AWS Backup

**Service Overview**

[AWS Backup](https://aws.amazon.com/backup) enables you to centralize and automate data protection across AWS services. AWS Backup offers a cost-effective, fully managed, policy-based service that further simplifies data protection at scale. AWS Backup also helps you support your regulatory compliance obligations and meets your business continuity goals. Together with AWS Organizations, AWS Backup enables you to centrally deploy data protection (backup) policies to configure, manage, and govern your backup activity across your organization’s AWS accounts and resources, including Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Block Store (Amazon EBS) volumes, Amazon Relational Database Service (RDS) databases (including Amazon Aurora clusters), Amazon DynamoDB tables, Amazon Elastic File System (EFS), Amazon FSx for Lustre, Amazon FSx for Windows File Server, and AWS Storage Gateway volumes.

**Supported features**

**Generally, AWS Backup offers the following features across all supported services.**

* Automated backup schedules and retention management
* [Centeralized backup monitoring](https://docs.aws.amazon.com/aws-backup/latest/devguide/monitoring.html)
* [KMS-integrated backup encryption](https://docs.aws.amazon.com/aws-backup/latest/devguide/encryption.html)
* [Cross-Region backup](https://docs.aws.amazon.com/aws-backup/latest/devguide/cross-region-backup.html)
* [Cross-account management](https://docs.aws.amazon.com/aws-backup/latest/devguide/manage-cross-account.html)
* [Cross-account backup](https://docs.aws.amazon.com/aws-backup/latest/devguide/create-cross-account-backup.html)

**AWS Backup ONLY offers the following feature with these select services.**

* Lifecycle to cold storage and item level restore with Amazon EFS
* [Continuous backup and point-in-time restore with Amazon RDS (excluding Aurora)](https://docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html)

**AWS Backup does NOT offer the following feature-service combinations.**

* DynamoDB does not support cross-Region OR cross-account backup
* Amazon RDS and Aurora do not support cross-Region AND cross-account backup in the same backup policy. You can choose one or the other. You can also use a custom AWS Lambda script to perform the second operation.

**Use cases / Considerations**

**Cloud-native backup**

AWS Backup provides a centralized console to automate and manage backups across AWS services. AWS Backup supports [Amazon EBS](https://aws.amazon.com/ebs/), [Amazon RDS](https://aws.amazon.com/rds/), [Amazon DynamoDB](https://aws.amazon.com/dynamodb/), [Amazon EFS](https://aws.amazon.com/efs/), [Amazon FSx](https://aws.amazon.com/fsx/), [Amazon EC2](https://aws.amazon.com/ec2/), and [AWS Storage Gateway](https://aws.amazon.com/storagegateway/), to enable you to backup key data stores, such as your storage volumes, databases, and file systems.

**Hybrid backup**

AWS Backup integrates with AWS Storage Gateway, a hybrid storage service that enables your on-premises applications to seamlessly use AWS Cloud storage. You can use AWS Backup to back up your application data stored in [AWS Storage Gateway](https://aws.amazon.com/storagegateway/) volumes. Backups of AWS Storage Gateway volumes are securely stored in the AWS Cloud and are compatible with [Amazon EBS](https://aws.amazon.com/ebs/), allowing you to restore your volumes to the AWS Cloud or to your on-premises environment. This integration also allows you to apply the same backup policies to both your AWS Cloud resources and your on-premises data stored on AWS Storage Gateway volumes.

**Governance**

AWS Backup works with other AWS tools to empower you to monitor its workloads. These tools include the following:

* Use **Amazon CloudWatch** and **Amazon EventBridge** to monitor AWS Backup processes.
  + You can use CloudWatch to track metrics, create alarms, and view dashboards.
  + You can use EventBridge to view and monitor AWS Backup events.

For more information, see [Monitoring AWS Backup events using EventBridge](https://docs.aws.amazon.com/aws-backup/latest/devguide/eventbridge.html) and [Monitoring AWS Backup metrics with CloudWatch](https://docs.aws.amazon.com/aws-backup/latest/devguide/cloudwatch.html).

* Use **AWS CloudTrail** to monitor AWS Backup API calls. You can identify the time, source IP, users, and accounts making those calls. For more information, see [Logging AWS Backup API calls with CloudTrail](https://docs.aws.amazon.com/aws-backup/latest/devguide/logging-using-cloudtrail.html).
* Use **Amazon Simple Notification Service** (Amazon SNS) to subscribe to AWS Backup-related topics such as backup, restore, and copy events. For more information, see [Using Amazon SNS to track AWS Backup events](https://docs.aws.amazon.com/aws-backup/latest/devguide/sns-notifications.html).

**Pricing considerations**

All info regarding AWS Backup pricing can be found in [AWS docs](https://aws.amazon.com/backup/pricing/)

**More details**

<https://aws.amazon.com/backup>

<https://aws.amazon.com/backup/features/>

<https://docs.aws.amazon.com/aws-backup/latest/devguide/whatisbackup.html>

[AWS re:Invent 2019: Deep dive on AWS Backup](https://www.youtube.com/watch?v=av8DpL0uFjc)

[Introducing AWS Backup: Automate and Centralize Data Protection in the AWS Cloud](https://www.youtube.com/watch?v=AI8hKeh7yCs)