Backup and Restore to AWS

Working with APN Partners

October 2019

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Introduction 1
What is Backup? 1
- Traditional Backup 2
- Hybrid Backup 2
- Cloud Backup 2
- Backup versus Replication 3

Cloud Connectors 3
- Arcserve UDP 4
- MSP 360 (formerly CloudBerry Backup) 4
- Cohesity 5
- Commvault 5
- Dell EMC NetWorker 5
- IBM Spectrum Protect 6
- IBM Spectrum Protect Plus 6
- N2W Software Cloud Protection Manager 7
- Rubrik Cloud Data Management 7
- Rubrik Datos IO RecoverX 7
- Veeam Backup & Replication 7
- Veritas Backup Exec 8
- Veritas NetBackup 8

Storage Gateways 9
- AWS Storage Gateway 9
- Dell EMC Data Domain 11
- HPE StoreOnce 11
- NetApp AltaVault 11
- Pure Storage ObjectEngine™ 12

Backup as a Service 12
- Druva inSync 12
- Druva Phoenix 13
- Clumio 13

Conclusion 13
Contributors 13
Further Reading 14
Document Revisions 14

Abstract

Today, many storage and backup administrators are looking for ways to extend their backup environments to Amazon Web Services (AWS). This paper outlines options for utilizing existing or leveraging new partner solutions to extend or fully migrate backup environments to AWS, as well as protect workloads running on AWS with partner solutions.

Introduction

Data is continuing to grow, which is driving the need to reconsider traditional backup environments. Storage administrators, backup administrators, and IT organizations are looking for the ability to extend data center backups to AWS and are looking to leverage backup solutions to help protect workloads running on AWS.

This whitepaper will explore various partner-based backup solutions and how they support working with various AWS services. This paper does not go in depth for each solution. For further details on individual solutions, links are provided to partners' website or documentation. For information about AWS backup strategies, see the AWS Backup and Restore Whitepaper.

What is Backup?

Backup and Restore solutions protect data from physical or logical errors, such as system failure, application error, or accidental deletion. Backup involves storing point-in-time copies of data. This data is often indexed to allow searching to find specific content, which can be at a granular level such as a virtual machine (VM) or a particular file.

Every backup solution is a slightly different, but many include similar components. The following are logical components of many popular backup software offerings. Sometimes these components are on a single server or appliance, and sometimes they can be distributed and scaled individually. Components may go by different names in each solution but maintain the same basic functions.

- **Catalog/Database** – The catalog or database generally holds the details of what has been backed up and where it is stored. It often also holds information like backup schedules, client, and server configuration.
- **Master Server** – The master server generally controls the backup environment. It is the main server and often hosts the backup database.
- **Media/Storage Server** – The Media or Storage server generally is responsible for connecting to the storage media disk, tape or object storage that stores the backup data.
- **Agent/Client** – The clients are the individual servers, storage, endpoints, and applications that are being backed up.
- **Proxy** – Some backup applications include proxies for accessing specific types of platforms, such as VMWare.

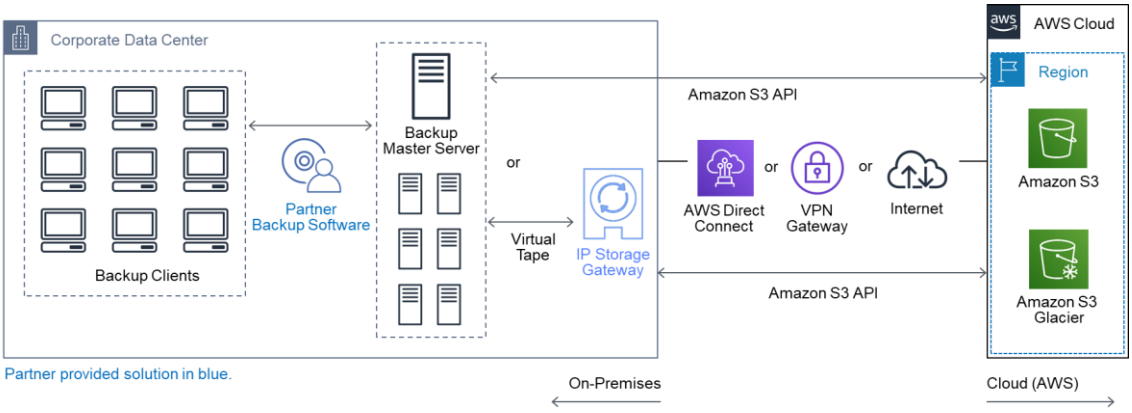

Figure 1: Backup to AWS using AWS Partner Network solutions

Traditional Backup

A traditional on-premises backup environment consists of a backup master and/or media server(s) that typically points to some type of disk storage as a primary backup target. Due to its cost profile, disk storage is generally only used for short-term retention. Secondary copies often are stored on tape storage for longer term retention. Depending on the business requirements the ratio of disk to tape can vary. These storage tiers are usually in a single datacenter, which is the same datacenter that hosts the primary data. Since the entire environment may reside in a single datacenter, many customers have a requirement to store a copy of the data in an offsite location. Due to the offsite requirement, customers who don't have a second datacenter often send copies of their tape to a tape storage provider.

Hybrid Backup

When customers begin to use AWS, backup workloads are often the first workloads customers move to the AWS Cloud. These customers also often want to extend their current on-premises backup solutions to AWS. Each Backup and Restore AWS Partner Network (APN) technology partner offers different methods to connect to AWS Cloud storage. The details of some of APN's Backup and Restore partners are below. In general, these backup solutions run in part or wholly on-premises. The software points to Amazon Simple Storage Service (Amazon S3) and/or Amazon S3 Glacier to either tier backup data, create a copy of backups, or act as the primary storage for backups.

Cloud Backup

As customers start moving their workloads to the AWS Cloud or launch new applications on AWS Cloud, they often turn to APN partner solutions to protect these workloads. To support this, many APN partner solutions can run on Amazon Elastic Compute Cloud (Amazon EC2). These backup solutions often work in very similar ways as they do on-premises and can allow customers to manage backups for their AWS workloads the same way they manage their on-premises environment.

Backup versus Replication

For many customers with large on-premises storage systems, replication can be a means of providing an offsite copy of data. Replication can be combined with snapshots on both the source and target array to provide point-in-time restores for data. This type of backup often has limitations, such as requiring the same storage system on both the source and target side and does not including granular indexing. This type of solution is often used for disaster recovery purposes, and is therefore out of scope for this document.

Cloud Connectors

Many APN partner Backup and Restore solutions include connecters for directly reading/writing to AWS storage, such as Amazon S3 or Amazon S3 Glacier. These connectors can be used with either existing on-premises installations or installations on Amazon EC2, where supported. Depending on the product, there are various levels of support, including tiering data, cloning data, or using AWS storage as a main data repository.

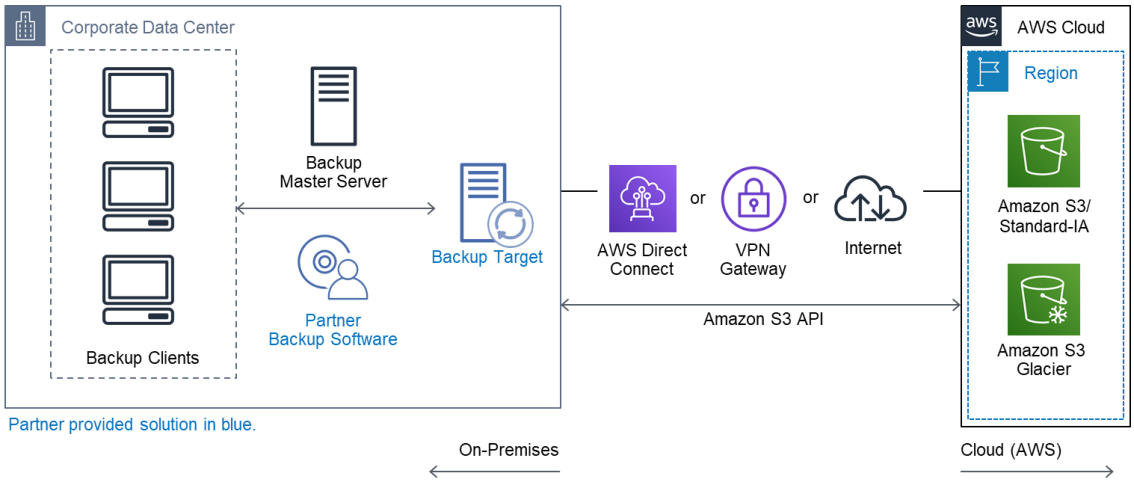

Figure 2: Back up to AWS from on-premises using cloud connectors

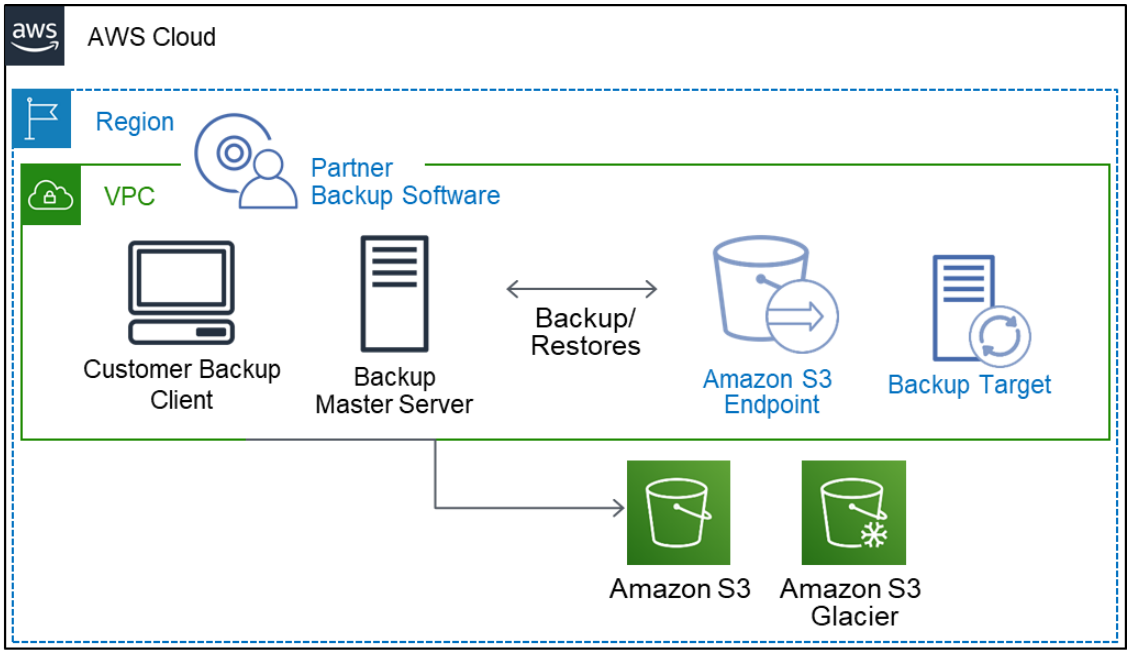

Figure 3: Back up of Amazon EC2 instances using cloud connectors

Arcserve UDP

Arcserve Unified Data Platform (UDP) supports backup to Amazon S3 directly from on-premises as well as running the UDP server on Amazon EC2. Arcserve UDP supports source-side global deduplication, encryption and compression and provides several deployment methods with AWS. These methods include backing up to Amazon S3, copying backups and individual files to Amazon S3, running a server on Amazon EC2, and replicating data between a server running on-premises and one running on Amazon EC2. Arcserve also supports a function called Instant Virtual Machine, which allows you to quickly create an Amazon EC2 instance from a backup stored on Amazon S3. Additional information can be found in the Arcserve deployment guide[1] and the Arcserve solutions guide[2].

MSP 360 (formerly CloudBerry Backup)

MSP 360 supports backing up directly to Amazon S3-Standard, Standard-Infrequent Access (S3-IA), One-Zone-IA (S3-ZIA), Intelligent-Tiering (S3-INT), Amazon S3 Glacier and Amazon S3 Glacier Deep Archive. MSP 360 can be configured to support Amazon S3 transfer acceleration. It also supports using Amazon S3 lifecycle policies, which can be managed in the MSP 360 client to support transitioning between different Amazon S3 and Amazon S3 Glacier storage classes.

MSP 360 supports encryption, compression, and deduplication. It also has a wide range of support for various clients and types of backups like image based, block level, application

aware, and network shares. MSP 360 operates on a per-client basis, with the clients directly talking to Amazon S3 to store the backups. For information on MSP 360, please visit the MSP 360 website.[3]

Cohesity

Cohesity is most commonly deployed as an on-site appliance, which can back up data locally and then move data, by policy, to Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive and includes support for Amazon S3 Glacier Vault Lock. Customers can configure policies that lifecycle the data to cloud storage as it ages out. Cohesity has client support for Microsoft SQL, Oracle, Microsoft Windows, Linux, Network Attached Storage (NAS) Shares and also virtual infrastructure support for VMware, Microsoft Hyper-V and Nutanix Acropolis. Cohesity also can be run as an Amazon EC2 instance, which can be used to restore workloads backed up from an on-premises instance in an Amazon S3 bucket to Amazon EC2. For more information, see the Cohesity AWS solution brief.[4]

Commvault

Commvault's architecture consists of a Commserve server and media agents. Media agents connect directly to Amazon S3, Amazon S3 Glacier, and Amazon S3 Glacier Deep Archive. Commvault provides support for all the current Amazon S3 storage classes available at the time of this document. Commvault can enable deduplication to any of the storage classes, including Glacier storage classes. Commvault also provides a combined storage class functionality where you can use an Amazon S3 storage class for metadata and an Amazon S3 Glacier storage class for data.

Commvault supports both AWS Snowball Edge and Snowball for off-line sync to cloud. You can also orchestrate snapshots, backup and restore from Amazon Elastic Block Store (Amazon EBS) snapshots, deduplicate, compress, and encrypt data both in transit and at rest.

Commvault can be deployed both on-premises and on AWS using Amazon EC2 instances for all components. For more information, visit the Commvault AWS microsite[5].

Dell EMC NetWorker

For Dell EMC NetWorker® to use AWS storage, there is an appliance called CloudBoost. The CloudBoost appliance acts as a global deduplication engine. There is CloudBoost client built into the NetWorker client in current versions. The clients are able to directly handle encryption, deduplication, compression and upload to object storage the net new bits. With this setup, the CloudBoost server only handles metadata operations so it can add additional clients without having to scale significantly.

NetWorker also supports cloning backups to a CloudBoost in which case backups on the clients would go to a NetWorker storage node and backups would be cloned and deduped on

CloudBoost appliance and sent to the Amazon S3 storage from the appliance. In this configuration, instead of each client sending to Amazon S3, the customer can have that filtered through the appliance to control bandwidth and be able to direct network routes for the specific IP, which some customers use in conjunction with AWS Direct Connect. For more information see the CloudBoost integration guide.[6]

IBM Spectrum Protect

IBM Spectrum Protect, formerly known as Tivoli Storage Manager (TSM), supports three main deployment patterns with AWS.

The first deployment pattern involves an IBM Spectrum Protect server that is installed on premises or on an Amazon EC2 instance, with primary backup and archive data landing on Amazon S3. This pattern could involve use of a direct-to-cloud architecture with accelerator cache or a small disk container pool with immediate tiering to a second cloud-container storage pool without accelerator cache.

The second deployment pattern would make use of AWS as the secondary site. Much like the first deployment pattern, here the IBM Spectrum Protect server at the secondary site could make use of a direct-to-cloud topology with a cloud pool featuring accelerator cache, or it could use a small disk container pool landing spot with immediate tiering to a cloud pool backed by object storage.

The third deployment pattern features specific use of disk-to-cloud tiering, available with IBM Spectrum Protect V8.1.3 and later, to allow for operational recovery data to reside on faster performing disk storage. Data that is older, archived, or both would be tiered to cloud-based object storage after a specified number of days. This deployment also could be performed at an on-premises site or within a cloud compute instance. However, the additional cost of having a larger capacity disk container pool should be factored into cost estimates with an in-the-cloud solution.

For more information on cloud-container see the IBM wiki.[7]

IBM Spectrum Protect Plus

IBM Spectrum Protect Plus is a data protection solution designed to provide near-instant recovery, replication, retention, and reuse for VMs, databases, and applications in hybrid environments. IBM Spectrum Protect Plus 10.1.3 on AWS is deployed as a hybrid solution in which the vSnap server, which hosts the backup repository, is hosted on AWS, with the management server, IBM Spectrum Protect Plus, is on premises. vSnap Server on AWS can be deployed in standalone or HA configuration, and uses Amazon EBS block storage as hot tier for storing backups. It also supports Amazon S3 and Amazon S3 Glacier as cloud storage tiers for cost effective, long term retention. Cloud workloads, such as Microsoft Exchange, Microsoft SQL Server, Oracle, DB2 and MongoDB running on Amazon EC2 are supported for data

protection. It also supports data reuse, for example, using backup data of on-prem applications for spinning up copies in AWS for DevOps, quality assurance, or testing purposes. For more information, visit the IBM Spectrum Protect Plus website[8]

N2W Software Cloud Protection Manager

N2W Software (N2WS) Backup & Recovery runs on AWS and supports backing up Amazon EC2 instances, Amazon Relational Database Service (Amazon RDS) instances, Amazon Redshift, Amazon DynamoDB and Amazon Elastic File System (Amazon EFS). N2WS Backup and Recovery can copy Amazon EC2 Instances, Amazon EBS Snapshots, Amazon RDS Snapshots and Amazon VPC settings to different AWS Regions and/or separate AWS accounts. N2WS supports file- and folder-level recovery, as well as the ability to copy Amazon EBS snapshots to Amazon S3. N2WS Backup & Recovery is available on the AWS Marketplace.[9] For more information, visit the N2WS AWS backup site.[10]

Rubrik Cloud Data Management

Rubrik is most commonly deployed as an on-site appliance, which can back up data locally and then move data, by policy, to Amazon S3, Amazon S3 Glacier including support for Amazon S3 Glacier Vault Lock. Customers can configure policies that lifecycle the data to cloud storage as it ages out. Rubrik has client support for Microsoft SQL, Oracle, Microsoft Windows, Linux, Network Attached Storage (NAS) Shares and also virtual infrastructure support for VMware, Microsoft Hyper-V and Nutanix AHV. Rubrik can also be run as an Amazon EC2 instance, which can used to restore workloads backed up from an on-premises instance in an Amazon S3 bucket to Amazon EC2. For more information, see the Rubrik AWS solution brief.[11]

Rubrik Datos IO RecoverX

Rubrik Datos IO RecoverX is a scale-out, elastic, software-only data management platform that runs on-premises or natively on AWS and delivers scalable and fully featured point-in-time backup and restore. RecoverX also provides data mobility to, from, and within AWS cloud for traditional applications and cloud-native applications. RecoverX can create application-consistent backups of databases running either on-premises or on Amazon EC2 and store the backups in Amazon S3.

For more information see the Datos IO website.[12]

Veeam Backup & Replication

Veeam Backup & Replication 9.5 Update 4b is typically deployed on-premises in VMware or Hyper-V environments, and also can be deployed on AWS on an Amazon EC2 instance or within a VMware Cloud™ on AWS environment. Veeam Backup & Replication can back up Windows and Linux hosts and supports item-level recovery through Veeam Explorers for

Microsoft Active Directory, Exchange, SharePoint, SQL Server, Oracle Database, and Storage Snapshots. Veeam Backup & Replication supports Amazon S3 Glacier and Amazon S3 Glacier Deep Archive through the AWS Storage Gateway configured in Virtual Tape Library (VTL) mode. Veeam Backup & Replication also supports offloading older backups directly to Amazon S3 through the Veeam Cloud Tier feature. For more information, visit the Veeam Backup & Replication product page.[13]

Veritas Backup Exec

Backup Exec is the Veritas solution for small and midsize businesses (SMB) and mid-market customers who are looking for a compelling backup solution that can span across the customers' diverse infrastructure requirements. Backup Exec has three main integration methods, using Amazon S3 as a storage target directly, using AWS Storage Gateway, and deploying on AWS to protect workloads running on AWS. Veritas Backup Exec is available in the AWS Marketplace[14]. For more information, visit the Veritas Backup Exec AWS microsite.[15]

Veritas NetBackup

Veritas NetBackup includes several options for integrating with AWS services. All components of the NetBackup solution, which include a master server and media server(s), can run on Amazon EC2.

Media server(s) that run on Amazon EC2 can store deduplicated backups on block storage, which is known as Media Server Deduplication Pool (MSDP). On AWS, the block storage would be Amazon EBS volumes attached to the Amazon EC2 instance.

Media servers also can be configured with a cloud connector. This enables the servers to directly store data onto all the storage classes of Amazon S3 or Amazon S3 Glacier. Data stored with the cloud connector is compressed. Amazon S3 Glacier is supported via the use of a zero-day lifecycle policy[16].

Lastly, NetBackup CloudCatalyst can be used as a gateway between the media server and Amazon S3. When NetBackup CloudCatalyst is deployed, it handles deduplication of the data before it is sent to Amazon S3 or Amazon S3 Glacier. NetBackup CloudCatalyst can be deployed as a physical or virtual appliance on-premises, not only reducing the amount stored in Amazon S3 but also reducing the amount of data sent over the wire. NetBackup CloudCatalyst also can be deployed on an Amazon EC2 instance. Along with the master and media server, Veritas NetBackup can be used to protect Amazon EC2 instances sending deduplicated data to Amazon S3, Amazon S3 Glacier, or Amazon S3 Glacier Deep Archive. For more information about NetBackup with AWS, see the NetBackup AWS microsite.[17]

Storage Gateways

Storage Gateways often are used in conjunction with backup software. Gateways can provide specialized functionality like protocol conversion, compression, deduplication, and caching. Different gateways support different front-end and back-end protocols and may offer just some or all of the aforementioned features.

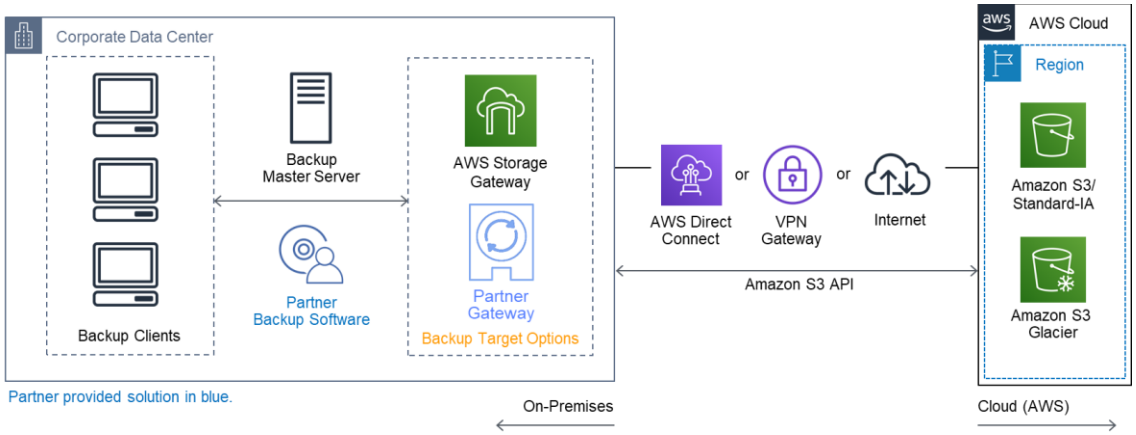

Figure 4: Back up to AWS using storage gateways

AWS Storage Gateway

AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. You can use the service for backup and archiving, disaster recovery, cloud bursting, storage tiering, and migration. Your applications connect to the service through a gateway appliance using standard storage protocols, such as NFS, SMB and iSCSI. The gateway connects to AWS storage services, such as Amazon S3, Amazon S3 Glacier, Amazon S3 Glacier Deep Archive and Amazon EBS, providing storage for files, volumes, and virtual tapes in AWS. The service includes a highly-optimized data transfer mechanism, with bandwidth management, automated network resilience, and efficient data transfer, along with a local cache for low-latency on-premises access to your most active data. For more information check the AWS storage gateway page.[18]

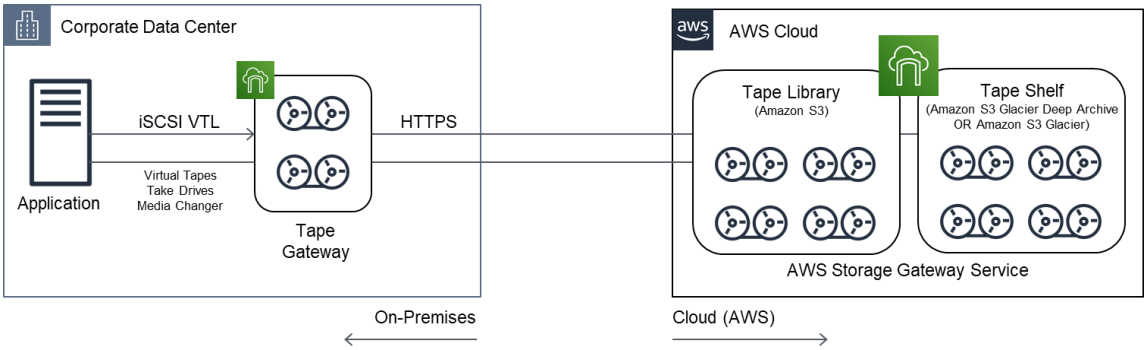

Figure 5: AWS Storage Gateway VTL Mode

The below backup applications are currently supported with Storage Gateway Virtual Tape Library (VTL) Mode. For the latest list check the VTL requirements document on the AWS site.[19]

Backup Application	**Medium Changer Type**
Arcserve Backup	*AWS-Gateway-VTL*
Bacula Enterprise V10.x	*AWS-Gateway-*
Commvault V11	*STK-L700*
Dell EMC NetWorker V8.x or V9.x	*AWS-Gateway-VTL*
IBM Spectrum Protect v7.x	*IBM-03584L32-*
Micro Focus (HPE) Data Protector 9.x	*AWS-Gateway-VTL*
Microsoft System Center 2012 R2 or 2016 Data Protection Manager	*STK-L700*
NovaStor DataCenter/Network 6.4 or 7.1	*STK-L700*
Quest NetVault Backup 10.0 or 11.x or 12.x	*STK-L700*
Veeam Backup & Replication V7 or V8	*STK-L700*
Veeam Backup & Replication V9 Update 2 or later	*AWS-Gateway-VTL*
Veritas Backup Exec 2014 or 15 or 16 or 20.x	*AWS-Gateway-VTL*
Veritas Backup Exec 2012 **Note:** *Veritas has ended support for Backup Exec 2012. For more information, see End of Support for Prior Backup Exec Versions.*	*STK-L700*
Veritas NetBackup Version 7.x or 8.x	*AWS-Gateway-VTL*

Dell EMC Data Domain

Dell EMC Data Domain is an appliance that can be deployed physically or virtually. The virtual appliance is known as Data Domain Virtual Edition (DDVE) and has some different limitations from the physical appliance, such as maximum capacity. Data Domain supports multiple front-end protocols such as CIFS/NFS and its own DD Boost protocol. Data Domain can integrate with and be supported by many popular backup software offerings.

Data Domain uses disk storage with deduplication. The primary storage for Data Domain is called the active tier. Data Domain also supports a secondary tier called cloud tier. The cloud tier is a separate deduplication domain from the active tier. There is a cache disk that is set up for the cloud tier that is separate than the disk storage used for the active tier. The data is either moved from the active tier to the cloud tier based on age of data or via an application policy from a supported backup application, such as Dell EMC NetWorker. Data Domain supports uploading to Amazon S3 and supports up to two times the size of the data in the active tier.

DDVE can run on-premises in a virtual environment or on AWS as an Amazon EC2 instance. When running on-premises, cloud tier is supported similar to how it is on the physical appliance. The version of DDVE that runs on AWS does not currently support cloud tier but supports using Amazon S3 for the active tier. When running on AWS only, DD Boost protocol is supported, which enables client-side deduplication so a minimum amount of traffic needs to be sent between the client and the DDVE instance.

DDVE is available through the AWS Marketplace. See the DDVE listing for more information.[20]

HPE StoreOnce

HPE StoreOnce is a scale-out backup target that can be deployed as a physical or a virtual appliance and makes use of deduplication to reduce the amount of local storage needed on the StoreOnce appliance. The virtual appliance, known as the HPE StoreOnce Virtual Storage Appliance (VSA), runs on VMware and Hyper-V hypervisors and supports up to 500 TB per VSA. HP StoreOnce also can provide (via additional licenses) encryption in-flight and at rest, and also supports Amazon S3 through the HPE Cloud Bank Storage feature. For more information, please visit the HPE StoreOnce appliance site.[21]

NetApp AltaVault

NetApp AltaVault has gone End of Life. If you are currently storing data with AltaVault on AWS, NetApp continues to support existing customers for five years past the End of Life date. If you need to store your data beyond five years or need to start sending your new data via another method, explore other solutions mentioned in this whitepaper or reach out to your AWS account team to help find the right solution for you. For more information, see the NetApp AltaVault site.[22]

Pure Storage ObjectEngine™

Pure Storage ObjectEngine™, based on StorReduce technology, is a storage gateway specifically designed to sit in front of Amazon S3 and/or Pure Storage FlashBlade™ and handles deduplication. Pure Storage ObjectEngine™, unlike some other gateways, is not designed to do protocol conversion but instead provides Amazon S3 protocol on both the front end and the back end. Pure Storage ObjectEngine™ handles global deduplication, often providing greater deduplication levels then some backup software can achieve with its own deduplication algorithms. Pure Storage ObjectEngine™ can be used with nearly any backup software that supports Amazon S3.

You can deploy Pure Storage ObjectEngine™ as an on-premises appliance. For more information visit the Pure Storage ObjectEngine™ Site.[23]

Backup as a Service

Backup as a Service is a Software as a Service (SaaS) offering that backs up a myriad of clients and devices without the need to manage any server or storage infrastructure as part of the backup environment. Agents are installed on the clients, but all other components of the backup environment run in the partner's AWS account.

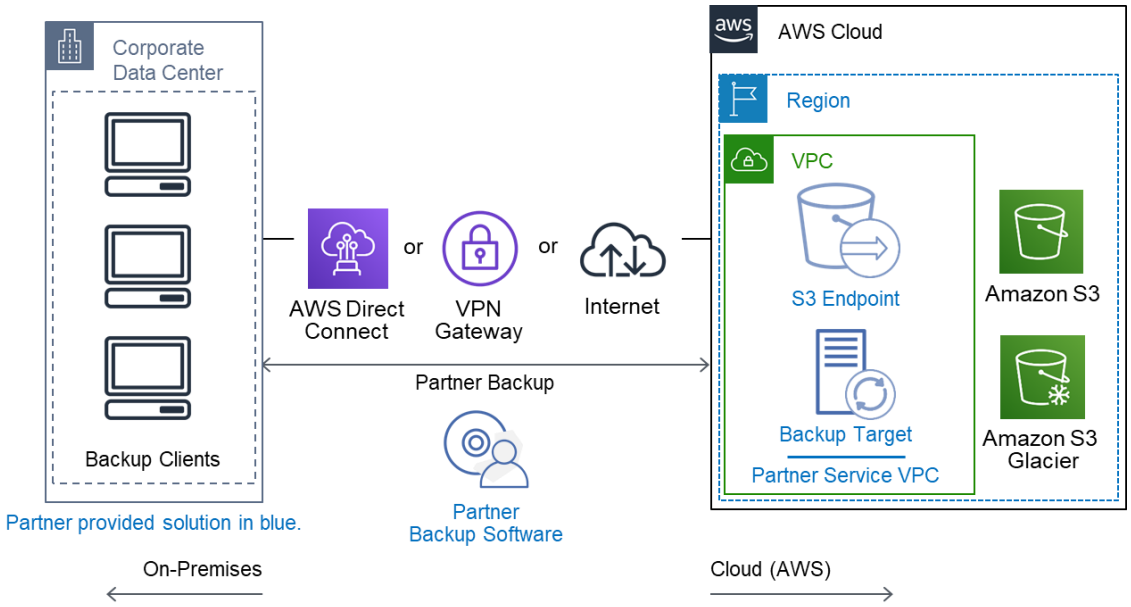

Figure 6: Software as a Service backup model

Druva inSync

Druva inSync provides a single pane of glass for protecting, preserving and discovering information across endpoints and cloud applications. Druva provides global deduplication and utility pricing

where customers pay for data usage post deduplication. More information about Druva inSync can be found on the Druva inSync site.[24]

Druva Phoenix

Druva Phoenix is designed to back up physical and virtual servers. In addition to backing up to Amazon S3, it supports moving archival and long-term retention backups to Amazon S3 Glacier. More information about Druva Phoenix can be found on the Druva Phoenix site.[25]

Druva CloudRanger

Druva CloudRanger is designed for cloud data protection. It supports backup & recovery of AWS services such as Amazon EC2, Amazon S3, Amazon RDS, Amazon Redshift, Amazon DocumentDB, and Amazon Neptune. It also provides automated disaster recovery functionality and Amazon EBS snapshot archiving capabilities to Amazon S3 Glacier and Glacier Deep Archive. More information about Druva CloudRanger can be found on the Druva CloudRanger site.[31]

Clumio

Clumio protects VMware Cloud™ on AWS environments, on-premises VMware deployments, and AWS services such as Amazon EC2 and Amazon EBS. Clumio backs up data to Amazon S3, encrypting data in transit and at rest. More information on Clumio can be found on the Clumio site.[26]

Conclusion

There are many options that you can use to back up your on-premises workloads to AWS or to protect your workloads running on AWS. Almost any major backup software has some option to store backups on AWS storage. It is important to understand the options that each backup software supports and how the software integrates other partner solutions like gateways to create a comprehensive solution that meets virtually any backup requirement.

Contributors

The following individuals and organizations contributed to this document:

- Henry Axelrod, partner solutions architect, Amazon Web Services
- Anthony Fiore, partner solutions architect, Amazon Web Services
- Girish Chanchlani, partner solutions architect, Amazon Web Services

Further Reading

For additional information, see the following:

- AWS Whitepapers[27]
- Amazon Simple Storage Service [28]
- Backup and Recovery Approaches using AWS[29]
- Backup and Recovery Partner Solutions [30]

Document Revisions

Date	Description
December 2019	Updated to reflect current offerings
October 2019	Updated to reflect current offerings
August 2018	First publication

Notes

[1] https://s13937.pcdn.co/wp-content/uploads/2018/02/Arcserve-UDP-On-AWS-Cloud-v3.1_Final.pdf
[2] https://s13937.pcdn.co/wp-content/uploads/2017/03/Arcserve-Solutions-for-AWS.pdf
[3] https://www.cloudberrylab.com/backup.aspx
[4] https://www.cohesity.com/solution/cloud/aws/
[5] https://www.commvault.com/solutions/by-technology/virtual-machine-and-cloud/amazon-web-services/backup-and-archive-to-the-cloud
[6] https://www.emc.com/collateral/TechnicalDocument/docu81525.pdf
[7] https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Storage%20Manager/page/Cloud-container%20storage%20pools%20FAQs
[8] https://www.ibm.com/us-en/marketplace/ibm-spectrum-protect-plus/
[9] https://aws.amazon.com/marketplace/seller-profile?id=b1157be6-ad44-4ba2-9db1-b95a423fd270
[10] https://n2ws.com/product
[11] https://www.rubrik.com/wp-content/uploads/2018/02/Solution-Brief-Rubrik-and-Amazon-Web-Services-AWS.pdf
[12] https://www.rubrik.com/product/datos-io-overview/
[13] https://www.veeam.com/vm-backup-recovery-replication-software.html
[14] https://aws.amazon.com/marketplace/pp/B075S3PKVR
[15] https://www.veritas.com/product/backup-and-recovery/backup-exec/amazon-web-services
[16] https://www.veritas.com/support/en_US/doc/58500769-127471507-0/v126612396-127471507
[17] https://www.veritas.com/protection/netbackup?inid=us_veritas_cloud_aws_products_netbackup
[18] https://aws.amazon.com/storagegateway/
[19] https://docs.aws.amazon.com/storagegateway/latest/userguide/Requirements.html#requirements-backup-sw-for-vtl
[20] https://aws.amazon.com/marketplace/pp/B07MPDNHT2
[21] https://www.hpe.com/us/en/storage/storeonce.html
[22] https://cloud.netapp.com/altavault
[23] https://www.purestorage.com/products/objectengine.html
[24] https://www.druva.com/products/insync/
[25] https://www.druva.com/products/phoenix/
[26] https://clumio.com/
[27] https://aws.amazon.com/whitepapers/
[28] https://aws.amazon.com/documentation/s3/
[29] https://d1.awsstatic.com/whitepapers/Storage/Backup_and_Recovery_Approaches_Using_AWS.pdf
[30] https://aws.amazon.com/backup-recovery/featured-partner-solutions/
[31] https://cloudranger.com/