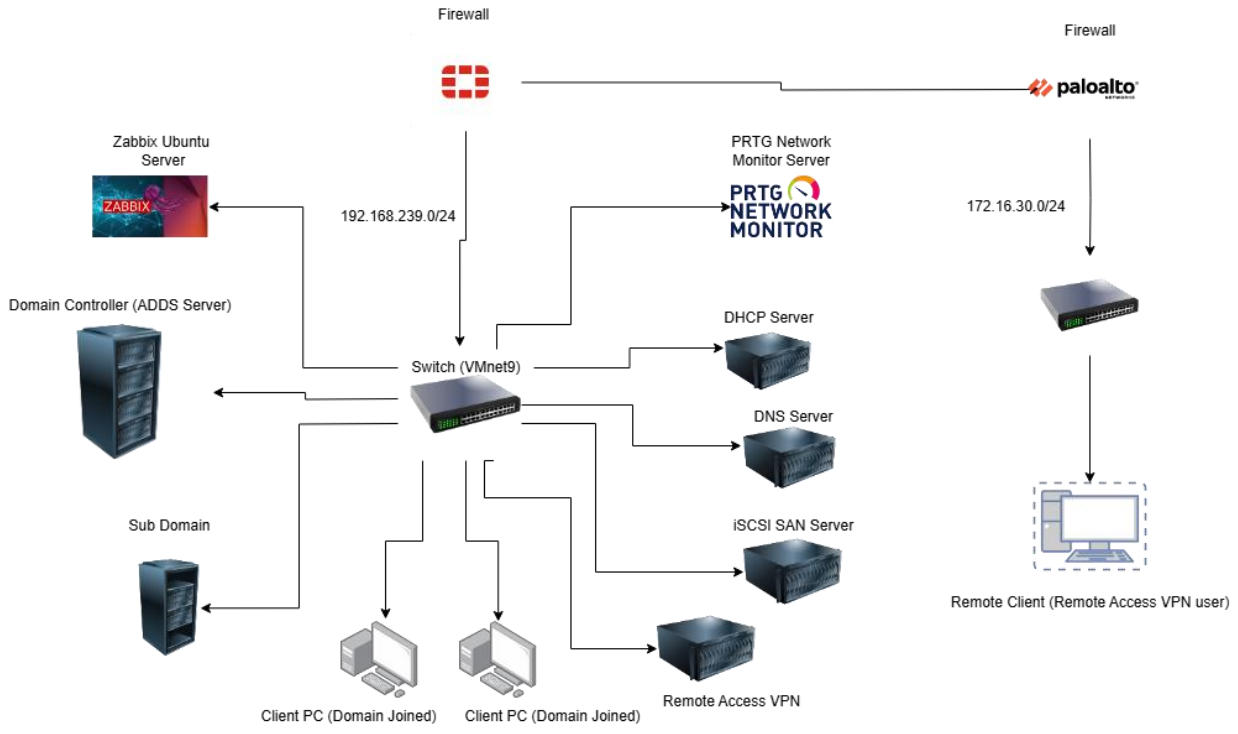
IT Infrastructure Deployment, Administration & Monitoring

By Md Muhtashim Jahin

This project involved the end-to-end deployment of an enterprise IT infrastructure designed for centralized management, security, and monitoring. The infrastructure consists of **7 Windows 22 Servers**, **1 Ubuntu Server**, **3 Client Machines (Windows 10)**, **2 Switches**, and **2 Firewalls (FortiGate & Palo Alto)**, all configured as a corporate network. **PRTG Network Monitor** and **Zabbix** are being used for Network Monitoring, Device Health, and Application Monitoring.

This project showcases my skills in IT Infrastructure Deployment & Design, System Administration, Network Configuration, Domain Management, VPN Implementation, Storage Provisioning, and Enterprise-Grade Monitoring using both **PRTG Network Monitor** and **Zabbix** Server & Application Monitoring.

Network Diagram



Services & Roles Deployed

- Deploy Domain Controller (ADDS Server) and add a client to the Domain (adatum.com).
- Sub-Domain Controller (bby.adatum.com).
- DHCP Server, Authorize the DHCP Server & Create a DHCP Scope
- DNS Server and Create Forward Lookup Zones (Secondary zone)
- iSCSI SAN Server
- Group Policy Objects (GPO)
- Remote Access Service (RAS) VPN Server
- Zabbix: Connect Servers, Firewall, and Clients to Zabbix for Device Monitoring.
- PRTG Network Monitor: Infrastructure Network Monitoring

Each Windows Server was assigned a dedicated role to ensure modular design and clear separation of services:

Active Directory Domain Services (ADDS) – Primary domain controller for centralized authentication.

Sub-Domain Controller – Facilitating organizational segmentation within the directory hierarchy.

DHCP Server – Dynamic IP address assignment across the internal network.

DNS Server – Internal name resolution for domain-based resources.

Remote Access VPN Server – Secure connectivity for remote users using RAS VPN.

iSCSI SAN Server – Centralized storage using iSCSI target services.

PRTG Monitoring Server – Real-time monitoring of network health, availability, and performance.

Zabbix Ubuntu Server is configured with **Zabbix**, providing Servers, Clients, and Applications monitoring and visibility.

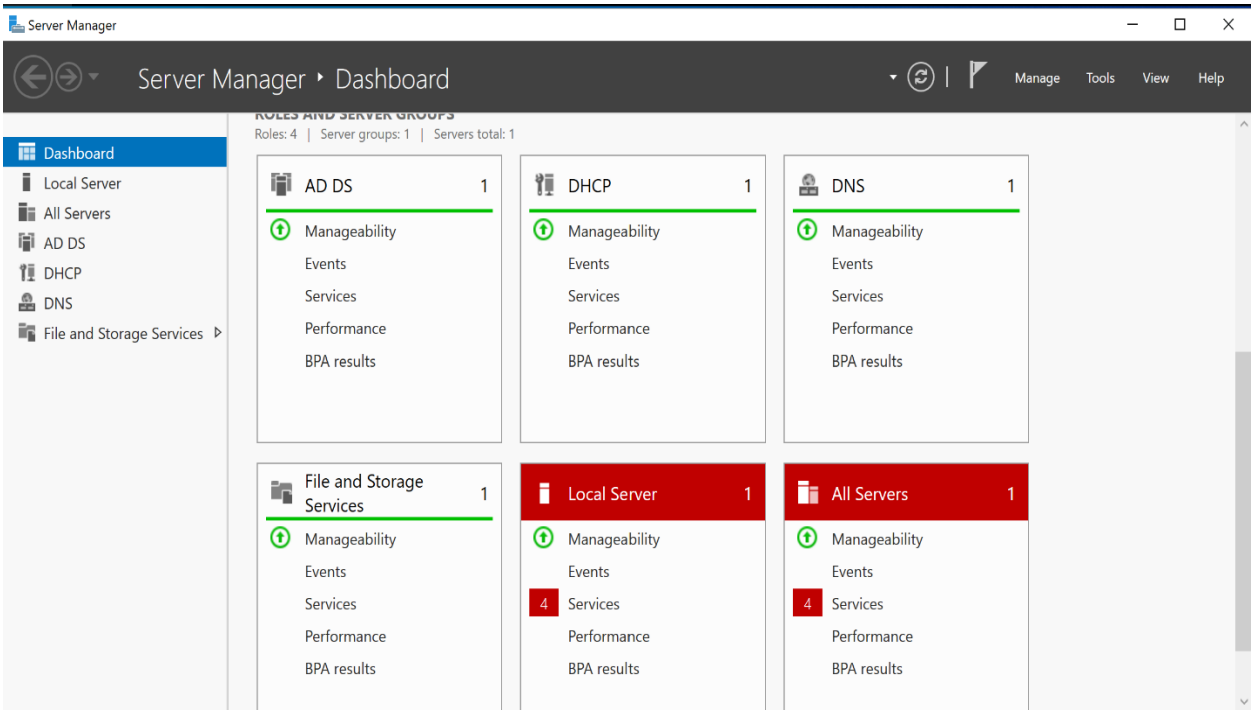
Client-side implementation included:

2 On-Site Clients: One joined to the root domain and the other to the sub-domain, simulating department-based access and policy segmentation.

1 Remote Client: Securely connected via Remote Access VPN to simulate external workforce access to internal network resources

A **FortiGate firewall** was configured to manage traffic flow, implement security policies, and enable VPN services, while two network switches handled VLAN segmentation and internal communication.

Deploy Domain Controller (ADDS Server) and add a client to the Domain (adatum.com)



Installing the ADDS Role on our Domain Controller Server

1. Log on to the server running Windows Server 2022 with Administrative Access.
2. Start Server Manager
3. Click Manage > Add Roles and Features
4. On the Select Installation Type page, Select Role-Based
5. Select The Server you want to make the Domain Controller
6. On the Server Roles Page, click the Active Directory Domain Services role.
7. When you are prompted to add features, click Add Features to accept the dependencies and click Next.
8. On the Confirmation Page, click install.

Promote the Server to Domain Controller

1. Click on the Yellow Triangle of Server Manager and Promote this server to a Domain Controller
2. In the Active Directory Domain Services Configuration Wizard, on the Deployment Configuration page, click Add a new Forest.
3. Click Next on DNS options. It will throw an error message. Ignore it, because we don't have any DNS role installed on this server.
4. On the Prerequisites Check page, click Install.
5. The Server will reboot

Add Client to the Domain

1. Ping the domain server.
2. Navigate to System and Security.
3. Select the Computer name, domain, and workgroup.
4. Add the domain.

Create a child domain (Sub-Domain)

1. Create a new server and join the domain. Ensure that you ping the domain for connectivity assurance.
2. Launch Server Manager, select Add role and features, and run the Add Role and Features Wizard.

3. Click Next.
4. Select Role-based installation.
5. On Select Server, choose the newly created server assigned for the Sub-Domain.
6. For the server role, select Active Directory Domain Servers.
7. Add required features (You can keep the defaults, if you're confused).
8. Review the information page and click Next.
9. Click install.

Promote the server to Domain Controller and configure it as a Child Domain.

1. Click on the notification flag (a yellow triangle)
2. Choose Add a new domain to an existing forest and Child Domain from the domain type. Provide the parent domain name, new domain name, and the credentials of an account that is part of the enterprise admin groups of your parent domain.
3. Choose Domain Name System (DNS) server and Global Catalog (GC). Provide the DSRM password and click Next.
4. On the DNS Options interface, on the “DNS Options” step, you will receive a warning. Review it and then click Next.
5. On the Additional Options interface, this tab will take a few seconds to load. Check it the NetBIOS domain name is correct; if not, change it to the required one. When satisfied, click Next.
6. On the Paths interface, click Next.
7. On the Review Options interface, click Next.
8. On the Prerequisites Check Interface, confirm that there are no issues, and then click Install.

Deploy a DHCP Server, Authorize the DHCP Server & Create a DHCP Scope

Deploy The DHCP Server

1. Login to your Domain Controller.
2. Launch Server Manager.
3. Select Add Roles and Features.

4. Select the server you want to deploy as DHCP Server.
5. Select the DHCP Server check box. Choose the features you need.
6. Confirm and Install the Server Role.

Authorizing the DHCP Server

1. Open the yellow notification flag and click Configure DHCP configuration.
2. Authorize the DHCP server to respond to DHCP Client requests. By forcing DHCP servers to be authorized, clients are protected from rogue domain-joined Windows DHCP servers that might maliciously affect network clients.

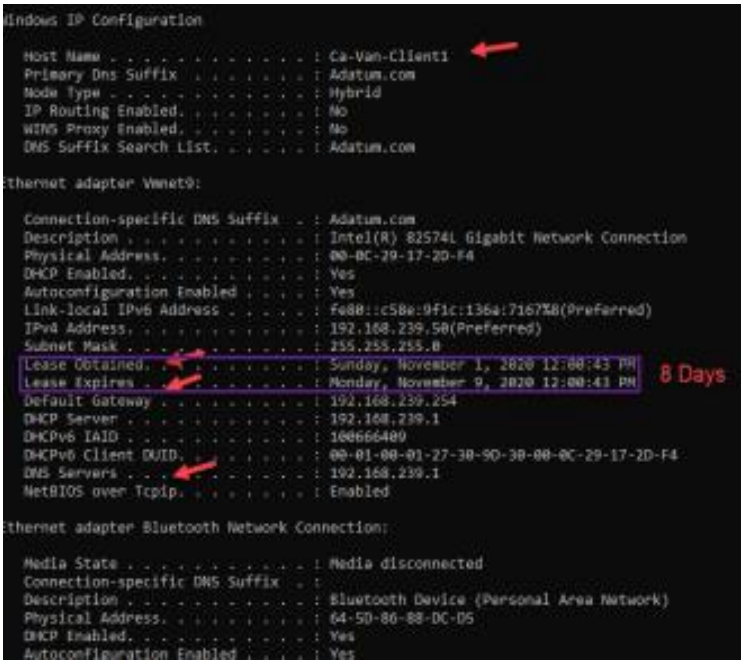
Create a DHCP Scope and Testing

1. Open Server Manager and Click Tools>DHCP.
2. Right-click on the IPv4 node and choose New Scope.
3. Type a Name for the Scope and click Next.
4. On the IP Address Range page, in the Start IP address text box, type the first in the range you want to assign. In the End IP Address text box, type the last address in the range. Choose the Subnet Mask you want to use.
5. On the Add Exclusions and Delay page, enter the IP address you want to exclude from the DHCP Service, to assign those IP addresses as static IP addresses for better management.
6. On the Lease Duration page, specify the leases for the addresses in the scope.
7. On the DHCP Options page, select I want to configure these options now.
8. On the Default Gateway, use the Edge Network Device IP address.
9. Type the Parent Domain Name and DNS Server IP Address.
10. Select Yes, I want to activate this scope now.

Test the DHCP Server

1. Login to your Client. Release the IP using iconfig/release and renew the IP using ipconfig/renew.
2. Type ipconfig/all in CMD

Congratulations! The DHCP Server is working.


indows IP Configuration
Host Name . . . . . : Ca-Van-Client1
Primary Dns Suffix . . . . . : Adatum.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : Adatum.com
thernet adapter Vmnet9:
Connection-specific DNS Suffix . : Adatum.com
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-17-2D-F4
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c58e:9f1c:136a:7167%8(Preferred)
IPv4 Address. . . . . : 192.168.239.50(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, November 1, 2020 12:00:43 PM
Lease Expires . . . . . : Monday, November 9, 2020 12:00:43 PM
8 Days
Default Gateway . . . . . : 192.168.239.254
DHCP Server . . . . . : 192.168.239.1
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-30-9D-30-00-0C-29-17-2D-F4
DNS Servers . . . . . : 192.168.239.1
NetBIOS over Tcpip. . . . . : Enabled
thernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 64-5D-86-88-DC-D5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

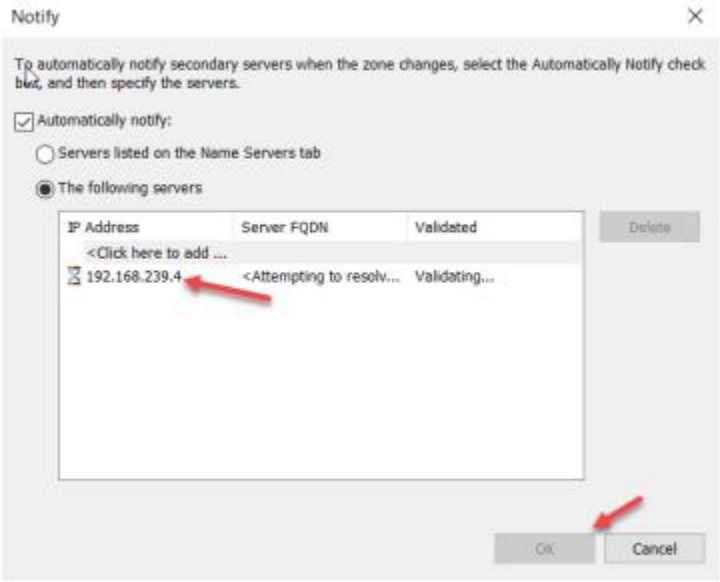
Deploy DNS Server and Create Forward Lookup Zones (Secondary zone)

Deploy the DNS Server

1. Create a new server and join the domain.
2. Install DNS Server Role.

Configure Forward Lookup Zones (Secondary Zone)

1. Launch Server Manager and Click Tools>DNS.
2. In DNS Manager, right-click Forward Lookup and select New Zone.
3. In the Zone type, choose Secondary Zone.
4. Type the name of Domain for which you are configuring DNS. Since the domain (adatum.com) has been installed, I will use adatum.com.
5. On the master DNS Server, you must type the IP of your domain.
6. Go to DNS Manager again and right-click to choose properties.
7. On the Zone Transfers tab, enable “Allow Zone Transfers”. Choose the Server IP so that the main DNS zone file can be copied to our Secondary Zone.

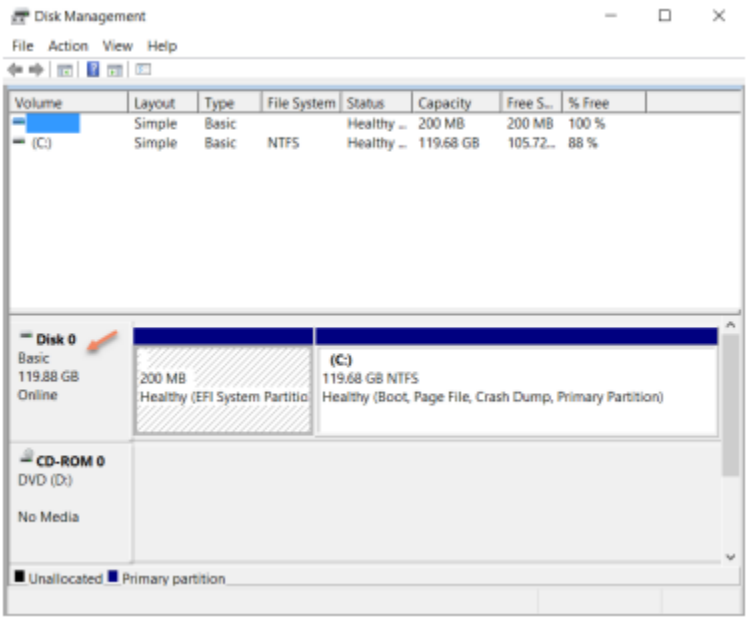


iSCSI SAN Server

Multiple protocols can be used to configure SANs. Fiber Channel SAN is expensive to implement. iSCSI SAN storage gives us an inexpensive and simple way to configure a connection to remote disks.

Create a Storage Pool and a Storage Space

1. Add at least 5 Hard drives to the Server to create a three-way mirroring.
2. Turn on the server and launch Server Manager.
3. Go to File and Storage Services>Storage Pools. Refresh if you cannot find any disks from the Physical disks.
4. Click “New Storage Pool”.
5. In the Storage Pool Name Field, type a name for storage space.
6. Select the disks for the pool and Click Create.



Create New Virtual Disk

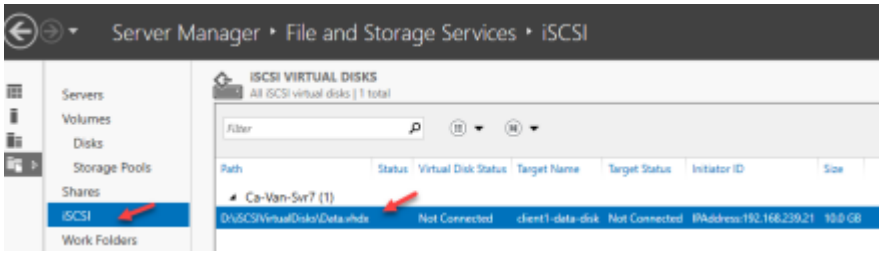
1. Right-click on the storage pool and then choose New Virtual Disk.
2. On the virtual disk name, give a name.
3. On Storage Layout, choose Mirror.
4. On Resiliency Settings, choose three-way mirror.
5. Choose Thin Provisioning.
6. Specify the Size.
7. Click Create.

Install iSCSI Target Server

1. Go to the Domain Controller Server and install the iSCSI Target Server role.
2. Select Role-Based installation.
3. On the Select Destination Server page, expand File and Storage Services, expand File and iSCSI Services, and click iSCSI Target Server and iSCSI Target Storage Provider. Click Next.
4. Click Install

Create an iSCSI Virtual Disk

1. Go to File and Storage Services and then click iSCSI.
2. On the Select Virtual Disk Location page, click a drive to store the iSCSI virtual disk and then click Next.
3. Give a name for the iSCSI Virtual Disk.
4. Specify the iSCSI Virtual Disk Size.
5. On the Add Initiator ID page, for the type, select IQN, DNS Name, IP Address, or MAC address. Then, in the Value text box, type the corresponding value for the initiator that matches the type.
6. Click Create.



Configure iSCSI Initiator

1. Login to your client, which one you have used for the iSCSI Initiator ID.
2. Go to iSCSI Initiator properties, type the iSCSI Server IP Address, and Quick Connect.
3. Check the Discovery > Target Portals.
4. Go to Disk Management. You will find an unknown disk.
5. Initialize it, and you are done.

Remote Access Service (RAS) VPN Server

If you are doing it on a Virtualized Environment, then make sure to use a different Network Adapter on your Remote Client and add another adapter to your RAS VPN

Server. If you are in a real environment, deploy a separate client and create 2 Firewall Policies to send and receive packets from 192.168.239.0/24 and 172.16.30.0/24 (Remote) subnets.

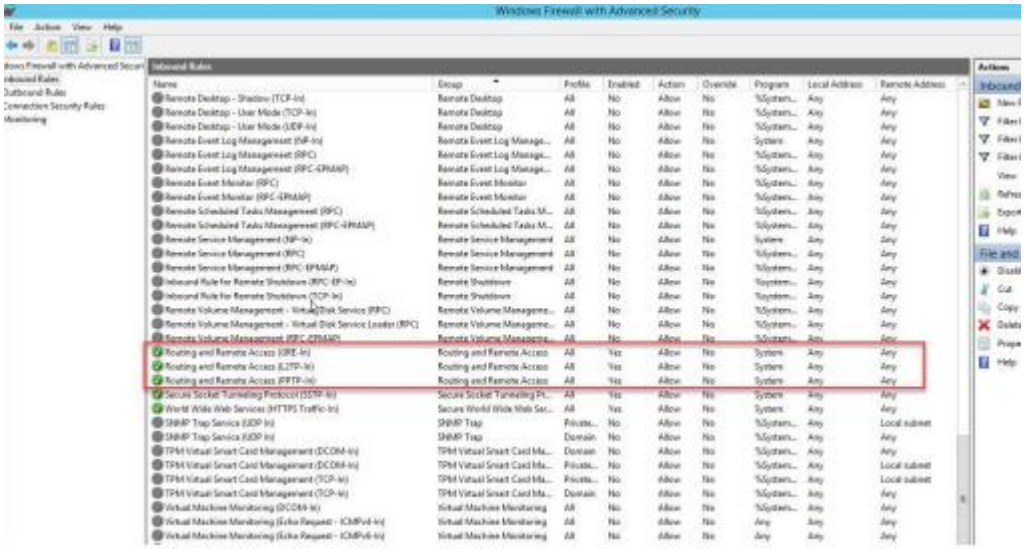
DC Server RAS VPN Server Remote Client

Svr1	Svr5	Client
Configure TCP/IP: IPv4 address: 192.168.239.1 Subnet Mask: 255.255.255.0 DNS Server 127.0.0.1	Configure TCP/IP: IPv4 address: 192.168.239.5 Subnet Mask: 255.255.255.0 DNS Server 192.168.239.1 IPv4 address: 172.16.30.10 Subnet Mask: 255.255.255.0	Configure TCP/IP: IPv4 address: 172.16.30.20 Subnet Mask: 255.255.255.0

Install and Configure Remote Access Service (RAS) VPN

1. Login to the RAS VPN Server and install Remote Access via Server Manager.
2. Launch the Getting Started wizard, and in the tab, click Deploy VPN Only
3. It then opens the Routing and Remote Access MMC. Right-click on the Server name and choose Configure and Enable Routing and Remote Access. On the Routing and Remote Access Server Setup Wizard, choose custom configuration.
4. Select “VPN Access”.
5. After you have clicked finish, you can now start the Routing and Remote Access service.
6. Go to the “Properties” and change the number of clients for better performance.

Configure the Windows Firewall



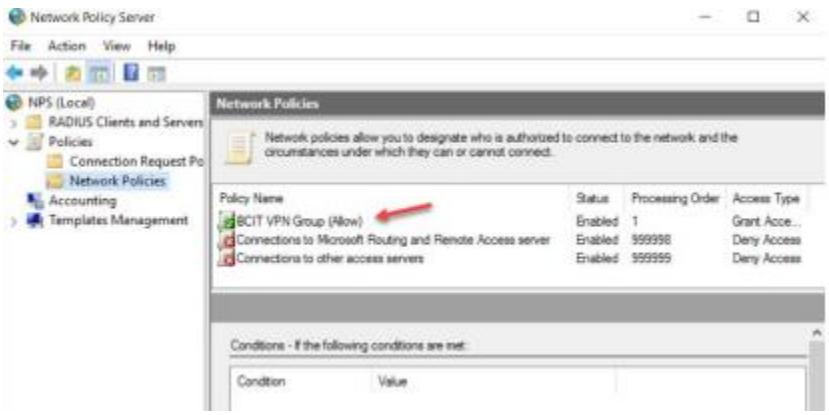
Create VPN Group and VPN User

1. Login to the Domain Controller and create an OU, a group, and add some users to the group. In my case, OU(Adatum), group (Adatum VPN Group), and General users like Jahin.

Configure Network Policy Server

Network Policy Server performs centralized authentication, authorization, and accounting for wireless authenticating switches and VPN connections.

1. Login to the VPN Server as Admin and Launch Server Manager.
2. Go to Routing and Remote Access>Remote Access Logging & Policies and then launch NPS.
3. Create a new Network Policy. Type the Network Policy name as “Adatum VPN Group” and select “Remote Access Server (VPN-Dial up)”
4. Add user group “Adatum VPN Group”
5. Set up Network Policies according to your organization’s preference.



Configure Remote Client (VPN Client)’

1. Go to Settings>Network & Internet>VPN>Add a VPN connection.
2. For VPN Provider, choose Windows (built-in). In the Connection name box, type a friendly name (Adatum VPN) for the VPN Profile.
3. For the VPN Type, choose the type of VPN connection you want to create (PPTP).
4. Select Save.