What Is AWS Backup?

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services in the cloud and on premises. Using AWS Backup, you can configure backup policies and monitor backup activity for your AWS resources in one place. AWS Backup automates and consolidates backup tasks that were previously performed service-by-service, and removes the need to create custom scripts and manual processes. With just a few clicks on the AWS Backup console, you can create backup policies that automate backup schedules and retention management.

AWS Backup provides a fully managed backup service and a policy-based backup solution that simplifies your backup management and enables you to meet your business and regulatory backup compliance requirements.

Supported resources

The following are AWS resources that you can back up and restore using AWS Backup.

Supported Service	Supported Resource
Amazon FSx	Amazon FSx file systems
Amazon Elastic File System (Amazon EFS)	Amazon EFS file systems
Amazon DynamoDB	DynamoDB tables
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon EC2 instances (excluding store-backed instances)
Amazon Elastic Block Store (Amazon EBS)	Amazon EBS volumes
Amazon Relational Database Service (Amazon RDS)	Amazon RDS databases (including all database engines)
Amazon Aurora	Aurora clusters
AWS Storage Gateway (Volume Gateway)	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
- KMS-integrated backup encryption
- Cross-Region backup
- Cross-account management
- Cross-account backup

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)

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.

AWS Backup overview

AWS Backup provides the following features and capabilities.

Centralized backup management

AWS Backup provides a centralized backup console, a set of backup APIs, and the AWS Command Line Interface (AWS CLI) to manage backups across the AWS services that your applications use. With AWS Backup, you can centrally manage backup policies that meet your backup requirements. You can then apply them to your AWS resources across AWS services, enabling you to back up your application data in a consistent and compliant manner. The AWS Backup centralized backup console offers a consolidated view of your backups and backup activity logs, making it easier to audit your backups and ensure compliance.

Policy-based backup

With AWS Backup, you can create backup policies known as *backup plans*. Use these backup plans to define your backup requirements and then apply them to the AWS resources that you want to protect across the AWS services that you use. You can create separate backup plans that each meet specific business and regulatory compliance requirements. This helps ensure that each AWS resource is backed up according to your requirements. Backup plans make it easy to enforce your backup strategy across your organization and across your applications in a scalable manner.

Tag-based backup policies

You can use AWS Backup to apply backup plans to your AWS resources by tagging them. Tagging makes it easier to implement your backup strategy across all your applications and to ensure that all your AWS resources are backed up and protected. AWS tags are a great way to organize and classify your AWS resources. Integration with AWS tags enables you to quickly apply a backup plan to a group of AWS resources, so that they are backed up in a consistent and compliant manner.

Lifecycle management policies

AWS Backup enables you to meet compliance requirements while minimizing backup storage costs by storing backups in a low-cost cold storage tier. You can configure lifecycle policies that automatically transition backups from warm storage to cold storage according to a schedule that you define.

Currently only Amazon EFS file system backups can be transitioned to cold storage. The cold storage expression is ignored for the backups of Amazon EBS, Amazon RDS, Amazon Aurora, Amazon DynamoDB, and AWS Storage Gateway.

Cross-Region backup

Using AWS Backup, you can copy backups to multiple different AWS Regions on demand or automatically as part of a scheduled backup plan. Cross-Region backup is particularly valuable if you have business continuity or compliance requirements to store backups a minimum distance away from your production data. For more information, see Creating backup copies across AWS Regions.

Cross-account management and cross-account backup

You can use AWS Backup to manage your backups across all AWS accounts inside your AWS Organizations structure. With cross-account management, you can

automatically use backup policies to apply backup plans across the AWS accounts within your organization. This makes compliance and data protection efficient at scale and reduces operational overhead. It also helps eliminate manually duplicating backup plans across individual accounts. For more information, see Managing AWS Backup resources across multiple AWS accounts.

You can also copy backups to multiple different AWS accounts inside your AWS Organizations management structure. This way, you can "fan in" backups to a single repository account, then "fan out" backups for greater resilience. Creating backup copies across AWS accounts.

Before you can use the cross-account management and cross-account backup features, you must have an existing organization structure configured in AWS Organizations. An *organizational unit* (OU) is a group of accounts that can be managed as a single entity. AWS Organizations is a list of accounts that can be grouped into organizational units and managed as a single entity.

Backup activity monitoring

AWS Backup provides a dashboard that makes it simple to audit backup and restore activity across AWS services. With just a few clicks on the AWS Backup console, you can view the status of recent backup jobs. You can also restore jobs across AWS services to ensure that your AWS resources are properly protected.

AWS Backup integrates with Amazon CloudWatch and Amazon EventBridge. CloudWatch allows you to track metrics and create alarms. EventBridge allows you to view and monitor AWS Backup events. For more information, see Monitoring AWS Backup events using EventBridge and Monitoring AWS Backup metrics with CloudWatch.

AWS Backup integrates with AWS CloudTrail. CloudTrail gives you a consolidated view of backup activity logs that make it quick and easy to audit how your resources are backed up. AWS Backup also integrates with Amazon Simple Notification Service (Amazon SNS), providing you with backup activity notifications, such as when a backup succeeds or a restore has been initiated. For more information, see Logging AWS Backup API calls with CloudTrail and Using Amazon SNS to track AWS Backup events.

Backup access policies

AWS Backup offers resource-based access policies for your backup vaults to define who has access to your backups. You can define access policies for a backup vault that define who has access to the backups within that vault and what actions they can take. This provides a simple and secure way to control access to your backups across AWS services, helping you meet your compliance requirements. To review AWS and customer managed policies for AWS Backup, see https://docs.aws.amazon.com/aws-backup/latest/devguide/security-iam-awsmanpol.html.

AWS Backup: How it works

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backing up of data across AWS services. With AWS Backup, you can create backup policies called *backup plans*. You can use these plans to define your backup requirements, such as how frequently to back up your data and how long to retain those backups.

AWS Backup lets you apply backup plans to your AWS resources by simply tagging them. AWS Backup then automatically backs up your AWS resources according to the backup plan that you defined.

The following sections describe how AWS Backup works, its implementation details, and security considerations.

Topics

How AWS Backup works with other AWS services

PDF

Many AWS services offer backup features that help you protect your data. These features include Amazon Elastic Block Store (Amazon EBS) snapshots, Amazon Relational Database Service (Amazon RDS) snapshots, Amazon DynamoDB

backups, AWS Storage Gateway snapshots, and others. AWS Backup implements its backup features using the existing capabilities of these AWS services.

Topics

Configuring services to work with AWS Backup

When new AWS services become available, you must enable AWS Backup to use those services. If you try to create an on-demand backup or backup plan using resources from a service that is not enabled, you receive an error message and cannot complete the process.

Note

Service opt-in settings are *Region-specific*. If you change the AWS Region that you're using, you must reconfigure the services that you use with AWS Backup.

To configure the services used with AWS Backup

1. Open the AWS Backup console at https://console.aws.amazon.com/backup.
2. In the navigation pane, choose **Settings**.
3. On the **Service opt-in** page, choose **Configure resources**. Use the toggle switches to enable or disable the services used with AWS Backup.
4. Choose **Confirm** when your services are configured.

AWS Backup uses existing backup capabilities of AWS services to implement its centralized features. For example, when you create a backup plan, AWS Backup uses the EBS snapshot capabilities when creating backups on your behalf according to your backup plan.

All per-service backup capabilities continue to be available. For example, you can make snapshots of your EBS volumes using the Amazon Elastic Compute Cloud (Amazon EC2) API. AWS Backup provides a common way to manage backups across AWS services both in the AWS Cloud and on premises. AWS Backup provides a centralized backup console that offers backup scheduling, retention management, and backup monitoring.

Note

Backups created with AWS Backup cannot be deleted using APIs that belong to the backed-up resource. For information about deleting recovery points using the AWS Backup API, see DeleteRecoveryPoint.

Working with Amazon FSx file systems

AWS Backup supports backing up and restoring Amazon FSx file systems. Amazon FSx provides fully managed third-party file systems with the native compatibility and feature sets for workloads, such as Microsoft Windows–based storage, high performance computing, machine learning, and electronic design automation.

Amazon FSx supports two file system types: Lustre and Windows File Server. You can back up any Amazon FSx for Windows File Server file system and any Amazon FSx for Lustre file system that has persistent storage and is not linked to a data repository such as Amazon S3. AWS Backup uses the built-in backup functionality of Amazon FSx. So backups taken from the AWS Backup console have the same level of file system consistency and performance, and the same restore options as backups that are taken through the Amazon FSx console.

If you use AWS Backup to manage these backups, you gain additional functionality, such as unlimited retention options, and the ability to create scheduled backups as frequently as every hour. In addition, AWS Backup retains your backups even after the source file system is deleted. This protects against accidental or malicious deletion.

Use AWS Backup to protect Amazon FSx file systems if you want to configure backup policies and monitor backup tasks from a central backup console that also extends support for other AWS services.

- How to back up resources: Getting started with AWS Backup
- How to restore Amazon FSx resources: Restoring an Amazon FSx file system

For detailed information about Amazon FSx file systems, see the Amazon FSx documentation.

Working with Amazon EC2

Using AWS Backup, you can schedule or perform on-demand backup jobs that include entire EC2 instances and Windows applications running on Amazon EC2, along with associated configuration data. This limits the need for you to interact with the storage (Amazon EBS) volume. Similarly, you can restore an entire Amazon EC2 instance from a single recovery point. A backup job can only have one resource. So you can have a job to back up an EC2 instance, and it will back up the root volume, all data volumes, and the associated instance configurations.

AWS Backup does not reboot EC2 instances at any time.

Backing Up Amazon EC2 Resources

When backing up an Amazon EC2 instance, AWS Backup takes a snapshot of the root Amazon EBS storage volume, the launch configurations, and all associated EBS volumes. AWS Backup stores certain configuration parameters of the EC2 instance, including instance type, security groups, Amazon VPC, monitoring configuration, and tags. The backup data is stored as an Amazon EBS volume-backed Amazon Machine Image (AMI).

You can also back up and restore your VSS-enabled Microsoft Windows applications. You can schedule application-consistent backups, define lifecycle policies, and perform consistent restores as part of an on-demand backup or a scheduled backup plan. For more information, see Creating Windows VSS backups.

AWS Backup does not back up the following:

- Configuration of the Elastic Inference accelerator, if it is attached to the instance.
- User data used when the instance was launched.

Note

For all instance types, only Amazon EBS backed EC2 instances are supported. Ephemeral storage instances (that is, instance store-backed instances) are not supported.

AWS Backup can encrypt EBS snapshots associated with an Amazon EC2 backup. This is similar to how it encrypts EBS snapshots. AWS Backup uses the same encryption applied on the underlying EBS volumes when creating a snapshot of the Amazon EC2 AMI, and the configuration parameters of the original instance are persisted in the restore metadata.

A snapshot derives its encryption from the volume as you have defined, and the same encryption is applied to the corresponding snapshots. EBS snapshots of a copied AMI will always be encrypted. If you use a KMS key during the copy, the key will be applied. If you don't use a KMS key, a default KMS key is applied.

- How to back up resources: Getting started with AWS Backup
- How to restore Amazon EC2 resources: Restoring an Amazon EC2 instance

For detailed information about Amazon EC2, see What is Amazon EC2? in the *Amazon EC2 User Guide for Windows Instances*.

Working with Amazon EFS

AWS Backup currently supports Amazon Elastic File System (Amazon EFS).

- How to back up resources: Getting started with AWS Backup
- How to restore Amazon EFS resources: Restoring an Amazon EFS file system

For detailed information about Amazon EFS file systems, see What is Amazon Elastic File System? in the *Amazon Elastic File System User Guide*.

Working with Amazon DynamoDB

AWS Backup currently supports Amazon DynamoDB (DynamoDB).

- How to back up resources: Getting started with AWS Backup
- How to restore DynamoDB resources: Restoring an Amazon DynamoDB database

For detailed information about DynamoDB, see What is Amazon DynamoDB? in the *Amazon DynamoDB Developer Guide*.

Working with Amazon EBS

AWS Backup currently supports Amazon Elastic Block Store (Amazon EBS) volumes.

- How to back up resources: Getting started with AWS Backup
- How to restore Amazon EBS volumes: Restoring an Amazon EBS volume

For detailed information about Amazon EBS volumes, see What is Amazon Elastic Block Store (Amazon EBS)? in the *Amazon EC2 User Guide for Linux Instances*.

For more information, see Creating an Amazon EBS Volume in the *Amazon EC2 User Guide for Linux Instances*.

Working with Amazon RDS and Amazon Aurora

AWS Backup currently supports Amazon RDS database engines and Aurora clusters.

- How to back up resources: Getting started with AWS Backup
- How to restore Amazon RDS resources: Restoring an Amazon RDS database
- How to restore Amazon Aurora clusters: Restoring an Amazon Aurora cluster

For more information about Amazon RDS, see What is Amazon Relational Database Service? in the *Amazon RDS User Guide*.

For detailed information about Aurora, see What is Amazon Aurora? in the *Amazon Aurora User Guide*.

Note

If you initiate a backup job from the Amazon RDS console, this can conflict with an Aurora clusters backup job, causing the error `Backup job expired before completion`. If this occurs, configure a longer backup window in AWS Backup.

Working with AWS Storage Gateway

Amazon EBS snapshots can be restored as AWS Storage Gateway volumes.

- How to back up resources: Getting started with AWS Backup

For detailed information about AWS Storage Gateway, see What is AWS Storage Gateway? in the *AWS Storage Gateway User Guide*.

How AWS services back up their own resources

For information about how to use specific AWS services to back up their resources, see the following:

- Amazon EC2 Related Services
- Using AWS Backup with Amazon EFS
- On-Demand Backup and Restore for DynamoDB
- Amazon EBS Snapshots
- Backing Up and Restoring Amazon RDS DB Instances
    - Overview of Backing Up and Restoring an Aurora DB Cluster
- Using AWS Backup with Amazon FSx for Windows File Server
- Using AWS Backup with Amazon FSx for Lustre
- Backing Up Your Volumes in AWS Storage Gateway

Managing backups using backup plans

PDF

In AWS Backup, a *backup plan* is a policy expression that defines when and how you want to back up your AWS resources, such as Amazon DynamoDB tables or Amazon Elastic File System (Amazon EFS) file systems. You can assign resources to backup plans, and AWS Backup automatically backs up and retains backups for those resources according to the backup plan. You can create multiple backup plans if you have workloads with different backup requirements.

The following sections provide the basics of managing your backup strategy in AWS Backup.

Topics

- Creating a backup plan
- Assigning resources to a backup plan
- Deleting a backup plan
- Updating a backup plan