**RPO (Recovery Point Objective) and RTO (Recovery Time Objective) on AWS**

Establishing Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for an application on AWS infrastructure is crucial for ensuring its resilience and continuity in the face of failures or disasters. Here's a guide on how to establish RTO and RPO based on AWS Well-Architected best practices:

1. **Understand Business Requirements**

* Engage with key stakeholders, including business owners, IT managers, and operations teams, to gather requirements.
* Conduct business impact analysis to determine the financial, operational, and reputational impact of downtime and data loss.
* Consider regulatory compliance requirements and industry standards that may influence RTO and RPO objectives.

1. **Identify Critical Workloads and Data**

* Conduct a thorough assessment of the application architecture to identify critical components and dependencies.
* Classify data based on its sensitivity, criticality, and importance to business operations.
* Prioritize workloads and data based on their impact on revenue generation, customer experience, and regulatory compliance.

1. **Leverage AWS Services for High Availability**

* Design your architecture to leverage AWS Regions and Availability Zones for fault tolerance and high availability.
* Utilize AWS managed services such as Amazon EC2 Auto Scaling, Amazon RDS Multi-AZ deployments, and Amazon S3 cross-region replication to distribute workloads and data across multiple availability zones or regions.
* Implement health checks, load balancing, and DNS failover mechanisms to automatically reroute traffic in the event of failure.

1. **Implement Backup and Restore Strategies**

* Define backup policies and procedures for each type of data and workload, considering factors such as retention period, frequency, and storage location.
* Utilize AWS backup services such as Amazon RDS automated backups, Amazon EBS snapshots, and Amazon S3 versioning to create point-in-time copies of your data.
* Test backup and restore procedures regularly to ensure data integrity and recoverability within the specified RTO and RPO.

1. **Test Disaster Recovery Procedures**

* Develop comprehensive disaster recovery plans that outline procedures for failover, failback, and restoration of services.
* Conduct tabletop exercises and simulated failover drills to validate the effectiveness of your disaster recovery procedures.
* Analyze the results of testing and exercises to identify areas for improvement and refine your recovery strategies.

1. **Monitor and Measure Performance**

* Implement robust monitoring and alerting mechanisms using AWS CloudWatch, AWS Config, and third-party monitoring tools.
* Define key performance indicators (KPIs) such as uptime, response time, recovery time, and data loss metrics to track the effectiveness of your recovery strategies.
* Continuously monitor and analyze performance data to identify trends, anomalies, and areas of optimization.

1. **Document and Review**

* Document your RTO and RPO objectives, architectural designs, and recovery strategies in detail.
* Maintain comprehensive documentation of configurations, procedures, and test results for auditing and compliance purposes.
* Conduct regular reviews and audits of your disaster recovery plans and infrastructure to ensure alignment with business requirements and best practices.

By following these detailed steps and leveraging AWS services and best practices, you can establish robust RTO and RPO objectives for your application on AWS infrastructure, ensuring its resilience and continuity in the face of disruptions.