

Disaster Recovery Overview

lkawsoft.com



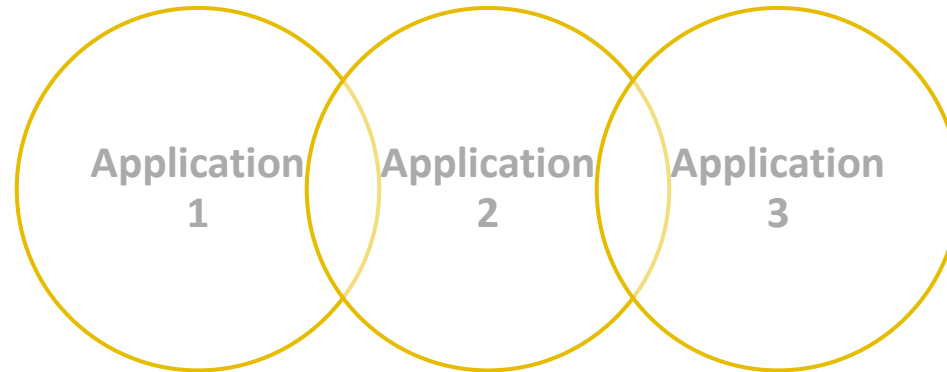
A person is sitting at a desk, writing in a spiral-bound notebook with a blue pen. A laptop is visible in the background, and the person is wearing a black watch. The word "Agenda" is overlaid in large white text.

Agenda

1. Overview
2. Use Cases
3. Metrics
4. Lifecycle
5. Design
6. Documentation
7. Infrastructure Standup
8. Prep Tasks
9. Exercise
10. Roadmap

DR Design

Application Migration by Hosting Site



App Owner: Michael R.	Architect: Larry M	PM: Robert S	
Application	App Lead	DevOps	DBA
Application 1	Person 1	Person 2	Person 3
Application 2	Person 4	Person 5	Person 6

Use Cases

DR Tests

Use Case 1 (High Availability)	Use Case 2 (Site Disaster Recovery)	Use Case 3 (Alternate Hosting)	Use Case 4 (Data Corruption)	Use Case 5 (Volumetric Attack)
App & DB Layer	Same Hosting Site (AWS)	Cross Cloud Hosting Site (AWS->Azure)	App & DB Layer	WAF Documentation Only

1. Use Case 1 is the testing of High Availability application and database systems by bringing down the primary and switching over to the secondary.
2. Use Case 2 is the Failover/Failback use case where the application is moved from the primary hosting site to the DR hosting site when the hosting sites are with the same hosting provider: AWS Virginia -> AWS Ohio. Only Failover timing is recorded for RTA.
3. Use Case 3 is the Failover use case where the application is moved from the primary hosting site to the DR hosting site when the hosting sites are provided by different providers: AWS -> Azure. This is sometimes referred to as cross cloud hosting sites. Only Failover timing is recorded for RTA.
4. Use Case 4 is the Data Corruption Use Case where data is deleted or corrupted on the application server and in the application database. The restoration of that data from backups is tested and timed.
5. Use Case 5 is the requirement to provide evidence of security defense against a volumetric (DDOS) attack.

Metrics

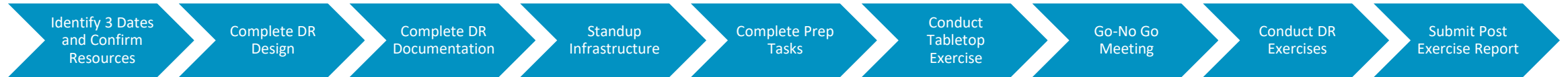
Length of Downtime and Impact on Data

1. Recovery Point Objective (RPO) - Recovery Point Objective is the maximum amount of data loss that would be acceptable to an organization in a Failover, Failback, Data Corruption event.
2. Recovery Time Objective (RTO) - Recovery Time Objective is the maximum length of time a computer, system, network, or application can be down following a failure, i.e. Failover, Failback, Data Corruption.
3. Recovery Point Achieved (RPA) - Recovery Point Actual measures the real data loss when this happens, which is usually based on the data lost between the failure and when the last backup was made.
4. Recovery Time Achieved (RTA) - Recovery Time Actual is the recorded amount time in which a given Disaster Recovery Event is executed, i.e. Failover, Failback, Data Corruption.

The metrics are the measure of pass or fail for your DR Exercise. RPO & RTO are the thresholds that you have agreed upon with the business. RPA & RTA are the actual recorded times during your DR Exercise. RPA & RTA cannot exceed RPO & RTO in order to receive approval from the Governance Program.

End To End Lifecycle

Length of Downtime and Impact on Data

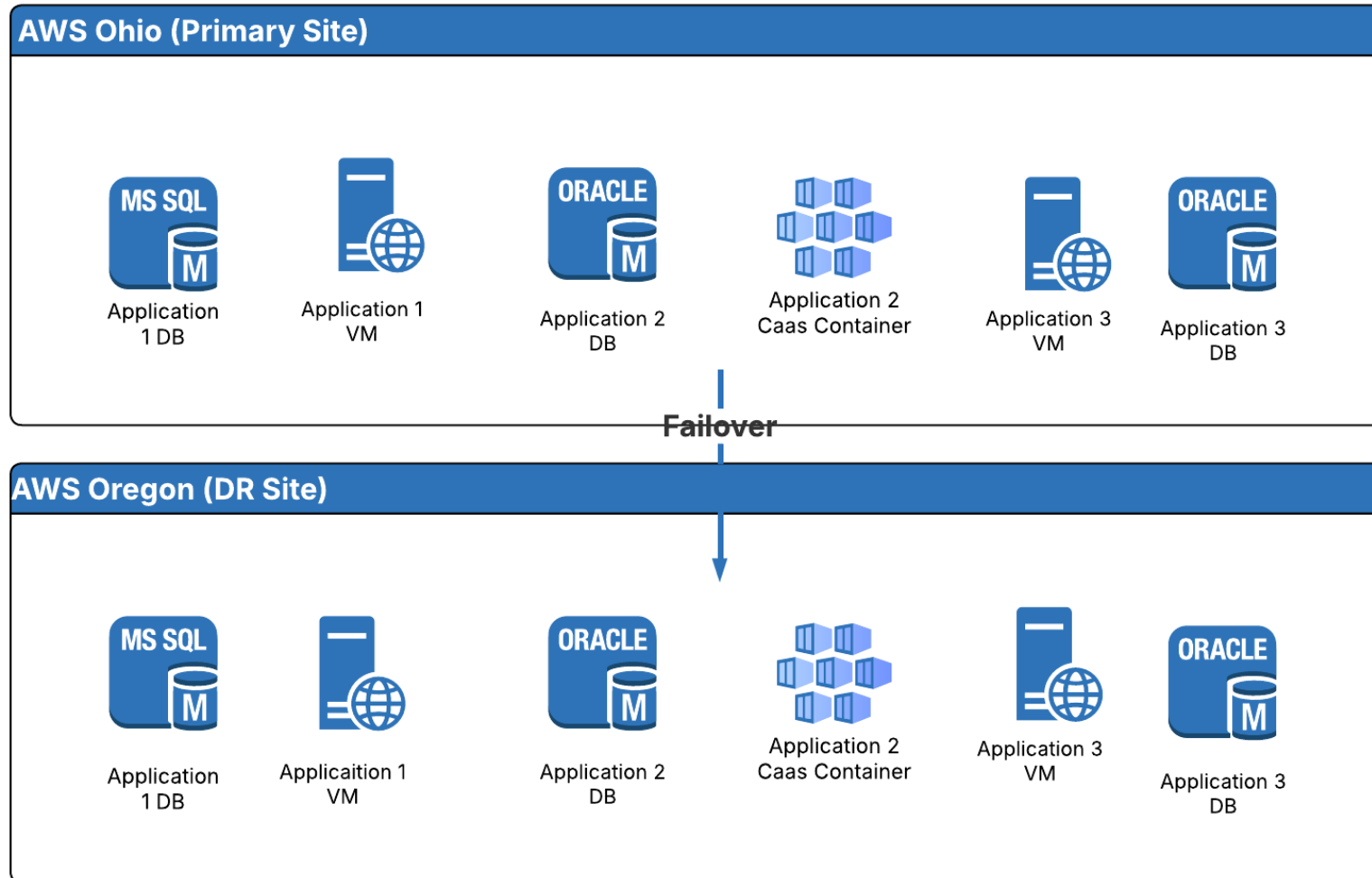


DR Diagram

A Birdseye View

My Ecosystem DR Design

Application 1 - Application 2 - Application 3



DR Documentation

Documents and Ownership

Document	Owner
Technical Recovery Procedure	DevOps + App Leads
Application Recovery Procedure	App Leads
Application Verification Procedures	QA
Business Impact Assessment	App Owner/App Manager
Disaster Recovery Plan	App Owner/App Manager
Solution Design Document	Architect/App Leads
Hour By Hour Plan	TPM + Team
Data Corruption Procedure	Business Analyst + App Leads

Infrastructure Standup and configuration

Starter List of Steps

1. Standup of Required Application Infrastructure: VM, CaaS Node, etc
2. Standup of Required DB Infrastructure
3. Deployment of Application Code to DR Infrastructure
4. Deployment of Database Schema's to DR Infrastructure
5. Configure Servers and Databases as Required, i.e. backups and replication of backups.
6. Network Configuration, i.e. Firewall Rules

Prep Tasks

Starter List of Steps

1. Confirm App and DB Backups are Working, On Schedule and Replicating
2. Confirm Load Balancer Configuration and Post Failover/Failback Recovery
3. Validate Application to DB Connectivity, If Possible
4. Refresh Databases If Required
5. Confirm All Credentials Will Be Available Such As Breakglass Accounts
6. Test Automation Scripts
7. Confirm That All DNS's Can Be Repointed Post-Failover/Failback

High Level DR Exercise Tasks

Task	Owner
Execute Hour By Hour Plan	Team
Collect Evidence and Upload	Team
Track Time in Clicktime	Team
Record RTA & RPA For The Exercise	TPM

Roadmap Planning

Think and Plan Ahead For Improvements



i.e. Cross Cloud
Failover/Failback

Real Time Database
Replication

?

Thank You