Disaster Recovery Site Setup and Test Procedures

Shaunak Patel

Applied Network Infrastructure and System Administration, Conestoga Collage

Prof. Ronak Patwa

Table of Contents

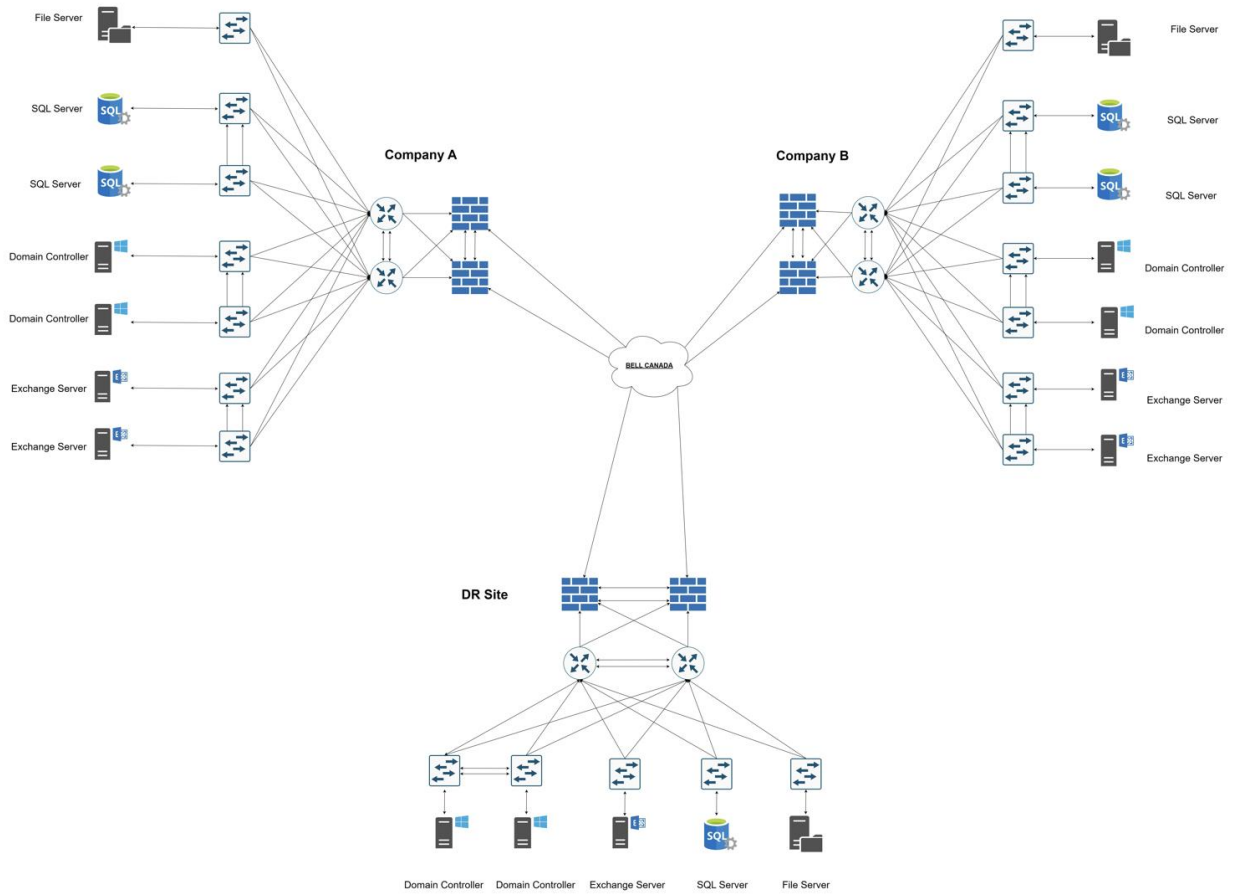
INTRODUCTION

In the strategic collaboration between Company A and Company B, a pivotal initiative is to enhance Company A's resilience in a region to frequent natural disasters, encompassing challenges such as power outages, flooding, and network disruptions. Company A's existing infrastructure is comprised of 2 Windows Server 2016 instances, 2 Exchange Server 2013 installations on Windows Server 2016, 2 SQL Server 2017 setups on Windows Server 2016, and a file server operating on Windows Server 2016. Recognizing the critical need for a robust disaster recovery plan, our proposed solution involves the deployment of a comprehensive infrastructure: 2 Windows Server 2016 machines, 1 Exchange Server 2013 on Windows Server 2016, 1 SQL Server 2017 on Windows Server 2016, and 1 file server on Windows Server 2016.

This comprehensive document not only includes a detailed network architecture diagram illustrating the interconnections and redundancies but also provides an IP addressing table for precise configuration details. Hardware requirements are outlined, ensuring compatibility and optimal performance for each component of the disaster recovery infrastructure. Furthermore, the procedural guidelines within the document offer a step-by-step roadmap for the implementation of the disaster recovery plan, covering everything from initial setup to ongoing maintenance and testing protocols.

Recognizing that successful integration goes beyond technical specifications, the document places a significant emphasis on building trust and collaboration between Company A and Company B. This holistic approach not only ensures the technical feasibility of the disaster recovery plan but also cultivates a culture of resilience, cooperation, and shared responsibility between the two entities.

Network Diagram:



IP Breakdown:

Company A:

Server	Hostname	IP Address	Subnet Mask
Domain Controller 1	WS_1	10.10.10.2	255.255.255.0
Domain Controller 2	WS_2	10.10.10.3	255.255.255.0
Exchange Server 1	ES_1	10.10.10.4	255.255.255.0
Exchange Server 2	ES_2	10.10.10.5	255.255.255.0
SQL Server 1	SQL_1	10.10.10.6	255.255.255.0
SQL Server 2	SQL_2	10.10.10.7	255.255.255.0
File Server	FS_1	10.10.10.8	255.255.255.0

Company B:

Server	Hostname	IP Address	Subnet Mask
Domain Controller 1	WS_3	10.10.10.9	255.255.255.0
Domain Controller 2	WS_4	10.10.10.10	255.255.255.0
Exchange Server 1	ES_3	10.10.10.11	255.255.255.0
Exchange Server 2	ES_4	10.10.10.12	255.255.255.0
SQL Server 1	SQL_3	10.10.10.13	255.255.255.0
SQL Server 2	SQL_4	10.10.10.14	255.255.255.0
File Server	FS_2	10.10.10.15	255.255.255.0

Disaster Recovery Site:

Server	Hostname	IP Address	Subnet Mask
Domain Controller 1	WS_5	10.10.10.16	255.255.255.0
Domain Controller 2	WS_6	10.10.10.17	255.255.255.0
Exchange Server	ES_5	10.10.10.18	255.255.255.0
SQL Server	SQL_5	10.10.10.19	255.255.255.0
File Server	FS_3	10.10.10.20	255.255.255.0

New Hardware for Site B:

- Windows Server 2016
    - Model: Dell PowerEdge R750.
    - Processor: Dual Intel Xeon Gold 6254.
    - RAM: 256GB DDR4 ECC.
    - Storage: 2x 1TB SSD (RAID 1) for OS, 4x 2TB SAS (RAID 10) for applications.
- Exchange Server
    - Model: HPE ProLiant DL360 Gen10.
    - Processor: Dual Intel Xeon Silver 4210.
    - RAM: 384GB DDR4 ECC.
    - Storage: 2x 480GB SSD (RAID 1) for OS, 8x 2TB SAS (RAID 10) for mailbox databases.
- SQL Server
    - Model: Dell PowerEdge R740.
    - Processor: Dual Intel Xeon Gold 6248.
    - RAM: 512GB DDR4 ECC.
    - Storage: 2x 800GB NVMe SSD (RAID 1) for OS, 6x 4TB SAS (RAID 5) for databases.
- File Server
    - Model: Dell PowerEdge R540.
    - Processor: Single Intel Xeon Silver 4210.
    - RAM: 128GB DDR4 ECC.
    - Storage: 2x 480GB SSD (RAID 1) for OS, 8x 4TB SAS (RAID 10) for file data.

Hardware Selection For DR Site:

Networking Equipment

- Switches: Cisco Catalyst 9300 Switches. It has better throughput, Orchestrate role-based access feature and so on. (Benefits of Upgrading to Cisco Catalyst 9300 Series Switches Feature Comparison, 2023)
- Routers: Cisco ISR 4351 Routers. It has increased bandwidth, WAN traffic management and so on. (Cisco 4351 Integrated Services Router, 2023)

- Firewalls: Palo Alto Networks PA-220.
- Load Balancer: F5 BIG-IP i7800.

Rack Equipment

- Server Rack: APC NetShelter SX 42U Server Rack.
- Power Distribution: APC Rack PDU.
- Cooling: APC InRow DX Precision Cooling.

Server Requirements

- Windows Server
    - Model: Dell PowerEdge R750.
    - Processor: Dual Intel Xeon Gold 6254.
    - RAM: 256GB DDR4 ECC.
    - Storage: 2x 1TB SSD (RAID 1) for OS, 4x 2TB SAS (RAID 10) for applications.
- Exchange Server
    - Model: HPE ProLiant DL360 Gen10.
    - Processor: Dual Intel Xeon Silver 4210.
    - RAM: 384GB DDR4 ECC.
    - Storage: 2x 480GB SSD (RAID 1) for OS, 8x 2TB SAS (RAID 10) for mailbox databases.
- SQL Server
    - Model: Dell PowerEdge R740.
    - Processor: Dual Intel Xeon Gold 6248.
    - RAM: 512GB DDR4 ECC.
    - Storage: 2x 800GB NVMe SSD (RAID 1) for OS, 6x 4TB SAS (RAID 5) for databases.
- File Server
    - Model: Dell PowerEdge R540.
    - Processor: Single Intel Xeon Silver 4210.
    - RAM: 128GB DDR4 ECC.
    - Storage: 2x 480GB SSD (RAID 1) for OS, 8x 4TB SAS (RAID 10) for file data.

Redundancy and High Availability:

- Power Supplies: Redundant power supplies for all servers.
- Network Connections: Redundant network interfaces for all servers.
- Network Switch Modules: Redundant switch modules for servers supporting multiple network connections.

Site A to Disaster Recovery Site Setup:

Network Connectivity:

To connect company A and disaster recovery site we are using MPLS technology. The reason for using this technology to connect these two sites is it's an more efficient, scalable and consistent way to forward our data. MPLS has advantages like enhanced security, optimized WAN performance, compatibility with legacy systems and many more. Apart from this we can easily manage and monitor issues like latency, packet loss and another performance issues between sender and destination compared to VPN. For implementing MPLS technology to connect company A and Disaster Recovery Site we are doing collaboration with Bell Canada. Below is basic steps to implement MPLS for both sites.

Implementation of MPLS:

- Order MPLS service from bell Canada. Here we have to specify location of Company A site and Disaster Recovery site. Specify bandwidth as 10 GBps fiber cable. (Scarpati, 2021)
- Then Bell Canada will setup their router at both sites and give required details to connect their router to our network.
- Afterwards, configure Muti Protocol BGP and enable LDP on all the interfaces of router for both sites.
- On external interfaces where we are going to connect our network configure VRF.

(Perkin, 2023)

Data Replication and Backup:

To achieve high availability while facing natural disaster we are using data replication and backup method. Data replication is a method in which we are copying data of company A to another location which is disaster recovery site. By having multiple up-to-date copies of data it won't be obsolete in case of natural disaster and we can recover it. (Raffo, 2019)

Data Replication Configuration:

Windows Server:

- Implement Windows Server Failover Clustering to ensure high availability.
- Configure shared storage for the cluster and enable the necessary features.
- Enable Cluster-Aware Updating to facilitate updates without downtime.

- Schedule regular updates to maintain security and performance.

Exchange Server:

- Set up Database Availability Groups for Exchange Server to enable database replication.
- Add mailbox databases to DAGs for automatic failover.
- Configure log shipping to replicate transaction logs between mailbox servers.
- Monitor and manage the replication process to ensure consistency.

SQL Server:

- Implement AlwaysOn Availability Groups to enable database replication and failover.
- Configure synchronous data replication based on recovery objectives.
- Utilize transactional replication for specific databases requiring real-time data synchronization.

File Server:

- Implement DFS for file server data replication across multiple servers.
- Configure replication schedules and bandwidth usage.

Data Backup Configuration:

Windows Server:

- Use Windows Server Backup to create regular full system backups.
- Configure backup schedules to ensure critical data is backed up consistently.
- Enable and configure volume shadow copy service for creating point-in-time snapshots of volumes.
- Schedule VSS snapshots to capture changes at regular intervals.

Exchange Server:

- Use built-in Exchange tools for regular database backups.
- Schedule full and incremental backups to capture mailbox changes.
- Enable item-level recovery to restore individual mailbox items without restoring the entire database.

SQL Server:

- Set up regular full and differential backups using SQL Server Backup.
- Consider backup compression to optimize storage usage.
- Create SQL Server Maintenance Plans to automate backup, integrity checks, and index optimization tasks.

File Server:

- Use Windows Server Backup to perform regular file-level backups.
- Schedule backups to capture changes in file server data.

Disaster Recovery Plan:

Failover Procedure:

Windows Server:

- Redirect Traffic
    - Update DNS records to point to the disaster recovery site.
    - Configure load balancers to redirect incoming traffic.
- Activate Failover Cluster
    - Windows Server Failover Clustering, initiate a failover to the disaster recovery site.
    - Monitor cluster status to ensure successful failover.
- Application and Service Validation
    - Validate the functionality of critical applications and services.
    - Test client access and ensure that all required services are running.

Exchange Server:

- Activate Database Availability Group (DAG)
    - Initiate a failover of the Database Availability Group (DAG) to the disaster recovery site.
    - Verify the status of mailbox databases on the failover server.
- Update DNS and Client Access
    - Update DNS records to reflect the new location of the Exchange Server.
    - Ensure that client access points are redirected to the disaster recovery site.
- Monitoring and Verification
    - Monitor the health of the Exchange environment.
    - Verify that email services are fully operational, and mail flow is restored.

SQL Server:

- Activate AlwaysOn Availability Groups
    - Initiate a failover to the disaster recovery site.
    - Monitor the status of database replicas to ensure synchronization.
- Update Connection Strings

    - Update connection strings in applications to point to the disaster recovery SQL Server instance.
    - Validate that applications can connect to the failover SQL Server.
- Testing Database Access
    - Execute test queries on databases to ensure data availability.
    - Validate that applications relying on SQL Server data function as expected.

File Server:

- Update Network Configuration
    - Update network configurations to redirect file access to the disaster recovery site.
    - Modify DNS records to reflect the new file server location.
- Activate DFS Replication
    - Initiate a failover to the disaster recovery server.
    - Monitor DFS replication status to ensure data synchronization.
- User Communications
    - Communicate with users and provide updated file access instructions.
    - Address any user-specific concerns or issues related to the failover.

Data Restoration Procedure:

Windows Server:

- Restore from Backup
    - Use Windows Server Backup to restore data.
    - Follow the restoration procedures for each specific server role.
- Post-Restoration Checks
    - Validate the integrity of the restored data.
    - Ensure that all applications and services are functional.

Exchange Server:

- Mailbox Database Restoration
    - Use the chosen backup solution to restore mailbox databases.
    - Verify the completeness of the database restoration process.
- Individual Mailbox Restoration
    - Perform individual mailbox restorations if needed.
    - Verify the accuracy of the restored mailbox data.

SQL Server:

- Database Restoration

    - Restore databases using SQL Server Backup.
    - Confirm the successful restoration of databases.
    - Validate the consistency of the recovered databases.

File Server:

- File System Restoration
    - Use Windows Server Backup tool to restore file system.
    - Confirm the completeness of the file restoration process.
- Permissions and Access Checks
    - Validate file permissions and access rights post-restoration.
    - Test user access to files and directories.

Disaster Recovery Test Procedure:

Windows Server:

- Initiate a failover of the application server to the disaster recovery site using the designated failover procedure.
- Monitor server status and services to ensure successful failover.
- Validate connectivity by accessing the application from a test client.
- Confirm that the application functions correctly at the disaster recovery site.

Exchange Server:

- Initiate a failover of the Exchange Server mailbox database to the disaster recovery site.
- Validate that clients can connect to the mailbox server and access emails.
- Simulate a data corruption scenario and initiate recovery from backups.
- Confirm that recovered emails and mailbox contents are accurate.

SQL Server:

- Initiate a failover of the SQL Server databases to the disaster recovery site.
- Execute test queries to validate the functionality of applications relying on the databases.
- Simulate a data loss scenario and perform a point-in-time recovery.
- Confirm the accuracy and consistency of recovered data.

File Server:

- Initiate a failover of the file server to the disaster recovery site.
- Validate user access to files and directories.
- Simulate a file deletion scenario and restore files from backups.

- Confirm the successful restoration of file data.

Company A to Company B Trust:

Details on Trust Setup Between Company A and B:

Configuration in Site A's Domain Controller:

- On a Domain Controller in Site A, open "Active Directory Domains and Trusts" from Administrative Tools.
- Right-click on the domain node for Domain A, select "Properties."
- Go to the "Trusts" tab and click "New Trust."
- Follow the wizard to create an outgoing trust to Domain B.
- Specify the DNS name of Domain B and complete the wizard.
- After creating the trust, verify it by right-clicking on the domain node for Domain A, selecting "Properties," and navigating to the "Trusts" tab.

Configuration in Site B's Domain Controller:

- On a Domain Controller in Site B, open "Active Directory Domains and Trusts."
- Right-click on the domain node for Domain B, select "Properties."
- Go to the "Trusts" tab and click "New Trust."
- Follow the wizard to create an incoming trust from Domain A.
- Specify the DNS name of Domain A and complete the wizard.
- After creating the trust, verify it by right-clicking on the domain node for Domain B, selecting "Properties," and navigating to the "Trusts" tab.

Verification:

- Use the "Domains and Trusts" console to validate the trust from both sides.
- Confirm that the trust status is "Verified" for both incoming and outgoing trusts.
- Test access to resources between domains. Ensure that users from Domain A can access resources in Domain B and vice versa.

Details on DNS Requirement for Trust Establishment:

Establishing trust between two Active Directory (AD) domains requires proper DNS configuration to ensure name resolution and seamless communication between the domains.

Prerequisites

- Ensure that both forward (name to IP) and reverse (IP to name) DNS resolution is functional in both domains.
- Confirm that the primary DNS suffix is correctly configured on all domain-joined computers in both domains.

DNS Configuration in Site A:

- In the DNS Manager on a Domain Controller in Domain A, confirm the presence of the AD-integrated forward lookup zone for Domain A.
- Ensure that the zone is configured to replicate to all DNS servers in the AD domain.
- Create a conditional forwarder in DNS Manager for Domain B in Domain A.
- Configure the conditional forwarder to forward DNS queries for Domain B to the DNS servers in Domain B.
- Confirm that the Name Server (NS) records for Domain A are correctly registered in the DNS zone of Domain B.

DNS configuration in Site B:

- In the DNS Manager on a Domain Controller in Domain B, confirm the presence of the AD-integrated forward lookup zone for Domain B.
- Ensure that the zone is configured to replicate to all DNS servers in the AD domain.
- Create a conditional forwarder in DNS Manager for Domain A in Domain B.
- Configure the conditional forwarder to forward DNS queries for Domain A to the DNS servers in Domain A.
- Confirm that the NS records for Domain B are correctly registered in the DNS zone of Domain A.

In firewall of both sites add new rule for UDP and TCP port 53 to allow traffic between both sites in both directions.

Conclusion

This comprehensive document outlines Company A's resilient disaster recovery setup, acknowledging the region's susceptibility to natural disasters. To connect both sites we are using MPLS technology which more efficient way for network connectivity. Addressing power outages, flooding, and network disruptions, the plan incorporates technologies such as failover clusters, DAG for Exchange, AlwaysOn Availability Groups for SQL, and DFS for file servers. Backed by a robust backup strategy encompassing full and differential backups, the document guides failover procedures, redirecting traffic seamlessly to the disaster recovery site for uninterrupted operations. Data restoration procedures for each server and detailed hardware requirements for the disaster recovery site provide a thorough understanding of infrastructure needs. The document emphasizes proactive testing procedures to identify and address weaknesses regularly. Additionally, it highlights the establishment of a trust relationship between Company A and Company B, supported by DNS configurations, fostering secure resource sharing and collaboration. In essence, this document contains Company A's strategic and collaborative approach to disaster recovery, ensuring operational continuity and safeguarding critical data in challenging environmental conditions.

References

Cisco 4351 Integrated Services Router. (2023, April 26). Cisco. https://www.cisco.com/c/en/us/support/routers/4351-integrated-services-router/model.html

Benefits of Upgrading to Cisco Catalyst 9300 Series Switches Feature comparison. (2023, August 17). Cisco. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-upgrading-cat-9300-fc-cte-en.html

PA-220 Firewall Overview. (n.d.). https://docs.paloaltonetworks.com/hardware/pa-220-hardware-reference/pa-220-firewall-overview

Perkin, R. (2023, January 26). *MPLS Configuration Tutorial » Cisco [Step by Step]*. Roger Perkin. https://www.rogerperkin.co.uk/ccie/mpls/cisco-mpls-tutorial/

Scarpati, J. (2021, June 24). *How to calculate network bandwidth requirements*. Networking. https://www.techtarget.com/searchnetworking/tip/How-to-calculate-network-bandwidth-requirements

Raffo, D. (2019, October 29). *Data replication technologies: What they are and how to use them*. Disaster Recovery. https://www.techtarget.com/searchdisasterrecovery/tutorial/Data-replication-technologies-and-disaster-recovery-planning-tutorial

J. (2023, March 16). *Create a failover cluster*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster

A. (2023, February 22). *Create a database availability group*. Microsoft Learn. https://learn.microsoft.com/en-us/exchange/high-availability/manage-ha/create-dags?view=exchserver-2019

Step-By-Step: Creating a SQL Server Always On Availability Group. (n.d.). TECHCOMMUNITY.MICROSOFT.COM. https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-creating-a-sql-server-always-on-availability-group/ba-p/648772#:~:text=The%20following%20steps%20will%20enable%20the%20Always%20On,OK%20when%20prompted%20to%20restart%20the%20Server%20service.

M. (2023, September 27). *What is an Always On availability group? - SQL Server Always On*. Microsoft Learn. https://learn.microsoft.com/en-us/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sql-server?view=sql-server-ver16

J. (2023, March 28). *DFS Replication overview*. Microsoft Learn. https://learn.microsoft.com/en-us/windows-server/storage/dfs-replication/dfsr-overview

J. (2023, November 27). *How trusts work for Microsoft Entra Domain Services - Microsoft Entra ID*. Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/domain-services/concepts-forest-trust