Disaster recovery with IBM Cloud Virtual Servers

Phase1:consider incorporating automated Recovery scripts or proactive monitoring for quicker response during disasters

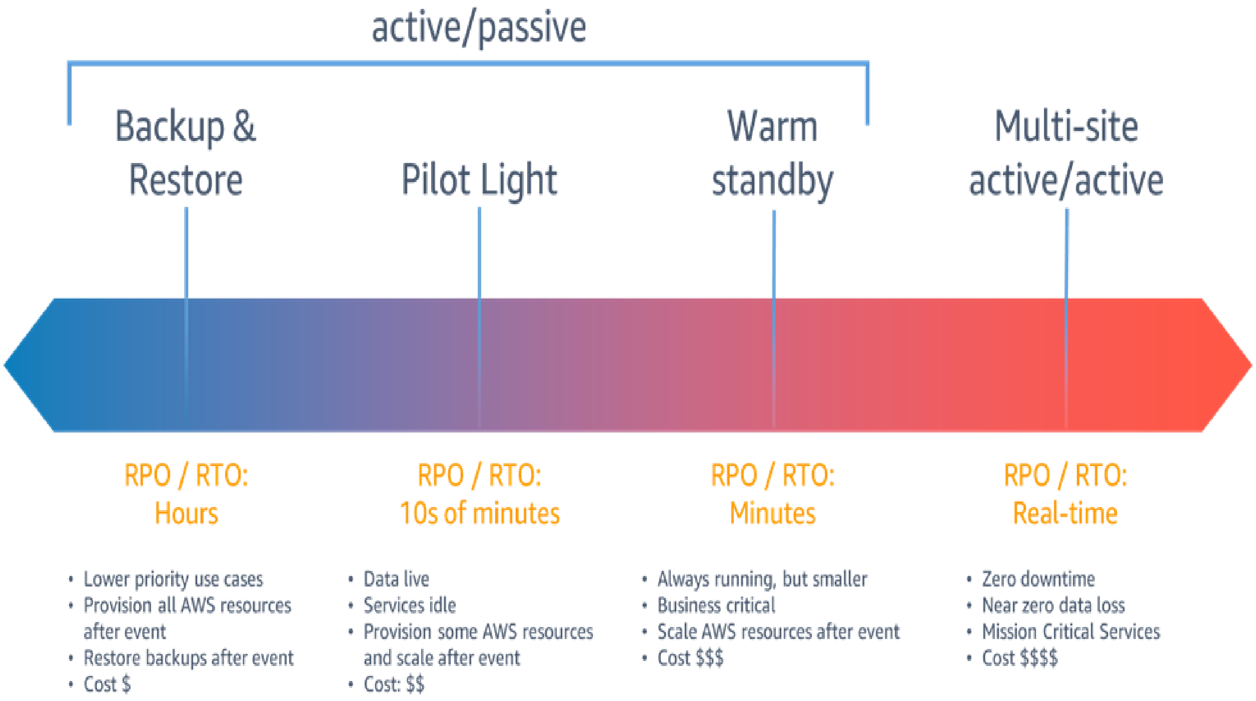
Disaster recovery strategies available to you within AWS can be broadly categorized into four approaches, ranging from the low cost and low complexity of making backups to more complex strategies using multiple active Regions. Active/passive strategies use an active site (such as an AWS Region) to host the workload and serve traffic. The passive site (such as a different AWS Region) is used for recovery. The passive site does not actively serve traffic until a failover event is triggered

It is critical to regularly assess and test your disaster recovery strategy so that you have confidence in invoking it, should it become necessary. Use AWS Resilience Hub to continuously validate and track the resilience of your AWS workloads, including whether you are likely to meet your RTO and RPO targets.

AWS services

Your workload data will require a backup strategy that runs periodically or is continuous. How often you run your backup will determine your achievable recovery point (which should align to meet your RPO). The backup should also offer a way to restore it to the point in time in which it was taken. Backup with point-in-time recovery is available through the following services and resources:

For a disaster event based on disruption or loss of one physical data center for a well-architected, highly available workload, you may only require a backup and restore approach to disaster recovery. If your definition of a disaster goes beyond the disruption or loss of a physical data center to that of a Region or if you are subject to regulatory requirements that require it, then you should consider Pilot Light, Warm Standby, or Multi-Site Active/Active.


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 $$$$

When choosing your strategy, and the AWS resources to implement it, keep in mind that within AWS, we commonly divide services into the data plane and the control plane. The data plane is responsible for delivering real-time service while control planes are used to configure the environment. For maximum resiliency, you should use only data plane operations as part of your failover operation. This is because the data planes typically have higher availability design goals than the control planes.

Backup and 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, you must redeploy the infrastructure, configuration, and application code in the recovery Region. To enable infrastructure to be redeployed quickly without errors, you should 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 your RTO. In addition to user data, be sure to also back up code and configuration, including Amazon Machine Images (AMIs) you use to create Amazon EC2 instances. You can use AWS CodePipeline to automate redeployment of application code and configuration.

With this approach, you must also mitigate against a data disaster. Continuous data replication protects you against some types of disaster, but it may not protect you against data corruption or destruction unless your strategy also includes versioning of stored data or options for point-in-time recovery. You can back up the replicated data in the disaster Region to create point-in-time backups in that same Region.