
📚 AWS Backup

🔹 What is AWS Backup?

AWS Backup is a **fully managed backup service** that simplifies and centralizes the process of backing up data across AWS services. It enables compliance with backup policies, improves data protection, and supports both AWS services and on-premises environments.

🔹 Key Features

Feature	Description
Centralized Backup	**Manage backups for multiple AWS services from a single place.**
Automated Backup Scheduling	**Define backup plans with specific schedules and retention policies.**
Cross-Region Backup	**Copy backups across AWS regions for disaster recovery.**
Cross-Account Backup	**Share and manage backups across AWS accounts (multi-account support).**
Lifecycle Management	**Automatically transition backups to cold storage or delete them.**
Backup Vaults	**Logical containers to organize and control access to backups.**
Backup Policies	**Use AWS Organizations to apply backup policies to multiple accounts.**
On-Premises Support	**Backup data from on-premises servers using AWS Storage Gateway.**
Compliance & Monitoring	**Audit trails using AWS CloudTrail and detailed reports for compliance.**

🔹 Supported AWS Services

As of the latest updates, AWS Backup supports:

- Amazon EC2 (via EBS snapshots)
- Amazon RDS (databases)
- Amazon DynamoDB
- Amazon EFS
- Amazon FSx (for Windows, Lustre, etc.)
- Amazon S3 (limited support, evolving)
- AWS Storage Gateway (on-premises data)
- Amazon DocumentDB
- Amazon Neptune
- AWS CloudFormation stacks (partially, for state recovery)

🔹 **Components of AWS Backup**

1. Backup Vault

- A **container** where backups (recovery points) are stored.
- Access is controlled via IAM policies and encryption keys.

2. Backup Plan

- A **policy** defining how and when to back up AWS resources.
    - Includes **rules** for scheduling, lifecycle, and retention.

    - Can assign resources to the plan using tags or ARNs.

3. Backup Rule

- Each backup rule within a plan defines:
    - Frequency (e.g., daily, weekly)
    - Start time
    - Retention period
    - Lifecycle transitions (e.g., move to cold storage after X days)

4. Recovery Point

- A **saved backup** of a resource at a specific time.
- Used for **restoring** the resource later.

5. Resource Assignment

- AWS resources can be assigned to backup plans using:
    - Tags (recommended for dynamic assignment)
    - Direct ARNs

🔹 **Backup Workflow**

Resource (EC2, RDS, etc.)
↓
Assigned to Backup Plan
↓

Backup Rule Schedules Backup
↓
Backup Stored in Backup Vault
↓
Recovery Point Created
↓
Lifecycle Actions (transition/delete)

🔹 **Security & Compliance**

- **Encryption**:
    - Supports encryption using AWS KMS (customer-managed or AWS-managed keys).
- **IAM Policies**:
    - Granular control over who can manage, view, restore, or delete backups.
- **Audit Logs**:
    - Integrated with AWS CloudTrail for full visibility.
- **Compliance Reporting**:
    - Use AWS Backup Audit Manager for policy compliance.

🔹 **Cold Storage**

- Reduced-cost storage tier.
- Automatically or manually transition backups after a defined number of days.

- Ideal for long-term archival (e.g., regulatory compliance).

🔹 **Pricing Overview**

- Based on:
    - Amount of backup storage (warm + cold).
    - Number and size of backups created.
    - Cross-region and cross-account copy charges.
    - Restore operations (data transferred and time consumed).

🔹 **Use Cases**

- **Disaster Recovery**: Cross-region backups for geographic redundancy.
- **Data Retention Compliance**: Meet industry requirements (e.g., HIPAA, SOC2).
- **Centralized Backup Management**: Simplify large enterprise backup across accounts.
- **On-Premises Protection**: Protect hybrid workloads with Storage Gateway.

🔹 **Pros and Cons**

✅ **Pros**

- Centralized and automated management

- Easy integration with other AWS services
- Strong security and compliance features
- Cross-region/cross-account support
- Cold storage for cost efficiency

⚠️ **Cons**

- Limited S3 support
- Can get expensive if not optimized
- Manual steps needed for some advanced use cases (e.g., cross-region restores)

🔹 **Tips for Using AWS Backup**

- Use **tag-based policies** for scalable and dynamic backup management.
- Implement **lifecycle policies** to manage storage costs.
- Monitor with **AWS Backup Audit Manager** for compliance tracking.
- Consider **AWS Organizations** for managing backup across multiple accounts.
- Schedule regular **restore testing** to validate your disaster recovery plan.
