section of the AWS Management Console.

b) Hosted connections are logical connections that an AWS Direct Connect Delivery Partner provisions on your behalf. When using hosted connections, you connect to the AWS network using one of the partner's ports. You request a hosted connection by contacting an AWS Direct Connect Delivery Partner directly.

3) Data Transfer Out (DTO): The cumulative network traffic sent through AWS Direct Connect to destinations outside of AWS. This is charged per gigabyte (GB), and unlike capacity measurements, DTO refers to the amount of data transferred, not the speed. When calculating DTO, exact pricing depends on the AWS Region or AWS Local Zone, and the AWS Direct Connect location you are using (see tables below). Data Transfer In refers to network traffic that is sent into AWS from outside, over AWS Direct Connect. AWS Direct Connect Data Transfer In is free, irrespective of location.

For detailed information about AWS Pricing, see: aws.amazon.com/directconnect/pricing.

How to Configure AWS Direct Connect

Prerequisites to Configure AWS Direct Connect:

1) **Select your Direct Connect locations:** Decide on your AWS Direct Connect locations, how many connections you would like to use, and the port size. Multiple ports can be used simultaneously for increased bandwidth or redundancy.

2) **Choose your physical connection type:** Choose between a dedicated connection or a hosted connection. A dedicated connection provides you exclusive access to cross connect, and offers multiple virtual interfaces. With a hosted connection, partners share the cross connect with multiple customers, and provide only a single virtual interface.

3) **Set up your logical virtual interfaces (VIFs):** Set up one or multiple VIFs over your physical connection: Transit virtual interfaces provide access to one or more AWS Transit Gateways. Public virtual interfaces allow access to AWS public services using public IP addresses. Private virtual interfaces provide access to Amazon VPC using private IP addresses.

4) **Proper network requirements:**

a. To use AWS Direct Connect, your network must meet the following conditions:

i. Your network is collocated with an existing AWS Direct Connect point-of-presence (AWS DX POP)

ii. You are working with an AWS Direct Connect partner who is a member of the AWS Partner Network (APN)

iii. You are working with an independent service provider to connect to AWS Direct Connect

b. By Default, Amazon will advertise all its public IP prefixes over the Public Direct Connect peering. If you utilize BGP filters to limit which prefixes are learned from Amazon, make sure to allow the BGP Community value for the corresponding Recovery Vault storage region. For more information, see Technical requirements for virtual interfaces to public AWS services.

c. The AWS Direct Connect network segment is configured to support:

i. 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices

ii. BGP and BGP MD5 authentication

d. AWS Direct Connect supports IPv4 and IPv6 communication protocols. IPv6 addresses provided by public AWS services are accessible through AWS Direct Connect public VIF.

e. Set up an Interconnection Option, which is a VPC Peering Connection: Update your VPC routing tables and 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 AWS storage. For more information, see AWS Direct Connect.

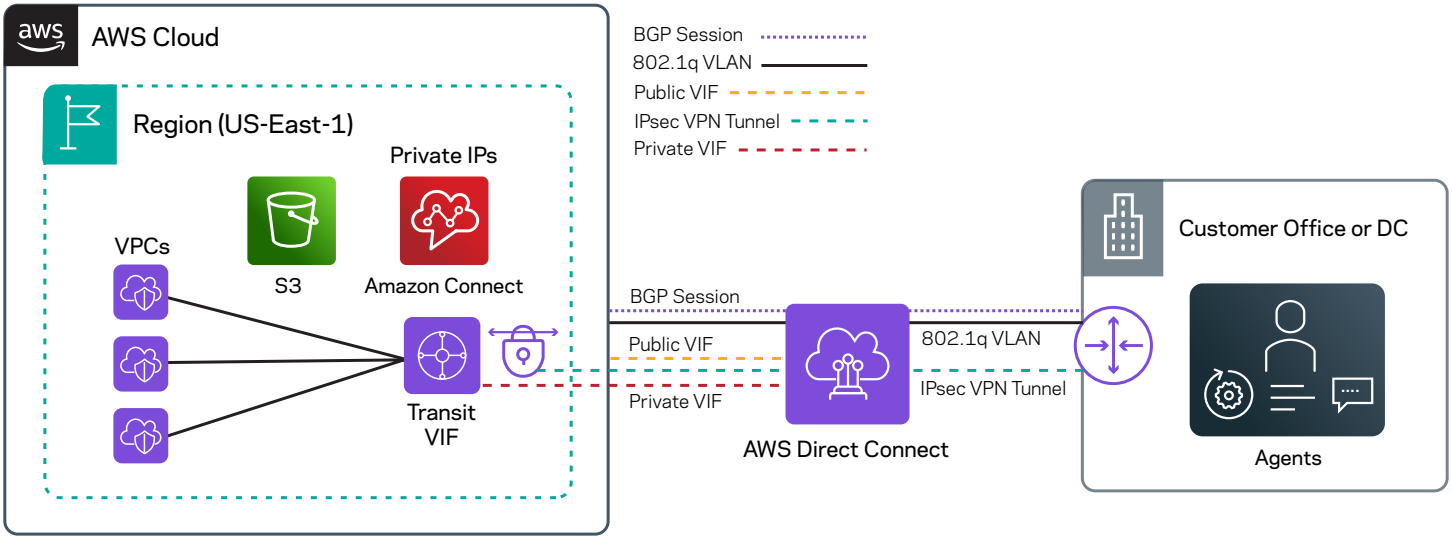


Figure 3. Reference diagram of VIF propagation over BGP

Steps to Set Up AWS Direct Connect:

To set up AWSa Direct Connect, you need to complete the following steps (fFor complete instructions, see AWS Direct Connect Setup):

1. Sign uUp for Amazon Web Services
2. Submit an AWS Direct Connect cConnection rRequest

(Note: You cannot change the port speed after you create the connection request.)

3. Complete the cCross cConnect

4. (Optional) Configure rRedundant cConnections with AWS Direct Connect

5. Performed by AMS (AWS Managed Service): Create a vVirtual iInterface
6. Performed by AMS: Download rRouter cConfiguration
7. Verify yYour vVirtual iInterface

Connecting to Veritas Alta Recovery Vault Storage with AWS Direct Connect

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

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

Note: Once configured, AWS Direct Connect is transparent to Veritas Alta Recovery Vault and NetBackup, irrespective of each other.

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 data is written in an immutable format.

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

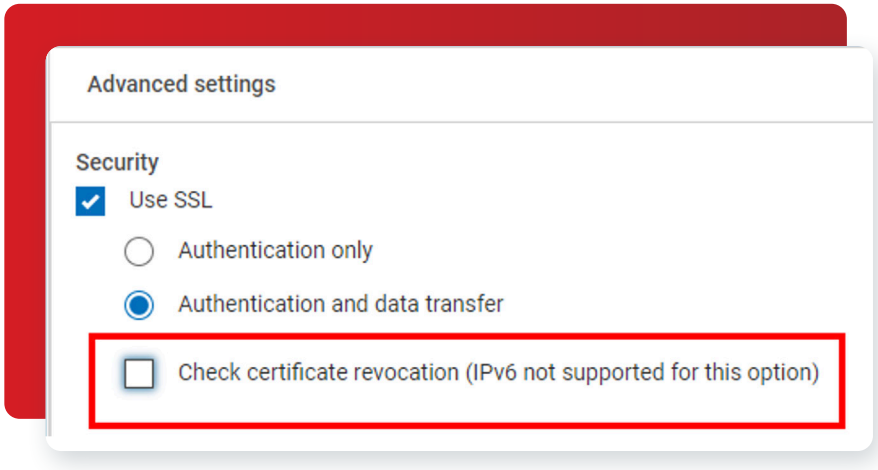
Note: This document is based on NetBackup 10.3 or later, for pre-10.3 steps, see the Veritas Alta Recovery Vault Deployment Guide.

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.



Note: For more information about Veritas Alta Recovery Vault security, see the Veritas Alta Recovery Vault Security Profile, and Veritas NetBackup Client Ports.

Connection Steps

Connecting to your Veritas Alta Recovery Vault storage is simple and can be done through the NetBackup WebUI. For complete steps, see the Veritas Alta Recovery Vault Deployment Guide.

Backup and Restore Testing

Backup and restore tests were performed with and without the Direct Connect (DX) circuit.

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

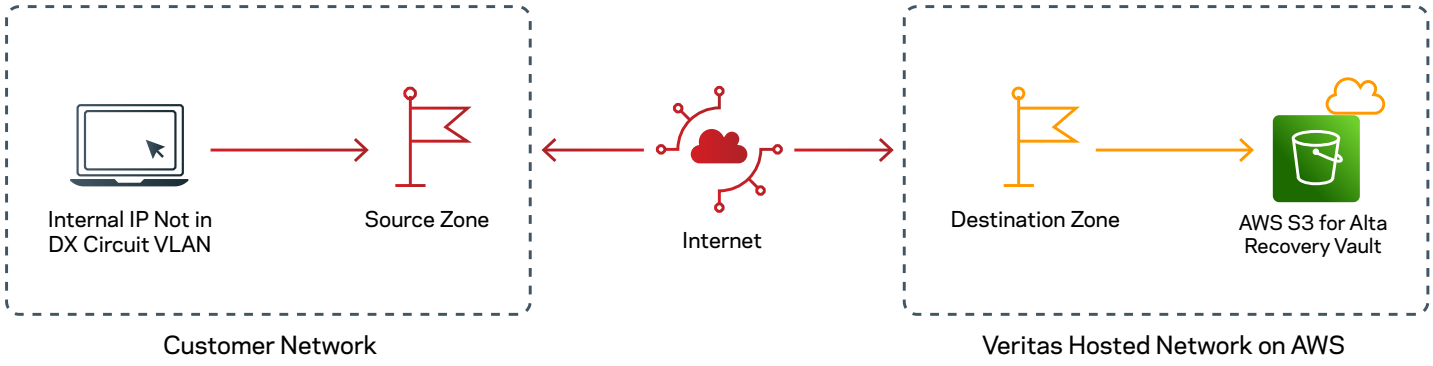


Figure 4. Backup and restore of a VM not in the DX circuit VLAN, routed over the internet to connect to Veritas Alta Recovery Vault

The third test involved the backup and restore of a VM within the Direct Connect VLAN. The network traffic followed the Direct Connect channel over the provider's circuit directly to AWS without traversing the public Internet.

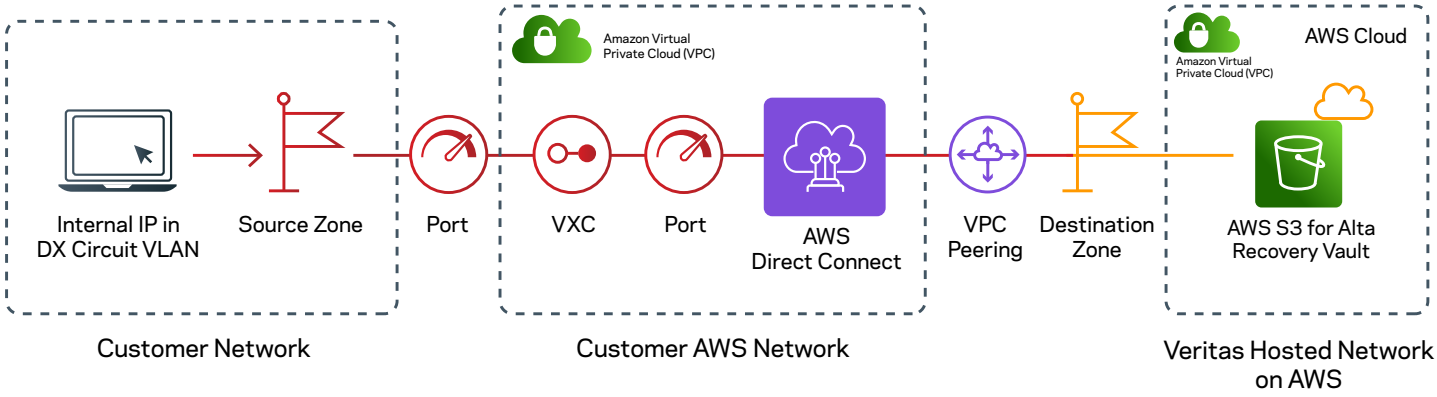


Figure 5. Backup and restore of a VM on the Direct Connect VLAN that uses Direct Connect to connect to Veritas Alta Recovery Vault

Testing results are based on the following configurations:

- Direct Connect location: us-east-1
- Physical Connection type: Hosted Connection
- Connectivity Provider
- Logical Virtual Interface: Private Virtual Interface VXC
- Physical Cross Connect (between the connectivity provider and cloud provider AWS) Port Speed used: 500 Mbps

(Note: You cannot change the port speed after you create the connection request in a dedicated connection)

- Veritas Alta Recovery Vault Amazon bucket region: us-east-1
- Veritas Alta Recovery Vault Amazon bucket storage class: Standard-IA
- Veritas Alta Recovery Vault bucket: Immutable (WORM-enabled)
- Peering: VPC public peering
- Note: A Hosted connection with 500 Mbps speed was selected for the following tests. Other available connection speeds:
    - Dedicated Connections, 1 Gbps, 10 Gbps, and 100 Gbps ports are available
    - Hosted Connections, connection speeds of 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, and 10 Gbps may be ordered from approved AWS Direct Connect partners. See AWS Direct Connect Partners for more information.

Backup Tests

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

- Test 1: Backup of a 5.97 GB file using the standard public internet
- Test 2: Backup of a 4.92 GB file using the standard public internet
- Test 3: Backup of a 5.76 GB file using a 500 Mbps Direct Connect circuit

The tests show the importance of connection type, and potential capacity benefits of Direct Connect.

Test No.	Direct Connect Used	NetBackup Version	File Size	Start	End	Total Time	Transfer Rate	Direct Connect Capacity/Type
1	No	10.3	5.97 GB	6:16:00 PM	6:18:41 PM	00:02:41	70.27 MB/sec	N/A
2	No	10.3	4.92 GB	6:21:21 PM	6:25:46 PM	00:04:25	23.12 MB/sec	N/A
3	Yes	10.3	5.76 GB	7:17:03 PM	7:19:08 PM	00:02:05	60.01 MB/sec	500 Mbps/ Hosted

Restore Tests:

The following table shows three restore tests that were performed. Your backup and recovery numbers will vary depending on the capacity of the network pipe(s), the type of connection, the type of virtual interface, and the data that is flowing over them.

- Test 1: Restore of a 5.97 GB file using the standard public internet
- Test 2: Restore of a 4.92 GB file using the standard public internet
- Test 3: Restore of a 5.76 GB file using a 500 Mbps Direct Connect circuit

The tests show the importance of connection type and potential capacity benefits of Direct Connect.

Test No.	Direct Connect Used	NetBackup Version	File Size	Start	End	Total Time	Transfer Rate	Direct Connect Capacity/Type
1	No	10.3	5.97 GB	6:21:09 PM	6:32:34 PM	00:11:25	9.14 MB/sec	N/A
2	No	10.3	4.92 GB	6:56:36 PM	7:12:06 PM	00:15:30	5.48 MB/sec	N/A
3	Yes	10.3	5.76 GB	7:28:02 PM	7:34:52 PM	00:06:50	14.62 MB/sec	500 Mbps/ Hosted

Direct Connect Backup and Restore Summary

The speed of your backup and restore jobs, whether on a Direct Connect circuit or not, will depend on the capacity 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 such aslike capacity of the Direct Connect circuit, latency, frame size, window size, location, type of connection, type of virtual interfacing, and moreetc.

- Test 1 in both backup and restore isare not the Direct Connect circuit. It and shows that with no network throttle, the speeds and feeds will increase dramatically. However, speed and feeds will depend on your non-Direct Connect circuit.
- Test 2 in both backup and restore isare not the Direct Connect circuit. It and shows that with no network throttle, the speeds and feeds will increase dramatically. However, speed and feeds will depend on your non-Direct Connect circuit.
- Test 3 in both backup and restore shows how NetBackup using the Direct Connect circuit completed fasterquicker than a standard iInternet circuit. This is most likely due to the point-to-point architecture built into Direct Connect.

Note: Internet speeds can be inconsistent due to other network traffic, which will affect backup and recovery speeds.

Note: For similar tests with Azure ExpressRoute, see the Veritas Alta Recovery Vault ExpressRoute Overview.

Conclusion

Customers can now choose to use AWS Direct Connect, which offers more reliability, faster speeds, consistent latencies, and higher security than typical connections over the public iInternet. Or customer mayor can continue to use standard transport layer securityTLS (TLSTransport Layer Security) security built into Veritas NetBackup. Either solution is supported and provides excellent connectivity for Veritas Alta Recovery Vault. Veritas Alta Recovery Vault not only simplifies the process of provisioning new storage in the cloud, itbut also reduces risk, allows for limitless scalability, lowers TCO, and automates resiliency. Through seamless integration with NetBackup, andtogether 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

AWS Direct Connect Overview

AWS Direct Connect – White Paper

AWS Direct Connect User Guide

Getting started with AWS Direct Connect

AWS Direct Connect for Amazon Connect Technical Overview White Paper

AWS Direct Connect Classic User Guide

AWS Direct Connect FAQs

Amazon Virtual Private Cloud Connectivity Options

AWS Direct Connect Routing Ppolicies and BGP Ccommunities User Guide

AWS Direct Connect + AWS Transit Gateway Connectivity Options White Paper

Transit VPC Connectivity Options White Paper

Blog : AWS VGW vs DGW vs TGW.

AWS Direct Connect for Amazon Connect Virtual Interfaces (VIF) White Paper

AWS Direct Connect Pricing

Veritas Alta Recovery Vault Azure ExpressRoute Overview Guide

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 91 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 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

V1984 10/23