A picture containing icon

Description automatically generated

New Zealand Diploma in System Administration Level 6

# **NET602: Network Services**

# Assessment/Aromatawai - Assessment 1 v2.3

# Case Study

Circle

Description automatically generated with low confidence

|  |  |  |  |
| --- | --- | --- | --- |
|  | Submission | FER1 | FER2 |
| Result | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Date | Click or tap to enter a date. | Click or tap to enter a date. | Click or tap to enter a date. |
| Assessor’s Signature |  |  |  |

|  |  |
| --- | --- |
| Student Name | Hui (Spark) ZHENG |
| Student ID | AEU3000774 |
| Student Signature | Spark |
| Assessor | Click or tap here to enter text. |

Contents

[Task 1.1 4](#_Toc174893089)

[Task 1.2 6](#_Toc174893090)

[Task 1.3 7](#_Toc174893091)

[Task 2.1 9](#_Toc174893097)

[Task 2.2 12](#_Toc174893098)

[Task 3.1 13](#_Toc174893099)

[Task 3.2 15](#_Toc174893100)

[Task 4.1 16](#_Toc174893101)

[Task 4.2 22](#_Toc174893102)

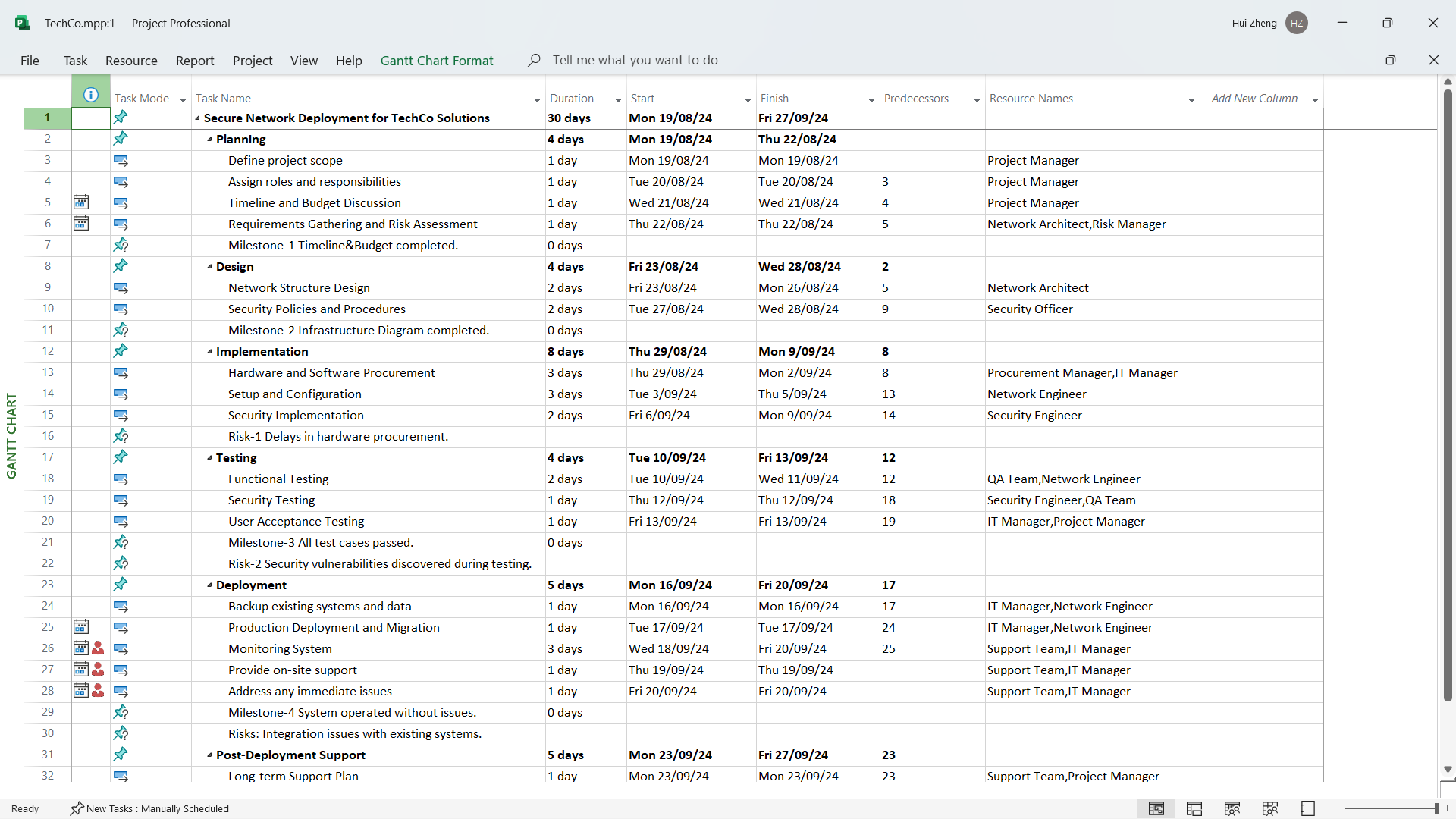
[Task 5.1 26](#_Toc174893103)

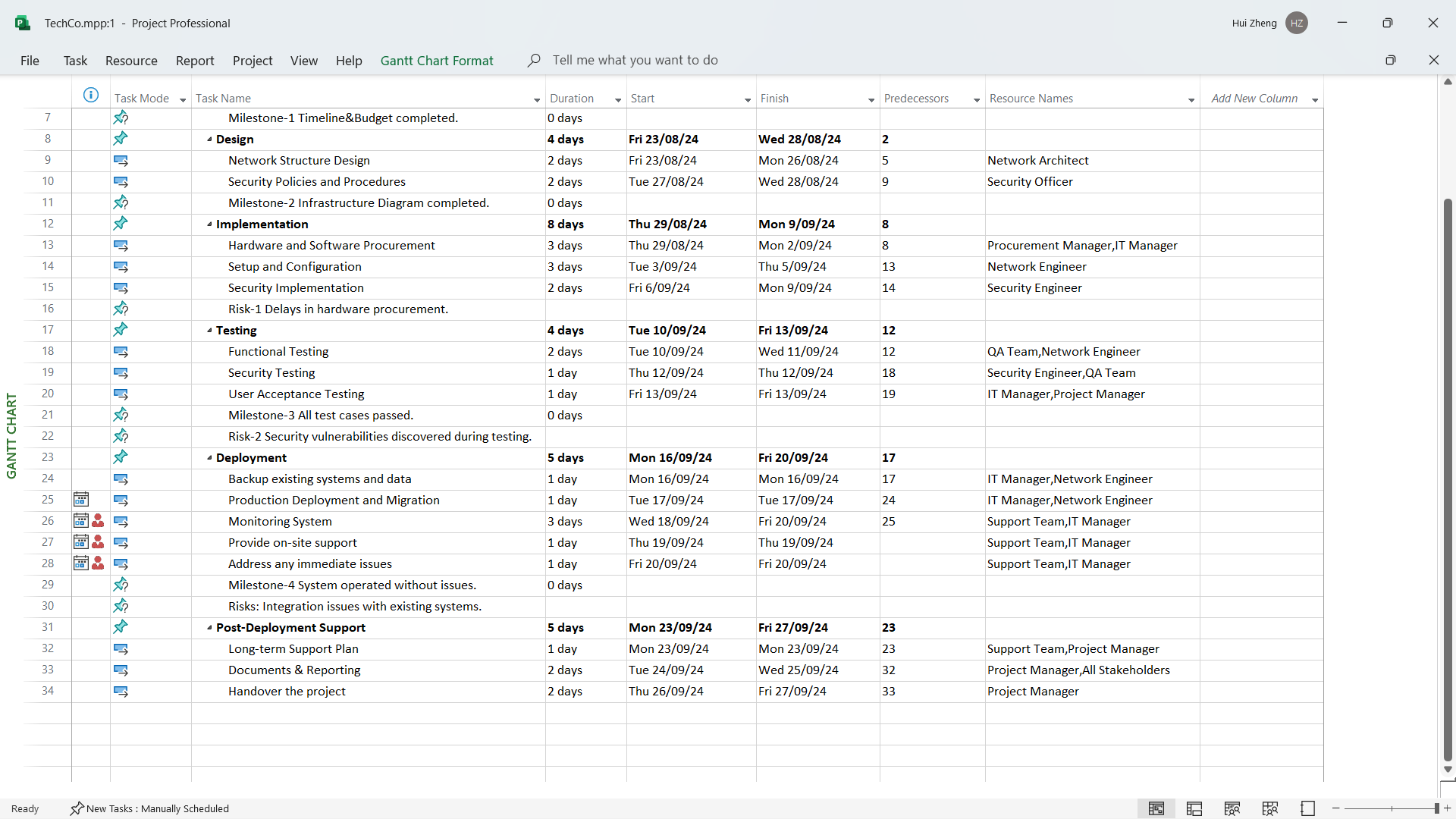
[References 28](#_Toc174893104)

## Task 1.1

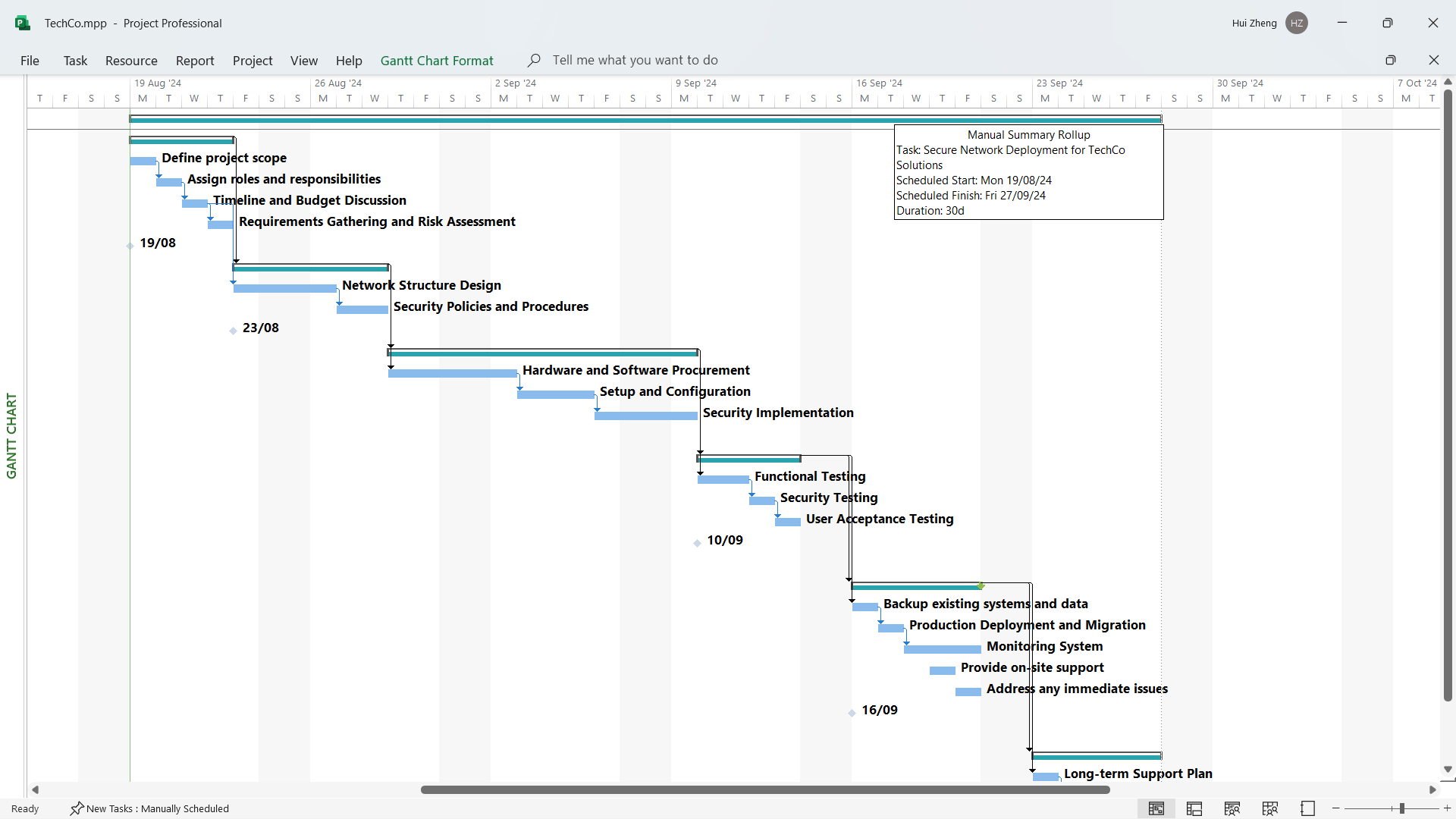
A project plan is developed with Microsoft Project.

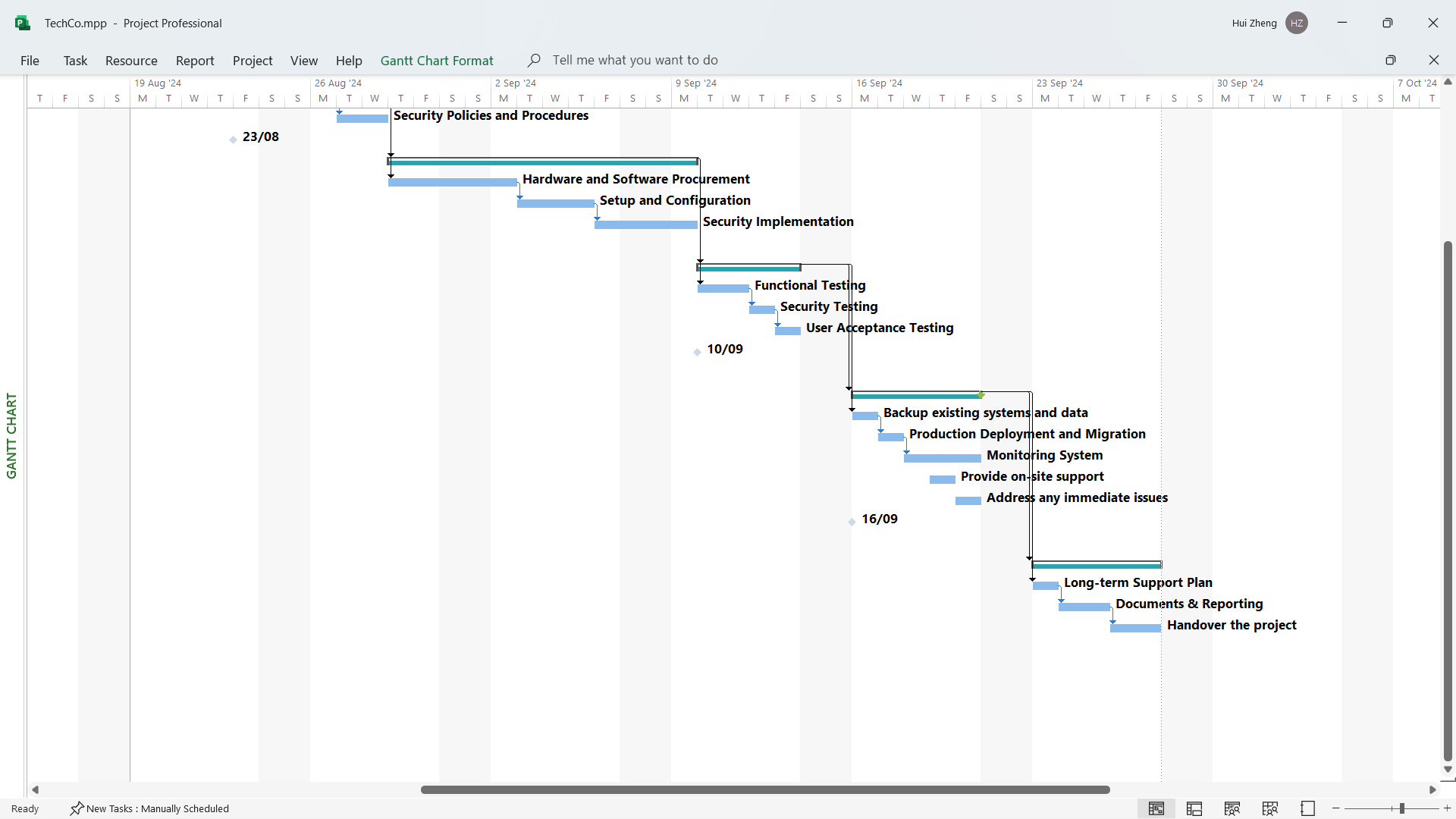
1. The plan with a start date, end date, responsibilities, tasks and subtasks, milestones, risks and post-deployment support is shown in the following screenshots:





1. Timeline is shown as the following screenshot:





## Task 1.2

Through a review the current network setup, we can identify several issues and areas for improvement:

1. The network setup employed by TechCo Solutions is a simple and flat configuration, lacking robust security measures.
2. The network is maintained on-premises.
3. There are no extensive security protections for employees working remotely.
4. For future growth, the company emphasizes a hybrid network approach and combine on-premises infrastructure with secure cloud solutions.
5. The current network infrastructure should be strengthened both security and scalability.

Based on business and technical requirements, the hardware list is:

1. A router, to connect to public network. For to support up to 80 users, more switches are needed to connect the whole network and a router which can handle more network traffic is needed.
2. A core switch, to connect all departments switches together. To work with router and the department switches.
3. Several department switches for each department. To segment the departments to secure the network access.
4. Several Access points devices for each department. For secure Wi-Fi access, several Access Points for each department are needed.
5. Several printers for each department. For secure file and printer sharing.
6. A NAS/File server for files sharing and backup. For local storage for data security and control, and customization needs, a NAS server is needed.

And the software list is:

1. VPN server, to secure remote access. For to secure remote access, a VPN solution is needed.
2. Firewall, to secure public access. For legacy ERP and CRM public secure access, a Firewall server is needed.
3. Domain Controller server, to centralized management. For centralized management of network services, user accounts and access control, a domain control server is needed.
4. Printer management service for printers sharing. For secure file and printer sharing, Printer Management Service is needed.
5. Backup management service for files backup.
6. Software Licenses for Windows Server.

Because the old hardware does not meet the business requirements and technical requirements at all, we need replace the most of them and migrate systems and data to new hardware. Especially for those network devices, i.e. the router, the core switch and the separated departments switches. With the hardware and software listed in this section, a new network with both security and scalability will be implemented as well as meet the business requirements and technical requirements.

## Task 1.3

### 1. Development Department Subnet (50 IPs)

For 2^6 = 64 > 50, and 32-6 = 26, for Development department we have:

Subnet mask: 192.168.1.0/26

Network ID: 192.168.1.1

Broadcast ID: 192.168.1.64

IP range: 192.168.1.2-192.168.1.63 (62 IPs)

### 2. Operations Department Subnet (30 IPs)

For 2^5 = 32 > 30, and 32-5 = 27, for Operations department we have:

Subnet mask: 192.168.1.0/27

Network ID: 192.168.1.65

Broadcast ID: 192.168.1.96

IP range: 192.168.1.66-192.168.1.95 (30 IPs)

### 3. Administration Department Subnet (20 IPs)

For 2^5 = 32 > 30, and 32-5 = 27, for Administration department we have:

Subnet mask: 192.168.1.0/27

Network ID: 192.168.1.97

Broadcast ID: 192.168.1.128

IP range: 192.168.1.98-192.168.1.127 (30 IPs)

### 4. Sales Department Subnet (10 IPs)

For 2^4 = 16 > 10, and 32-4 = 28, for Sales department we have:

Subnet mask: 192.168.1.0/28

Network ID: 192.168.1.129

Broadcast ID: 192.168.1.144

IP range: 192.168.1.130-192.168.1.143 (14 IPs)

### 5. Servers Subnet (6 IPs)

For 2^3 = 8 > 6, and 32-3 = 29, for servers we have:

Subnet mask: 192.168.1.0/29

Network ID: 192.168.1.145

Broadcast ID: 192.168.1.152

IP range: 192.168.1.146-192.168.1.151 (6 IPs)

## Task 2.1

1. Select Hardware Components:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** |  | **Specification** | **Cost** | **Quantity** | **Justification** |
| Ubiquiti UXG-PRO ("Ubiquiti UniFi UXG-PRO,"2024) |  | - 1.7 GHz quad-core processor  - (2) WAN ports (GbE RJ45 and 10G SFP+) with failover support  - (2) LAN ports (GbE RJ45 and 10G SFP+)  - 1U-sized, rack-mountable device | $1,196 | 1 | Ubiquiti USG-PRO is chosen as the router for its lower cost, compatibility with other network devices, and its performance is enough to meet enterprise requirements. |
| Ubiquiti USW-PRO-24 ("Ubiquiti UniFi Switch Gen2 USW-PRO-24,"2024) |  | - (24) Gigabit RJ45 ports - (2) 10G SFP+ ports - Layer 2 and Layer 3 features - UniFi SmartPower RPS DC input | $847 | 1 | Ubiquiti USW-PRO-24 is chosen for a core Switch, it provides SFP ports to connect with the router and Gigabit ports to connect the department switches. |
| Ubiquiti USW-PRO-48 ("Ubiquiti UniFi Switch Gen2 USW-PRO-48,"2024) |  | - (48) Gigabit RJ45 ports - (4) 10G SFP+ ports - Layer 2 and Layer 3 features - UniFi SmartPower RPS DC input - Near-silent cooling - 1.3" touchscreen display - Managed by UniFi Network Controller | $1,034 | 2 | Ubiquiti USW-PRO-48 is chosen as switches for the Development Department and Operations Department. These 2 departments need more ethernet ports. |
| Ubiquiti USW-PRO-24 ("Ubiquiti UniFi Switch Gen2 USW-PRO-24,"2024) |  | - (24) Gigabit RJ45 ports - (2) 10G SFP+ ports - Layer 2 and Layer 3 features - UniFi SmartPower RPS DC input | $847 | 2 | Ubiquiti USW-PRO-24 is chosen as switches for the Administration Department and Sales Department.  These 2 departments need less ethernet ports. 24 ports are enough for them. |
| Ubiquiti U6-PRO AX5300 ("Ubiquiti Access Point AX5300,"2024) |  | -Dual-band WiFi 6 (802.11ax) -5 GHz (4x4 MU-MIMO) band with a 4.8 Gbps throughput rate -2.4 GHz (2x2 MIMO) band with a 573.5 Mbps throughput rate -Operates at full 4x4 MIMO with 160 MHz bandwidth -300+ concurrent client capacity | $370 | 4 | Ubiquiti U6-PRO AX5300 is chose for Access Points for each department for its capacity and compatibility with other network devices. |
| HP Color LaserJet Pro MFP 4301dw Printer ("HP Business Printer,"2024) |  | - A4 Colour Laser Multifunction Printer, Perfect For Business - Print, Copy and Scan, Duplex Printing - Dynamic Security enabled printer - Print speed up to 33/33 ppm black & color (letter/A4) - Apple AirPrint, Ethernet networking, Mopria, USB, Wireless (Wi-Fi), Bluetooth, Print Anywhere, Wireless direct printing | $600 | 4 | HP enterprise printer is chosen as printers for each department for its high performance to meet the enterprise requirements. |
| ASUSTOR AS3304T ("Asustor NAS AS3304T,"2024) |  | - Equipped with Realtek RTD1619B 1.7GHz quad-core processor - Superfast 2.5-Gigabit Ethernet - 2 GB DDR4 RAM | $700 | 1 | ASUSTOR AS3304T is chosen as NAS for backup service. It has 4 bays to scale up in the future grow-up. |
| SAMSUNG 870 EVO 1TB 2.5” Internal SSD ("Samsung 870 EVO 1TB SSD,"2024) |  | - 2.5 inch  - SATA 6 Gb/s Interface, compatible with SATA 3 Gb/s & SATA 1.5 Gb/s interface  - 1TB | $200 | 4 | SSD for NAS. SSD is much faster than HDD. And Samsung 870 EVO SSD has high quality and 4TB capacity is enough for current requirements. |
| HPE DL20 Gen11 ("HPE DL20 Gen11,"2024) |  | - HPE ProLiant DL20 Gen11 E-2436 2.9GHz 6-core 1P 16GB-U 4SFF 500W PS Server  - HPE 32GB (1x32GB) Dual Rank x8 DDR4 3200 Unbuffered Standard Memory Kit  - HPE 960GB SATA 6G Read Intensive SFF BC SSD  - HPE Broadcom BCM5719 Ethernet 1Gb 4-port BASE-T RJ45 PCIe Network Adapter  - HPE 3 Year Tech Care Basic DL20 Gen11 HW Service - 9x5xNBD on-site | $4,830 | 1 | HPE DL20 Gen11 is chosen to host Windows Server 2022. Since Firewall and VPN server will be deployed on a standalone Mini PC, the virtualization feature of server is not necessary, and the large number of CPU cores is not compulsory requirement. |
| PB MSI CUBI 5 Mini PC Intel Core i3-1215U 6 Cores ("PB MSI Cubi 5 Mini PC,"2024) |  | - 16GB RAM, 500GB SSD  - WiFi AX+BT  - Dual LAN, 1x SATA, 1x Thunderbolt, USB 3.2, HDMI/DisplayPort, VESA Ready, No OS | $650 | 1 | This mini-PC has two LAN ports, and it suits to set up Firewall and VPN Server at the same time. |

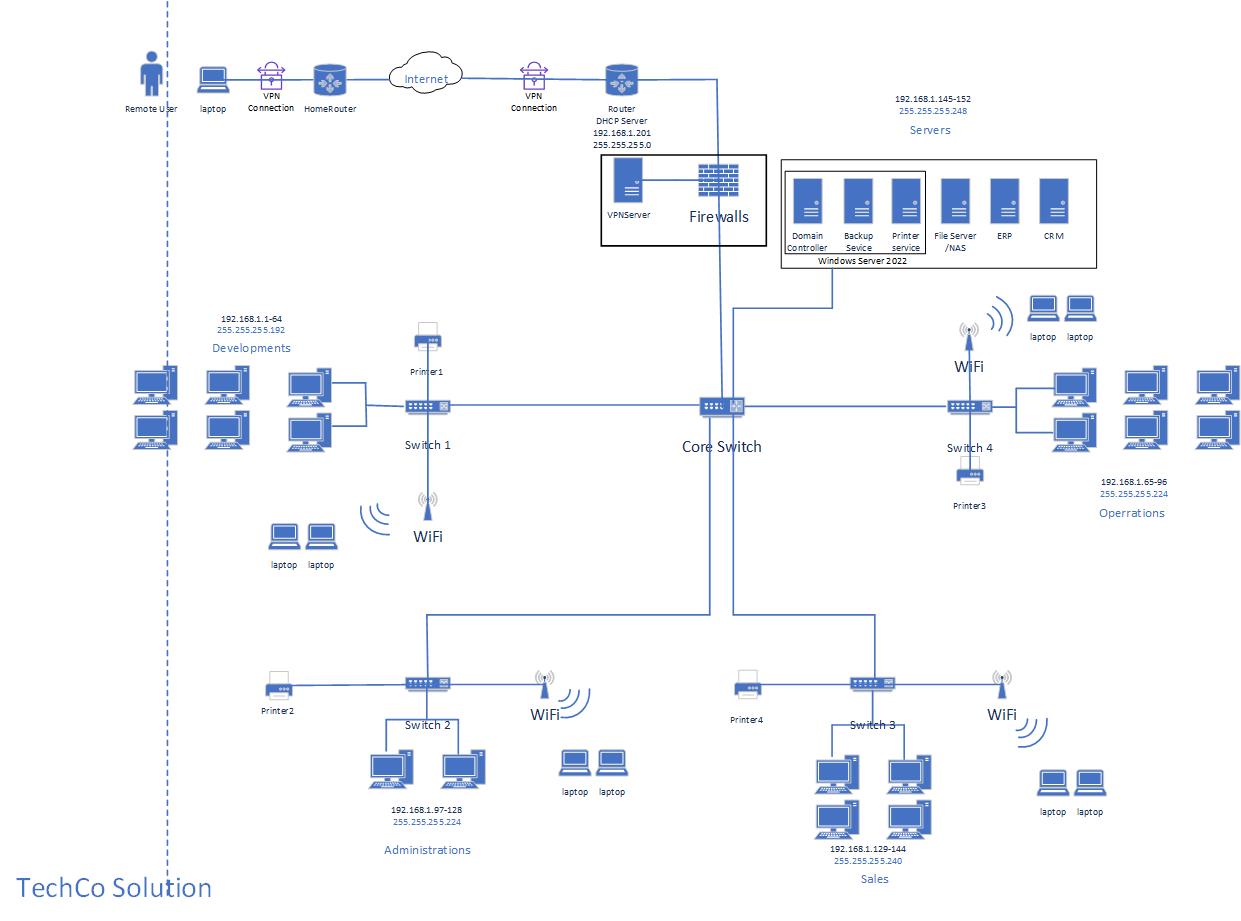
1. Select Software Solutions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** |  | **Specification** | **Cost** | **Quantity** | **Justification** |
| Windows Server 2022 ("Windows Server Licenses,"2024) |  | Standard 16 Core OEI DVD | $1,610 | 1 | Windows Server 2022 integrates Domain Controller, DNS Server, Printer Management Service, Backup Service all together for centralized user accounts management and access control. |
| pfSense ("Download pfSense community edition,"2024) |  | Version: 2.7.2 | Free | 1 | pfSense is popularly used free software as a Firewall server. To choose free software could save money under the budget. |
| Open VPN ("OpenVPN Community downloads,"2024) |  | Version: 2.6.12 | Free | 1 | Open VPN is popularly used free software as a VPN server. To choose free software could save money under the budget. |

Total cost of hardware and software is 21,835 with discounts provided by PBTech Ltd. And it is under the budget constraint.

## Task 2.2

The detailed network infrastructure diagram is shown as following, against with Task 1.3 and Task 2.1 information:



## Task 3.1

In the Task 2.2, the network structure has several potential vulnerabilities:

1. No monitoring and prevention system. The real time attacks could not be detected and responded quickly. This can lead to severe damage before the action is taken. And NZ privacy protection laws require active monitoring and logging, lack of monitoring could result in no-compliance, leading to fines and legal action.
2. No MFA system. If the password of users is leaked, the network will be vulnerable. The attacker can easily access sensitive data and systems, such as domain controller or file server.
3. No proper network segmentation, the data may be accessed between different departments. Once attackers gain access to one part of the network, they can easily jump to other parts of the network, increasing the chances of widespread compromise.
4. Unencrypted data on NAS. The data may be leaked in plaintext. If attacker gain the access to the NAS, unencrypted data can be easily stolen and lead to data breaches. Especially for TechCo Solutions, its data is the most important assets.
5. Only local storage. In the event of hardware failure, natural disasters, or theft, all data stored locally could be permanently lost if there are no backups, and without off-site backups or cloud storage, there is no redundancy. This increases the risk of total data loss in case of an incident.

To Strengthen those potential vulnerabilities, the following security mechanisms should be implemented:

1. IDS/IPS system should be deployed to monitoring and prevent the network. After IDS/IPS system deployed, the network attack will be detected in real time and be blocked or contained. It integrates with Firewall and VPN server to provide comprehensive visibility and protection across the network.
2. MFA system should be deployed to protect the user’s password. MFA requires users to provide two verification factors to get access to network information. MFA integrates with Domain controller, VPN server and other key network services, ensuring that all user access points are secured. MFA significantly reduces the risk of unauthorized access due to compromised credentials, as attacker would need more than just a password to get entry.
3. VLAN should be deployed on the core switch to segment the different departments. VLAN can isolated network segments for each department. VLANs are configured on the core switch and the department switches and each VLAN has its own security policy including access control, firewall rules and monitoring. In case of a breach, the threat is contained within the affected segment, minimizing overall impact.
4. Encrypt the data on NAS to protect the data. Data encryption can be implemented on the NAS through built-in encryption tools. Encrypting data at rest on the NAS ensures that even if the data is accessed by unauthorized users, it cannot be read without the proper decryption keys.
5. Use cloud storage to protect the data. Azura cloud storage is chosen since it is provided by Microsoft and can be integrated easily with Windows server and Windows client OS. Azure cloud storage provides redundancy, ensuring that data can be recovered in case of hardware failure, ransomware attacks, or physical damage to local storage.

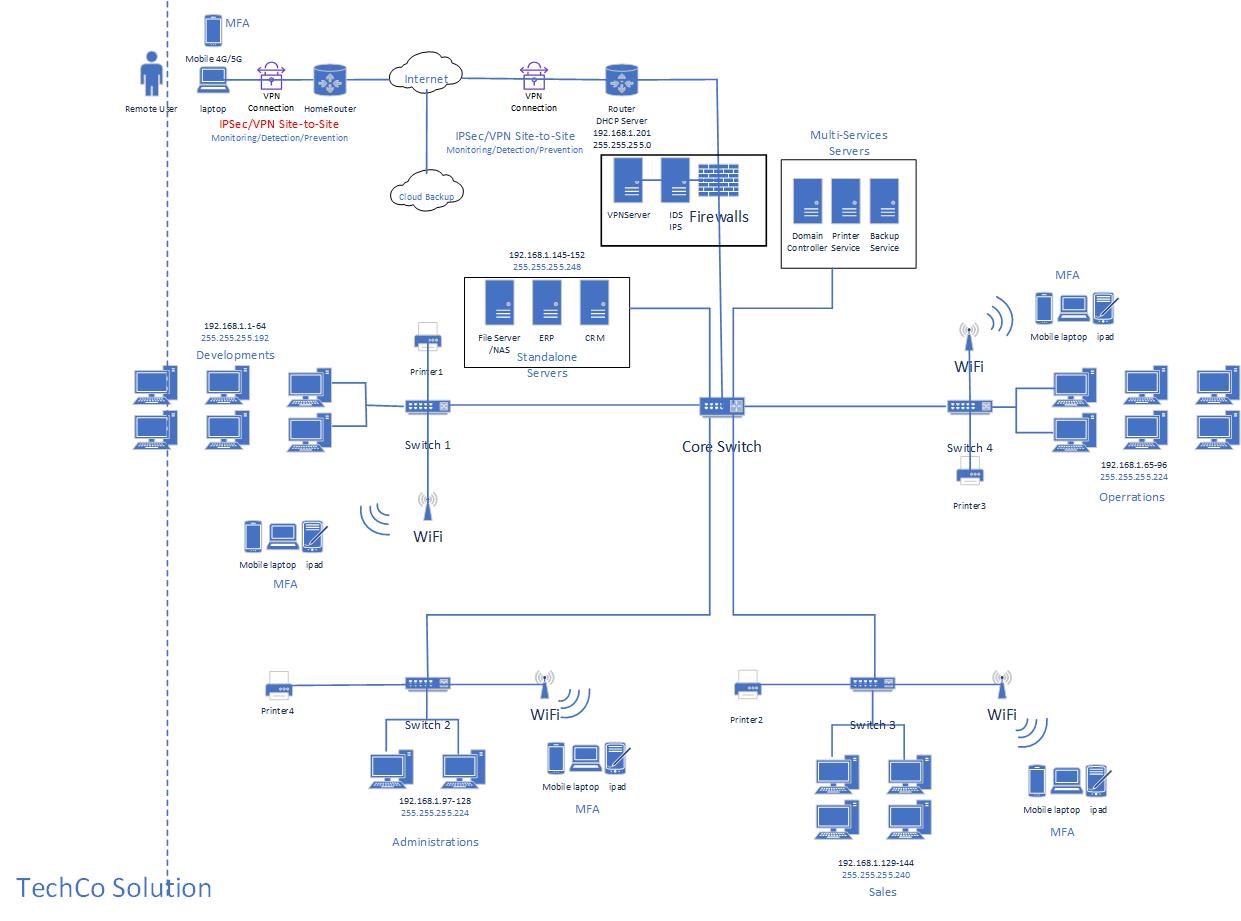
No extra hardware is required. For MFA system, the apps could be deployed to user’s mobile phones/tablets.

The extra software is as following:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** |  | **Specification** | **Cost** | **Quantity** | **Justification** |
| Snort ("Snort 3 release,"2024) |  | Version: Snort v3.3.3.0 | Open Source | 1 | Snort is chosen as IDS/IPS Server for it is popularly used free software and to choose free software could save money under the budget. |
| Microsoft Authenticator ("Download Microsoft authenticator,"2024) | Microsoft Authenticator - Apps on Google Play | latest | Free | everyone | Microsoft Authenticator is a MFA App supporting Android and IOS. |
| Azure Cloud Storage ("Azure Blob Storage pricing,"2024) | VMS Solution Sdn Bhd | 4TB | $82/Month | 12 | Azure Cloud storage is provided by Microsoft and can be integrated easily with Windows server and Windows client OS. |

## Task 3.2

The enhanced network infrastructure diagram is shown as following:



## Task 4.1

1. Create PowerShell script and execute it to configure printer management features and GPOs.

*##########################################*

*##### Spark Zheng 16/08/2024 #############*

*##########################################*

*# Install Printer Services*

*Install-WindowsFeature -Name Print-Server -IncludeManagementTools*

*#Restart-Computer*

*$PrinterDriverName = "Lexmark Universal v2 XL"*

*$PrinterName="iac-printer"*

*Add-PrinterDriver -Name $PrinterDriverName*

*# add a printer on server side.*

*Add-Printer -Name $PrinterName -DriverName $PrinterDriverName -PortName "LPT1:"*

*Set-Printer -Name $PrinterName -Shared $true*

*#Get-Command -Module GroupPolicy*

*New-GPO -Name PrinterPolicy*

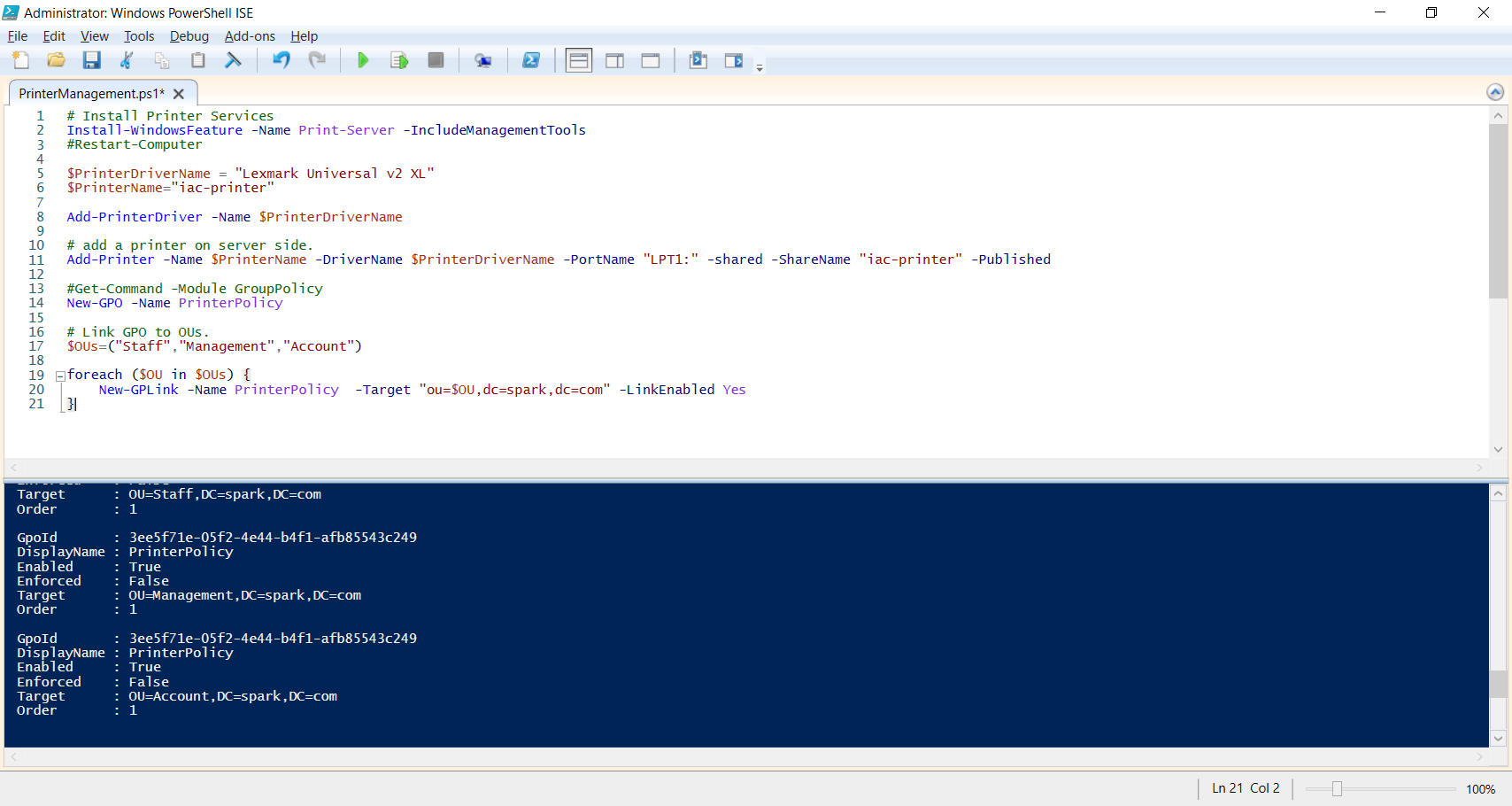
*# Link GPO to OUs.*

*$OUs=("Staff","Management","Account")*

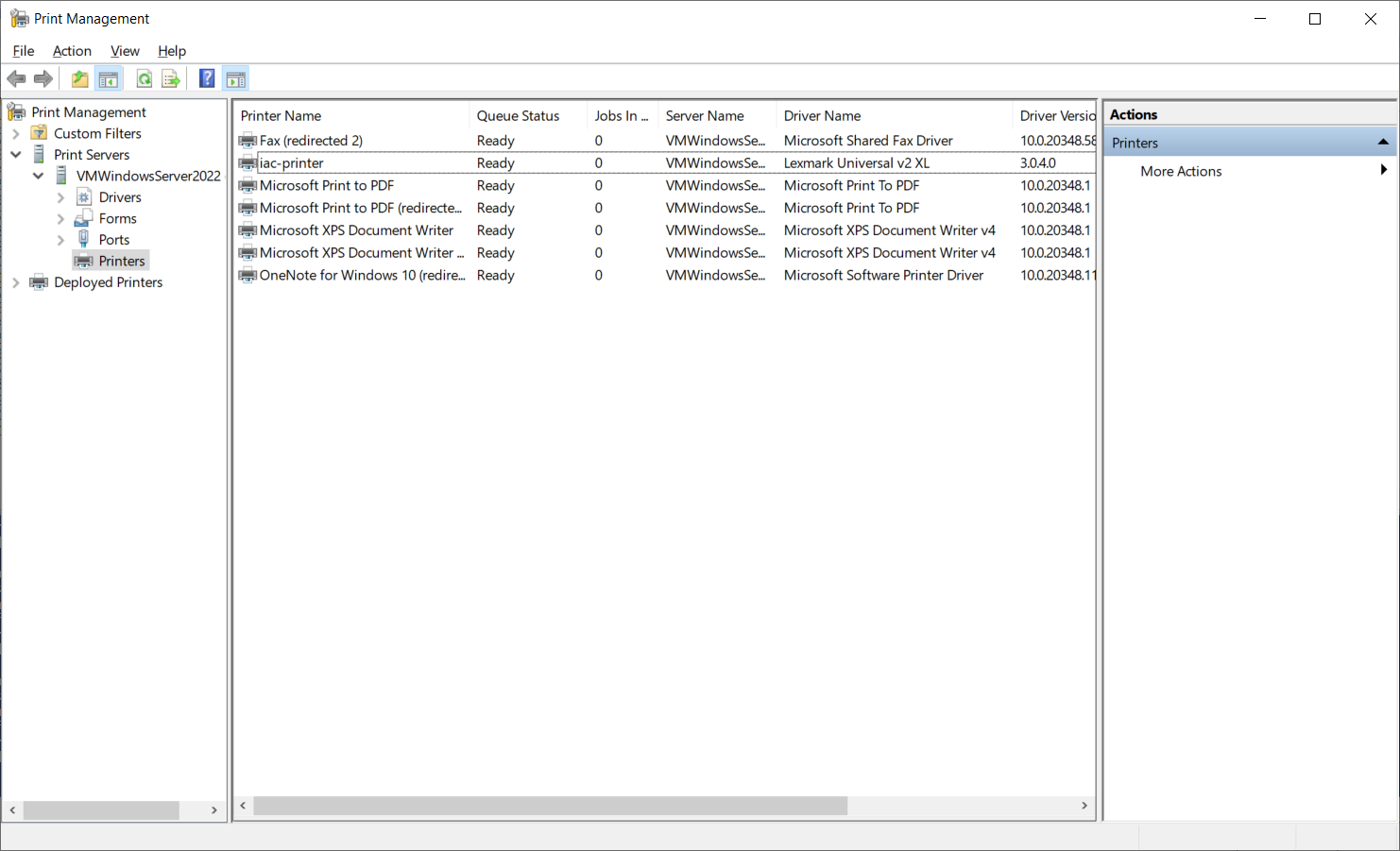
*foreach ($OU in $OUs) {*

*New-GPLink -Name PrinterPolicy -Target "ou=$OU,dc=spark,dc=com" -LinkEnabled Yes*

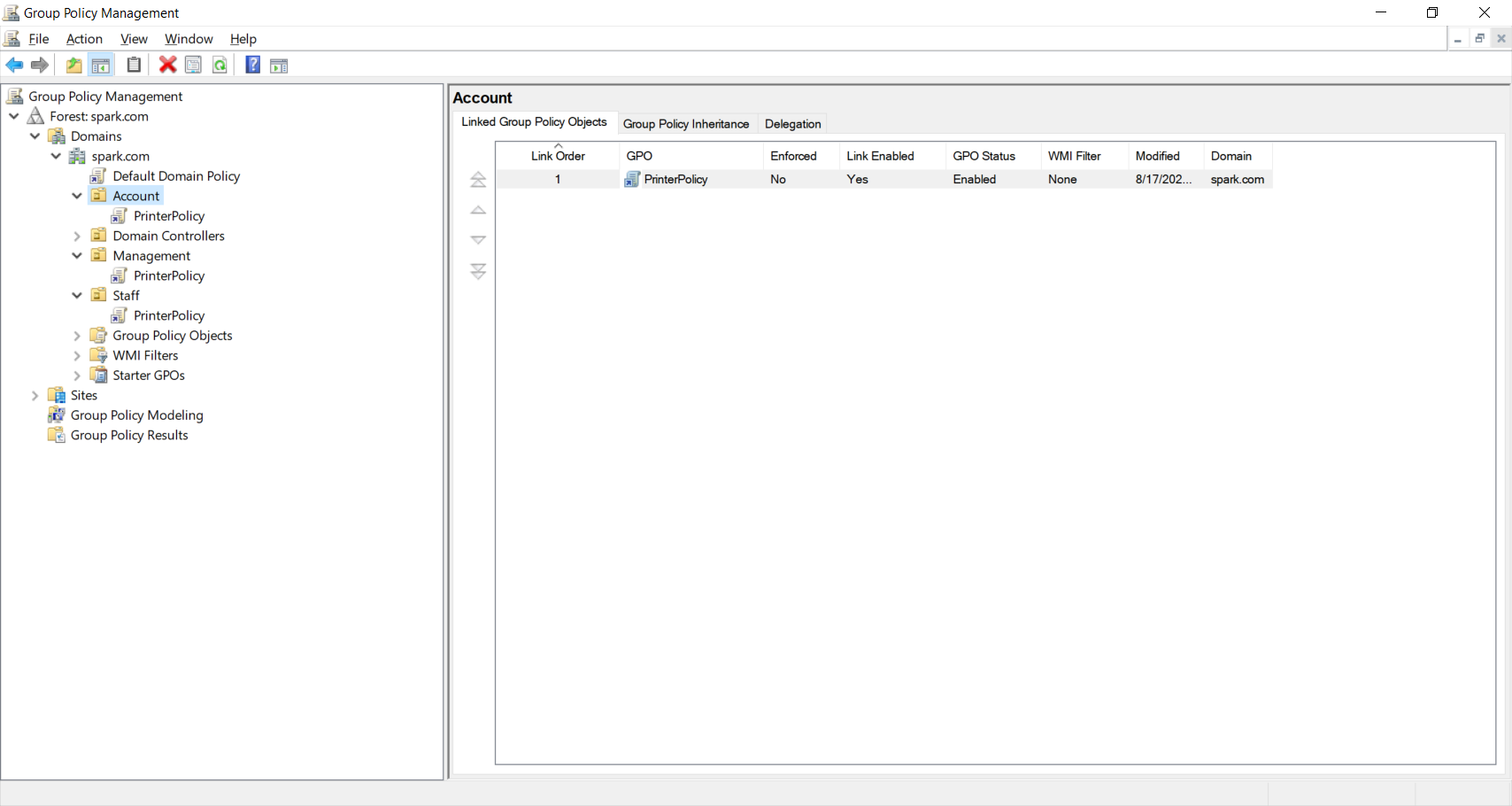
*}*



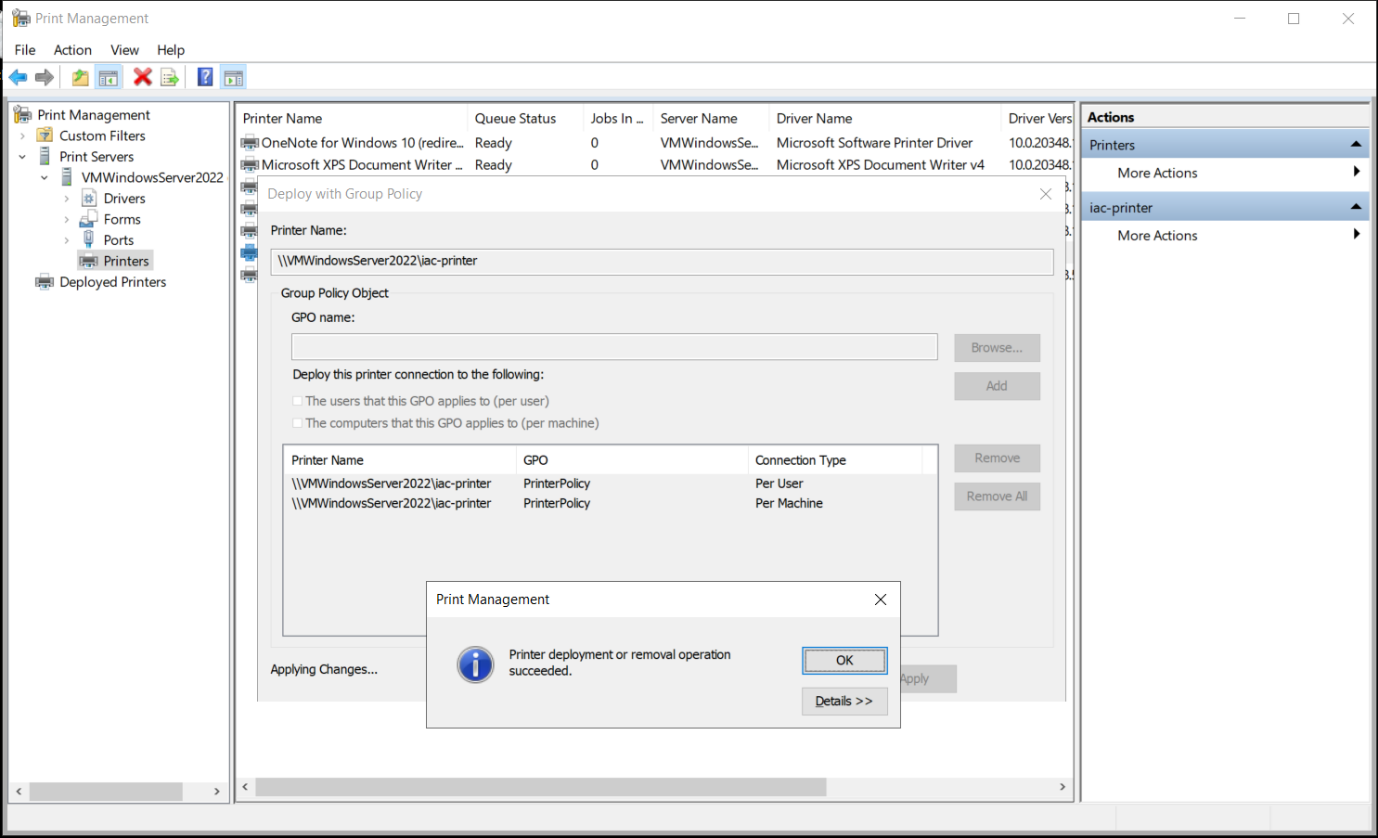
1. Printer is added through the PowerShell script.



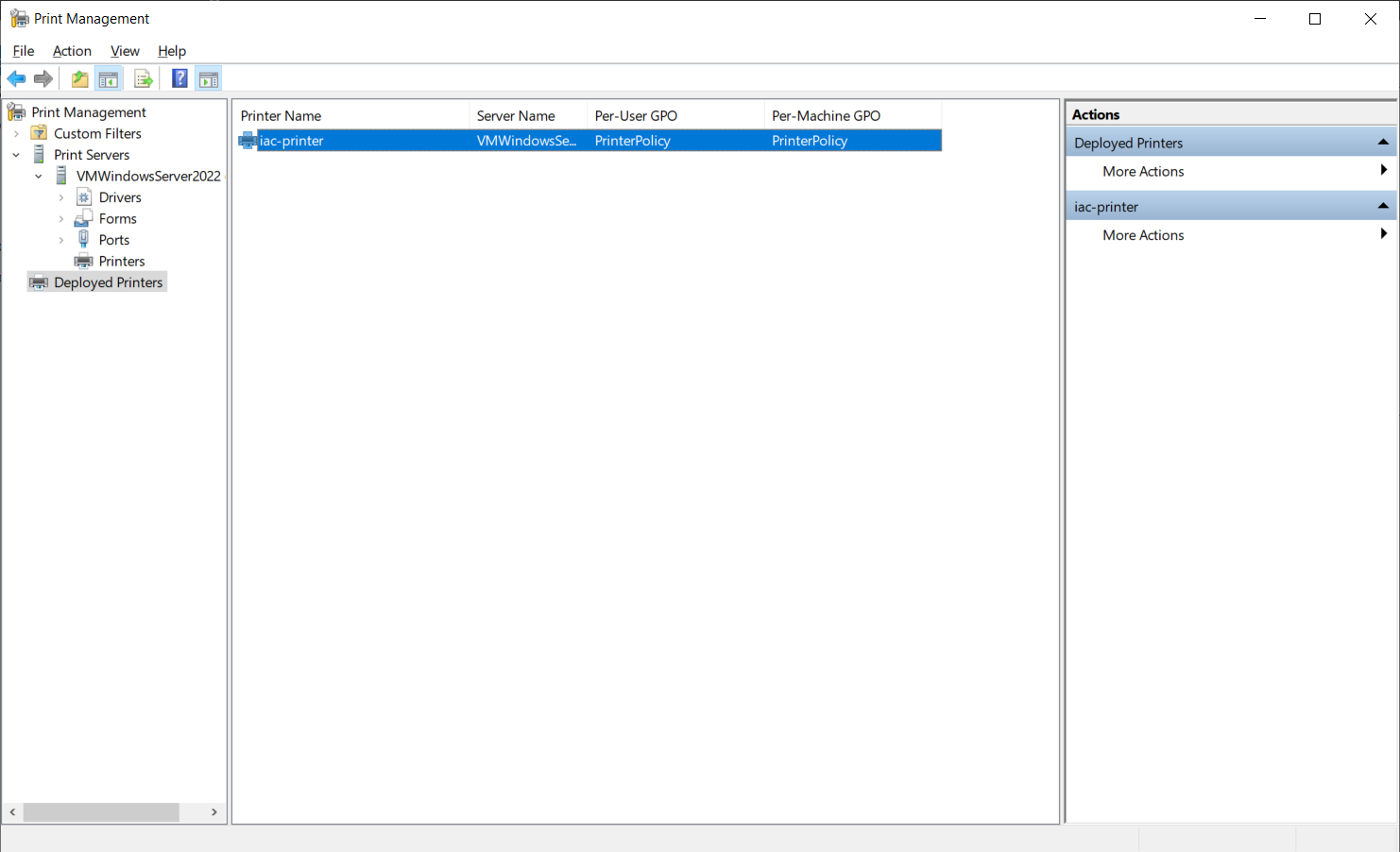
1. GPOs are added through the PowerShell script.



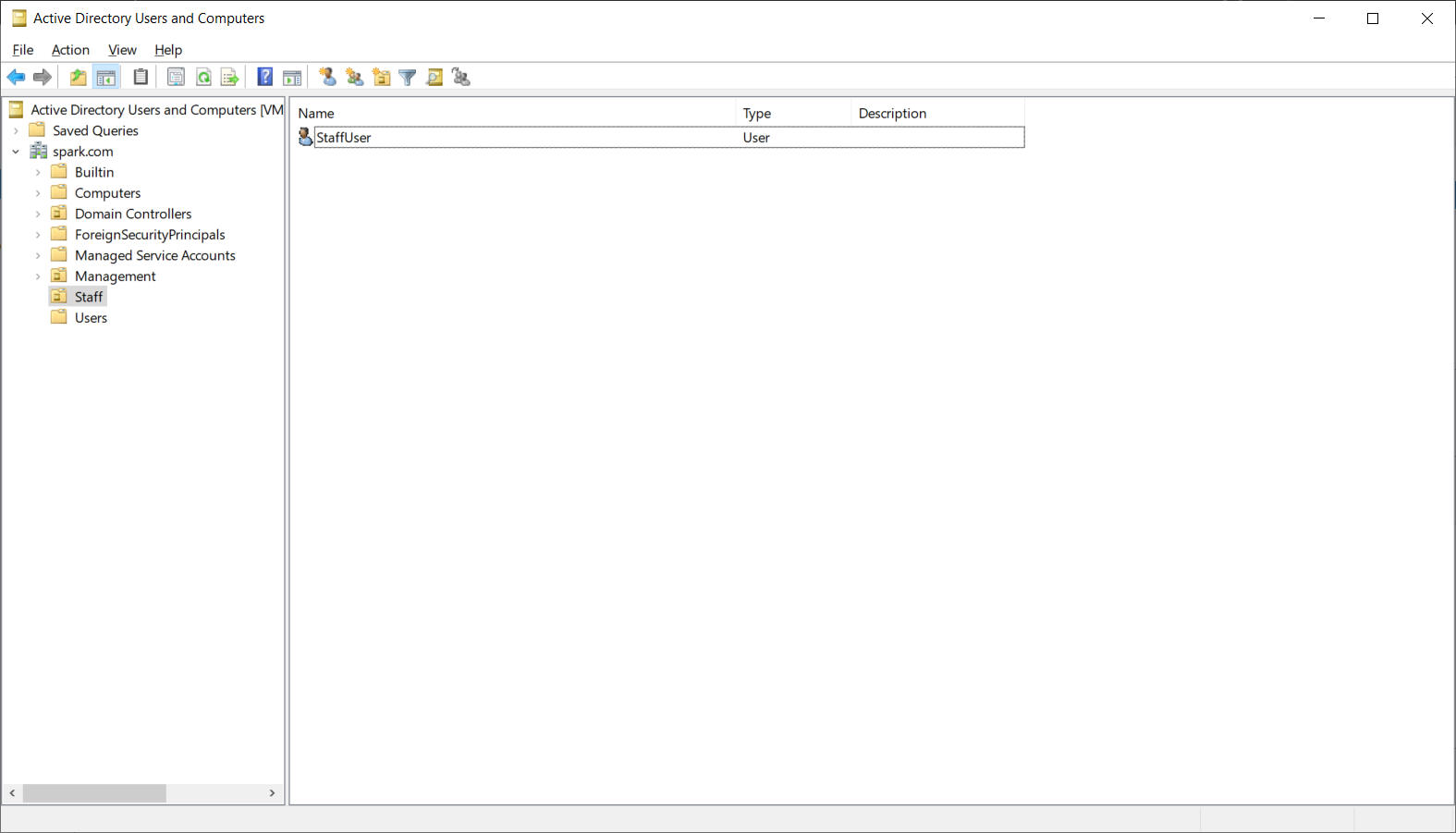
1. Deploy printer against the GPOs with Printer Management Service.

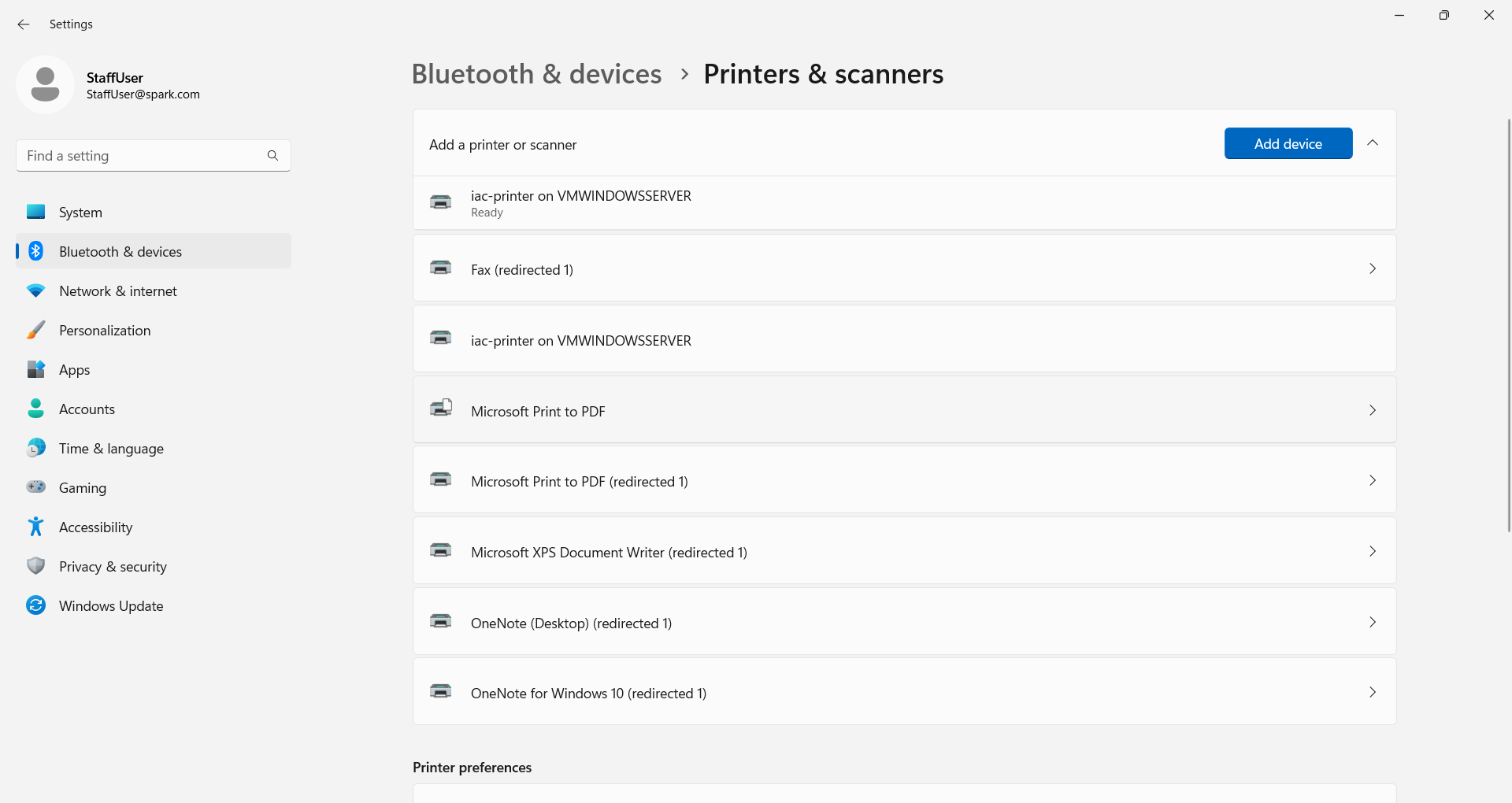


1. Deployed printer in Printer Management Service.



1. Create a user for Staff OU and add printer for this user on the client computer

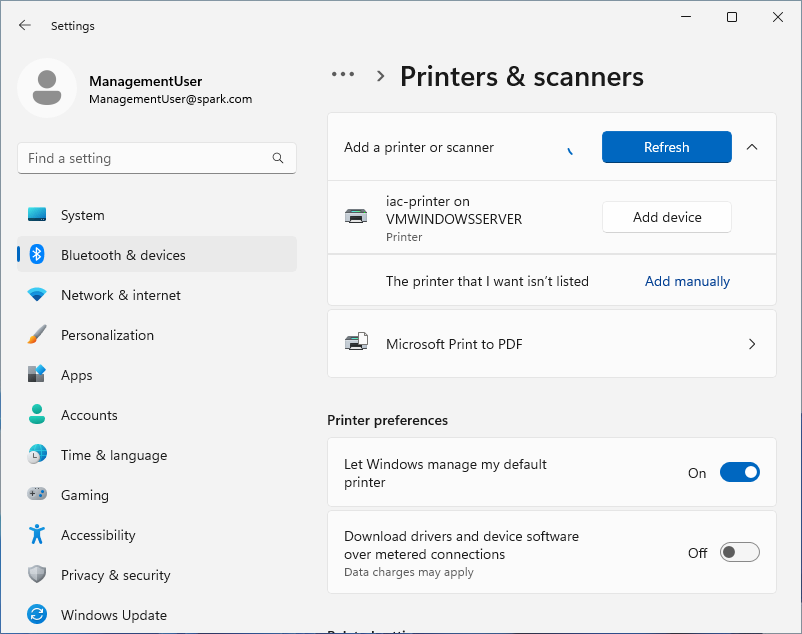




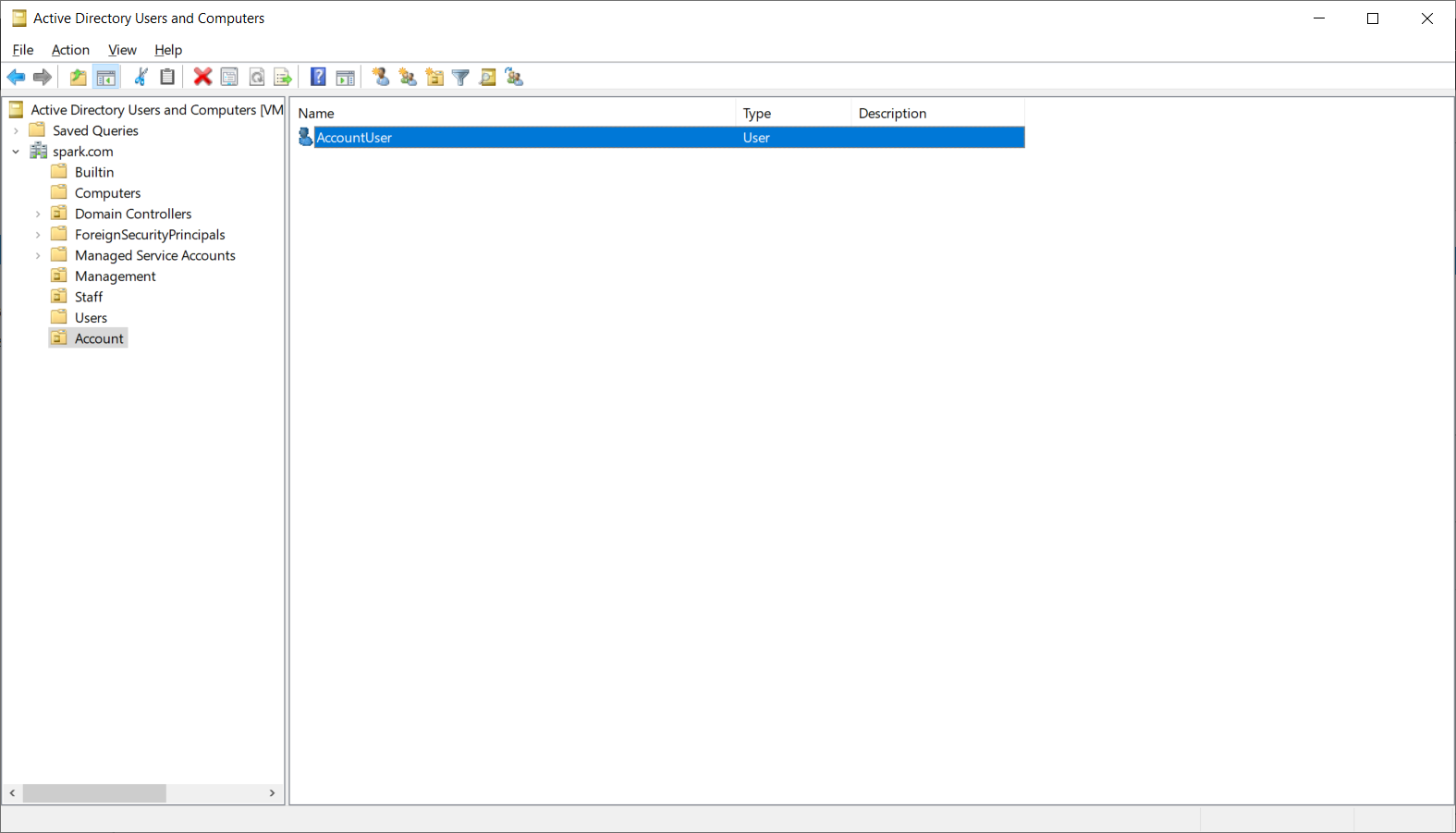
1. Create a user for Management OU and add printer for this user on the client computer

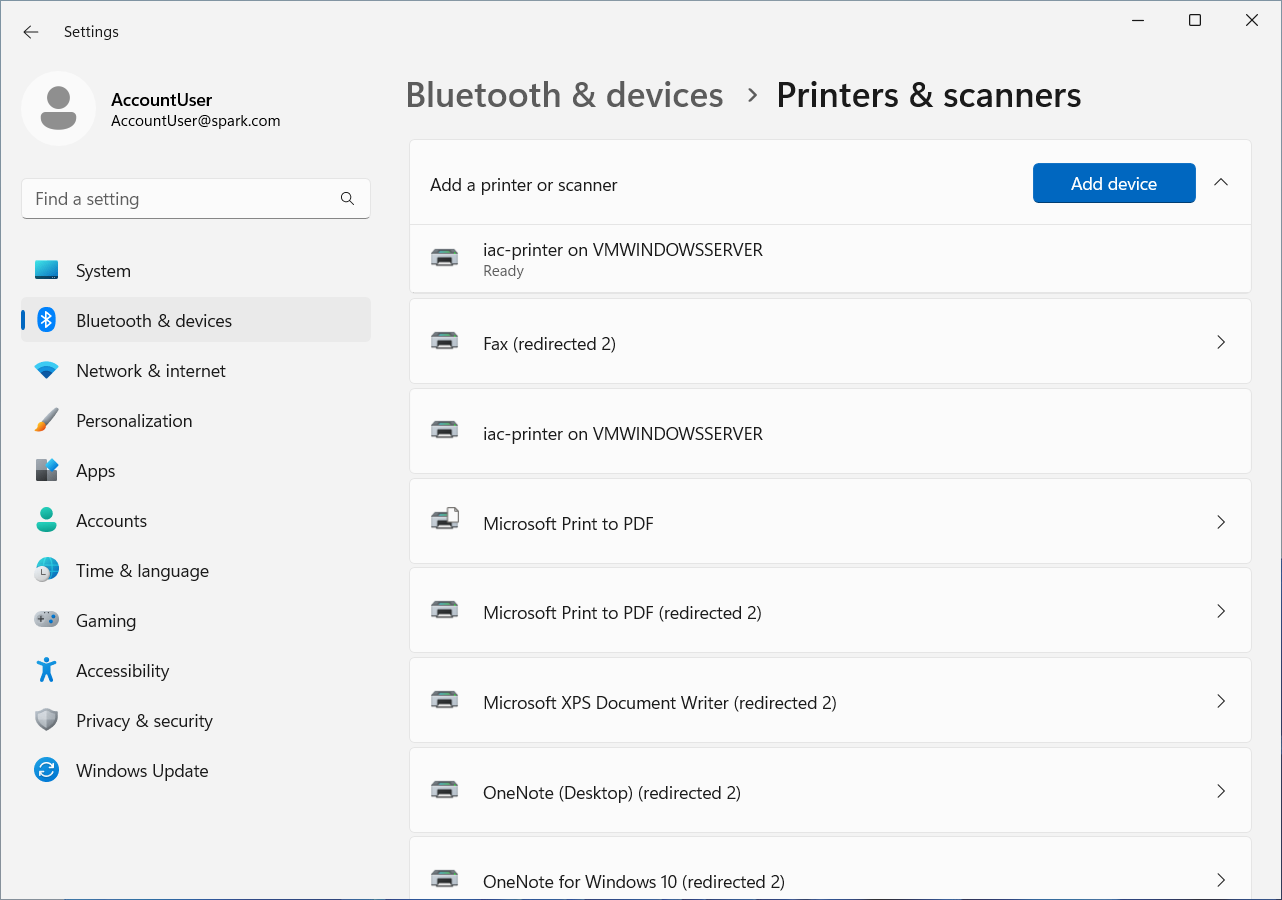
A screenshot of a computer

Description automatically generated



1. Create a user for Account OU and add printer for this user on the client computer





## Task 4.2

1. Create and execute the PowerShell script to configure a scheduled backup policy.

##########################################

##### Spark Zheng 16/08/2024 #############

##########################################

# Install Printer Services

Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools

*# Create a new Windows backup policy*

*$Policy = New-WBPolicy*

*# Configure the path of the files to backup*

*$FileSpec = New-WBFileSpec -FileSpec "C:\"*

*# Add the file path to the backup policy*

*Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec*

*# Prepare the Credential to access backup storage*

*$User = "administrator"*

*$PWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force*

*$Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $PWord*

*# Configure the backup location*

*BackupLocation = New-WBBackupTarget -NetworkPath "\\VMWINDOWSSERVER\BackupFolder" -Credential $Credential*

*# Add the target location to the backup policy*

*Add-WBBackupTarget -Policy $Policy -Target $BackupLocation*

*# Set backup time*

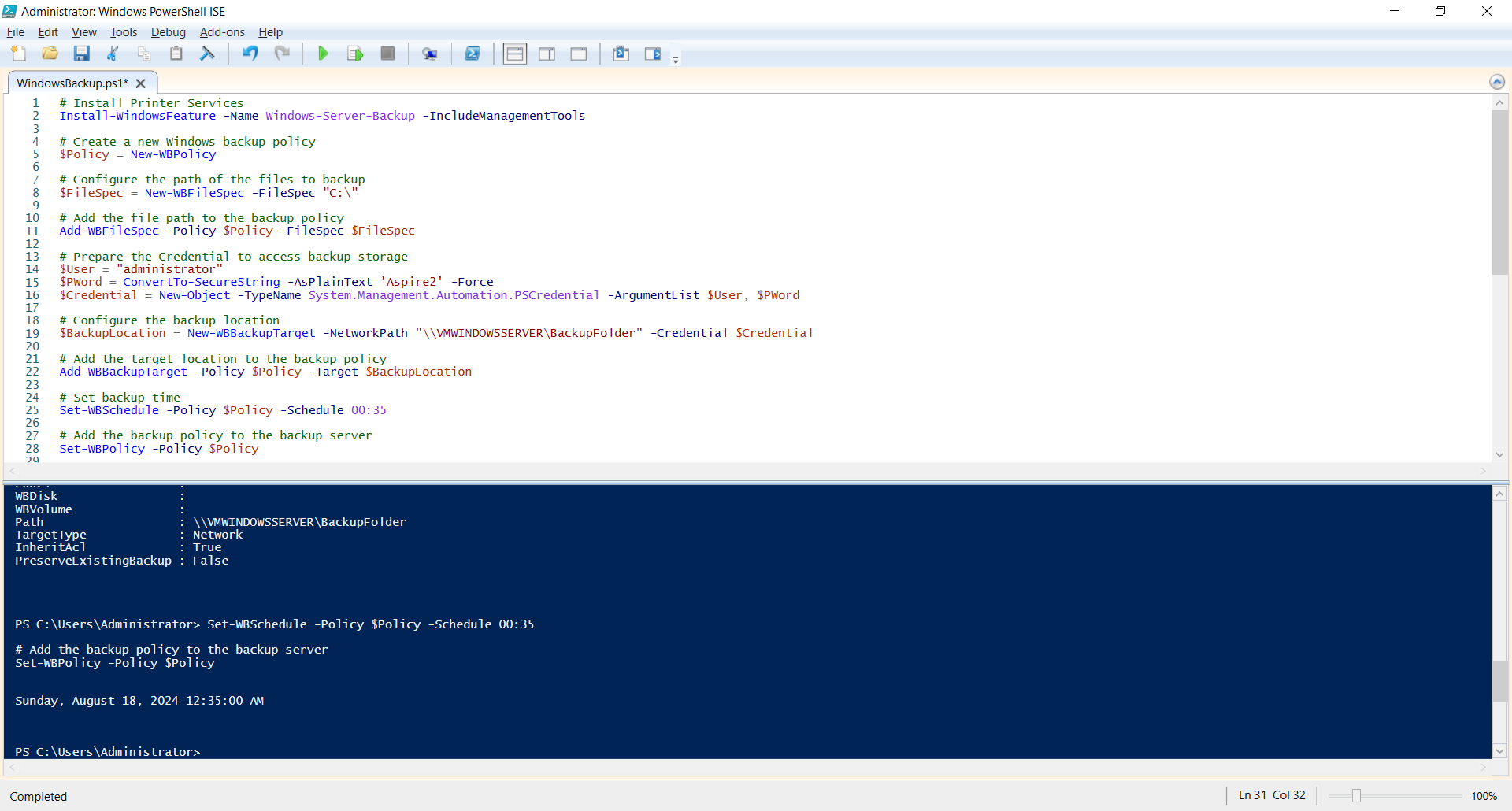
*Set-WBSchedule -Policy $Policy -Schedule 00:20*

*# Add the backup policy to the backup server*

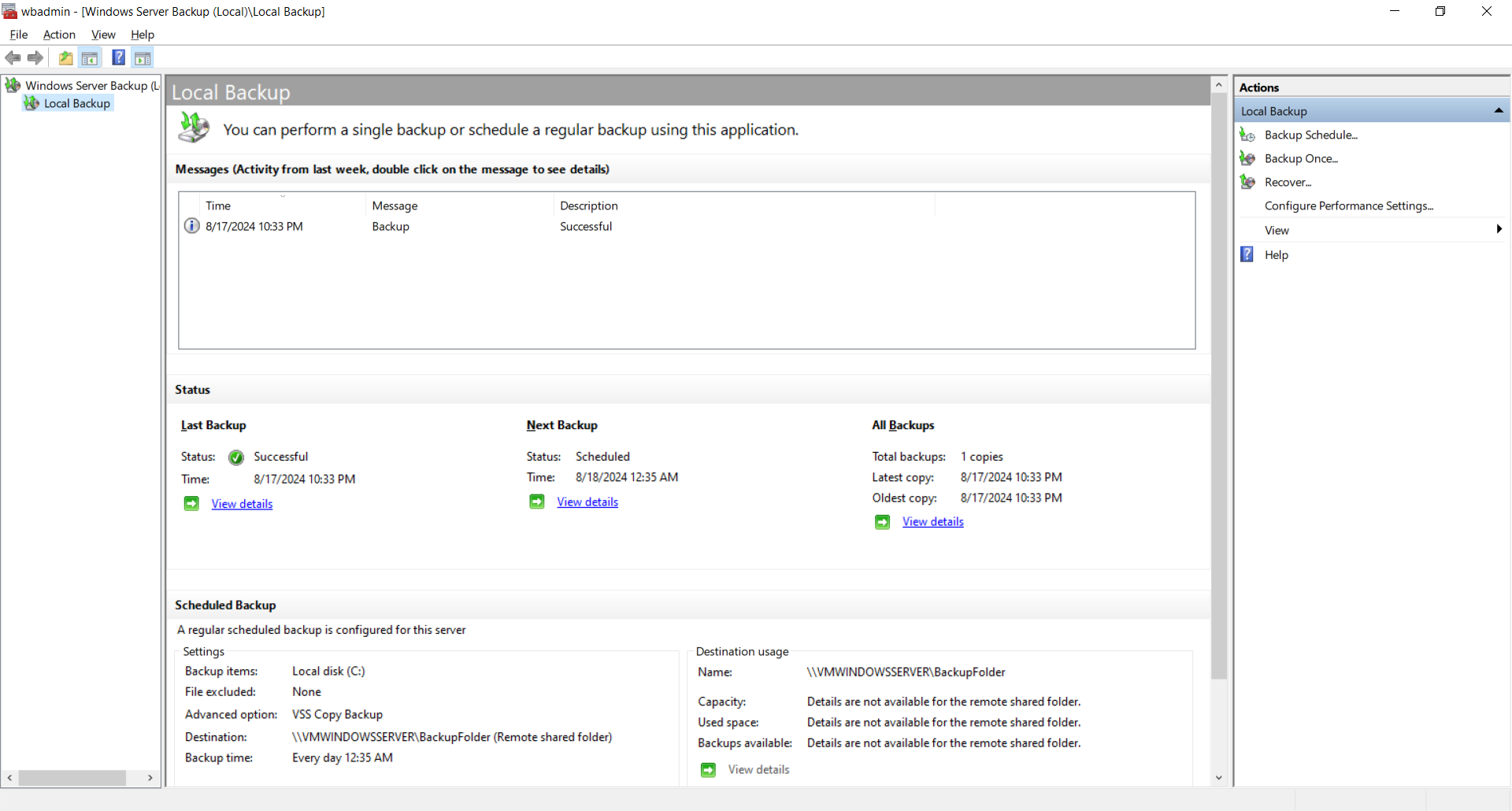
*Set-WBPolicy -Policy $Policy*

*# for once time backup execute start cmdlet directly.*

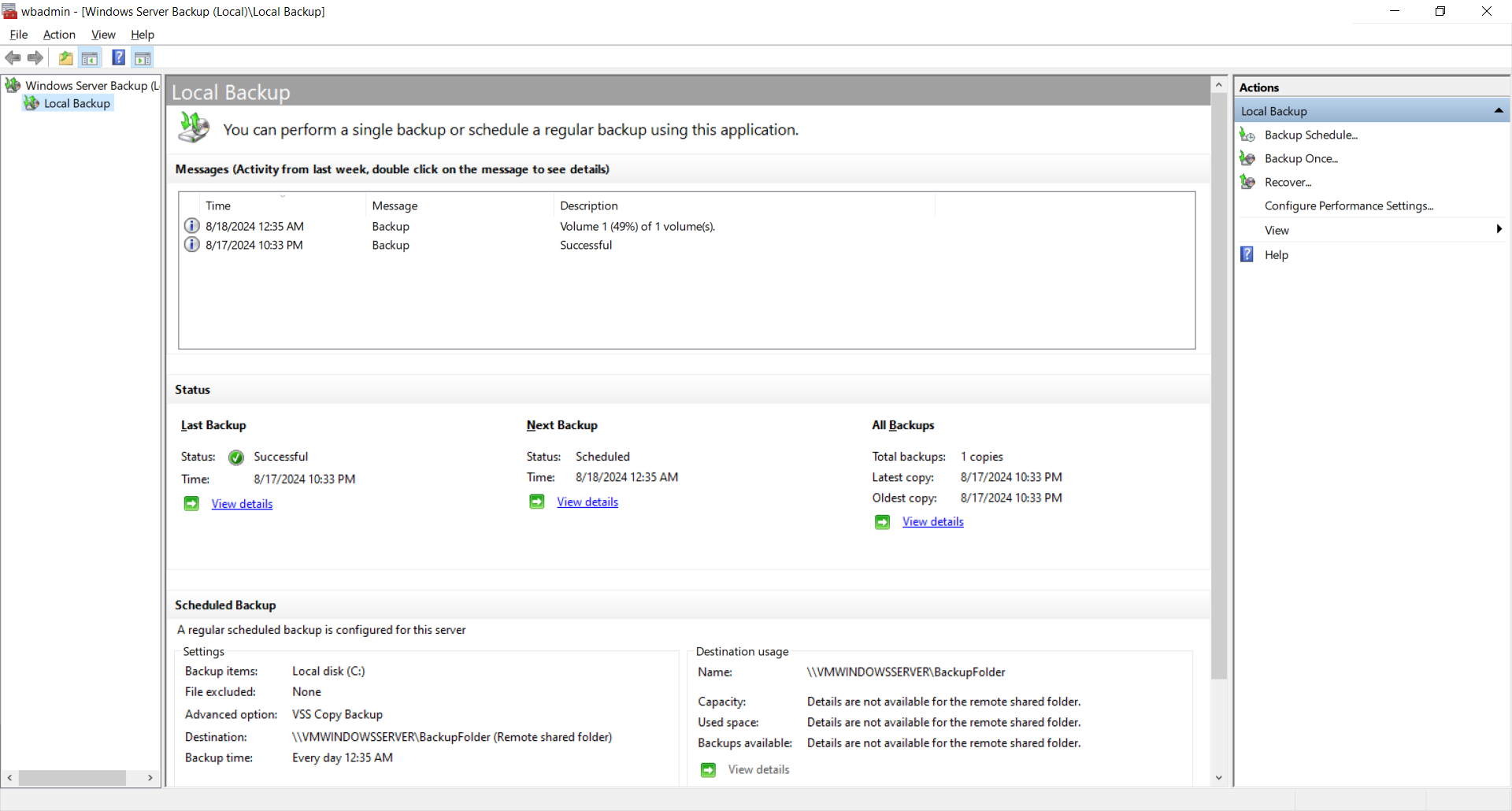
*#Start-WBBackup -Policy $Policy*



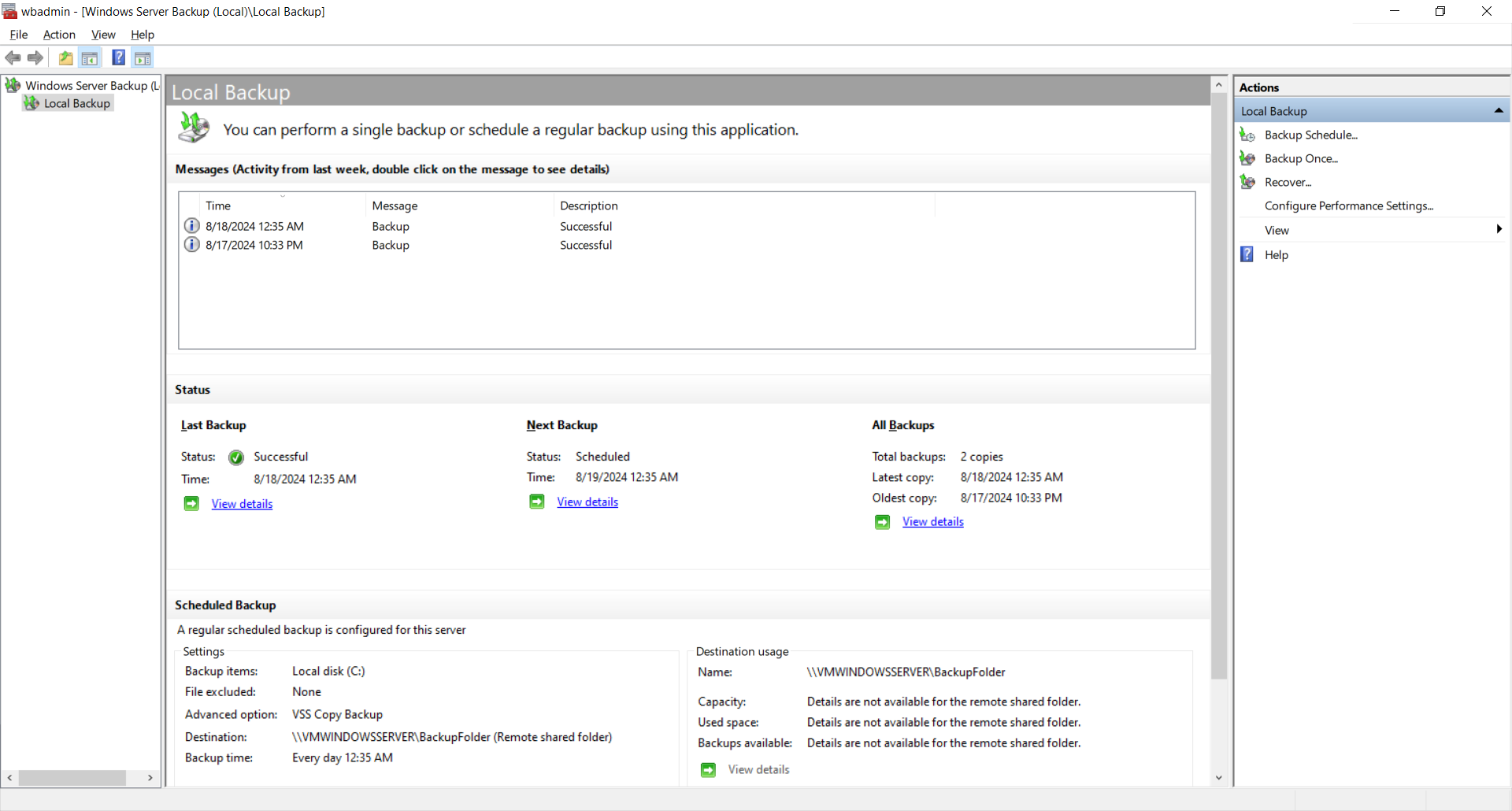
1. Check in Windows Server Backup console and the Next Backup is scheduled.



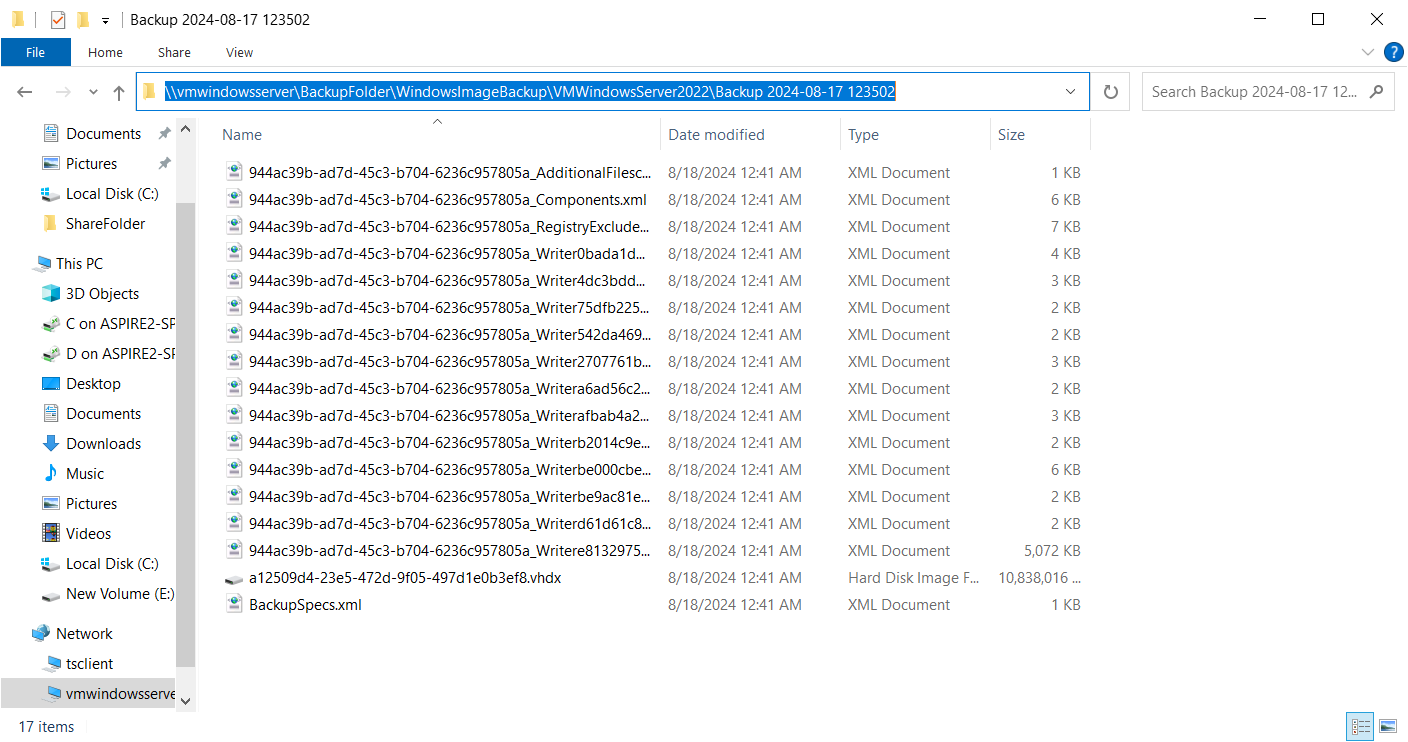
1. Check in Windows Server Backup console and the scheduled task is running.



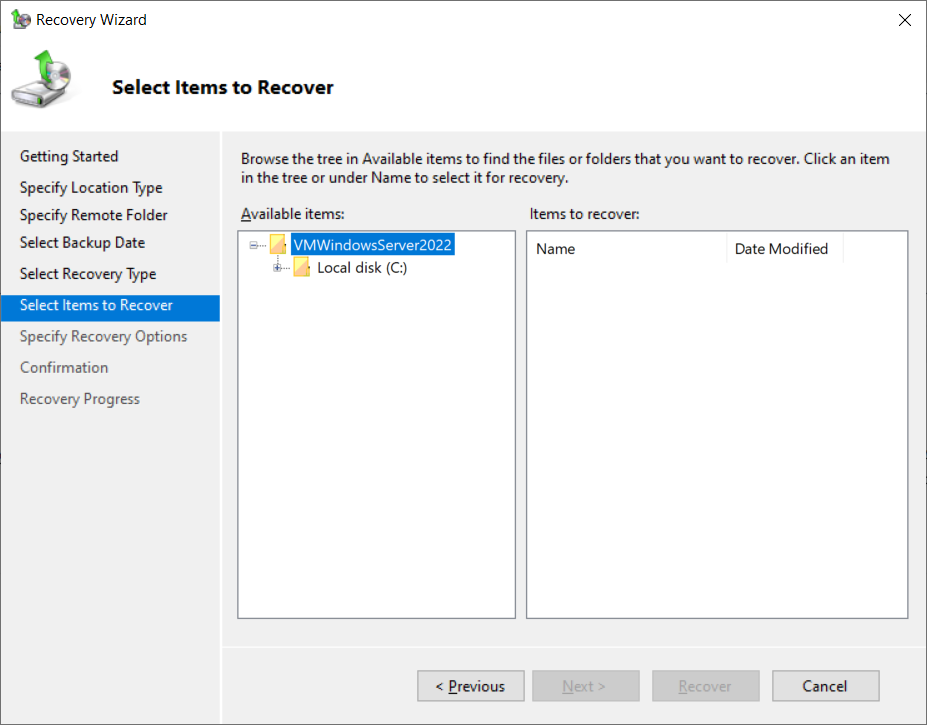
1. Check in Windows Server Backup console and the scheduled task is successful.



1. Check the backup folder in the network path, the entire C drive files are there.



1. Check in Windows Server Backup console and the entire C drive backup can be found through Recover options.



## Task 5.1

To ensure data privacy and protect user information against New Zealand Privacy Act ("Privacy Act 2020,"2023), 3 professional and ethical practices are adopted for TechCo Solutions design and deployment:

1. Access control and User Authentication.
   * Implement strict access control mechanisms and multi-factor authentication (MFA) to ensure that only authorized users can access sensitive data.
   * In TechCo Solution secured network, the users of Account can access the salary data of employees, but the user from other departments are restricted to access the salary data with role-based access control.
   * By limiting the access to the salary data based on roles, the risk of unauthorized access is minimized. MFA add an additional layer of security, ensuring that even if the password of users leaked, the account remains protected.
2. Secure Remote Access
   * To deploy Virtual Private Network (VPN) to secure remote access, as well as with MFA to enforce strong password policies.
   * In TechCo Solution secured network, the staff working at home must connect back to the network of TechCo Solutions through VPN.
   * This practise ensures that remote access is secure, reducing the risk of unauthorized access through insecure Internet connections. At same time, MFA add an additional layer of security for the remote users.
3. Data Encryption for both local storage and transmission.
   * Ensure that the sensitive data is encrypted when it is stored on the local storage and transit on the network. Industrial standard encryption protocol such as AES-256 and SSL/TLS should be adopted.
   * In TechCo Solution secured network, the source code of development department of TechCo solutions is encrypted in the local storage with AES-256. When to transit documents between TechCo Solutions and its customers, SSL/TLS protocol is used.
   * This practise ensures that in case of unauthorized access to the local storage, the encrypted source code could not be read directly. And SSL/TLS protocol protects the document could not be attacked in the middle of network during the transmission between customers and TechCo Solutions.

To ensure that overall ethical practices are established for the network solution, the following strategies should be adopted to effectively manage legal considerations and adhere to NZ data protection regulations ("Privacy Act 2020,"2023):

1. The IT administrator and the team should stay informed about legislation.
   * This includes enrolling in courses or obtaining certification from the organization focused on the privacy laws of New Zealand.
   * Staying informed about legislation ensures that the IT team can adjust the organization’s practices to remain compliant with legal requirements.
   * This proactive approach helps prevent non-compliance issues, reduces the risk of penalties, and upholds the organization's ethical commitment to protecting data and respecting privacy rights.
2. Regular monitor updates and changes in NZ data protection laws.
   * Utilize automated tools and subscription services to monitor updates and changes in New Zealand's data protection laws.
   * Schedule monthly or quarterly meetings specifically dedicated to reviewing any changes or updates in data protection laws. Maintain comprehensive documentation of all legislative updates and the organization’s response to them. By regularly monitoring updates and changes in data protection laws, the organization ensures that it remains compliant with the latest legal requirements.
   * This vigilance demonstrates a commitment to maintaining high ethical standards and adapting to evolving legal landscapes, thereby protecting the rights of individuals and the integrity of the organization.
3. Data breach response plan should be completed in advance.
   * This plan should cover all aspects of a breach, including detection, containment, eradication, recovery, and post-incident analysis.
   * It should be aligned with the legal requirements of the Privacy Act 2020, including mandatory breach notification rules.
   * A well-prepared data breach response plan ensures that the organization can quickly and effectively respond to incidents, minimizing damage and legal repercussions.
4. Employee training about data protection act should be hold regularly.
   * Implement mandatory data protection training programs for all employees, including new hires during onboarding and existing staff at regular intervals.
   * These programs should cover the Privacy Act 2020, emphasizing key principles, the importance of compliance, and the specific roles of employees in protecting personal data.
   * Regular and role-specific training ensures that all employees are aware of their responsibilities under the Privacy Act 2020, reducing the risk of accidental breaches and promoting a culture of compliance.

## References

1. Ubiquiti UniFi UXG-PRO. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/NETUBI2203/Ubiquiti-UniFi-UXG-PRO-Next-generation-Gateway-Pro.
2. Ubiquiti UniFi Switch Gen2 USW-PRO-24. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/SWHUBI824000/Ubiquiti-UniFi-Switch-Gen2-USW-PRO-24-24-Port-Giga
3. Ubiquiti UniFi Switch Gen2 USW-PRO-48. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/SWHUBI848000/Ubiquiti-UniFi-Switch-Gen2-USW-PRO-48-48-Port-Giga.
4. Ubiquiti Access Point AX5300. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/NAPUBI615300/Ubiquiti-UniFi-U6-Pro-Dual-Band-AX5300-Semi-Outdoo.
5. HP Business Printer. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/PTRHPL5738150B/HP-Business-Printer-Startup-Pack-Includes-one-4301.
6. Asustor NAS AS3304T. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/NASAST33042/Asustor-Drivestor-4-Pro-Gen2-AS3304T-v2-4-Bay-NAS.
7. Samsung 870 EVO 1TB SSD. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/HDDSAM62730/Samsung-870-EVO-1TB-25-Internal-SSD-V-NAND---SATA3.
8. HPE DL20 Gen11. (2024, August 18). PB Tech. https://www.pbtech.co.nz/system-builder/builder/P65396\_B21
9. PB MSI Cubi 5 Mini PC. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/WKSPB30012/PB-MSI-CUBI-5-Mini-PC-Intel-Core-i3-1215U-6-Cores
10. Windows Server Licenses. (2024, August 18). PB Tech. https://www.pbtech.co.nz/product/OSYMSO08328/Microsoft-Windows-Server-2022-Standard-16-Core-OEI.
11. Download pfSense community edition. (2024, August 18). pfSense. https://www.pfsense.org/download/
12. OpenVPN Community downloads. (2024, July 18). OpenVPN. https://openvpn.net/community-downloads/
13. Snort 3 release. (2024, August 18). Github. https://github.com/snort3/snort3/releases.
14. Download Microsoft authenticator. (2024, August 18). Microsoft Support. https://support.microsoft.com/en-us/account-billing/download-microsoft-authenticator-351498fc-850a-45da-b7b6-27e523b8702a
15. Azure Blob Storage pricing. (2024, August 18). https://azure.microsoft.com/en-us/pricing/details/storage/blobs
16. Privacy Act 2020. (2023, July 1). New Zealand Legislation. https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html