Network Infrastructure Deployment Project

Emma Julien

SVAD 121-51P

May 6th, 2025

Table of Contents:

Executive Summary:

The project described seeks to develop and deploy a secure and functional IT network for a vertically integrated sales and manufacturing company with seventy five employees and roughly forty PC's. The goal of this is to develop dependable infrastructure of a network that is able to overall improve day-to-day operations for the company, allows for growth, and provides additional security measures. From the implementation of new centralized management protocols, with specific file access for each department, deployment of automatic system updates, and reliable remote access, the company will see improvements in their productivity, a significant lack of downtime when issues occur, and additional support.

The objectives of this project are to provide and deploy a full domain based network, implement department local file sharing, network printers,automatic update control, and a backup system for restoring critical data critical to the company. Employees will have access to any company resources they may need in a secure and remote way, which will improve company productivity and flexibility. Each phase of implementation will go through rigorous amounts of testing to ensure that everything will continue to run smoothly.

There is not a project without some sort of risk associated with it. The risks for this implementation could potentially be several temporary service disruptions throughout the deployment process, however these challenges will be dealt with through scheduling, thorough employee training, and continuous system or network backups. There are costs associated with this project, as well. The benefits of this implementation greatly outweigh the associated costs that may be associated with it such as purchasing the software or licensing if this has not already been purchased, any hardware necessary, and potential security that will be discussed below. These short term costs are overall covered when the long term effects are thought about due to the reduced regular maintenance the network will need, the higher level of protection for the company's data, and the new ability for the company to have scalable growth for the future.

The goal is to have this project implementation take place over a roughly six week time frame, including the planning, testing, and finally the full deployment phase. Once the deployment takes place, and all the proper testing has been completed, the company will have a network that is more reliable, secure, and efficient to use on a day to day basis.

Business Scenario

The company requesting the new IT network infrastructure is a vertically integrated company with roughly seventy five staff members with around forty PC's, which means the business has grown to where the current infrastructure in place will no longer support the company's needs effectively. There isn't a centralized file system currently, and teams are unable to have secure ways to store their data specific to their departments. During the current era, where more and more employees begin to desire remote work, employees must have access to their data from a secure and remote location, while also allowing for additional growth of the company.

Solution Request

The company has requested a new and improved network infrastructure to do continuous growth, and requires a more stable and secure way to access their data, and have a more manageable IT system in order to support the company. The current system lacks organization, data and file accessibility and security, the ability for remote connection, decentralized user management, and automatic updates for the system. Providing and implementing a centralized domain structure with the implementation of Active Directory, new organization units, or OU's, and new group policies that will allow for increased security and simplify the overall user experience. There will also be a new file print server, which will have specific department permissions, a secure remote access ability, and a recovery system in order to prevent long term outages.

High Level Approach

The intention of this project is to provide and implement an IT infrastructure that has the ability to provide for the new company needs and daily operations. This would entail setting up a centralized domain structure through Active Directory in order to be able to manage users and any devices safely and securely. Essential processes, such as, print and file sharing, auto updates, encryption of any data necessary, and a secure way to access the network remotely, will be implemented according to the company's needs. Group policies will also be implemented so settings are standard across the board. This solution provides a solid foundation from which the company will be able to grow in the future.

Technical Architecture

This network implementation is being done as a completely on premises solution using all Windows Servers technology. All services, such as Active Directory, file sharing, printer sharing and management, and automatic updates, will be hosted at the company itself rather than in the cloud. Deciding to go with a totally online approach was a decision made to avoid the costs that come with maintaining cloud services and to prevent an overly complicated first network.

Windows Server 2022 is making up the server infrastructure, which would include Active Directory, DNS and DHCP servers in order to maintain network control, and Windows Server Update Services to perform regular system updates. File and print sharing and management was handled through Windows roles already provided with the OS. Then the group policies will implement the security protocols which allows these to be easily maintained and familiar.

Project Management Approach

From a project management approach, the implementation is broken down into three different milestones or phases of the process. Each one has a specific set of goals and focuses on a specific technical grade and builds upon the previous milestone or phase.

1. Milestone/Phase 1: This phase mainly focuses on laying down the foundation for the whole network. This includes setting up the domain server, configuring the DNS and DHCP settings, establishing a baseline rule for the naming conventions, and preparing for future workstation deployment.
2. Milestone/Phase 2: This phase builds upon the previous foundation built in phase 1 by implementing file and print servers, and establishing their user permissions, and configuring the main group policies. This phase ensures that security of data is ensured.
3. Milestone/Phase 3: This phase has the most advanced services being implemented. Once again, building on the previous two phases already implemented, this includes installing and setting up centralized system updates, file encryptions, backup and any recovery planning, and plans for monitoring in order to set a baseline for the environment performance.

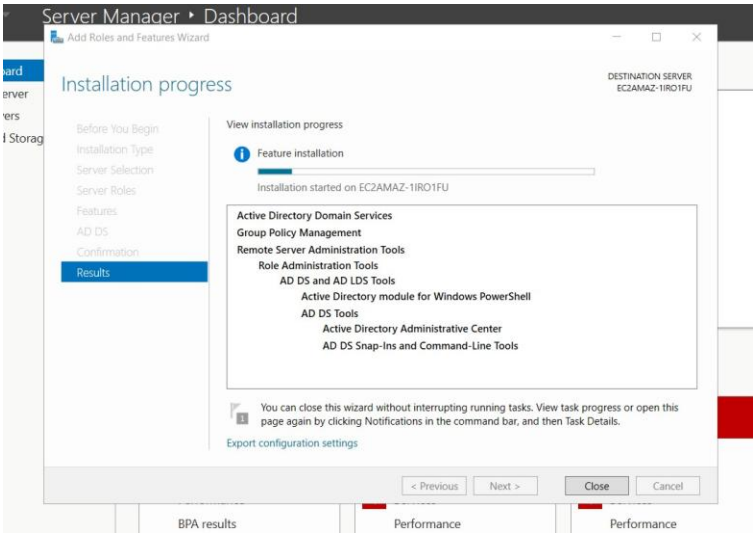
Each phase requires detailed planning, configuration, testing, and thorough documentation in order to verify that every task is completed effectively.

Technical Documentation

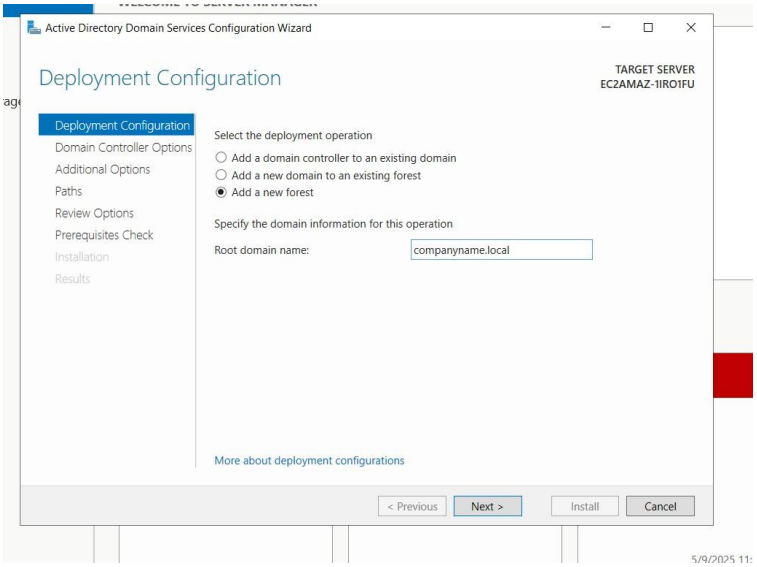
Phase/Milestone 1:

Domain Setup: The goal of the domain setup is to establish a centralized Active Directory domain in order to manage all users and any resources.

- Install Active Directory Domain Services
- Server Manager - Add Roles and Features
- Check the box for Active Directory Domain Services and hit next on the wizard until install is an option.



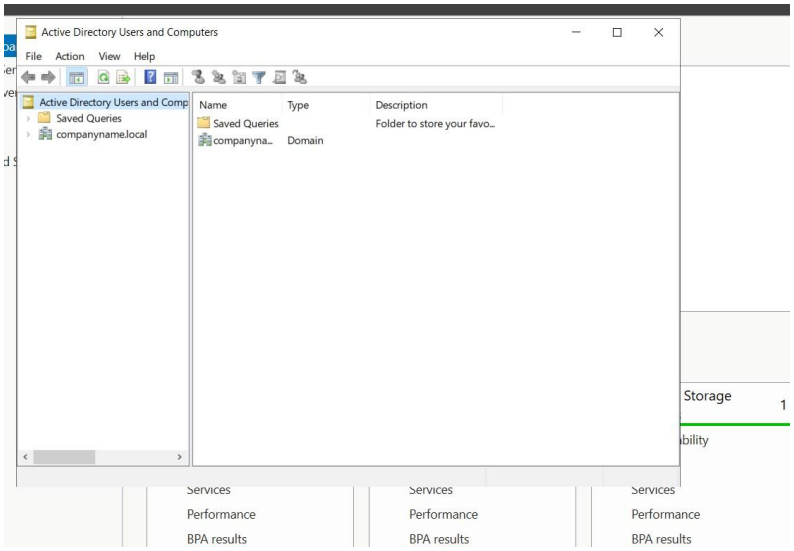
- Promote this server to a domain controller
- Click the notification flag in the top right of server manager and select promote this server to a domain controller.
- Select add a new forest in the wizard, and set the root domain to companyname.local. (Since no name for the company was provided I used generic ones for the setup.)
- Set a Directory Services Restore Mode, or DSRM password to finish the wizard - in this example Pa55w.rd was used.



Organization Unit Structure:

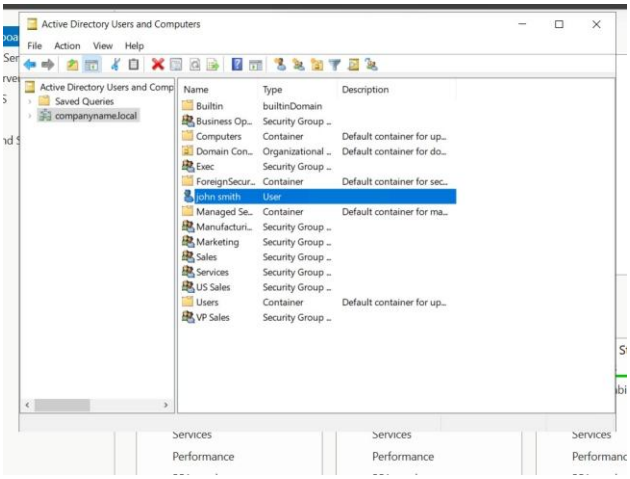
The goal of implementing organizational units is to promote efficient management for the company.

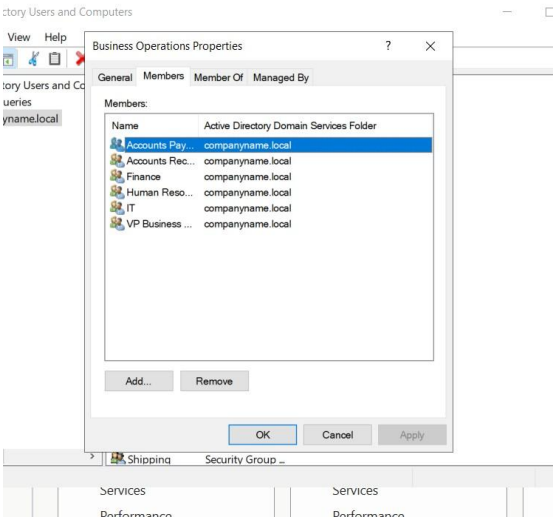
- Create OUs for both users and computers.
- Select Active Directory Users and Computers
- Right-click on domain root and select new and then organizational unit.



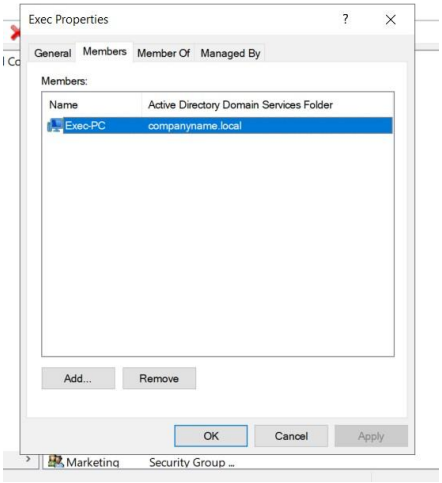
- Create the following OU structure
- Groups for Sales, Marketing, Exec, and Business Operations

- Within the sales group include groups for VP sales, US Sales, Marketing, and Service. (The reason we keep VPs as a group instead of a user is for easy turnover if necessary.)
- Now repeat for the Marketing and Business Operations groups
- Within the marketing groups, create groups for VP Marketing, shipping, receiving, receiving2, and parts.
- Within the business operation group, create groups for VP Business Operations, Finance, IT, Human Resources, Accounts Receivable, and Accounts Payable.
- Individual Users will be added to these groups, for example, the CEO would be added to the Exec group.



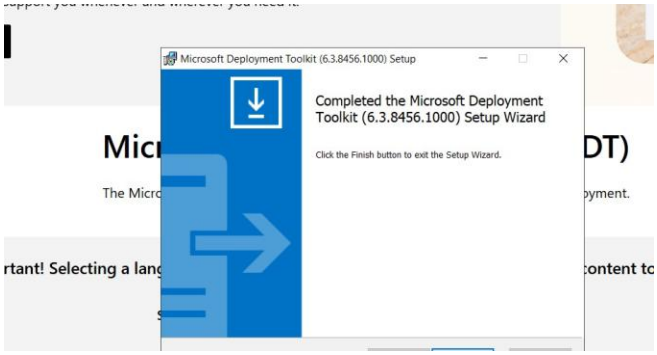


- Then add PCs for each one of these groups and use the naming function of groupname-pc and add them to the coordinating group.

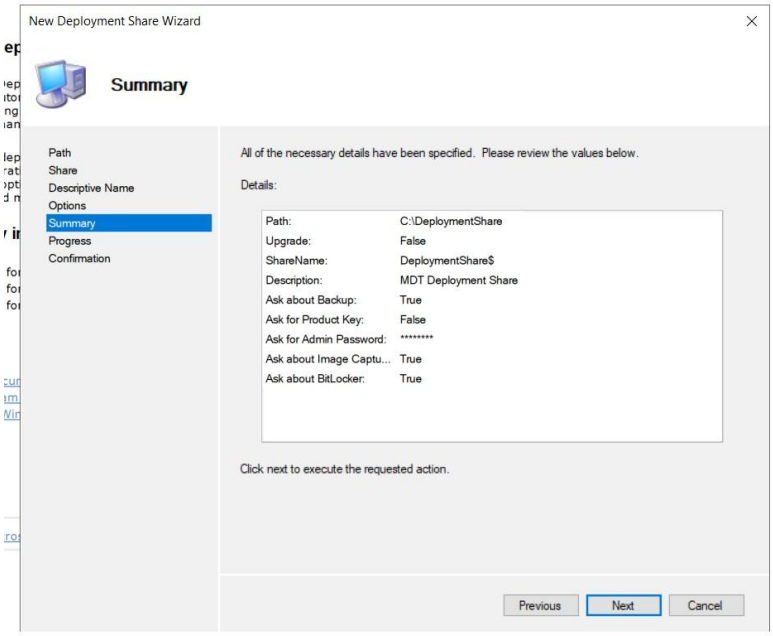


Workstation Imaging and Deployment:

- Microsoft Deployment Toolkit
- Navigate to the microsoft website and download and install MDT - you will need windows 10 adk installed to make this possible to install properly.



- Create a deployment share
- Open the deployment workbench
- Right click on deployment shares and select new deployment share - Follow the wizard leaving the default in the system.

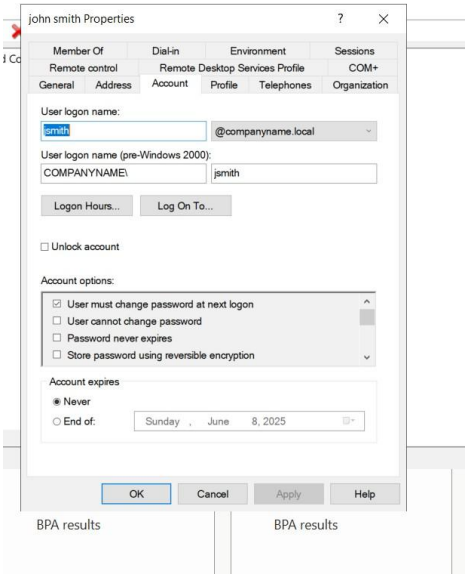


- Add an operating system
- Right click on operating systems under the deployment share that was just created.
- Select import operating system (note: you will need to have an OS ISO file in a folder available to set this up - download windows 10 from microsoft if necessary)
- Specify the path to the file with the ISO in it.

- Add applications
- Right click applications and select the one that says new application.
- Select the source files and click finish
- Create task sequence
- Right click task sequence and select create new task sequence.
- Specify the task sequence ID, name, and then select the OS you want to use and any applications that must be installed.
- Configure Deployment Settings
- Right click deployment shares and select properties.
- Configure the settings for boot images, rules, and scripts.

Naming Conventions:

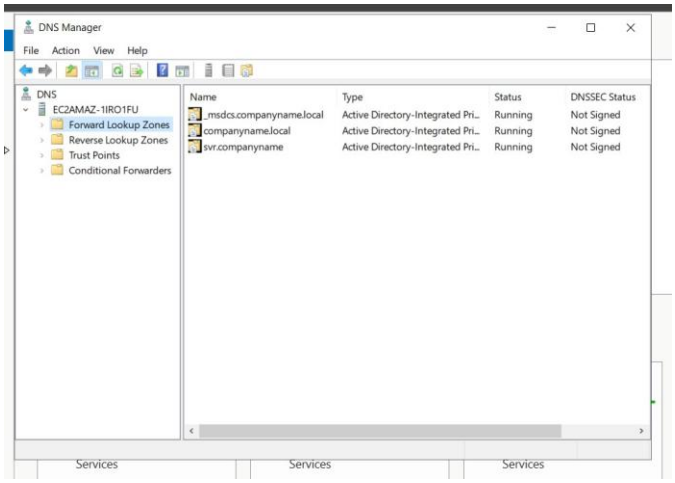
- This is to standardize user and device naming across the company and network - Naming Scheme
- Users: firstname.lastname (ie. emma.julien)
- Groups: Grp-Department (ie. Grp-Sales)
- Workstations: WinWS-Dept-Initials (ie. WinWS-Sales-EJ) (windows workstations will have win mac workstations will have MacWS) - Servers: SRV-Number (ie. Srv-File01)



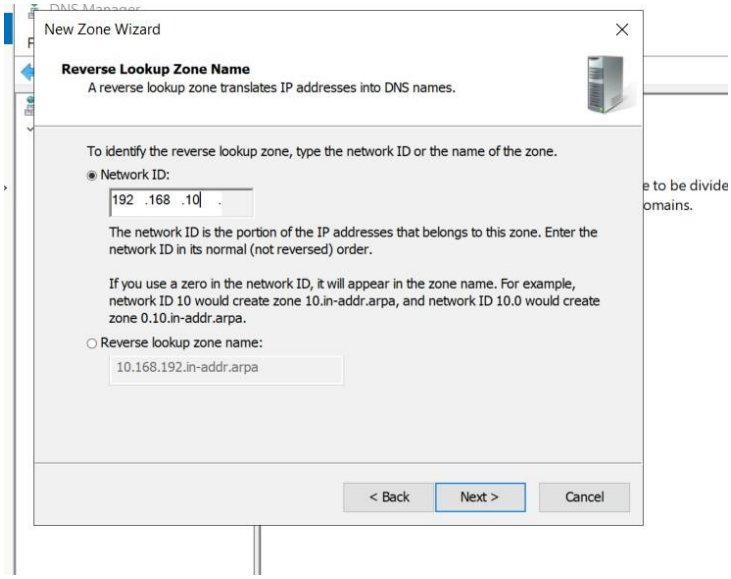
DNS Configuration:

- The goal is to configure the DNS for the internal name resolution - Configure forward lookup zone - Open DNS Manager

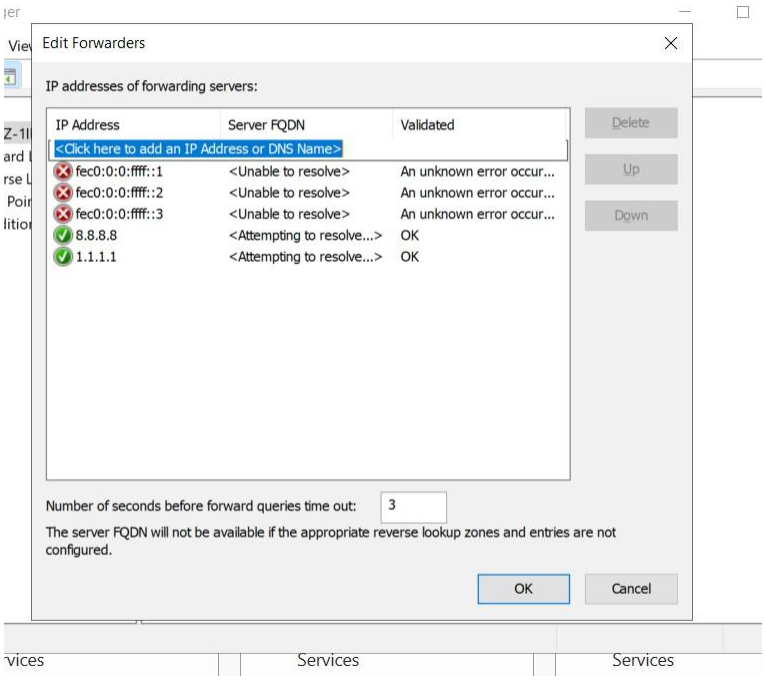
- Right click forward lookup zone and select new zone.
- Set up new zone through the wizard with the name companyname.local.



- Configure Reverse Lookup Zone
- Right click reverse lookup zone and select new zone - Create new zone using valid IP address

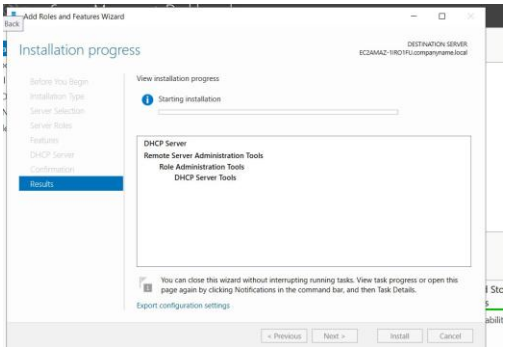


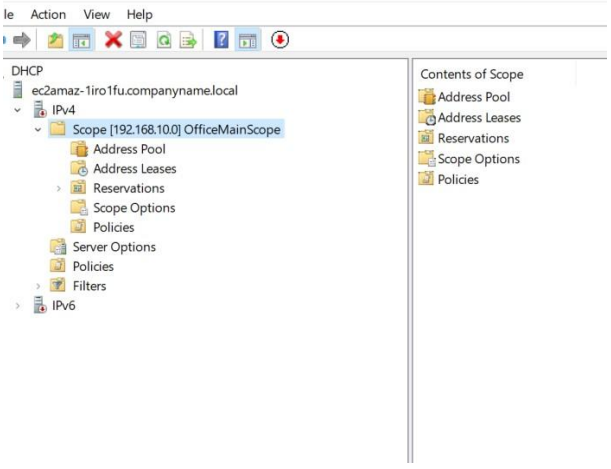
- Set up Fowarders
- Right click DNS Server and select properties.
- Go to the forwarders tab and add public DNS Servers such as 8.8.8.8



DHCP Configuration:

- The objective for DHCP Configuration is to plan DHCP Scopes and find options for IP address distribution.
- Scope configuration
- Subnet: 192.168.10.0/24
- Scope Range: 192.168.10.50-192.168.10.200

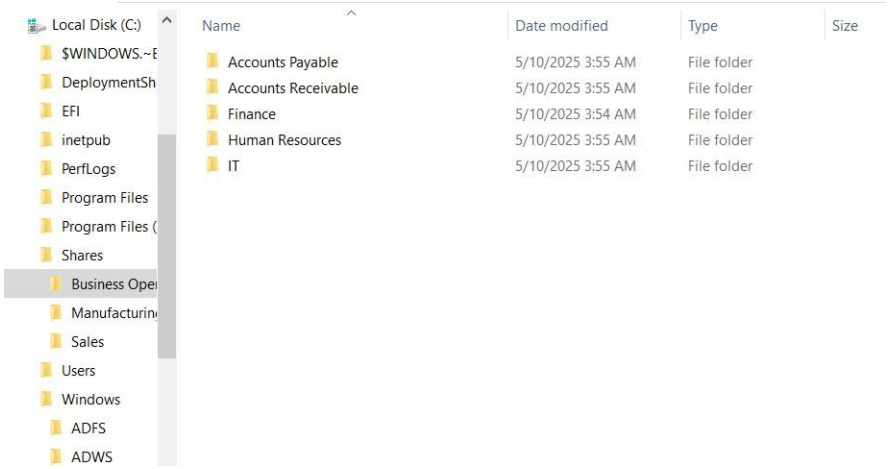




Phase/Milestone 2:

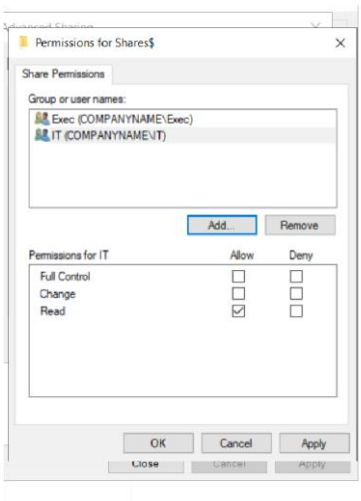
File Server Setup and Shared Folders:

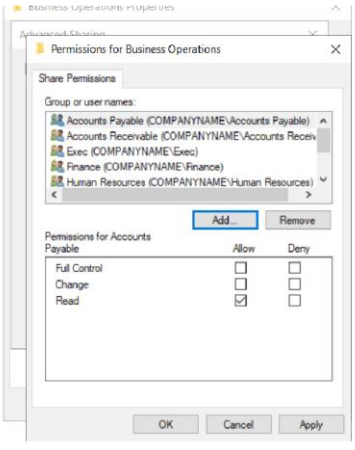
- Objective is to create shared department specific folders and provide proper access controls
- Create folders for each department (ie. Sales, Exec, Manufacturing, Business Operations)
- Within each folder for the department create folders for each group in each department



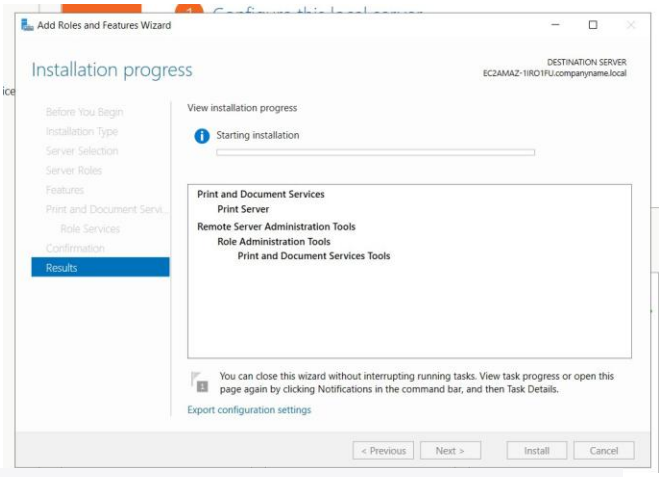
- To edit sharing right click each folder - select properties - share tab - advanced sharing
- Enable share this folder selection and provide it a name (ie. Sales)
- Click permissions - remove everyone
- Add the corresponding security groups and allow full access - (exec for example should have read access on all but not full access)
- Click ok and repeat for every folder

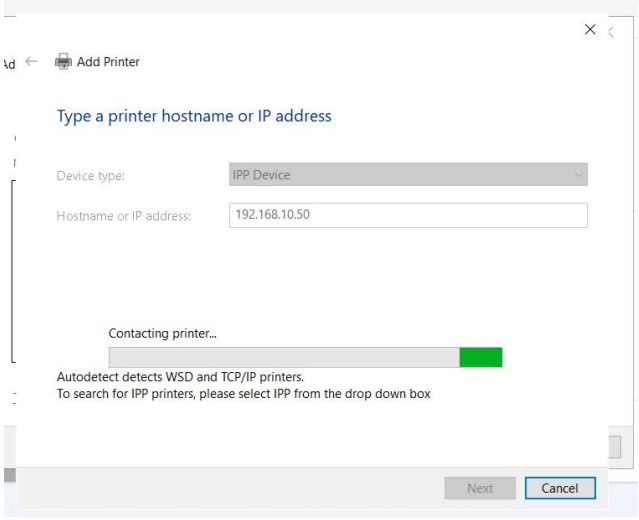
Print Server Configuration:

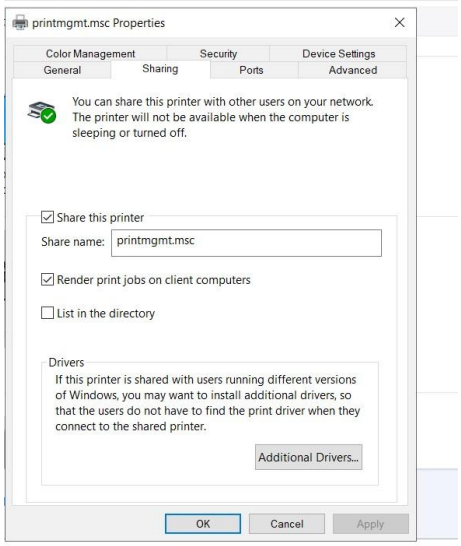




- The objective is to deploy shared printers and provide controlled options
- Install necessary print drivers and connect the printers



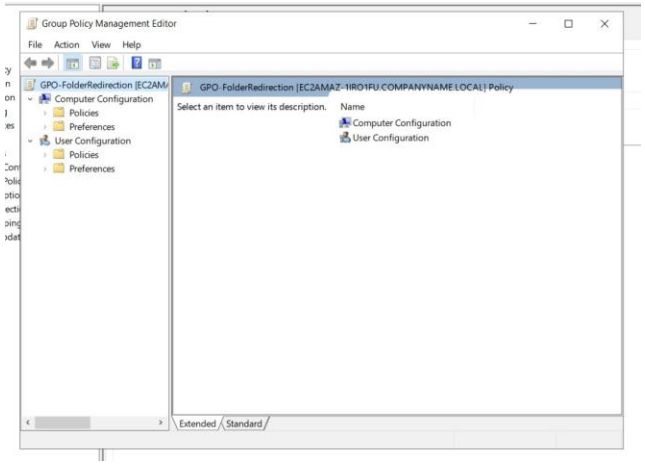


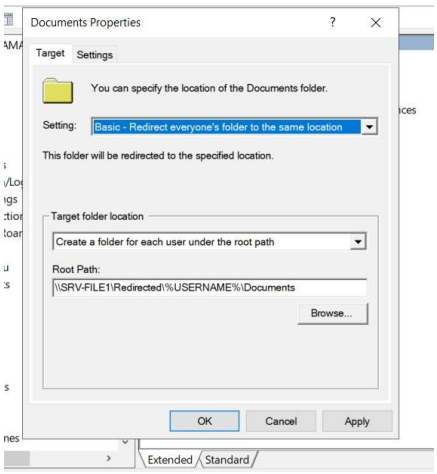


- Navigate to control panel - devices and printers
- Right click printer - printer properties - share with name (ie. PRN-HR-1)
- Select PRN-Exec-1 and select properties - advanced settings - set priority for CEO to 99
- PRN-Color-1 - set to restricted access in properties and advanced settings
- Select security tab of printer properties - remove everyone - add corresponding groups - set print permission.

Group Policy Configuration:

- Objective is to apply GPO's to manage file encryption, folder redirection, and roaming profiles
- GPO Setup in Group Policy Management Console
- GPO-EncryptedFile
- User configuration - policies - Windows Settings - EFS - Deploy Data Recovery agent certificate for recovery.





- GPO-FolderRedirection
- Setup to redirect documents, desktops, and favorites
- User configuration - Windows Settings - Folder Redirection
- Redirect to : \\SRV-File-1\Users\%username% - GPO-RoamingProfiles
- Set profile path
- User configuration - policies - admin templates - system - user profiles
- Set roaming path to for all users \\SRV-File-1\Profiles\%username%
- Deployment of printers via GPO
- Computer configuration - preferences - control panel - settings - printers
- Add each printer based on security group

Remote Access VPN Plan:

- Objective is to provide secure remote access via a vpn.
- Server manager - add roles and features
- Select remote access - check routing and remote access
- After install is complete - open RRAS console - right click server - configure and enable routing and remote access
- Select VPN access
- Under ports configure number of allowed connections
- Use the network policy server to only members of the VPN-Users group

Phase/Milestone 3:

Setup WSUS:

- The Objective is be able to implement and control updates via WSUS - Install windows server update services from the web
- Choose a local folder to store updates
- Synchronise with microsoft update
- Select require product categories (ie. Windows 10) - Create Computer Groups
- Testgroups, workstations, and servers - In GPMC, configure:
- Settings - set WSUS location: computer configuration - admin templates - windows updates
- Enable specify intranet microsoft update service location
- Http://SRV-WSUS1

Data Encryption (using BitLocker)

- Objection is the ability to encrypt client data and protect recovery - BitLocker Setup:
- Open group policy management - Create GPO-BitLocker
- Navigate to computer configuration - admin templates - windows components - BitLocker Drive Encryption
- Enable both require additional authentication at startup and store recovery keys in active directory
- EFS Setup
- Ensure EFS certificate is distributed by GPO
- Users should be able to encrypt specific files/folders

Backup and Recovery Plan:

- The objective is to be able to automate system and data backups - Configure Daily Backups
- System state in domain controllers
- File shares
- WSUS data
- Use NAS or external disk for primary storage
- Set cloud backup (Azure backup) for redundancy
- Perform monthly restore tests to ensure backup integrity

Redundancy and High Availability

- Objective is to ensure fault tolerance
- Deploy two domain controllers - (ie. SRV-DC01 and SRV-DC02)
- Use RAID 1 or 5 for all servers
- Use dual power supplies and UPS
- Set up NIC Teaming
- Use DFS Replication between servers

Monitoring Solutions:

- Objective is to be able to detect issues before they affect user experience - Tools to deploy and their purpose:
- PRTG/Zabbix - to monitor server, network, disks, and RAM
- Event Viewer - to maintain centralized log monitoring
- Windows Admin Center - Dashboard to maintain remote management - Set up email alerts for the following
- Low disk space
- High cpu usage
- Failed logins or backups

Problem Solving and Troubleshooting

- Problems and potential solutions that could pop up during deployment.
- When installing WDT a Windows ISO image must be downloaded in a file to boot it on the system - ensure there is enough space on the disk or complete disk management to install and setup properly
- Ensure group naming remains consistent throughout the process - Print servers and providing access to the correct groups relied heavily on group names and can easily cause issues if not properly followed.

Conclusion:

The aim of this project was to implement and develop a scalable, centralized and secure network infrastructure for a small manufacturing and sales company. Throughout this deep dive into the implementation process a functional Windows Server domain environment was deployed including Active Directory, DNS, DHCP, Group Policies, file and print services and a secure remote access. Each phase was developed to meet the business needs to the best of their ability. Two domain controllers were recommended to have one for backup, and hosting both as physical servers on-site was recommended in

order to keep cost down and allow for easier management. WSUS was chosen as the update software since it allows users to preview and approve deployments and updates before they are rolled out. The outcome of the deployment is a minimal but effective infrastructure that will allow for future growth in the company, security, and remote connectivity. Most areas have a baseline infrastructure, but there is always room for improvement with future implementations. Additional user training will be necessary, due to all the new storage features and policies. Folder redirection may have slow login times eventually due to disk quotas. Any group policy replications must be monitored regularly to prevent a policy mishap. Eventually, it would also benefit the company to implement two factor authentication to provide additional security for remote access. In order to plan for improvements, if we were to plan a fourth phase of implementation it would include implementing a hybrid backup approach, which would be a bit more difficult to learn to manage, but would allow for greater flexibility overall, providing endpoint detection for better security, and automating use onboarding and offboarding.Overall, through this planning and documentation it was demonstrated that the design and configuration of the company's IT infrastructure was met and was able to lay the groundwork for future improvements.

References

frankroj. (2023, October 13). *Prepare for deployment with MDT (Windows 10) - Windows 10.*

Learn.microsoft.com. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-

10/deployment/deploy-windowsmdt/prepare-for-windows-deployment-with-mdt

WSUS: Definition, Functionalities and Benefits. (2025, February 13). Motadata. https://www.motadata.com/it-glossary/wsus/

JasonGerend. (n.d.). *Plan Your WSUS Deployment*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/plan/plan-your-wsus-deployment

Microsoft. (2024, June 18). *BitLocker overview - Windows Security*. Microsoft Learn.

https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/

Sales, E. (2022, July 22). *Key benefits of Azure Backup*. Rand Group.
https://www.randgroup.com/insights/microsoft/azure/key-benefits-of-azure-backup/