

AWS Backup and Recovery Procedures for Cloud-Hosted Data

Standard Operating Procedure (SOP)

**Table of Contents**

[1. Purpose 3](#_Toc188428626)

[2. Scope 3](#_Toc188428627)

[3. Roles and Responsibilities 3](#_Toc188428628)

[4. Backup Strategy 3](#_Toc188428629)

[4.2 Backup Types and Frequency 4](#_Toc188428630)

[4.3 Backup Destinations 4](#_Toc188428631)

[5. Backup Procedures 4](#_Toc188428632)

[5.1 Configure AWS Backup Service 4](#_Toc188428633)

[5.2 Implement Backup Encryption 5](#_Toc188428634)

[5.3 Automate and Monitor Backups 5](#_Toc188428635)

[5.4 Backup Validation 5](#_Toc188428636)

[6. Recovery Procedures 5](#_Toc188428637)

[6.1 Recovery Planning 5](#_Toc188428638)

[6.2 Data Recovery Steps 5](#_Toc188428639)

[6.3 Disaster Recovery in Cross-Region Scenarios 6](#_Toc188428640)

[7. Security and Compliance 6](#_Toc188428641)

[7.1 Access Control 6](#_Toc188428642)

[7.2 Auditing and Logging 6](#_Toc188428643)

[7.3 Compliance Adherence 7](#_Toc188428644)

[8. Testing and Maintenance 7](#_Toc188428645)

[8.1 Regular Testing 7](#_Toc188428646)

[8.2 Review and Update SOP 7](#_Toc188428647)

[9. Documentation and Reporting 7](#_Toc188428648)

[10. Emergency Contacts 7](#_Toc188428649)

[11. References 8](#_Toc188428650)

[Additional Considerations 8](#_Toc188428651)

# 1. Purpose

To establish a standardized process for backing up and recovering data hosted on Amazon Web Services (AWS), ensuring data integrity, availability, and compliance with business continuity requirements.

# 2. Scope

* This SOP applies to all cloud-hosted data within the organization's AWS environment, including:
* **Compute Resources**: Amazon Elastic Compute Cloud (EC2) instances, Elastic Container Service (ECS), and Lambda functions.
* **Storage Services**: Amazon Simple Storage Service (S3), Elastic Block Store (EBS) volumes, and Amazon Elastic File System (EFS).
* **Databases**: Amazon Relational Database Service (RDS), DynamoDB, and Amazon Redshift.
* **Network Configurations**: Virtual Private Clouds (VPCs), security groups, and load balancers.
* **IAM Configurations**: Identity and Access Management policies and roles.

# 3. Roles and Responsibilities

* IT Operations Manager
  + Oversees the backup and recovery strategy.
  + Ensures compliance with organizational policies and regulations.
* Backup Administrator
  + Configures and maintains backup plans and policies.
  + Monitors backup jobs and resolves failures.
* Disaster Recovery (DR) Coordinator
  + Develops and updates the disaster recovery plan.
  + Coordinates recovery efforts during an incident.
* System Administrators
  + Identify critical systems and data requiring backups.
  + Test recovery procedures for their respective systems.
* Security Officer
  + Ensures backups comply with security standards.
  + Manages encryption keys and access controls.

# 

# 4. Backup Strategy

## 4.1 Data Classification

Classify data based on its criticality:

* **Tier 1 (Critical Data)**: Essential for business operations (e.g., production databases).
* **Tier 2 (Important Data)**: Important but not immediately critical (e.g., internal documents).
* **Tier 3 (Non-Critical Data)**: Least critical (e.g., test environments).

## 4.2 Backup Types and Frequency

|  |  |  |  |
| --- | --- | --- | --- |
| **Data Tier** | **Backup Type** | **Frequency** | **Retention Period** |
| Tier 1 | Incremental / Differential | Every 6 hours | 90 Days |
| Tier 1 | Full Backup | Daily (Off-peak hours) | 180 Days |
| Tier 2 | Incremental | Daily | 60 Days |
| Tier 2 | Full Backup | Weekly | 120 Days |
| Tier 3 | Full Backup | Monthly | 90 Days |

## 4.3 Backup Destinations

* **Primary Backup Storage**: Amazon S3 with versioning and encryption enabled.
* **Archival Storage**: Amazon S3 Glacier for long-term retention.
* **Cross-Region Replication**: Backups replicated to a different AWS region for disaster recovery.

# 5. Backup Procedures

## 5.1 Configure AWS Backup Service

1. **Access AWS Backup Console**:
   * Navigate to the AWS Backup service in the AWS Management Console.
2. **Create Backup Plans**:
   * Define backup plans for each data tier, specifying the backup schedule, frequency, and retention policies.
   * Use AWS Backup's JSON editor or the visual interface.
3. **Assign Resources**:
   * Tag AWS resources with consistent key-value pairs (e.g., Backup:Tier1).
   * Assign resources to backup plans using tags.
4. **Set Lifecycle Policies**:
   * Define policies to transition backups to cold storage (e.g., move to Glacier after 30 days).

## 5.2 Implement Backup Encryption

* Enable server-side encryption for all backups using AWS Key Management Service (KMS).
* Rotate encryption keys annually or as per compliance requirements.

## 5.3 Automate and Monitor Backups

* **Automation**:
  + Utilize AWS Lambda functions and CloudWatch Events to automate backup triggering if necessary.
* **Monitoring**:
  + Use Amazon CloudWatch to set up alerts for backup job successes, failures, and missed schedules.
  + Configure Amazon Simple Notification Service (SNS) for alert notifications via email or SMS.

## 5.4 Backup Validation

* Perform checksum validation to ensure data integrity.
* Run quarterly sample restores to verify backup reliability.

# 6. Recovery Procedures

## 6.1 Recovery Planning

* **Recovery Time Objective (RTO)**: Maximum acceptable downtime (e.g., Tier 1: 2 hours).
* **Recovery Point Objective (RPO)**: Maximum acceptable data loss in time (e.g., Tier 1: 6 hours).

## 6.2 Data Recovery Steps

1. **Identify the Data Loss Incident**:
   * Determine the scope and impact.
   * Prioritize recovery based on data tiers.
2. **Initiate Recovery from AWS Backup**
   * **Using AWS Backup Console**:
     + Navigate to the "Protected Resources" section.
     + Select the resource and choose the appropriate recovery point.
     + Click "Restore" and configure restore options.
   * **Using AWS CLI**:
     + Run aws backup start-restore-job with necessary parameters.
3. **Configure Restored Resources**
   * Update configurations such as VPC settings, security groups, and IAM roles.
   * Verify that restored resources are segregated from production until tested.
4. **Validate Restored Data**
   * Check data integrity and consistency.
   * Perform application-level tests to ensure functionality.
5. **Switch Over to Restored Resources**
   * After validation, redirect traffic or users to the restored systems.
   * Monitor systems closely for any anomalies.

## 6.3 Disaster Recovery in Cross-Region Scenarios

* **Activate DR Plan**:
  + If the primary region is unavailable, initiate the DR plan in the secondary region.
* **Recover Infrastructure**:
  + Deploy infrastructure using IaC templates (e.g., CloudFormation stacks).
* **Data Restoration**:
  + Restore data from cross-region backups stored in S3 or Glacier.

# 7. Security and Compliance

## 7.1 Access Control

* Implement least privilege access using IAM roles and policies.
* Restrict backup and recovery permissions to authorized personnel only.

## 7.2 Auditing and Logging

* Enable AWS CloudTrail for logging all backup and recovery activities.
* Store logs in an S3 bucket with restricted access and versioning.

## 7.3 Compliance Adherence

* Ensure backup and recovery processes comply with regulations like GDPR, HIPAA, or PCI DSS.
* Perform regular compliance audits and update procedures accordingly.

# 8. Testing and Maintenance

## 8.1 Regular Testing

* **Backup Tests**:
  + Monthly test restores for Tier 1 data.
  + Quarterly test restores for Tier 2 data.
* **Disaster Recovery Drills**:
  + Semi-annual DR simulations to assess readiness.

## 8.2 Review and Update SOP

* **Annual Review**:
  + Update the SOP to reflect changes in the environment or compliance requirements.
* **Feedback Incorporation**:
  + Encourage team members to suggest improvements.

# 9. Documentation and Reporting

* **Backup Reports**:
  + Generate and review weekly backup status reports.
* **Incident Reports**:
  + Document any backup failures or data loss incidents promptly.
* **Change Logs**:
  + Maintain records of any changes made to backup configurations or procedures.

# 10. Emergency Contacts

* **IT Operations Manager**: [Name], [Contact Information]
* **Backup Administrator**: [Name], [Contact Information]
* **DR Coordinator**: [Name], [Contact Information]
* **AWS Support**: Access AWS Support Center via the console or call the support line as per your AWS Support Plan.

# 11. References

* **AWS Backup Documentation**
  + AWS Backup User Guide
* **AWS Security Best Practices**
  + AWS Security Documentation
* **Compliance Standards**
  + AWS Compliance Programs

## Additional Considerations

* **Infrastructure as Code (IaC)**:
  + Use AWS CloudFormation or Terraform to codify your infrastructure for consistent deployments and easier recovery.
* **Version Control**:
  + Store IaC scripts and backup configurations in a version control system like Git.
* **Automation Tools**:
  + Consider AWS Systems Manager for automating operational tasks across resources.
* **Cost Management**:
  + Implement AWS Cost Explorer to monitor and optimize the costs associated with backups.