AWS Disaster Recovery Plan

Contents

Introduction

Today's business environment is increasingly reliant on IT systems and digital data.

Organizations, large and small, critically depend on their IT infrastructures to maintain operations, serve customers, and store sensitive information. However, no infrastructure is immune to potential threats that can cause major disruptions, such as natural disasters, hardware failures, cyberattacks, or other unforeseen events.

Questions about the durability and scalability of backup methods are commonplace, including this one: How does the cloud help meet the backup and archival needs?

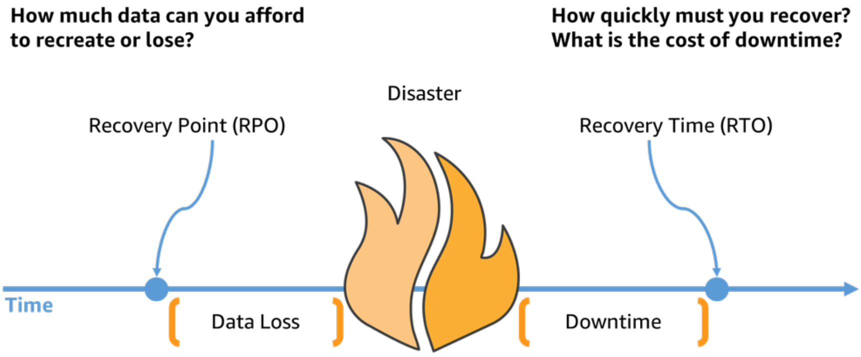
This is why it is imperative that SonarSource takes a proactive approach to disaster preparedness and response. This AWS-specific Disaster Recovery Plan (DRP) aims to ensure that the organization can continue to operate even in the event of a major disruption to its IT operations.

It is an essential document that defines the procedures, responsibilities and resources necessary to minimize downtime, reduce data loss and ensure business continuity.

Disaster Recovery Plan objectives

Because a disaster event can potentially take down the workload, the objective for DR should be bringing the workload back up or avoiding downtime altogether. The use of the following objectives will help respond to requirements:

- Recovery time objective (RTO): The maximum acceptable delay between the interruption of service and restoration of service. This determines an acceptable length of time for service downtime.
- Recovery point objective (RPO): The maximum acceptable amount of time since the last data recovery point. This determines what is considered an acceptable loss of data.


How much data can you afford to recreate or lose?
How quickly must you recover? What is the cost of downtime?
Disaster
Recovery Point (RPO)
Recovery Time (RTO)
Time
Data Loss
Downtime

For RTO and RPO, lower numbers represent less downtime and data loss. However, lower RTO and RPO cost more in terms of spend on resources and operational complexity. Therefore, it is necessary to choose RTO and RPO objectives that provide appropriate value for the workload.

Other objectives are also to minimize data loss by adopting appropriate backup and recovery strategies. This means that all critical data must be backed up regularly and it is necessary to ensure that these backups are accessible and recoverable when needed. The goal is to minimize any data loss, which is essential to maintaining the integrity of our business and the trust of our customers.

Additionally, for the disaster recovery plan to be effective, it is essential to provide clear and understandable procedures. All personnel involved in implementing the plan must be able to follow the procedures unambiguously. This includes detailed instructions on how to restore AWS resources, redirect traffic to backup systems, and reestablish communications.

Disaster recovery preparation is about more than creating the initial plan. It is necessary to commit to testing and updating the plan regularly to ensure that it remains operational and reflects the changing needs of the organization. Regular testing ensures that procedures are working as intended and identifies any gaps or weak points.

Finally, a crucial objective is to put in place effective communication and notification procedures in the event of a disaster. This includes internal and external communication to inform relevant stakeholders, including employees, customers, suppliers and relevant authorities. Clear and timely communication is essential to effectively manage the crisis and minimize potential damage.

By pursuing these goals, the ability to address potential challenges and disasters is strengthened, ensuring continuity of operations and protection of digital assets on AWS.

Roles and responsibilities

Responsible for the Disaster Recovery Plan (DRP):

- <Name>: This person is responsible for overall oversight of the DRP plan on AWS. Responsibilities include planning, implementation, ongoing management and coordination of all activities related to disaster recovery. The DRP Manager must ensure that the plan is well understood and respected by all stakeholders.

Disaster Recovery Team:

- <Name of Disaster Recovery Team>: This team is made up of designated members with technical and operational skills. Their main role is to implement disaster recovery procedures when necessary. Specific team responsibilities include:
  - Restoring AWS Resources: Perform recovery procedures to restore critical AWS resources according to defined recovery time objectives (RTOs).
  - Disaster Recovery Testing: Participate in regular disaster recovery testing to ensure procedures are working properly and identify areas for improvement.
  - DRP Plan Updates: Collaborate in the maintenance and continuous updating of the DRP plan based on developments in the AWS infrastructure and the needs of the organization.

Other Specific Roles:

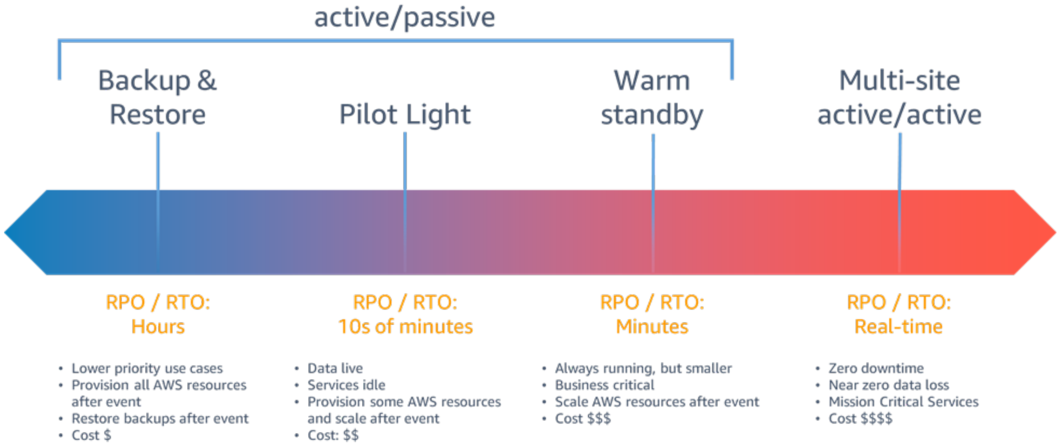
In addition to the DRP Manager and Disaster Recovery Team, there may be other specific roles designated based on the needs of the organization. These roles may include:

- Communication Manager: Responsible for internal and external communication in the event of a disaster. It must ensure that all stakeholders are informed quickly and efficiently.
- Notification Manager: Responsible for coordinating the notification of stakeholders, including employees, customers, suppliers and relevant authorities.
- Backup Manager: Responsible for setting up and managing backups of critical data, ensuring their availability in the event of disaster recovery.
- Security Manager: Ensures coordination of security measures specific to disaster recovery, including data protection during the transition to backup systems.
- Responsible for Vendor Management: Manages relationships with third-party service providers involved in disaster recovery, such as AWS cloud services or business continuity solution providers.

Each role should have clearly defined responsibilities, disaster activation procedures, and established communication channels for effective coordination. It is essential that each team member fully understands their role and responsibilities to ensure successful implementation of the DRP plan on AWS.

Disaster recovery strategies

Disaster recovery strategies available within AWS can be broadly categorized into four approaches, ranging from the low cost and low complexity of making backups to more complex strategies using multiple active Regions.


active/passive
Backup & Restore
Pilot Light
Warm standby
Multi-site active/active
RPO / RTO: Hours
RPO / RTO: 10s of minutes
RPO / RTO: Minutes
RPO / RTO: Real-time
• Lower priority use cases
• Provision all AWS resources after event
• Restore backups after event
• Cost $
• Data live
• Services idle
• Provision some AWS resources and scale after event
• Cost: $$
• Always running, but smaller
• Business critical
• Scale AWS resources after event
• Cost $$$
• Zero downtime
• Near zero data loss
• Mission Critical Services
• Cost $$$$

Backup & Restore

Backup and restore is a suitable approach for mitigating against data loss or corruption. This approach can also be used to mitigate against a regional disaster by replicating data to other AWS Regions, or to mitigate lack of redundancy for workloads deployed to a single Availability Zone. In addition to data, it is necessary to redeploy the infrastructure, configuration, and application code in the recovery Region. To enable infrastructure to be redeployed quickly without errors, it is obligated to always deploy using infrastructure as code (IaC) using services such as AWS CloudFormation or the AWS Cloud Development Kit (AWS CDK). Without IaC, it may be complex to restore workloads in the recovery Region, which will lead to increased recovery times and possibly exceed the RTO. In addition to user data, be sure to also back up code and configuration, including Amazon Machine Images (AMIs) used to create Amazon EC2 instances.

Pilot Light

With the pilot light approach, the user replicate the data from one Region to another and provision a copy of the core workload infrastructure. Resources required to support data replication and backup, such as databases and object storage, are always on. Other elements, such as application servers, are loaded with application code and configurations, but are "switched off" and are only used during testing or when disaster recovery failover is invoked. In the cloud, there is the flexibility to deprovision resources when there are not needed anymore, and provision them when necessary. A best practice for “switched off” is to not deploy the resource, and then create the configuration and capabilities to deploy it (“switch on”) when needed. Unlike the backup and restore approach, the core infrastructure is always available and the user have the option to quickly provision a full scale production environment by switching on and scaling out the application servers.

Warm standby

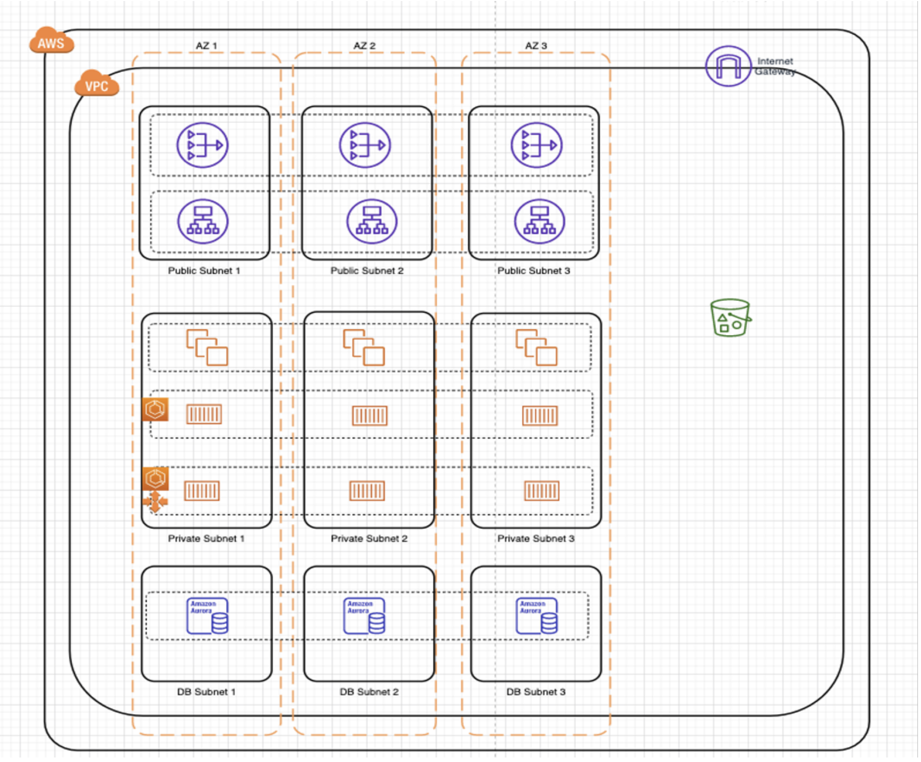
The warm standby approach involves ensuring that there is a scaled down, but fully functional, copy of the production environment in another Region. This approach extends the pilot light concept and decreases the time to recovery because the workload is always-on in another Region. This approach also allows to more easily perform testing or implement continuous testing to increase confidence in the ability to recover from a disaster.

Multi-site active/passive

Multi-site active/active serves traffic from all regions to which it is deployed, whereas hot standby serves traffic only from a single region, and the other Region(s) are only used for disaster recovery. With a multi-site active/active approach, users are able to access the workload in any of the Regions in which it is deployed. This approach is the most complex and costly approach to disaster recovery, but it can reduce the recovery time to near zero for most disasters with the correct technology choices and implementation (however data corruption may need to rely on backups, which usually results in a non-zero recovery point). Hot standby uses an active/passive configuration where users are only directed to a single region and DR regions do not take traffic. Most customers find that if they are going to stand up a full environment in the second Region, it makes sense to use it active/active. Alternatively, if the do not want to use both Regions to handle user traffic, then Warm Standby offers a more economical and operationally less complex approach.

AWS resources inventory

This is an inventory of the resource deployed in the architecture:



- S3 bucket to store ".tfstate" file
- Region: us-east-1
    - Internet gateway
    - 1 VPC
    - AZs: us-east-1a, us-east-1b, us-east-1c
        - In each AZ:
            - Public subnets
                - NAT Gateway
                - Application load balancer
            - Private subnets
                - EC2 instances
                - ECS clusters with ECR repository to store images
            - Database subnets
                - RDS database

Procedures

EBS Snapshot-based protection

Amazon EBS provides the ability to create snapshots (backups) of any Amazon EBS volume. It takes a copy of the volume and places it in Amazon S3, where it is stored redundantly in multiple Availability Zones. The first snapshot is a full copy of the volume; ongoing snapshots store incremental block-level changes only.

This is a fast and reliable way to restore full volume data. If there is a need for a partial restore, it is possible to attach the volume to the running instance under a different device name, mount it, and then use operating system copy commands to copy the data from the backup volume to the production volume.

When a snapshot is created, it protect the data directly to durable disk-based storage. The User can use the AWS Management Console, the command line interface (CLI), or the APIs to create the Amazon EBS snapshot.

It is possible to schedule and run the “aws ec2 create-snapshot” commands on a regular basis to back up the EBS data. The economical pricing of Amazon S3 makes it possible to retain many generations of data. And because snapshots are block-based, the user consume space only for data that’s changed after the initial snapshot was created.

Database backup

Amazon RDS provides two different methods for backing up and restoring the DB instances:

- Automated backups enable point-in-time recovery of the DB instance. Automated backups are turned on by default when the user create a new DB instance. Amazon RDS performs a full daily backup of the data during a window that the user define when he create the DB instance. He can configure a retention period of up to 35 days for the automated backup. Amazon RDS uses these periodic data backups in conjunction with the transaction logs to enable to restore the DB instance to any second during the retention period, up to the LatestRestorableTime (typically, the last five minutes). To find the latest restorable time for the DB instances, the user can use the DescribeDBInstances API call or look on the Description tab for the database in the Amazon RDS console.
- DB snapshots are user-initiated backups that enable to back up the DB instance to a known state as frequently as possible, and then restore to that state at any time. The user can use the Amazon RDS console or the CreateDBSnapshot API call to create DB snapshots. These snapshots have unlimited retention. They are kept until he use the console or the DeleteDBSnapshot API call to explicitly delete them.

Amazon RDS includes features for automating database backups. Amazon RDS creates a storage volume snapshot of the database instance, backing up the entire DB instance, not just individual databases.

AWS Backup

AWS Backup is a service managed by Amazon Web Services (AWS) that simplifies managing backups and recovery of your AWS resources, including Elastic Block Store (EBS) volumes, RDS databases, EC2 instances, and more. others. It allows to create and manage centralized backup plans for AWS resources. Here's how it is possible to use AWS Backup:

1. **Creating an AWS Backup Plan:**

To start using AWS Backup, you must create a backup plan. An AWS Backup plan defines backup rules and policies for a specific group of resources. You can create a backup plan by following these steps:

- Log in to the AWS console.
- Go to the AWS Backup service.
- Click “Create a backup plan”.
- Choose a name for your backup plan and configure backup rules, including frequency, retention, and resources to include.

2. **Association of Resources with the Safeguard Plan:**

Once you have created a backup plan, you must associate your AWS resources with that plan. You can associate resources manually or use tags to automate this step. AWS Backup supports backup of multiple resource types, including EBS, RDS, EC2, DynamoDB, and more.

3. **Creating Backup Copies:**

AWS Backup automatically creates backup copies at the frequency and retention specified in your backup plan. You don't need to manage individual backups for each resource.

4. **Restore from AWS Backup:**

When you need to restore a resource from a backup, you can use AWS Backup to perform the restoration. You can restore an individual resource, or all resources associated with a backup plan. AWS Backup allows you to specify a restore date to restore the resource to a previous state.

5. **Monitoring and Management of Backups:**

AWS Backup provides backup monitoring and management capabilities. You can monitor the status of your backups using CloudWatch metrics and CloudTrail logs. You can also manage backup plans, retention policies, and resource associations from the AWS Backup console.

6. **Automation with Tagging Policies:**

You can use tags to automate the association of resources with specific backup plans. By adding tags to resources, you can define backup policies based on those tags, simplifying backup management for complex AWS environments.

AWS Backup dramatically simplifies AWS backup management by centralizing backup and restore operations into a single service. It also offers compliance features to ensure your backups meet your organization's regulatory requirements.

Conclusion

Creating this Disaster Recovery Plan (DRP) for a simple architecture on Amazon Web Services (AWS) is a crucial step to ensure business continuity in the event of a major incident. This plan details the procedures, roles, and objectives that underpin our approach to disaster management in the AWS Cloud.

The simple AWS architecture, although limited in complexity, requires adequate preparation to deal with unexpected events. We have implemented measures to ensure the continued availability of our critical resources, minimize data loss and reduce downtime in the event of a disaster.

Throughout this process, we have identified key responsibilities, trained our staff on recovery procedures, and scheduled regular testing to ensure our DRP is operational. Each member of our team understands their role and knows how to respond when needed.

Although our architecture on AWS is simple, disaster recovery preparation remains essential. AWS provides a robust platform to implement our plan, with backup, recovery, and resource management services that simplify building a resilient infrastructure.

By adopting this Disaster Recovery Plan for our simple AWS architecture, we are committed to maintaining business continuity, protecting our data and ensuring the trust of our customers. We will continue to evaluate and improve our plan to stay prepared for any eventuality, even in a basic IT environment.

The simplicity of our architecture does not diminish our commitment to preparedness and resilience, as we understand that even the smallest disruptions can have a significant impact. By investing in this DRP, we strengthen our ability to face potential challenges and ensure the continuity of our operations.