Disaster Recovery Plan for On-Premises Data Center

Rack of Networking Equipment and Windows Servers

1. Introduction

1.1 Purpose

The purpose of this disaster recovery plan is to outline the procedures and responsibilities to recover the networking equipment and Windows servers in the event of a disaster affecting the on-premises data center.

1.2 Scope

This plan covers the recovery of networking equipment and Windows servers hosted in the on-premises data center.

2. Risk Assessment

2.1 Identified Risks

List of potential risks:

- Hardware failure
  - *Example*: Critical networking equipment or server hardware failure leading to service disruption. This could include failures in routers, switches, or storage systems.
- Natural disasters
  - *Example*: Earthquakes, floods, or fires damaging the physical infrastructure of the data center, resulting in data loss or extended downtime.
- Power outages
  - *Example*: Prolonged power outages affecting the data center, leading to service interruptions and potential data corruption.
- Cybersecurity incidents
  - *Example*: Malware attacks, data breaches, or ransomware compromising the integrity and confidentiality of data, as well as disrupting normal operations.

3. Recovery Strategies

3.1 Backup and Restoration

Backup Strategy:

- Frequency of Backups:
  - Implement a daily backup schedule for critical data and configurations.
  - Perform incremental backups throughout the day to minimize data loss.
- Storage Location:
  - Store backups on a separate, secure storage system within the data center.
  - Utilize off-site backups for additional redundancy, ensuring data safety in case of on-site disasters.
- Backup Verification
  - Regularly test backups to ensure data integrity and the ability to restore systems.
  - Maintain a log of backup verification results for auditing purposes.

Restoration Procedures:

- Data Restoration:
  - In the event of data loss, initiate the restoration process from the latest verified backup.
  - Follow documented procedures to restore critical data to its original state.
- Server Configuration Restoration:
  - Maintain documentation detailing server configurations.
  - Utilize configuration management tools to automate server rebuilds based on predefined configurations.
- Testing and Validation:
  - Regularly conduct restoration drills to validate the effectiveness of the restoration procedures.
  - Involve relevant teams to ensure coordination and efficiency during the restoration process.

3.2 High Availability Measures

Redundant Networking Equipment:

- Hardware Redundancy:
  - Deploy redundant networking devices, such as switches and routers, to eliminate single points of failure.
  - Implement technologies like High Availability (HA) clustering for seamless failover.
- Diverse Network Paths:
  - Establish diverse network paths to ensure continued connectivity in the event of a network component failure.
  - Regularly test failover mechanisms to validate their effectiveness.

Failover Configurations:

- Server Clustering:
  - Implement server clustering for Windows servers to distribute workloads across multiple servers.
  - Configure failover clusters to automatically redirect traffic to healthy servers in case of a failure.

- Database Replication:
  - Utilize database replication for critical databases to maintain a synchronized copy on a standby server.
  - Configure automatic failover mechanisms to switch to the standby server in case of a primary server failure.

Load Balancing:

- Application Load Balancers:
  - Implement load balancing for applications to distribute incoming traffic across multiple servers.

    - Use load balancing algorithms to optimize resource utilization and ensure even distribution.
- Global Server Load Balancing (GSLB):
    - Implement GSLB to distribute traffic across multiple geographically dispersed data centers.
    - Ensure seamless failover in case of a data center outage.

4. Recovery Procedures

4.1 Emergency Response

Immediate Actions:

- Incident Detection:
    - Implement monitoring tools to detect potential disasters, such as network outages, server failures, or security breaches.
    - Set up alerts and notifications for immediate response.
- Communication Protocols:
    - Establish a clear communication plan that includes contact information for all relevant stakeholders, including IT personnel, management, and external vendors if necessary.
    - Utilize communication channels such as email, messaging platforms, and phone calls for timely updates.
- Emergency Response Team Activation:
    - Define and document roles and responsibilities for the emergency response team.
    - Activate the team promptly when a disaster is detected, ensuring that each member is aware of their responsibilities.

Initial Damage Assessment:

- Assessment Teams:
    - Form assessment teams to evaluate the extent of the damage in different areas, including networking, servers, and data storage.
    - Prioritize assessments based on criticality and potential impact on business operations.
- Documentation:
    - Document initial findings and observations, including hardware damage, data loss, or security incidents.
    - Use a standardized form or tool to ensure consistent reporting across assessment teams.
- Communication of Initial Findings:
    - Communicate initial assessment findings to the emergency response team and key stakeholders.
    - Provide clear and concise information about the status and potential impact on business operations.

4.2 Server Recovery

Recovery Steps:

- Prioritize Critical Systems:

    - Identify and prioritize critical Windows servers based on business impact and dependencies.
    - Classify servers into tiers (e.g., Tier 1 for mission-critical, Tier 2 for important, etc.).
- Restore Domain Controllers:
    - If applicable, start by restoring domain controllers to ensure proper authentication and directory services.
    - Verify the health of the Active Directory environment before proceeding.
- Recover Database Servers:
    - Restore database servers if they host critical applications, ensuring data integrity and consistency.
    - Verify database connections and dependencies on other servers.
- Application Servers:
    - Recover application servers, considering dependencies on databases and external services.
    - Configure necessary application settings and integrations.
- Web Servers:
    - Restore web servers and reconfigure web applications if applicable.
    - Test web server functionality and connectivity.
- File Servers:
    - Recover file servers and restore critical file shares.
    - Verify permissions and access controls on file resources.
- Backup Servers and Monitoring Tools:
    - Prioritize the recovery of backup servers and monitoring tools to support ongoing operations.
    - Ensure the availability of tools for continuous monitoring and alerting.

Dependencies and Validation:

- Dependency Mapping:
    - Maintain up-to-date documentation detailing server dependencies, including applications, databases, and external services.
    - Use this documentation to guide the order of server recovery.
- Validation Procedures:
    - Develop validation procedures to ensure the successful recovery of each server.
    - Conduct functional tests to verify that applications and services are operating as expected.
- Communication and Coordination:
    - Establish communication channels between teams involved in server recovery.
    - Ensure coordination with application owners, database administrators, and other relevant stakeholders.
- Rollback Plan:
    - Develop a rollback plan in case issues arise during the recovery process.

- Define criteria for determining whether a rollback is necessary, and the steps involved.

Post-Recovery Activities:

- Documentation Update:
  - Update documentation with details of the recovery process, including any deviations from the original configuration.
  - Ensure that all changes are accurately reflected in configuration management tools.
- Post-Recovery Testing:
  - Conduct post-recovery testing to validate the stability and performance of recovered systems.
  - Address any issues discovered during testing and make necessary adjustments.
- Communication of Recovery Status:
  - Communicate the status of server recovery to relevant stakeholders, including IT teams and business units.
  - Provide information on any temporary measures in place and the expected timeline for full restoration.

4.3 Networking Equipment Recovery

Recovery Steps:

- Backup Network Configurations:
  - Regularly backup configurations of networking devices, including routers, switches, and firewalls.
  - Store configurations securely, preferably offsite or in a separate location within the data center.
- Identify Primary Points of Failure:
  - Identify primary points of failure within the network infrastructure.
  - Prioritize the recovery of critical networking devices based on their impact on overall connectivity.
- Replace or Repair Faulty Hardware:
  - In case of hardware failure, replace or repair faulty networking equipment.
  - Ensure replacement devices are properly configured to align with the backup configurations.
- Configuration Restoration:
  - Use the previously backed-up configurations to restore settings on the replaced or repaired networking equipment.
  - Pay special attention to items such as IP addresses, VLAN configurations, and routing protocols.
- Connectivity Testing:
  - Conduct thorough connectivity testing to ensure proper communication between networking devices.
  - Verify that routing tables are accurate, VLANs are functioning correctly, and firewalls are allowing necessary traffic.
- External Connectivity:

- Test external connectivity by verifying internet connectivity and communication with external services.
- Confirm that VPN connections, if applicable, are restored and functioning as expected.

Documentation and Validation:

- Network Topology Documentation:
  - Maintain up-to-date documentation of the network topology, including the layout of networking devices, IP addressing schemes, and interconnections.
  - Use this documentation during the recovery process to ensure consistency.
- Configuration Management:
  - Leverage configuration management tools to automate the deployment and monitoring of networking configurations.
  - Track changes and updates to configurations to support troubleshooting and future recovery efforts.
- Connectivity Validation Procedures:
  - Develop procedures for systematic connectivity testing during and after the recovery process.
  - Include protocols for identifying and addressing any issues discovered during testing.
- Collaboration with Internet Service Providers (ISPs):
  - Establish communication channels with ISPs in advance to expedite external connectivity restoration.
  - Clearly define responsibilities and coordination procedures to streamline recovery efforts.

Post-Recovery Activities:

- Documentation Update:
  - Update network documentation to reflect any changes made during the recovery process.
  - Include details on replaced hardware, configuration adjustments, and lessons learned.
- Post-Recovery Testing:
  - Conduct post-recovery testing to validate the stability and performance of the network.
  - Address any issues discovered during testing and make necessary adjustments.
- Communication of Recovery Status:
  - Communicate the status of network recovery to relevant stakeholders, including IT teams and business units.
  - Provide information on any temporary measures in place and the expected timeline for full restoration.

5. Testing and Maintenance

5.1 Regular Testing

Testing Schedule:

- Frequency of Testing:

  - Conduct a comprehensive disaster recovery test at least annually.
  - Schedule additional targeted tests for specific components or scenarios, such as network-only tests or application-specific recovery exercises.
- Testing Window:
  - Define a specific testing window that minimizes impact on production systems.
  - Notify relevant stakeholders about the testing schedule well in advance.
- Scenario Variation:
  - Rotate through different disaster scenarios to ensure the effectiveness of recovery procedures in various situations.
  - Include scenarios such as hardware failures, cybersecurity incidents, and natural disasters.

Testing Procedures:

- Notification and Activation:
  - Simulate the detection of a disaster and initiate an emergency response plan.
  - Evaluate the effectiveness of notification processes and the prompt activation of the recovery team.
- Recovery Process Execution:
  - Execute the documented recovery procedures step by step.
  - Include both IT personnel and relevant business unit representatives to assess coordination.
- Validation of Restored Systems:
  - Validate the functionality and performance of restored systems.
  - Test critical applications, databases, and network connectivity to ensure they meet defined service levels.
- Documentation Review:
  - Review the documentation during the testing process to identify any inconsistencies or outdated information.
  - Update documentation as necessary based on the lessons learned during the test.
- Post-Test Evaluation:
  - Conduct a post-test evaluation with key stakeholders to gather feedback.
  - Identify areas for improvement, both in terms of technical procedures and communication protocols.

5.2 Updates and Maintenance

Infrastructure Changes:

- Regular Reviews:
  - Conduct regular reviews of the on-premises infrastructure to identify changes in hardware, networking equipment, and server configurations.
  - Schedule quarterly or semi-annual infrastructure reviews to capture updates and improvements.
- Configuration Management:
  - Implement configuration management tools to track changes in server configurations and networking settings.

- Integrate these tools with the disaster recovery plan to automatically update documentation.

Procedure Updates:

- Change Management Integration:
  - Integrate the disaster recovery plan with the organization's change management process.
  - Require that any changes to the production environment trigger a review and potential update of the disaster recovery plan.
- Regular Testing Insights:
  - Use insights from regular testing exercises to identify areas for improvement in the recovery procedures.
  - Update the plan based on lessons learned from testing experiences.

Documentation and Communication:

- Document Control:
  - Establish a version control system for the disaster recovery plan documentation.
  - Clearly document changes, including the date of modification and a brief description of updates.

- Communication Channels:
  - Maintain open communication channels with relevant teams, including IT operations, system administrators, and business units.
  - Encourage feedback and insights that can contribute to the continuous improvement of the plan.