**Assignment (1.12)**

**Brief**

**Group Presentation**

Work with your group to define your own business and your own recovery plan based on discussed threats that might be happen to your business

1. Define your business

2. Define your assets

3. Define your possible threat

4. Define Your RTO and RPO

**Submission**

* Submit the URL of the GitHub Repository that contains your work to NTU black board.

**A Disaster Recovery Plan is required for the following reasons: to stay productive, create a positive brand reputation, avoid losing to competitors and promotion internal competence**

**Define your business**: A leading smart commerce platform in Asia, with offices in SEA and U.S locations that have help more than a quarter million merchants open their online stores with a view to supporting their brands to achieve national and international growth. The business sees consistent connectivity and access for customers as essential for success.

**Define your assets:** A list of asset inventory coverall devices in network, workstations, I/O Processors, data communication equipment, system printer, software and other miscellaneous items e.g. file cabinet contents/documentation and printing supplies etc.,

**Define your possible threats**: serious interruption in business performance could shut down company’s communications, network , and even lead to data loss. Typical threats to the business include: cyberattacks, network downtime, application failure , data center issues and natural disasters.

**Define your RTO and RPO:** define recovery objectives for downtime and data loss, they are important considerations in selecting an appropriate DR strategy for our workload. A disaster recovery matrix (fig 1) can help understand how workload critically related to recovery objectives (in terms of Low, Medium, High and Critical). Next we choose a strategy (fig 2) that meets the our workload’s recovery objective, for example, backup and store, standby (active/passive) or active/active.

A warm standby model (please refer to attached architecture, fig 3, RTO < 10 mins and RPO < 10 mins) is recommended in light of critical workload in relation to the recovery objective of RTO/RPO. The services are run at reduced capacity but fully functional version in the recovery region. When the time comes for recovery, the system is scaled up quickly to handle production load.

This strategy replicates data from the primary Region to data resources in the recovery Region, such as [Amazon Relational Database Service (Amazon RDS)](http://aws.amazon.com/rds) DB instances. These data resources are ready to serve requests. In addition to replication, this strategy requires us to create a continuous backup in the recovery Region. This is because when human action type disasters occur, data can be deleted or corrupted, and replication will replicate the bad data. Backups are necessary to enable you to get back to the last known good state (Aurora cluster Snapshot).

Resources used for the workload infrastructure are deployed in the recovery Region for this strategy. This includes support infrastructure such as [Amazon Virtual Private Cloud (Amazon VPC)](http://aws.amazon.com/vpc) with subnets and routing configured, [Elastic Load Balancing](http://aws.amazon.com/elasticloadbalancing), and [Amazon EC2 Auto Scaling](http://aws.amazon.com/ec2/autoscaling) groups. As required for an active/passive strategy, it requires a means to route traffic to the primary Region, and then fail over to the recovery Region when recovering from a disaster (Route 53).

We need to regularly test failover to our recovery site to ensure proper operation and that RTO and RPO are met. In this model, we should fail over to the standby regularly, regardless of need.



Figure 1: A Disaster Recovery Matrix

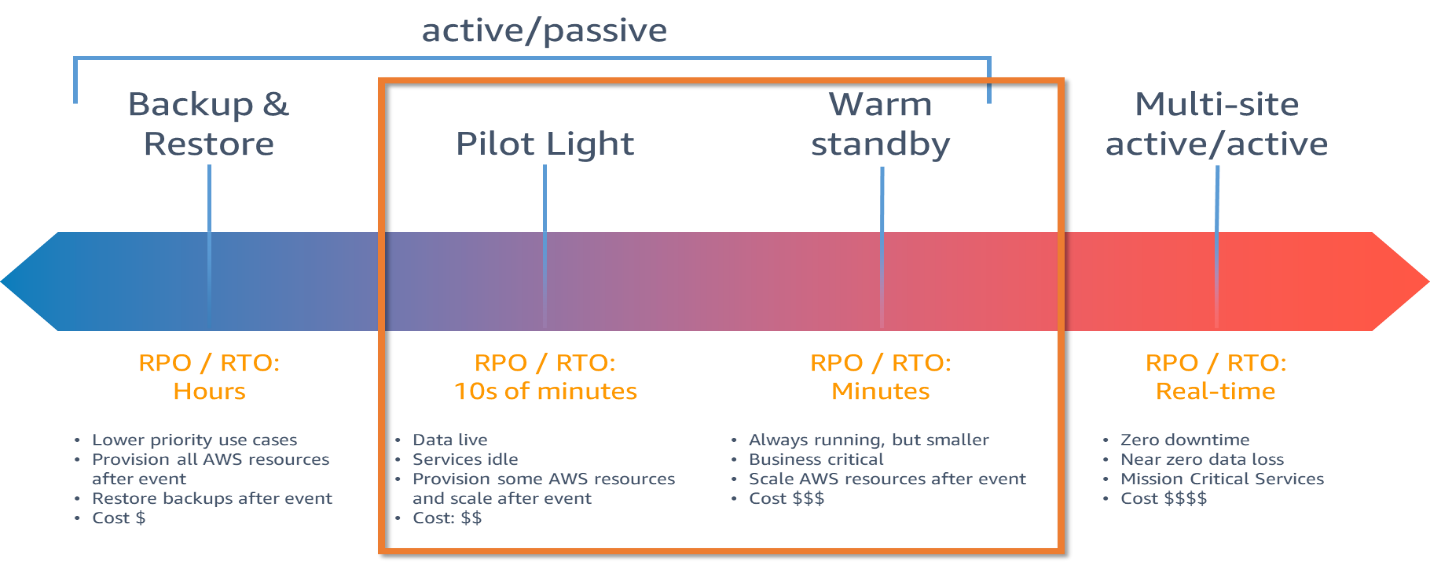


Fig 2: Disaster Recovery Strategies

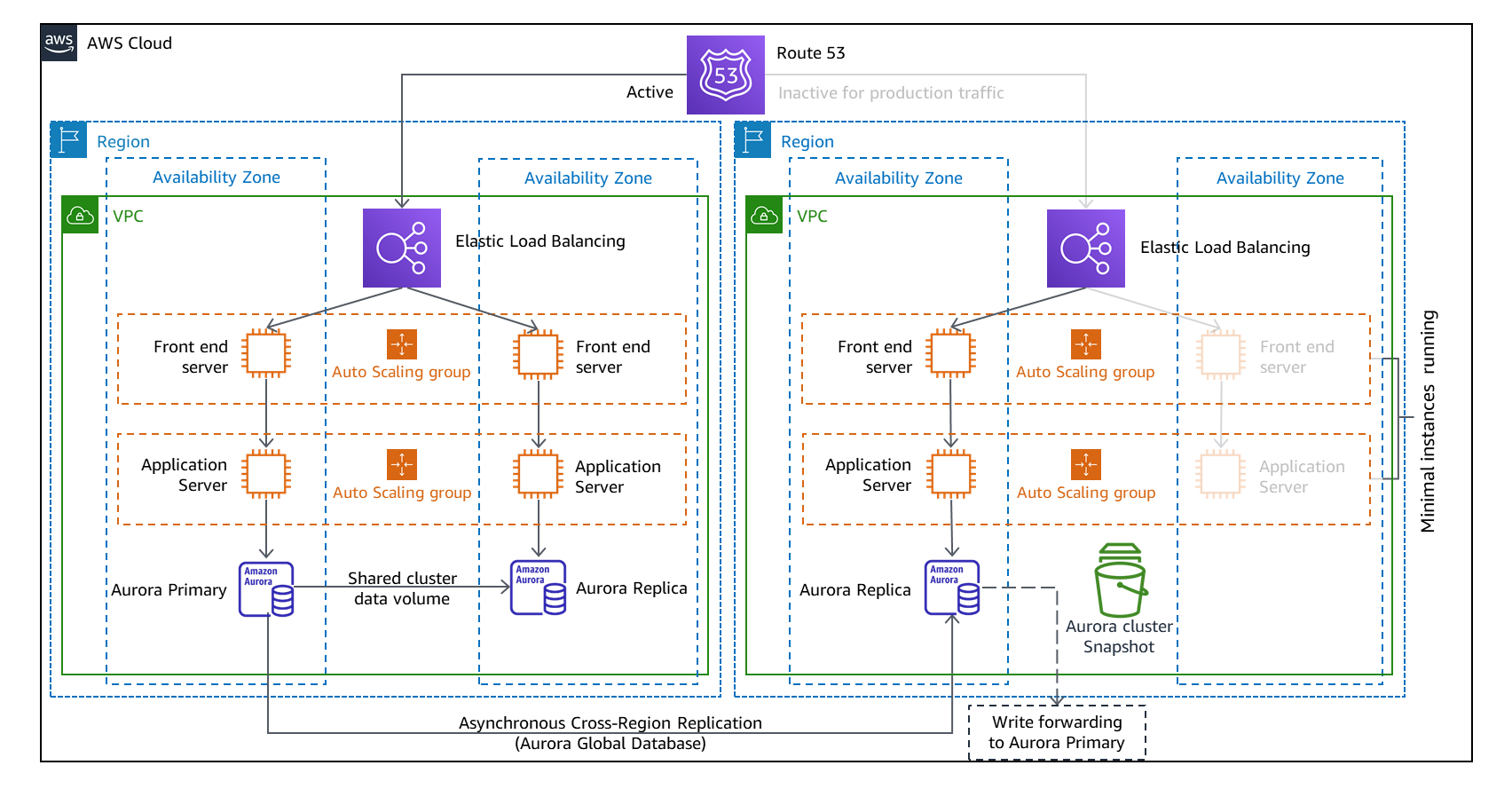


Fig 3: Warm Standby Architecture