Et bilde som inneholder tekst, skjermbilde, diagram, Parallell

Automatisk generert beskrivelseNetwork Topology:

Et bilde som inneholder tekst, skjermbilde, programvare, Dataikon

Automatisk generert beskrivelseScreenshots

Et bilde som inneholder skjermbilde, display, tekst, datamaskin

Automatisk generert beskrivelse

Et bilde som inneholder tekst, elektronikk, skjermbilde, programvare

Automatisk generert beskrivelseEt bilde som inneholder skjermbilde, tekst, programvare

Automatisk generert beskrivelse

Notes on security

I used Windows Server 2022 and Ubuntu, so I’ll focus on security for these server types. I’ll write about some steps to take into account with security.

For windows server 2022:

1. Update the server with the latest security patches.
2. Firewall can be used to block or limit incoming/outgoing traffic based on rules that’s setup.
3. Managing user permissions and giving users limited roles for what they can do on the server. You can also force users to use a strong password and if needed, force users to change passwords.
4. If Microsoft Defender isn’t enough for the server, you could potentially go with a more heavy third-party antivirus program.
5. You could setup your server on a within a VLAN (Virtual LAN) as this isolates network traffic.
6. SSH Key Authentication instead of passwords for SSH

For Ubuntu Server:

1. Keep the server updated with “sudo apt update”
2. Use Fail2Ban on your server, this is an intrusion prevention software that does multiple security tasks, such as Log Monitoring and conditional IP Blocking.
3. SSH Key Authentication instead of passwords for SSH
4. netstat for monitoring network activites.
5. Disable root login and use sudo instead for admin commands.

For the servers I setup, I did sudo apt update for my Ubuntu server. And I downloaded all updates and turned on virus and threat detection for my windows server.