

Service Name

AWS Backup

Service Overview

AWS Backup is a fully managed service that centralizes and automates data protection across AWS services, in the cloud, and on-premises. It allows users to configure backup policies and monitor backup activity for AWS resources in one place, removing the need for custom scripts and manual processes. The service consolidates backup tasks that were previously performed service-by-service, enabling consistent and compliant backup strategies across organizations. AWS Backup supports policy-based backup management, automated scheduling, and cross-Region/cross-account backup capabilities for comprehensive data protection.

Key Use Cases

- **Centralized backup management:** Consolidate backup policies and monitoring across multiple AWS services from a single console
- **Regulatory compliance:** Meet business and regulatory requirements with automated backup policies, audit reporting, and WORM capabilities
- **Disaster recovery:** Implement cross-Region backup replication and automated recovery testing to ensure business continuity
- **Ransomware protection:** Use logically air-gapped vaults, vault lock, and malware scanning to protect against cyber threats
- **Multi-account governance:** Apply organization-wide backup policies across AWS Organizations with centralized monitoring and reporting

Features

- **Centralized Backup Management:** Single console to manage backup policies and monitor activity across all AWS services
- **Policy-Based Backup:** Create backup plans with automated scheduling, retention, and lifecycle management
- **Tag-Based Backup Policies:** Apply backup plans to resources using AWS tags for scalable backup strategy implementation
- **Cross-Region and Cross-Account Backup:** Automatically replicate backups across AWS Regions and accounts for enhanced security
- **AWS Backup Audit Manager:** Monitor compliance posture and generate reports for governance and regulatory requirements
- **Backup Vault Lock (WORM):** Write-once-read-many configuration prevents deletion or modification of backups

- **Incremental Backups:** Efficient storage with full initial backups followed by incremental changes only
- **Backup Search and Item-Level Restore:** Search and restore specific files or objects from EBS snapshots and S3 backups
- **Malware Protection:** Integration with Amazon GuardDuty for automated malware scanning of recovery points
- **Restore Testing:** Automated validation of backup recoverability to meet RTO/RPO targets

Value Proposition

AWS Backup provides the only fully managed, centralized backup solution across AWS services, eliminating the complexity of managing multiple backup tools and custom scripts. It offers enterprise-grade features like WORM compliance, cross-Region replication, and automated restore testing that would be costly and complex to build independently:

- The service integrates seamlessly with AWS Organizations for multi-account governance and provides comprehensive audit capabilities for regulatory compliance
- With pay-as-you-go pricing, no upfront costs, and automatic lifecycle management to reduce storage costs, AWS Backup delivers significant operational efficiency while ensuring data protection meets business and compliance requirements

Service Integration

AWS Backup integrates with over 20 AWS services including Amazon EC2, Amazon S3, Amazon EBS, Amazon RDS, Amazon Aurora, Amazon DynamoDB, Amazon EFS, Amazon FSx, Amazon DocumentDB, Amazon Neptune, Amazon Redshift, Amazon Timestream, and VMware workloads. It also integrates with AWS Organizations for multi-account management, AWS IAM for access control, AWS KMS for encryption, Amazon CloudWatch for monitoring, AWS CloudTrail for audit logging, and Amazon GuardDuty for malware protection. The service works with AWS Cost Explorer for cost management and AWS Config for compliance tracking.

Onboarding and Offboarding

Getting started with AWS Backup requires an AWS account and at least one supported AWS resource. Users must first opt-in AWS services through the AWS Management Console to enable AWS Backup management:

- The process involves creating backup plans that define schedules and retention policies, then assigning resources using tags or explicit resource selection
- AWS Backup provides default backup plans and policies to accelerate implementation

- Prerequisites include configuring appropriate IAM roles and policies, enabling service opt-in for specific resource types like Aurora and DocumentDB, and setting up backup vaults for organizing and securing backup data

Getting Started Guide: <https://docs.aws.amazon.com/aws-backup/latest/devguide/getting-started.html>

Data Removal

AWS Backup provides multiple options for data removal including automated lifecycle policies to delete expired backups and manual deletion of recovery points through the console or API. Users can permanently delete backup data or stop future backups while retaining existing data. For secure offboarding, Backup Vault Lock in Compliance mode prevents deletion during retention periods. Organizations can remove AWS Backup configurations while preserving data in underlying AWS services, ensuring complete data lifecycle management.

Backup/Restore and Disaster Recovery

AWS Backup provides comprehensive backup and disaster recovery capabilities including automated backup scheduling, cross-Region replication, point-in-time recovery for supported services, and restore testing validation. The service supports both continuous backups with sub-second RPO and periodic backups based on defined schedules. Recovery options include full resource restoration, item-level recovery, and cross-account recovery scenarios for comprehensive disaster recovery strategies.

Backup Capabilities

AWS Backup itself is a backup service that provides centralized backup management for other AWS resources. It works seamlessly with AWS Backup (itself) by providing the core backup infrastructure, policies, and management capabilities. The service offers incremental backups, encrypted storage, cross-Region replication, and automated lifecycle management to optimize backup storage costs and ensure data protection across all supported AWS services.

Disaster Recovery

AWS Backup supports disaster recovery through cross-Region backup replication, automated restore testing, and integration with AWS Elastic Disaster Recovery for complementary capabilities. While AWS Backup focuses on backup-based recovery (hours RTO/RPO), it complements AWS Elastic Disaster Recovery which provides continuous replication with sub-minute RTO/RPO. Together, these services provide comprehensive disaster recovery options for different recovery time objectives.

Recovery Objectives

AWS Backup helps customers meet RPO objectives through configurable backup frequencies from continuous (sub-second RPO) to periodic schedules. RTO objectives are supported through restore testing that validates recovery times, cross-Region backup copies for faster regional recovery, and item-level restore capabilities that reduce recovery scope. Automated restore testing ensures backup recoverability and validates that recovery processes meet defined RTO targets.

Service Constraints

Service Quotas: <https://docs.aws.amazon.com/aws-backup/latest/devguide/aws-backup-limits.html>

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

Technical Requirements

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

User Guide: <https://docs.aws.amazon.com/aws-backup/latest/devguide/getting-started.html>

API Reference: <https://docs.aws.amazon.com/aws-backup/latest/devguide/api-reference.html>

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: <https://aws.amazon.com/backup/pricing/>

Cost Optimization

AWS Backup offers several unique cost optimization features including automated lifecycle management that transitions backups to lower-cost cold storage, backup tiering for Amazon S3 that reduces costs by up to 30% for long-term storage, and incremental backup technology that only stores changed data. The service provides backup deduplication, automated deletion of expired backups, and cost allocation tags for detailed cost tracking. Organizations can optimize costs through policy-based retention management and cross-Region backup strategies that balance cost with recovery requirements.

Savings Considerations

Primary cost savings from AWS Backup include elimination of custom backup solution development and maintenance costs, reduced storage expenses through incremental backups and lifecycle policies, and operational efficiency gains from centralized management. The service offers significant savings through automated backup scheduling that reduces manual labor, consolidated backup infrastructure that eliminates per-service backup tools, and pay-as-you-go pricing with no upfront costs. Additional savings come from backup tiering options, cross-Region cost optimization, and automated compliance reporting that reduces audit preparation time and costs.