IT Technical Support Final Project

System Administration Consultation

Scenario:

Civil Registry Government

Team Members:

Mohamed Ibrahiem

Moamen Elsayed

Youssef Taher

Hassan Mostafa

Omar Mosoud

Date: 5/10/2024

1. Introduction

This report outlines the improvements made to the IT infrastructure of the Civil Registry Government agency located in Alexandria, Egypt. The project aimed to enhance network security, improve system performance, and ensure compliance with government regulations. The agency was facing challenges such as outdated systems, lack of security protocols, and insufficient infrastructure to handle increasing demands.

We implemented several changes using Windows Server and Windows 10 through Hyper-V. These changes focused on user management, file sharing, network security, and system policies. Additionally, network components like switches and firewalls were added to further secure and optimize the system.

2. Scenario Overview

The Civil Registry Government agency is responsible for issuing certificates and ID cards to the local population. The current infrastructure includes:

Network: One router with a visible SSID and no advanced security settings.

Devices: Two PCs used by a small number of employees.

Servers: Cloud-based database connections, but unsecured.

Data Backup: No backup system in place.

Employees: Eight employees, only three of whom use PCs.

Our goal was to address security vulnerabilities, improve the IT infrastructure, and establish a scalable system for future needs. Additionally, implementing network components such as switches and firewalls was critical for enhanced performance and security.

3. Improvements Made

3.1 User Management

We created a total of four users on Windows Server and Windows 10 machines using Hyper-V:

Two users for managing certificates.

Two users for managing ID cards.

The users were assigned to specific groups to restrict access based on their roles:

For certificates, we created:

1. **Certificates Read and Write Group:** Members in this group can read and write certificate files.

2. **Certificates Read-Only Group:** Members in this group can only read certificate files.

For ID cards, we created:

1. ID Cards Read and Write Group: Members in this group can read and write ID card files.

2. ID Cards Read-Only Group: Members in this group can only read ID card files.

The four users were assigned as follows:

One user was added to the Certificates Read and Write group.

One user was added to the Certificates Read-Only group.

One user was added to the ID Cards Read and Write group.

One user was added to the ID Cards Read-Only group.

3.2 File Sharing and Security

We shared the Certificates and ID Cards folders from the server and configured sharing and security permissions to ensure that:

Each user can only access the files assigned to their role.

Users cannot perform actions (read/write) outside of their permissions.

This was achieved by setting up:

NTFS Permissions: On each folder, we configured specific access rights (read, write) for each group.

Shared Folder Permissions: The shared folders were configured to prevent unauthorized access.

3.3Data Backup Implementation

As mentioned in the scenario, there was no backup system in place. To address this, we implemented an Incremental Backup solution, which ensures that data is backed up regularly with minimal system strain. Incremental backups were configured to save only the changes made since the last backup, optimizing storage and reducing the time needed for backups.

This solution not only secures critical data but also ensures the ability to recover from potential data loss.

3.4Network Security and Components

We implemented several network security measures and added key infrastructure components:

Hiding the SSID: The network SSID was hidden to prevent unauthorized devices from easily discovering the network.

Adding a Switch: A new switch was added to support additional devices and enhance network performance.

Installing a Firewall: A firewall was configured to provide an additional layer of security, ensuring that unauthorized access to the network is blocked.

Blocking Internet Access: Users were restricted from accessing the internet to maintain focus on their tasks and improve security.

Disabling USB Access: USB access was disabled on user computers to prevent the introduction of unauthorized external storage devices.

3.5 Group Policy Implementation

We configured several Group Policies (GPOs) as per the scenario to manage system settings:

Network Access Policies: Configured to prevent unauthorized access to the internal network.

USB Device Policies: Set policies to block the use of USB drives on user machines, ensuring no external devices can be connected.

Internet Access Policies: Policies were implemented to block internet access for all users except administrators.

Hide C: Drive from Users: We also implemented a policy to hide the C: drive from users, ensuring they cannot access or modify system files or directories not related to their tasks.

Additionally, we applied the incremental backup policy to ensure that important data is regularly backed up with minimal system strain, as mentioned in the scenario.

3.6 Active Directory and Domain Controller Setup

We introduced Active Directory (AD) to centralize user and device management, enabling streamlined control of user permissions, roles, and access to shared resources.

A Domain Controller (DC) was set up as the central point for managing the AD infrastructure, providing secure authentication for users and enforcing group policies. This ensures that all user interactions with the system are controlled and monitored.

3.7 Layer 3 Switch and VLAN Configuration

To organize network traffic and enhance security, we introduced a Layer 3 Switch, which allows routing between VLANs (Virtual Local Area Networks) to ensure efficient communication between different parts of the network.

We divided the network into several VLANs based on the devices used by each department:

1. VLAN 1 - Management Network:

Devices: Computers used by management and high-level staff like the IT team.

Purpose: Designed for employees who need access to sensitive resources and important data.

2. VLAN 2 - Certificates Department Network:

Devices: Computers used for handling certificates.

Purpose: Dedicated to devices that manage certificates to protect sensitive citizen data.

3. VLAN 3 - ID Cards Department Network:

Devices: Computers used for managing and issuing ID cards.

Purpose: Isolated from other departments to enhance security for identity management.

4. Challenges and Solutions

4.1 Legacy Systems

The agency was using outdated systems that were difficult to upgrade. We addressed this by creating a phased modernization plan where new systems would be introduced gradually without disrupting daily operations.

4.2 Scalability

Given the agency's growing needs, we ensured that the IT infrastructure could be easily scaled by using virtual machines (VMs) through Hyper-V, making it easier to add new users and devices as required.

4.3 Compliance

Ensuring compliance with government regulations was critical. We conducted compliance audits and adjusted the security settings (hiding SSID, adding firewalls, restricting file access) to meet the required standards.

5. Conclusion

The improvements made to the Civil Registry Government's IT infrastructure enhanced overall security, streamlined operations, and ensured compliance with governmental standards. By setting up user groups, managing file permissions, and implementing strict security policies, we minimized the risk of unauthorized access to sensitive data. The addition of critical network components like switches and firewalls also ensured optimal performance and security. Additionally, the scalable infrastructure allows for future growth without compromising security or efficiency.

6. Recommendations for Future Enhancements

Continuous Monitoring: Implement network monitoring tools to regularly check for potential security breaches.

Employee Training: Provide regular training for employees on security best practices and the importance of data protection.

System Updates: Ensure that both software and hardware systems are regularly updated to maintain optimal performance and security.