AWS Architecture Blog

Disaster Recovery with AWS managed services, Part 1: Single Region

by Dhruv Bakshi and Brent Kim | on 12 NOV 2021 | in Amazon Elastic Kubernetes Service, Amazon ElastiCache, Amazon OpenSearch Service, Amazon Redshift, Architecture, RDS for PostgreSQL | Permalink | Share

This 3-part blog series discusses disaster recovery (DR) strategies that you can implement to ensure your data is safe and that your workload stays available during a disaster. In Part I, we'll discuss the single AWS Region/multi-Availability Zone (AZ) DR strategy.

The strategy outlined in this blog post addresses how to integrate AWS managed services into a single-Region DR strategy. This will minimize maintenance and operational overhead, create fault-tolerant systems, ensure high availability, and protect your data with robust backup/recovery processes. This strategy replicates workloads across multiple AZs and continuously backs up your data to another Region with point-in-time recovery, so your application is safe even if all AZs within your source Region fail.

Implementing the single Region/multi-AZ strategy

The following sections list the components of the example application presented in Figure 1, which illustrates a multi-AZ environment with a secondary Region that is strictly utilized for backups. This example architecture refers to an application that processes payment transactions that has been modernized with AWS managed services. We'll show you which AWS services it uses and how they work to maintain the single Region/multi-AZ strategy.

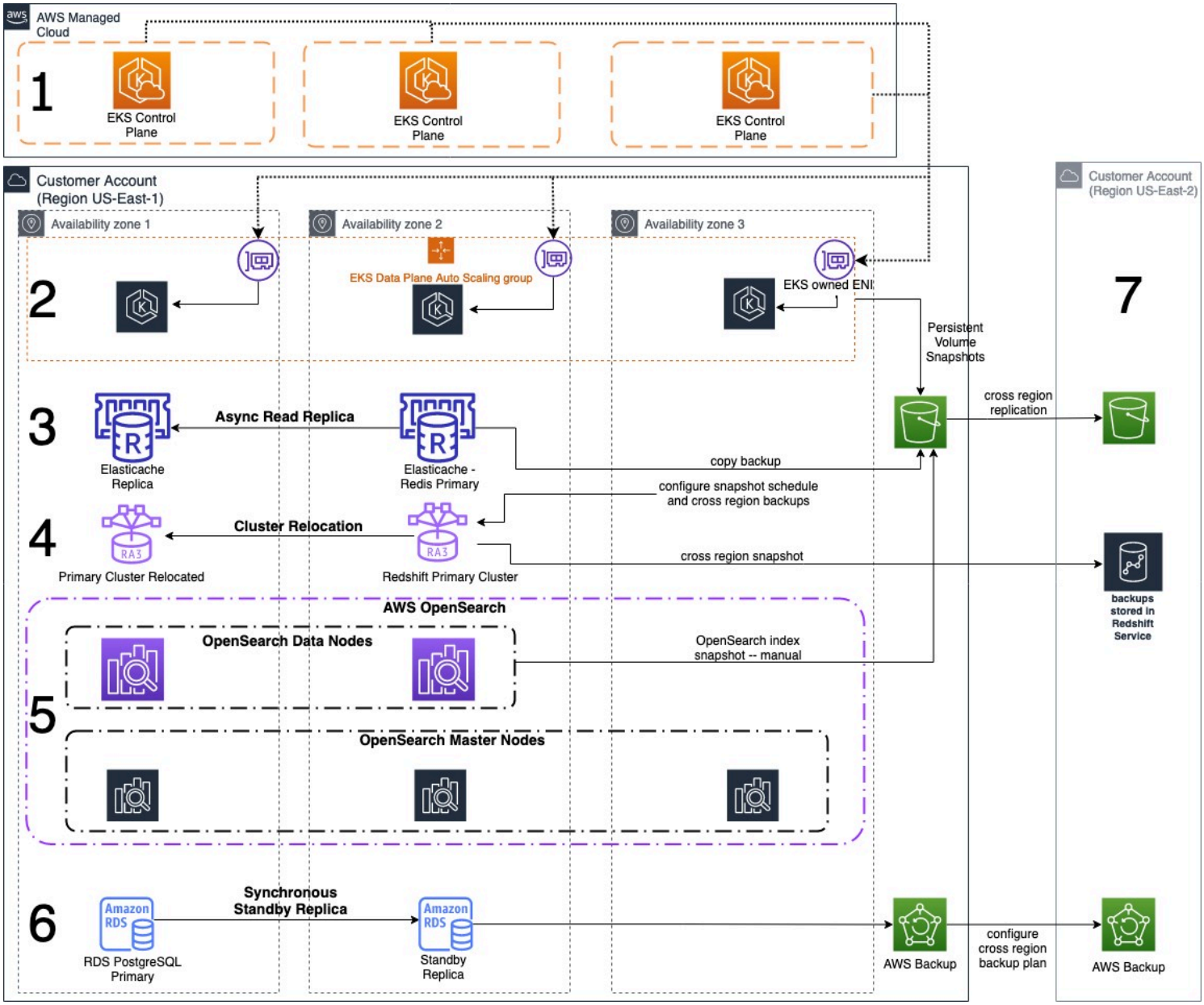

Figure 1. Single Region/multi-AZ with secondary Region for backups

1. Amazon EKS control plane

Amazon Elastic Kubernetes Service (Amazon EKS) runs the Kubernetes management infrastructure across multiple AZs to eliminate a single point of failure.

This means that if your infrastructure or AZ fails, it will automatically scale control plane nodes based on load, automatically detect and replace unhealthy control plane instances, and restart them across the AZs within the Region as needed.

2. Amazon EKS data plane

Instead of creating individual Amazon Elastic Compute Cloud (Amazon EC2) instances, create worker nodes using an Amazon EC2 Auto Scaling group. Join the group to a cluster, and the group will automatically replace any terminated or failed nodes if an AZ fails. This ensures that the cluster can always run your workload.

3. Amazon ElastiCache

Amazon ElastiCache continually monitors the state of the primary node. If the primary node fails, it will promote the read replica with the least replication lag to primary. A replacement read replica is then created and provisioned in the same AZ as the failed primary. This is to ensure high availability of the service and application.

An ElastiCache for Redis (cluster mode disabled) cluster with multiple nodes has three types of endpoints: the primary endpoint, the reader endpoint and the node endpoints. The primary endpoint is a DNS name that always resolves to the primary node in the cluster.

4. Amazon Redshift

Currently, Amazon Redshift only supports single-AZ deployments. Although there are ways to work around this, we are focusing on cluster relocation. Parts II and III of this series will show you how to implement this service in a multi-Region DR deployment.

Cluster relocation enables Amazon Redshift to move a cluster to another AZ with no loss of data or changes to your applications. When Amazon Redshift relocates a cluster to a new AZ, the new cluster has the same endpoint as the original cluster. Your applications can reconnect to the endpoint and continue operations without modifications or loss of data.

Note: Amazon Redshift may also relocate clusters in non-AZ failure situations, such as when issues in the current AZ prevent optimal cluster operation or to improve service availability.

5. Amazon OpenSearch Service

Deploying your data nodes into three AZs with Amazon OpenSearch Service can improve the availability of your domain and increase your workload's tolerance for AZ failures.

Amazon OpenSearch Service automatically deploys into three AZs when you select a multi-AZ deployment. This distribution helps prevent cluster downtime if an AZ experiences a service disruption. When you deploy across three AZs, Amazon OpenSearch Service distributes master nodes equally across all three AZs. That way, in the rare event of an AZ disruption, two master nodes will still be available.

Amazon OpenSearch Service also distributes primary shards and their corresponding replica shards to different zones. In addition to distributing shards by AZ, Amazon OpenSearch Service distributes them by node. When you deploy the data nodes across three AZs with one replica enabled, shards are distributed across the three AZs.

Note: For more information on multi-AZ configurations, please refer to the AZ disruptions table.

6. Amazon RDS PostgreSQL

Amazon Relational Database Service (Amazon RDS) handles failovers automatically so you can resume database operations as quickly as possible.

In a Multi-AZ deployment, Amazon RDS automatically provisions and maintains a synchronous standby replica in a different AZ. The primary DB instance is synchronously replicated across AZs to a standby replica. If an AZ or infrastructure fails, Amazon RDS performs an automatic failover to the standby. This minimizes the disruption to your applications without administrative intervention.

Backing up data across Regions

Here is how the managed services back up data to a secondary Region:

- Manage snapshots of persistent volumes for Amazon EKS with Velero. Amazon Simple Storage Service (Amazon S3) stores these snapshots in an S3 bucket in the primary Region. Amazon S3 replicates these snapshots to an S3 bucket in another Region via S3 cross-Region replication.
- Create a manual snapshot of Amazon OpenSearch Service clusters, which are stored in a registered repository like Amazon S3. You can do this manually or automate it via an AWS Lambda function, which automatically and asynchronously copy objects across Regions.
- Use manual backups and copy API calls for Amazon ElastiCache to establish a snapshot and restore strategy in a secondary Region. You can manually back your data up to an S3 bucket or automate the backup via Lambda. Once your data is backed up, a snapshot of the ElastiCache cluster will be stored in an S3 bucket. Then S3 cross-Region replication will asynchronously copy the backup to an S3 bucket in a secondary Region.
- Take automatic, incremental snapshots of your data periodically with Amazon Redshift and save them to Amazon S3. You can precisely control when snapshots are taken and can create a snapshot schedule and attach it to one or more clusters. You can also configure a cross-Region snapshot copy, which automatically copies your automated and manual snapshots to another Region.
- Use AWS Backup to support AWS resources and third-party applications. AWS Backup copies RDS backups to multiple Regions on demand or automatically as part of a scheduled backup plan.

Note: You can add a layer of protection to your backups through AWS Backup Vault Lock and S3 Object Lock.

Conclusion

The single Region/multi-AZ strategy safeguards your workloads against a disaster that disrupts an Amazon data center by replicating workloads across multiple AZs in the same Region. This blog shows you how AWS managed services automatically fails over between AZs without interruption when experiencing a localized disaster, and how backups to a separate Region ensure data protection.

In the next post, we will discuss a multi-Region warm standby strategy for the same application stack illustrated in this post.

Related information

- Disaster Recovery on AWS Series
- Use Fault Isolation to Protect Your Workload

- Design your Workload to Withstand Component Failures

TAGS: Disaster recovery, Disaster Recovery with AWS Managed Services series