**Disaster Recovery Solution and Topology**

**1. Hosting Environment** Vortex IQ’s application is hosted on **Amazon Web Services (AWS)**, leveraging the robust and scalable infrastructure provided by AWS to ensure high availability, data protection, and rapid recovery of business-critical systems. AWS offers multiple services and features to support Vortex IQ’s disaster recovery strategy.

**2. Disaster Recovery Topology on AWS**

* **Multi-Region Architecture**:
 Vortex IQ’s application is deployed across **multiple AWS regions**, specifically in **US-East (N. Virginia)** and **EU-West (Ireland)**. This multi-region setup ensures redundancy and minimizes the risk of downtime in the event of a regional failure. Critical data and applications are replicated across these regions for seamless failover.
* **Data Replication and Backup**:
 All critical data, including application databases and user data, are **replicated** across AWS regions using services like **Amazon RDS (Relational Database Service)** for database redundancy and **Amazon S3** for object storage. **Daily automated backups** are performed and stored securely in **AWS S3 buckets**, with encrypted storage to ensure data integrity and confidentiality.
* **Automated Failover with Elastic Load Balancer**:
 Vortex IQ leverages **AWS Elastic Load Balancing (ELB)** to distribute incoming traffic across multiple AWS instances in different regions. In case of a failure in one region, traffic is automatically rerouted to the healthy region, ensuring continuous service availability and minimal downtime.
* **CloudWatch Monitoring**:
 **Amazon CloudWatch** is used to monitor the health of all AWS resources and trigger **automatic failover mechanisms** when necessary. CloudWatch monitors metrics such as server health, application performance, and infrastructure usage, providing early warnings in case of failures.

**3. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)**

* **RTO**: The maximum acceptable downtime for critical business functions is **4 hours**. AWS’s multi-region setup ensures that critical systems can be restored from another region within this time frame.
* **RPO**: The maximum acceptable data loss is **1 hour**, achieved through **real-time data replication** across AWS regions and frequent backups to ensure data consistency.

**4. Recovery Strategy**

* **Active-Active Configuration**:
 Vortex IQ’s disaster recovery solution follows an **active-active configuration**, meaning that services are continuously running in both regions. This ensures that in the event of a regional failure, Vortex IQ can quickly failover to the secondary region without service interruption.
* **Failover and Failback**:
 In case of a disaster, the **AWS Route 53** service is used for **DNS failover** to automatically redirect traffic to the backup region. Once the primary region is restored, a failback procedure is executed to return the services to the original region with minimal disruption.

**5. Security and Compliance**

* **Data Encryption**:
 All critical data is encrypted both at rest and in transit using **AWS Key Management Service (KMS)** for encryption key management and **SSL/TLS** for secure communication between services.
* **Compliance with Regulatory Standards**:
 Vortex IQ's AWS-hosted environment is compliant with **GDPR**, **SOC 2**, and other industry standards, ensuring that the disaster recovery solution adheres to regulatory and legal requirements for data protection.

**6. Disaster Recovery Testing and Continuous Improvement**

* **Regular Testing**:
 Disaster recovery tests are conducted **every 6 months** to ensure that failover mechanisms, backup systems, and communication protocols function as expected. These tests simulate disaster scenarios, such as region outages or database failures, to evaluate recovery time and effectiveness.
* **Post-Test Review**:
 After each disaster recovery test, a comprehensive review is conducted to identify any areas for improvement, and the Disaster Recovery Plan (DRP) is updated accordingly. Feedback from these tests ensures the solution remains effective and up to date.

**7. Communication and Reporting**

* **Disaster Recovery Communication**:
 In the event of a disaster, Vortex IQ uses **AWS SNS (Simple Notification Service)** to alert key stakeholders, including customers, internal teams, and third-party vendors, about the status of recovery efforts. Regular updates are provided through the communication platform (Slack, Email).
* **Disaster Recovery Reports**:
 Detailed **Disaster Recovery Test Reports** are generated after each test, documenting recovery timelines, actions taken, and any lessons learned. These reports are archived for compliance purposes and used for continuous process improvement.

Vortex IQ’s **disaster recovery solution** hosted on **AWS** ensures business continuity with high availability, redundant systems, real-time data replication, and seamless failover capabilities. By leveraging AWS's cloud infrastructure, Vortex IQ is prepared to handle any disaster scenario while maintaining service reliability and data integrity.