**DISASTER RECOVERY WITH IBM CLOUD VIRTUAL SERVERS**

**ABSTRACT**

The project involves creating a disaster recovery plan using IBM Cloud Virtual Servers. The objective is to safeguard business operations by developing a plan that ensures continuity for an on-premises virtual machine in unforeseen events. This plan will include setting up backup strategies, configuring replication, testing the recovery process, and guaranteeing minimal downtime. The project encompasses defining the disaster recovery strategy, implementing backup and replication, validating recovery procedures, and ensuring business continuity.

**Assessment and Planning**:

* + Identify critical virtual machines (VMs) in your on-premises environment that need disaster recovery protection.
  + Define Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for each VM. These will help determine the backup and recovery strategies.
  + Assess the resources and requirements for replication, such as bandwidth and storage capacity.

**Choose IBM Cloud Virtual Server Configuration**:

* + Select IBM Cloud Virtual Server configurations that match or exceed the specifications of your on-premises VMs.
  + Determine the geographical location of the IBM Cloud data center that will host your virtual servers for disaster recovery.

**Backup Strategy**:

* + Implement regular backups of on-premises virtual machines to the IBM Cloud. You can use IBM Cloud services like IBM Cloud Backup or other backup solutions compatible with IBM Cloud.
  + Ensure that backup schedules align with your RPO requirements.
  + Test backup data integrity and retention policies.

**Replication Setup**:

* + Configure continuous data replication from your on-premises VMs to the IBM Cloud Virtual Servers. You can use tools like IBM Cloud Object Storage for data replication.
  + Set up failover mechanisms to automatically switch to the cloud VMs in case of a disaster.
  + Monitor the replication process and ensure it meets your RPO.

**Testing and Validation**:

* + Regularly test the disaster recovery process to ensure it works as expected. This includes both planned tests and drills and unannounced tests.
  + Document the steps for failover, failback, and recovery.
  + Validate that the cloud-based VMs can successfully take over the workload and data.

**Downtime Minimization**:

* + Configure load balancers and traffic management to minimize downtime during failover and failback.
  + Implement a robust DNS failover strategy to redirect traffic to the cloud VMs when needed.
  + Ensure that all dependencies and applications required for business continuity are available in the cloud environment.

**Monitoring and Alerts**:

* + Implement robust monitoring tools to keep track of the health and performance of both on-premises and cloud-based VMs.
  + Set up alerts for any anomalies or issues, and ensure that the IT team is notified promptly.

**Documentation and Training**:

* + Maintain detailed documentation of the disaster recovery plan, including configurations, contact information, and procedures.
  + Train the relevant personnel in using the disaster recovery plan and conducting tests.

**Regular Maintenance**:

* + Periodically review and update the disaster recovery plan to account for changes in your infrastructure, applications, and business requirements.
  + Keep your cloud resources up to date to ensure they meet the necessary performance and security standards.

**Compliance and Security**:

* + Ensure that your disaster recovery plan complies with industry regulations and security standards.
  + Regularly audit and assess the security of your cloud-based resources.

**ABSTRACT**

Disaster Recovery Strategy: Define the disaster recovery strategy and objectives, including recovery time objectives (RTO) and recovery point objectives (RPO). Backup Configuration: Configure regular backups of the on-premises virtual machine to capture critical data and configurations. Replication Setup: Implement replication of data and virtual machine images to IBM Cloud Virtual Servers to ensure up-to-date copies. Recovery Testing: Design and conduct recovery tests to validate the recovery process and guarantee minimal downtime. Business Continuity: Ensure that the disaster recovery plan aligns with the organization's overall business continuity strategy.

**Disaster Recovery Strategy:**

* Define the disaster recovery strategy, which should outline the overall approach to recovering from unforeseen events.
* Establish clear objectives, including Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). RTO defines the acceptable downtime, while RPO defines the acceptable data loss window.

**Backup Configuration:**

* Configure regular backups of critical on-premises virtual machines. Ensure that these backups capture not only data but also system configurations, applications, and any custom settings.
* Define backup schedules based on RPO requirements. Frequent backups reduce data loss in case of a disaster.

**Replication Setup:**

* Implement data and virtual machine image replication to IBM Cloud Virtual Servers. This should be a continuous or near-real-time process to minimize data loss.
* Ensure that the replication process is robust, reliable, and capable of handling changes in data and configurations.

**Recovery Testing:**

* Design and conduct recovery tests regularly to validate the entire recovery process. These tests can include both planned and unplanned scenarios.
* Document the step-by-step procedures for recovering from a disaster, and ensure that your IT team is trained to execute them effectively.
* Testing should involve failover to the cloud-based virtual servers, testing the applications, and ensuring data integrity.

**Business Continuity:**

* Ensure that the disaster recovery plan aligns with the organization's broader business continuity strategy.
* Coordinate with key stakeholders to define business-critical functions and prioritize their recovery.
* Establish communication plans and contact lists to ensure that all relevant personnel are informed and can respond effectively during a disaster.

Additionally, consider the following:

**Communication Plan:**

* Develop a robust communication plan that outlines how information will be disseminated to employees, customers, and other stakeholders during a disaster.

**Documentation and Compliance:**

* Maintain detailed documentation of the disaster recovery plan, including configurations, contact information, and procedures.
* Ensure that the disaster recovery plan complies with any industry regulations and security standards relevant to your organization.

**Monitoring and Alerting:**

* Implement monitoring tools and alerting systems to proactively identify issues and anomalies in your disaster recovery environment.
* Set up alerts to notify relevant personnel immediately in case of a disaster or when predefined thresholds are exceeded.

**Regular Plan Review:**

* Periodically review and update the disaster recovery plan to account for changes in your infrastructure, applications, and business requirements.

**Security Considerations:**

* Pay special attention to security during the disaster recovery process. Ensure that data is encrypted during transit and at rest, and that access controls are in place.