

Scale to Amazon Web Services with Backup Exec

Overview

Backup Exec™ delivers powerful, flexible and trusted data protection designed for your entire infrastructure regardless of platform: virtual, physical or cloud. With Backup Exec, you get fast, reliable protection of data and systems at every level as well as advanced integration with the most recent releases of Microsoft Server, Microsoft Hyper-V and VMware vSphere. In a matter of minutes, you can recover anything including virtual machines, servers, databases, files and granular application objects. Protect one to thousands of VMs from a single user console, optimizing performance and efficiency. Backup Exec saves time, optimizes costs and helps ensure your critical information is always protected and easily recoverable.

Veritas and Amazon Web Services (AWS) have worked together to provide businesses with the best information management solutions. The AWS-Veritas partnership is based on many years of collaboration, development and support, with proven results in enterprises and SMBs worldwide. The close relationship between Veritas and AWS ensures that Backup Exec customers will benefit from the innovation and the highest-quality data protection in the cloud with AWS. Also, AWS cloud support for Backup Exec continues to expand the off-site storage options available to customers, now including AWS Glacier and Glacier Deep Archive. Organizations can immediately embrace new platforms and workloads for their IT application needs, confident in the knowledge they can transform their IT infrastructure while keeping their data safe.

Business Value

It's no secret that the industry is rapidly evolving toward hybrid IT architectures and this journey will include extending the on-premises data center to both public and private clouds. In fact, a Veritas cloud survey reports that two-thirds (67 percent) of enterprises already use or plan to use a multi-cloud model and a quarter of respondents (25 percent) plan to use four or more cloud providers.¹

Managing and protecting data no matter where it resides is a key success factor when leveraging the cloud. To simplify and accelerate your journey toward digital transformation, it's important to ensure your data protection solution enables you to easily unify and extend the management of workloads and data whether on-premises, in the cloud, at globally dispersed remote locations, on disk or on tape.

Whether backing up to the cloud, protecting workloads within the cloud or recovering from the cloud or connections back to on-premises, Backup Exec integrates with a broad selection of cloud service providers to seamlessly unify data protection across the multi-cloud.

Underlying Principles

The cost and flexibility of the cloud are driving organizations to consider strategies that leverage the affordability of public cloud services and the agility of private clouds or a combination of the two. Cloud-based backup and recovery offers its own benefits, including a reduction in capital expenses (CapEx) due to the elimination of on-site storage and servers while still meeting retention and compliance requirements.

Although the reduction in costs can be compelling when moving workloads for backup, archiving and recovery to the cloud, concerns about security and performance may still exist, especially for public cloud solutions. At the same time, organizations running production environments in the cloud need a solution that extends current capabilities, enabling the flexible movement of data without creating new processes or requiring additional time and staffing. The ideal solution will not only support the evolution toward software-defined data centers, virtualization and disaster recovery as a service (DRaaS), but will also modernize recovery and continuity efforts with the nearly limitless capacity to scale and meet elastic demand.

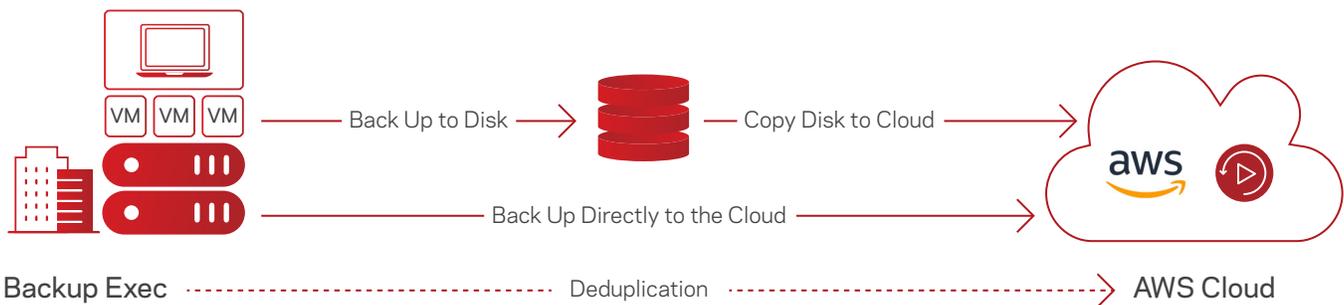
AWS Cloud

AWS is an open, flexible, enterprise-grade cloud computing platform. AWS integrates with your existing IT environment through the largest network of secure private connections, hybrid database and storage solutions and data residency and encryption features—so your assets stay right where you need them. AWS is the cloud storage solution for modern applications that rely on durability, availability and scalability to meet the needs of customers. AWS is massively scalable, allowing you to store and process hundreds of terabytes of data, and is accessible from anywhere in the world, from any type of application, whether it's running in the cloud, on the desktop, on an on-premises server or on a mobile or tablet device.

There are two scenarios to consider when integrating your backup and recovery strategy with the AWS cloud infrastructure:

Protect Data with AWS—Copy on-premises data to and restore it from AWS via the Backup Exec AWS cloud connector or a cloud storage gateway like NetApp Cloud Backup. Possible backup strategies using the new AWS cloud connector include:

- **Disk to Disk to Cloud (D2D2C)**—Data is initially backed up to on-site disk, deduplication storage, appliance or VTL, and a copy is then sent to AWS
- **Disk to Cloud (D2C)**—Deduplicated data is backed up over the WAN directly to AWS and there is no on-site storage of backup data



Protect Data within AWS—Workloads and data are protected within the AWS cloud environment using Backup Exec infrastructure hosted in AWS. Possible backup strategies by hosting backup infrastructure alongside workloads in the cloud include:

- Cloud-to-cloud (C2C) backup
- Cloud to on-premises backup

Protect Data With AWS

With the ability to optimize data transfer and reduce risk, Backup Exec brings the benefits of AWS to organizations that want to augment existing on-premises disk and tape storage.

- Integrate seamlessly with Backup Exec
- Manage the backup and recovery of data in and out of AWS in minutes thanks to Backup Exec's easy setup
- Leverage the scalability of AWS to store and process hundreds of terabytes of data to support your workload needs
- Eliminate tape backups and reduce storage costs with deduplication

Backup Exec AWS Cloud Connector

Backup Exec integrates with AWS via the Backup Exec AWS cloud connector (see Figure 1), allowing IT departments to manage AWS for backup and recovery as easily as on-premises storage, but with scalability, improved flexibility and lower costs. Organizations can leverage AWS as a new storage tier or as a secondary off-site location for disaster recovery.



Figure 1. Access the Backup Exec Azure cloud connector under the Storage Configuration Wizard.

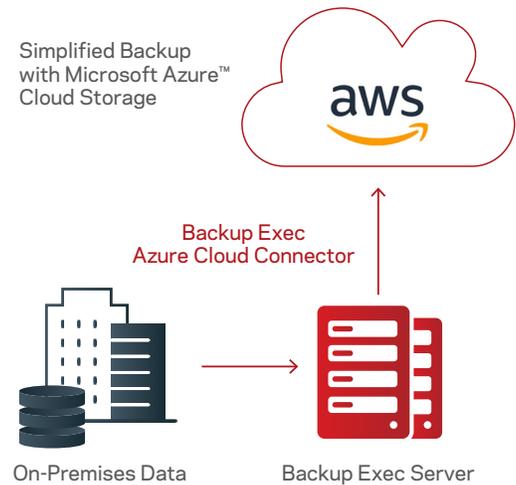


Figure 2. Backup Exec can transfer and store data in AWS using the Backup Exec AWS cloud connector.

The Backup Exec AWS cloud connector enables connections to AWS hot and cold storage tiers.

In this scenario, the on-premises data center runs normal backup operations and backup data is copied to AWS storage, including S3, AWS Glacier and AWS Glacier Deep Archive via the Backup Exec AWS cloud connector (see Figure 2).

With this approach, you can move archived data or data you don't frequently access to the cloud via the cloud connector and keep critical data that you need to access more frequently on-premises.

Benefits of this approach with Backup Exec include:

- Visibility into your data no matter where it resides
- Shift of storage costs to a pay-as-you-go OpEx model
- Storage of data off-site so it will be available if a disaster should strike
- Source operational recovers by on-premises storage
- Protection against ransomware attacks with the Ransomware Resilience feature

Nothing to install

The Backup Exec AWS cloud connector does not require an additional license or option for Backup Exec. Backup Exec includes the fully integrated AWS cloud connector to attach AWS targets to the organization. Just enter the interoperability access key and the secret key, choose the storage bucket to authenticate and the Backup Exec Storage configuration wizard will do the rest for you. (See Figure 3.)

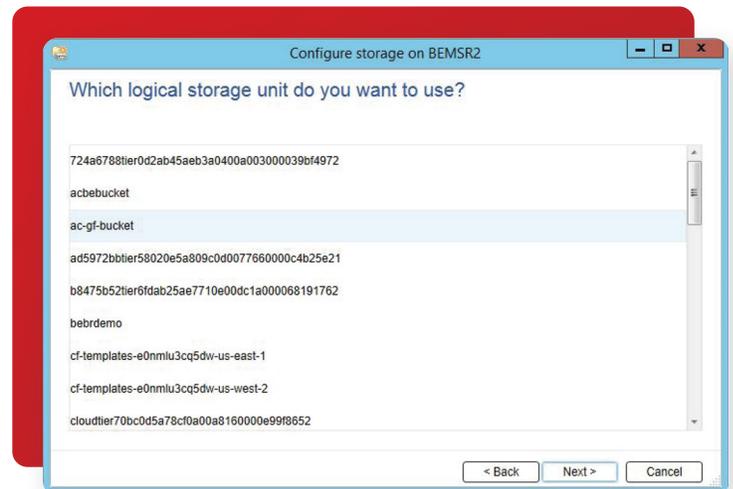


Figure 3. AWS logical storage unit selection.

Protect Data Within AWS

Organizations looking to shift from CapEx to OpEx spending are moving workloads to the cloud. Backup Exec extends backup and recovery capabilities to the cloud to support this evolution. Backup Exec delivers the flexibility to protect data in AWS without requiring new tools or processes or additional time and resources.

Backup Exec is available as a ready-to-install offering in the AWS Marketplace, AWS's online store for public cloud system tools and applications. You can install preconfigured Backup Exec software using the AWS Marketplace template with a one-click deployment to a server hosted in AWS.

Installing Backup Exec from the AWS Marketplace lets you benefit immediately from an inexpensive, easy-to-deploy and easy-to-operate solution to protect AWS workloads. Together with Backup Exec's proven success in on-premises business applications, you get a true single management interface for all data: whether virtual, physical or cloud.

Backup Exec in the AWS Marketplace comes with all features activated for a free, 60-day trial. Backup Exec is licensed "BYOL" or Bring Your Own License. You must purchase a valid license from an authorized Veritas [reseller](#).

In addition, Backup Exec extends current on-premises policies and procedures to the Backup Exec infrastructure and workloads hosted in AWS while simplifying management with on-demand configuration.

With Backup Exec, the use of Optimized Duplication (Opt-Dup) can also turn a cloud deployment into a disaster recovery strategy by providing replication to cloud storage and recovery-in-place when a recovery is needed (see Figure 4).

Enables Offsite Disaster Recovery with AWS

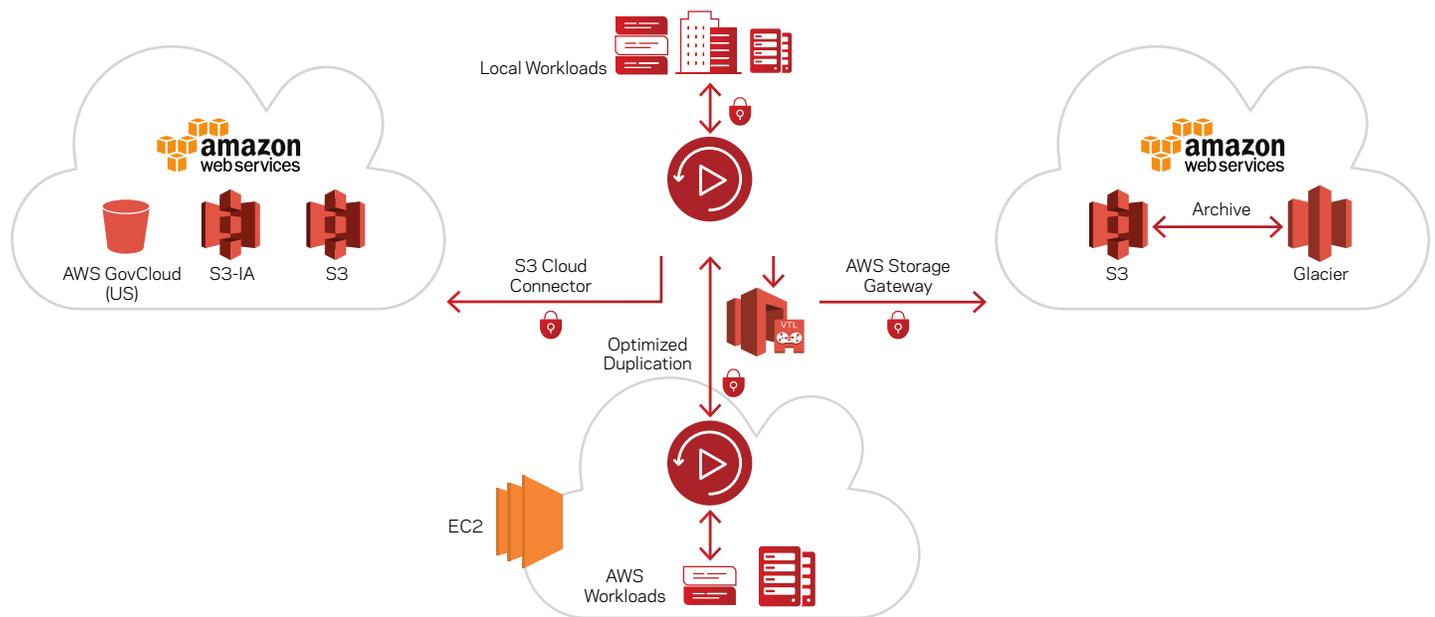


Figure 4. Install Backup Exec in AWS to protect cloud-hosted data and workloads.

Deployment of Backup Exec Server in AWS allows for the same level of protection as that available in the data center, all while improving security for data in flight and at rest.

Backup Exec will ensure cloud storage environments are protected and applications running in the cloud can be recovered in the case of a disaster or corruption. When the Backup Exec platform is extended to protect a cloud storage environment, you can feel confident moving your applications to the cloud because you can rely on your existing Backup Exec infrastructure to protect your AWS environment.

In this scenario, AWS cloud-based workloads are protected by hosting Backup Exec infrastructure in AWS alongside the workloads. This strategy provides full visibility and control of cloud-based data protection from the on-premises data center.

Benefits of this approach with Backup Exec include:

- Flexibility and freedom to deploy workloads based on business needs without compromising data protection
- A unified Backup Exec management interface and catalog regardless of workload location
- Automatic replication, backup and recovery of many locations with Backup Exec Optimized Duplication
- Easy and seamless replication to and recovery of data from remote branch offices and data centers in AWS
- Simplified and improved disaster recovery through the combined Backup Exec and AWS resources
- Greater visibility across the entire virtual landscape whether data is located in on-premises data centers or cloud-based servers

Data Lifecycle Management

Backup Exec uses data lifecycle management to automatically delete expired backup sets on AWS. You specify how long to keep backup data when you create a backup job that is sent to AWS. When the specified amount of time to keep the backup data expires, Backup Exec's data lifecycle management feature deletes the backup sets and reclaims the space unless there are dependent backup sets such as incrementals.

By default, Backup Exec keeps the most recent backup sets that are necessary to restore any backed-up component of a server, even if the backup sets expire. If backup sets are dependent on other backup sets, then Backup Exec does not delete the backup sets until all expiration dates on the backup sets have been reached. Even if the backup set is displayed as expired, the data is available until all dependent backup sets expire as well.

Security and Encryption

All data is secured using SSL during data transfer from Backup Exec to the cloud-based storage device. Backup Exec encrypts the data inline before it is sent to the cloud, and jobs must have encryption enabled to encrypt the data in cloud storage.

When you encrypt data, you protect it from unauthorized access. Anyone who tries to access the data has to have an encryption key that you create. Backup Exec supports two levels of encryption security: 128-bit Advanced Encryption Standard (AES) and 256-bit AES. The 256-bit AES encryption provides a stronger level of security because the key is longer than for 128-bit AES; however, 128-bit AES encryption enables backup jobs to process more quickly.

Download a Backup Exec 60-day Free Trial

Veritas provides 60-day, fully functional trialware so you can experience all the benefits of Backup Exec, including AMS cloud backups. To download a free 60-day copy of Backup Exec including all agents and options, please visit www.backupexec.com/trybe.

Sign up for an AWS Subscription

Before you can start backing up to AWS with Backup Exec, you need an AWS subscription. If you don't already have one, simply request a 30-day trial.

With proven real-world deployments and top notch technologies, customers will benefit from the Veritas engagement and support model and simplified, flexible purchasing options. With Veritas on AWS solutions, organizations looking to run existing on-premises services across AWS deployments will now have even greater opportunities to reduce costs and increase productivity while accelerating their journey to the cloud.

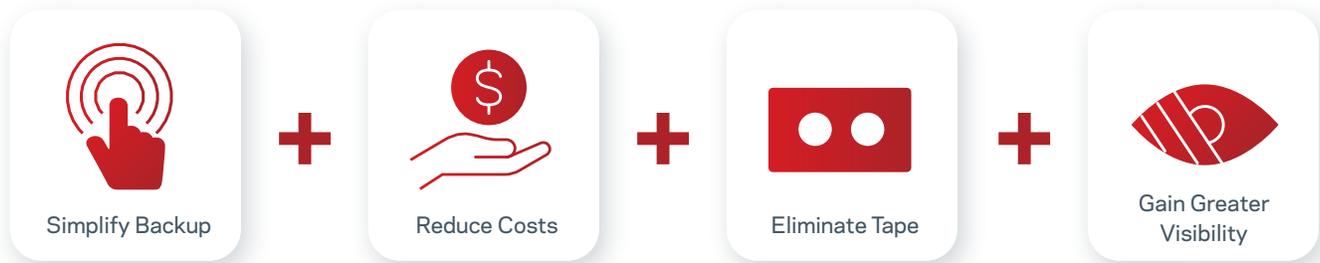
Launch a test drive, or to learn more visit www.veritas.com/protection/backup-exec/amazon-web-services.

How do you get Started?

1. Sign up for an [AWS account](#).
2. Find Backup Exec in the [AWS Marketplace](#).
3. Deploy the Backup Exec application image into an appropriate AWS machine instance.
4. Purchase an appropriate Backup Exec license from an [authorized reseller](#) and install it in the Backup Exec server.

Backup Exec with AWS Cloud Benefits

- Simplify data protection to secure, scalable cloud-based AWS services
- Reduce and convert CapEx to a more predictable and manageable pay-as-you-go OpEx cost structure
- Replace cumbersome and expensive tape backup and administration process with easy-to-use AWS storage



Summary

As many businesses increasingly leverage the cloud for applications and services, they want to protect and manage those environments with a backup and recovery solution they can trust. By taking the same proven solutions they have come to rely on and extending them to private clouds or storage providers integrated with Backup Exec, organizations can enjoy peace of mind knowing their information is protected by the Backup Exec platform.

Safeguarding your valuable data with Backup Exec delivers a host of key business benefits. Because Backup Exec can write data to the cloud, you gain the flexibility of adding cloud storage to reduce operational expenses or as part of a global disaster recovery strategy. Plus, you can use cloud storage backup to replace or augment tape-based off-site storage for disaster recovery readiness.

Regardless of whether your organization has already moved workloads to the cloud or you want to leverage the benefits of cloud storage for backup and recovery of on-premises data, Backup Exec delivers multiple cloud options in a single platform.

1. Veritas [2017 Truth in Cloud Report](#)

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact