AWS Backup

Centralized backup management

AWS Backup provides a centralized backup console, a set of backup APIs, and a command line interface to manage backups across the AWS services on which your applications run. With AWS Backup, you can centrally manage backup policies that help meet your backup requirements and apply them to your AWS resources across AWS services. AWS Backup's centralized backup console offers a consolidated view of your backups and backup activity logs, making it easier to audit your backups and to enable compliance.

Policy-based backup solution

With AWS Backup, you can create backup policies called backup plans that enable you to define your backup requirements and then apply them to the AWS resources you want backed up. You can create separate backup plans that are designed to meet specific business and regulatory compliance requirements. Backup plans make it easy to help you implement your backup strategy across your organization and across your applications.

Tag-based backup policies

AWS Backup allows you to apply backup plans to your AWS resources by simply tagging them, making it easier to implement your backup strategy across your applications. 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.

Backup scheduling

AWS Backup allows you to create backup schedules that you can customize to help you meet your business and regulatory backup requirements. You can also choose from predefined backup schedules based on common best practices. AWS Backup is designed to backup your AWS resources according to the policies and schedules you define. A backup schedule includes the backup start time, backup frequency, and backup window.

Retention management

With AWS Backup, you can set backup retention policies that are designed to retain and expire backups according to the business or regulatory backup compliance requirements you set. Backup retention management is designed to minimize backup storage costs by retaining backups for only as long as they are needed.

Backup activity monitoring

AWS Backup provides a dashboard that helps you to monitor backup and restore activity across AWS services. With just a few clicks in the AWS Backup console, you can view the status of recent backup jobs and restore jobs across AWS. AWS Backup integrates with AWS CloudTrail, which provides you with a consolidated view of backup activity logs that helps you to audit what and how your resources are backed up. AWS Backup also integrates with Amazon Simple Notification Service (SNS), which can alert you on backup activity, such as when a backup succeeds or a restore has been initiated.

AWS Backup Audit Manager

AWS Backup Audit Manager is designed to help you to audit and report on the compliance of your data protection policies to help you meet your business and regulatory needs. AWS Backup Audit Manager provides built-in compliance controls and allows you to customize these controls to define your data protection policies (e.g., backup frequency or retention period). It is designed to detect violations of your defined data protection policies and can prompt you to take corrective actions. With AWS Backup Audit Manager, you can evaluate backup activity and generate audit reports that can help you demonstrate compliance with regulatory requirements.

Lifecycle management policies

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

Incremental backups

AWS Backup is designed to store your periodic backups incrementally. The first backup of an AWS resource is designed to back up a full copy of your data. For each successive incremental backup, only the changes to your AWS resources are designed to be backed up. Incremental backups enable you to benefit from the data protection of frequent backups while minimizing storage costs.

Backup data encryption

AWS Backup is designed to encrypt your backup data at rest and in transit, helping you secure your backup data and meet compliance requirements. AWS Backup is designed to encrypt your backup data using encryption keys managed by the AWS Key Management Service (KMS), eliminating the need to build and maintain a key management infrastructure. AWS Backup is designed so the keys used to encrypt your AWS Backup data are independent of the keys used to encrypt the resources that the backups are based on. Having separate encryption keys for your production and backup data provides an important layer of protection for your applications.

Backup access policies

With AWS Backup, you can set resource-based access policies on backup vaults. A backup vault is a container used for organizing your backups. Resource-based access policies enable you to control access to backups in a backup vault across all users, rather than having to define permissions for each user. This provides a secure way to help you control access to your backups across AWS services and meet your backup compliance requirements.

Amazon Elastic Cloud Compute instance backups

AWS Backup is designed to provide backup and recovery for EC2 at the instance level without the need for custom scripts or third-party solutions. Customers are now able to schedule backup jobs that include whole EC2 instances, limiting the need to interact with the storage (Amazon Elastic Block Store (Amazon EBS)) layer. Additionally, AWS Backup is designed so customers will be able to restore entire EC2 instances from a single recovery point, simplifying the recovery process.

Item-level recovery for Amazon Elastic File System

AWS Backup offers a fast and easy way for customers to restore an individual file or directory from the backup of an Amazon EFS file system. With AWS Backup, customers can restore an individual file from a centralized console without having to restore an entire file system, reducing the recovery time.

Cross-Region backup

AWS Backup is designed so customers can copy backups across multiple AWS services to different regions, from a central console, making it easier to meet compliance and disaster recovery needs. With AWS Backup, customers can copy backups either manually, as on-demand copy, or as part of a scheduled backup plan to multiple different Regions. Customers can also recover from those backups in the new Region, reducing the risk of downtime and helping meet disaster recovery and business continuity requirements.

Cross-account backup

AWS Backup supports cross-account backup, enabling AWS customers to copy their backups across their AWS accounts within their AWS organizations. AWS Backup is designed so customers can copy backups either manually, as on-demand copy, or as part of a scheduled backup plan to only the trusted destination accounts in the organization. In the event anything happens to a backup and its source account, customers can restore from the destination account or, alternatively, to the third account. Cross-account backup feature provides customers an additional layer of protection should the source account experience disruption from accidental or malicious deletion, disasters, or ransomware.

Additional Information

For additional information about service controls, security features and functionalities, including, as applicable, information about storing, retrieving, modifying, restricting, and deleting data, please see https://docs.aws.amazon.com/index.html. This additional information does not form part of the Documentation for purposes of the AWS Customer Agreement available at http://aws.amazon.com/agreement, or other agreement between you and AWS governing your use of AWS's services.