System and Network Administration Project

By: Anwar Ali Zeidani

Contents

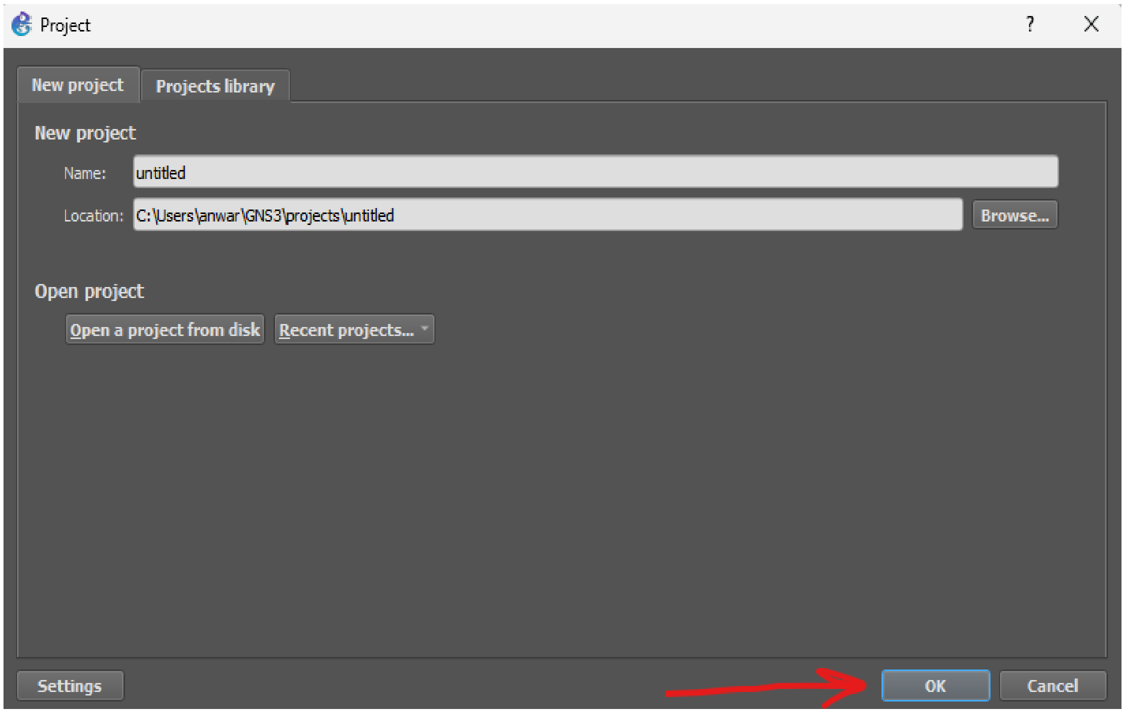
Part 1:Setting Up the GNS3 Environment:

Install GNS3 and import VMs

To install the latest gns3 version visit the official website (https://gns3.com/software/download)

You must login to get the software.

After installing gns3 and setup we create a project.

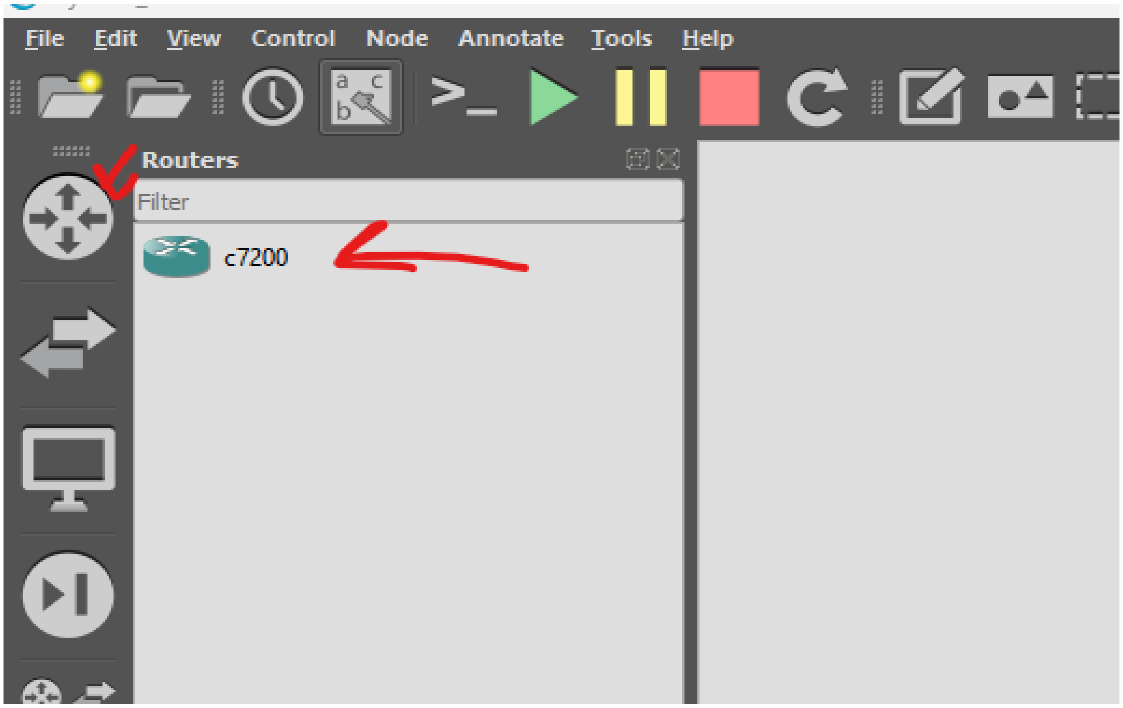


Name: untitled

Location: C:\Users\anwar\GNS3\projects\untitled

Now, we need to import gns3 appliance that we needed in our topology. We need a router image I choose the cisco c7200 from this github repository (https://github.com/hegdepavankumar/Cisco-Images-for-GNS3-and-EVE-NG)

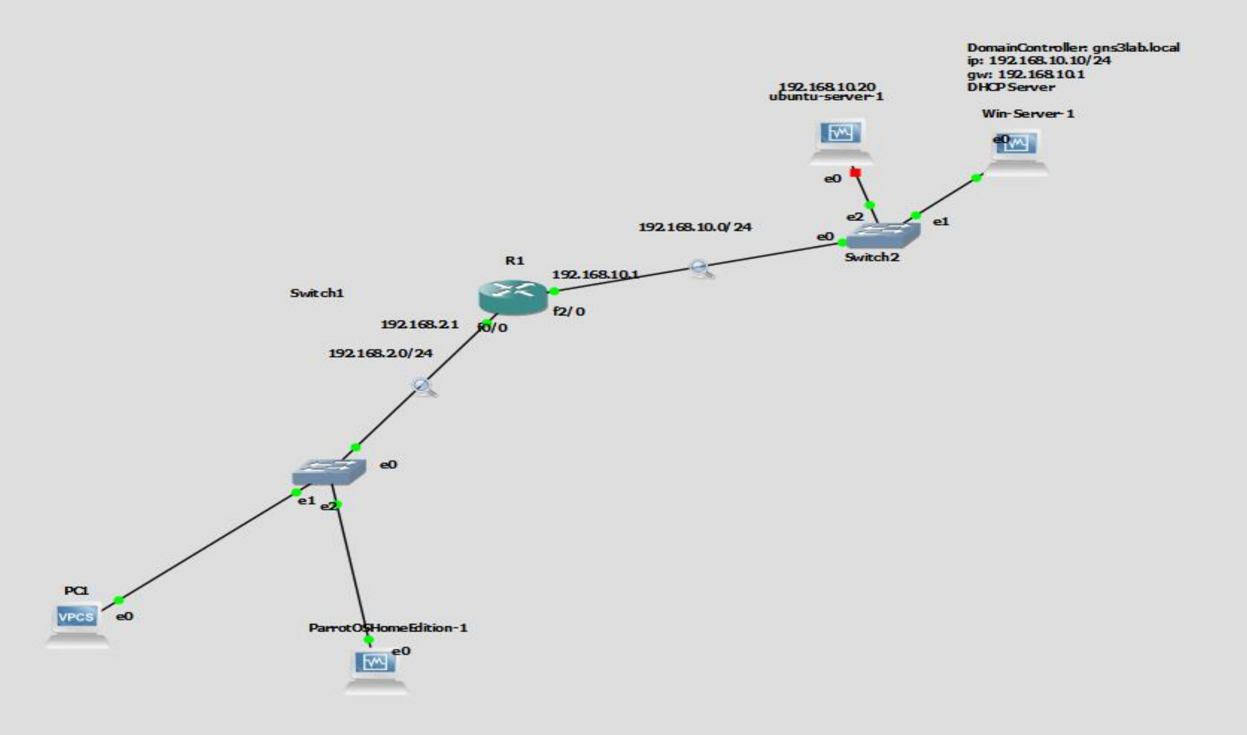
Download the image and open gns go to edit>Preferences>Dynamips>IOS routers>new>select_your_c7200_router_image, Apply and exit you will see the router inside the routers on the left of the gns



As we see in the above picture.

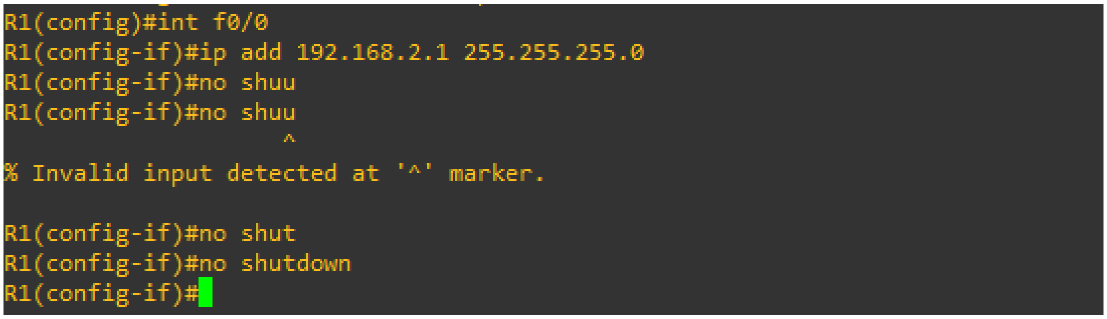
Build the Network Topology

Our network topology will consist of two switches, one router, two client PC's, Windows server, and Linux server.



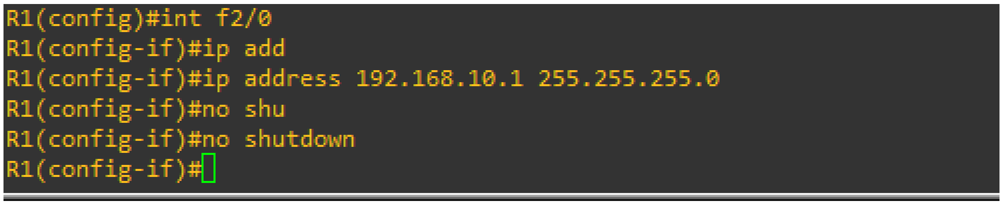
Lets configure our router first we need to set ip addresses to port f0/0 and f2/0.

To enable the console right click on the router and click on console.



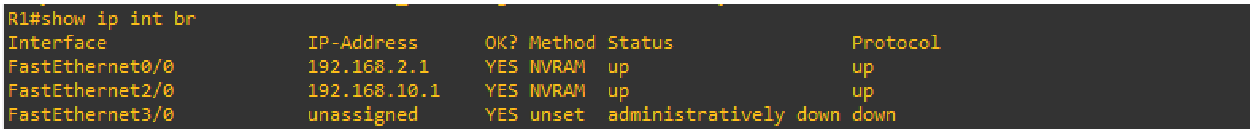
```
R1(config)#int f0/0
R1(config-if)#ip add 192.168.2.1 255.255.255.0
R1(config-if)#no shuu
R1(config-if)#no shuu
                    ^
% Invalid input detected at '^' marker.

R1(config-if)#no shut
R1(config-if)#no shutdown
R1(config-if)#
```

Int f0/0 are configured with IP 192.168.2.1



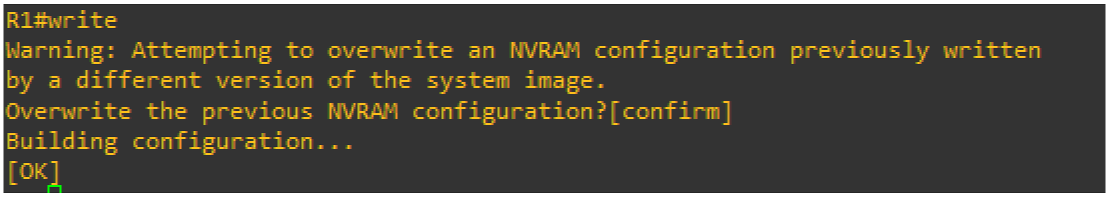
```
R1(config)#int f2/0
R1(config-if)#ip add
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shu
R1(config-if)#no shutdown
R1(config-if)#
```

Int f2/0 are configured with IP 192.168.10.1



```
R1#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.2.1     YES NVRAM  up                    up
FastEthernet2/0            192.168.10.1    YES NVRAM  up                    up
FastEthernet3/0            unassigned      YES unset  administratively down down
```

Always make sure that your configuration are work correctly then save the configuration in nvram.



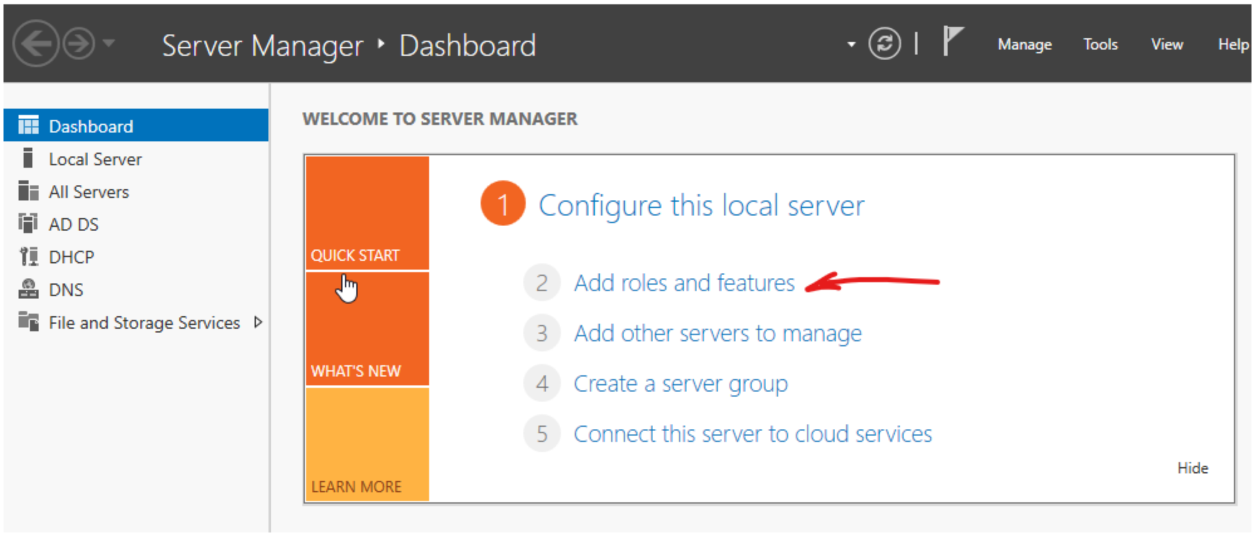
```
R1#write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
```

Using write command.

Part2: Windows Server Configuration (Active Directory & DHCP)

Install Windows Server & Promote to Domain Controller

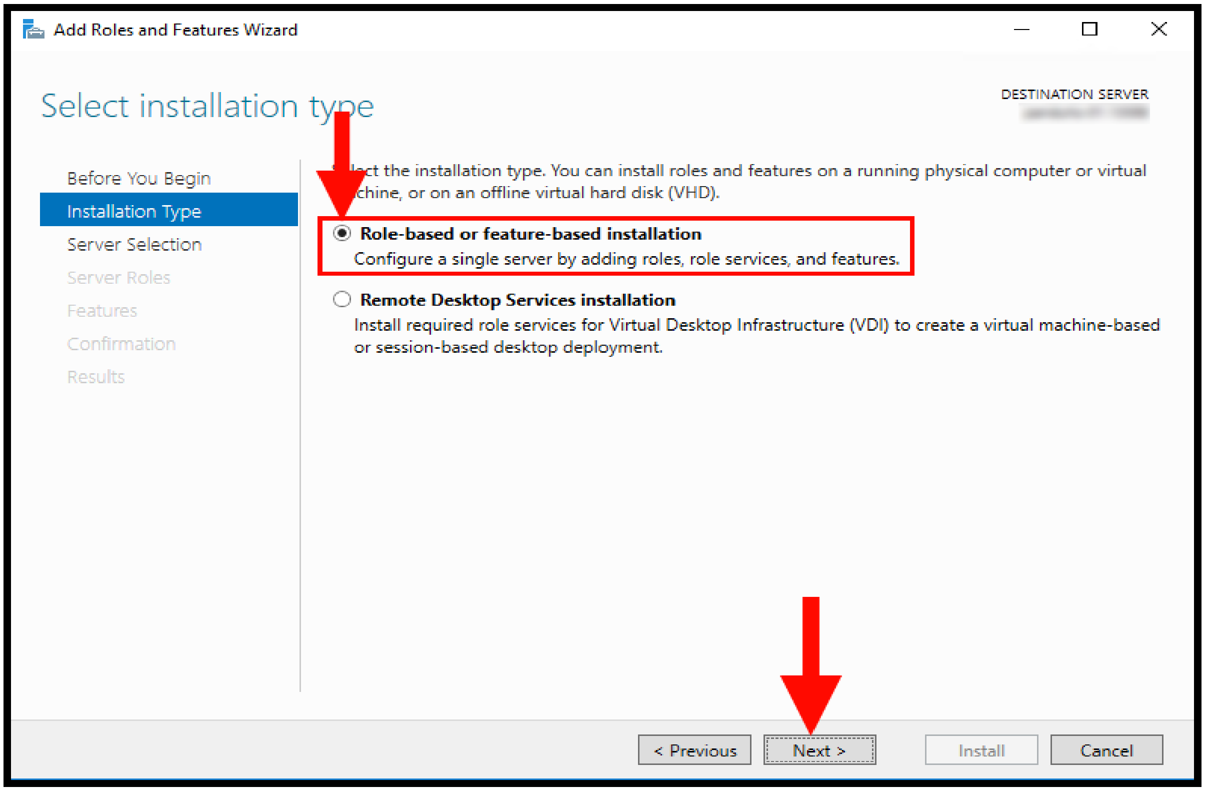
1) Install Active Directory Domain Services (AD DS).


Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services ▷
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide

1. **Open Server Manager**:
   - After logging into your Windows Server, Server Manager should open automatically. If not, you can open it from the Start menu.
2. **Add Roles and Features**:
   - In Server Manager, click on **"Manage"** in the top right corner, then select **"Add Roles and Features"**.
   - Click **"Next"** on the "Before You Begin" page.

3. **Select Installation Type**:

   - Choose **"Role-based or feature-based installation"** and click **"Next"**.



Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
[redacted]

ect the installation type. You can install roles and features on a running physical computer or virtual chine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

4. **Select Destination Server**:

   - Ensure your server is selected from the server pool (it should be the local server by default). Click **"Next"**.

5. **Select Server Roles**:

   - From the list of roles, check the box next to **"Active Directory Domain Services"**.

   - A dialog box will appear asking to "Add features that are required for Active Directory Domain Services". Click **"Add Features"**.

   - Click **"Next"**.

6. **Select Features**:

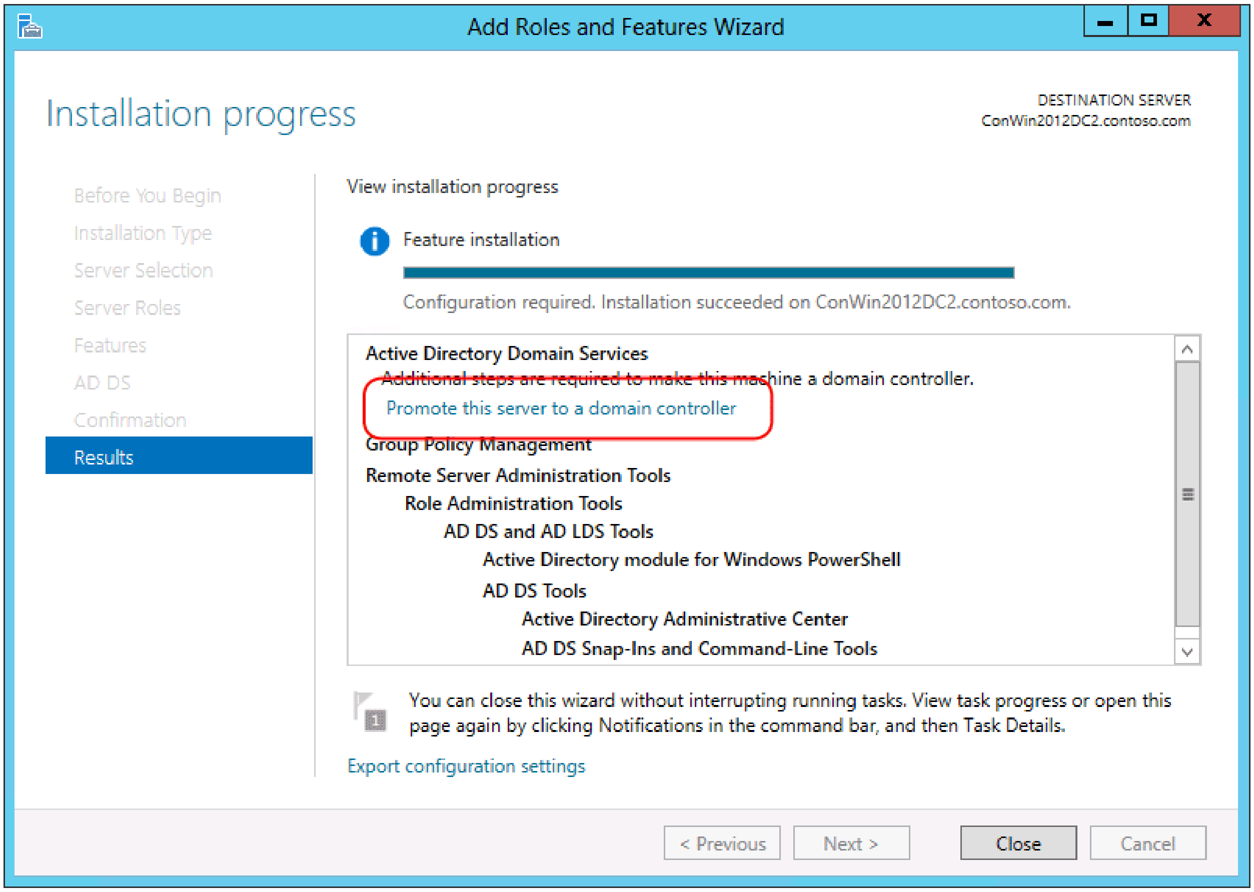
   - On the "Features" page, you don't typically need to add any additional features unless specified for a particular scenario. Click **"Next"**.

7. **AD DS Confirmation**:
    - Review the "Active Directory Domain Services" description. Click **"Next"**.
8. **Confirmation**:
    - Review your selections. You can optionally check **"Restart the destination server automatically if required"** (though a restart is usually not needed until after promotion).
    - Click **"Install"**.
9. **Installation Progress**:
    - The installation process will begin. Once it completes, you will see a message indicating that the installation succeeded and a link to "Promote this server to a domain controller". **Do not close this wizard yet.**

Step 2: Promote the Server to a Domain Controller

After the AD DS role is installed, you need to promote the server to a domain controller.

1. **Start the Promotion Wizard**:
    - In the "Add Roles and Features Wizard" results page, click the **"Promote this server to a domain controller"** link.
    - Alternatively, you can click the yellow warning flag in Server Manager and select "Promote this server to a domain controller".



Installation progress

DESTINATION SERVER
ConWin2012DC2.contoso.com

View installation progress

Feature installation

Configuration required. Installation succeeded on ConWin2012DC2.contoso.com.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

2. **Deployment Configuration**:
   - This is a crucial step. You have three options:
     - **Add a domain controller to an existing domain**: Use this if you already have an Active Directory domain and want to add another domain controller for redundancy or load balancing.
     - **Add a new domain to an existing forest**: Use this if you want to create a child domain within an existing Active Directory Forest.
     - **Add a new forest: This is the option you'll choose for your first domain controller in a new Active Directory environment.**
   - Select **"Add a new forest"**.

    - In the **"Root domain name"** field, enter your desired domain name (e.g., gns3lab.local). Use a .local suffix for internal networks or a public domain name you own.
    - Click **"Next"**.

Domain Controller Options:

- **Forest functional level** and **Domain functional level**: Choose the highest functional level supported by all domain controllers in your forest/domain. For a new environment, you can typically select the latest Windows Server version available.
- **Domain Name System (DNS) server**: This option will be checked by default and should remain checked as your domain controller will also act as a DNS server.
- **Global Catalog (GC)**: This option will be checked by default and should remain checked.
- **Read-only domain controller (RODC)**: Do not check this for your first domain controller.
- **Directory Services Restore Mode (DSRM) password**: Enter a strong password for DSRM. This password is used when you need to boot the domain controller into a special mode for recovery purposes. **Remember this password!**
- Click **"Next"**.

DNS Options:

- You might see a warning about DNS delegation. This is normal for a new forest as DNS hasn't been fully configured yet. Click **"Next"**.

Additional Options:

- **NetBIOS domain name**: This will be automatically populated based on your root domain name (e.g., YOURCOMPANY). You can change it if needed, but it's usually fine to leave it as is.
- Click **"Next"**.

Prerequisites Check:

- The wizard will perform a prerequisite check to ensure all conditions are met. If any warnings or errors appear, resolve them before proceeding. You will typically see a warning about DNS delegation, which is expected.

- Click **"Install"**.

Installation and Restart:

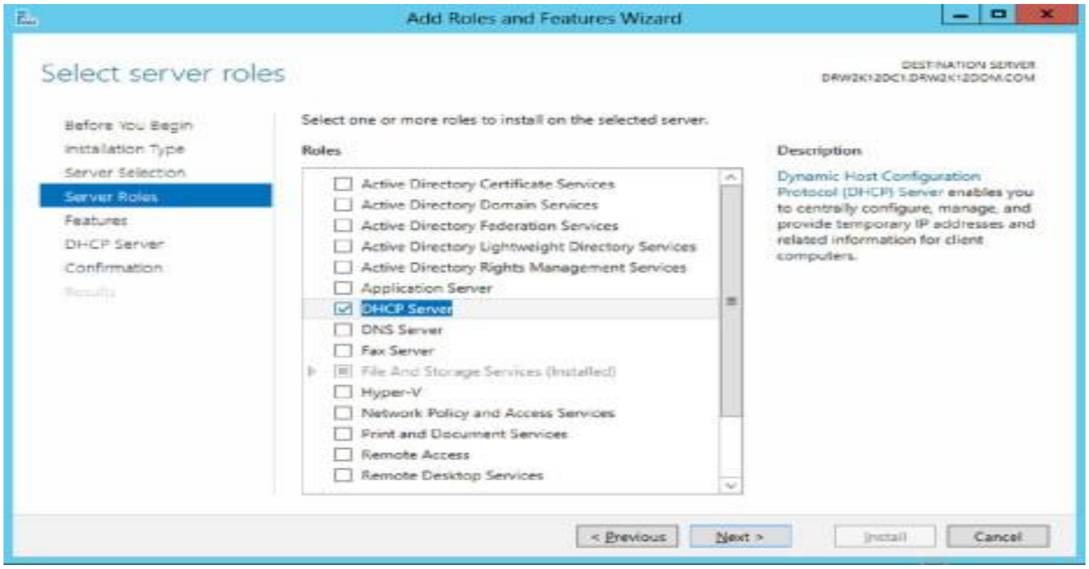
- The promotion process will begin. This can take some time.
- Once complete, the server will automatically restart.

Configure DHCP Server

Install the DHCP Server Role

1. **Open Server Manager**:
   - If not already open, open Server Manager from the Start menu.
2. **Add Roles and Features**:
   - Click on **"Manage"** > **"Add Roles and Features"**.
   - Click **"Next"** on the "Before You Begin" page.
3. **Select Installation Type**:
   - Choose **"Role-based or feature-based installation"** and click **"Next"**.
4. **Select Destination Server**:
   - Ensure your domain controller is selected. Click **"Next"**.

5. **Select Server Roles**:
   - From the list of roles, check the box next to **"DHCP Server"**.
   - A dialog box will appear asking to "Add features that are required for DHCP Server". Click **"Add Features"**.
   - Click **"Next"**.



Select server roles

DESTINATION SERVER
DRW2K12DC1.DRW2K12DOM.COM

Select one or more roles to install on the selected server.

Roles

□ Active Directory Certificate Services
□ Active Directory Domain Services
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
☑ DHCP Server
□ DNS Server
□ Fax Server
▣ File And Storage Services (Installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services

Description

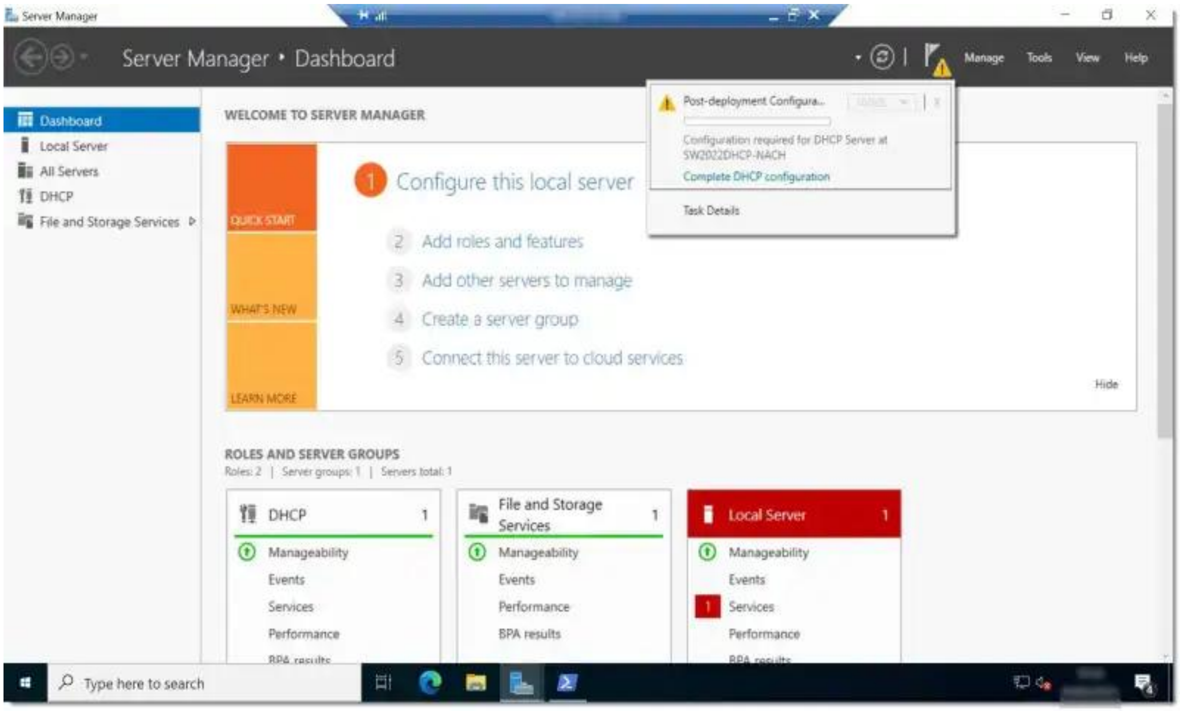
Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

6. **Select Features**:
   - On the "Features" page, click **"Next"**.
7. **DHCP Server Confirmation**:
   - Review the "DHCP Server" description. Click **"Next"**.
8. **Confirmation**:
   - Review your selections. You can optionally check **"Restart the destination server automatically if required"**.
   - Click **"Install"**.
9. **Installation Progress**:
   - The installation process will begin. Once it is completed, you will see a message indicating that the installation succeeded and a link to "Complete DHCP configuration".

Create a DHCP Scope

After installing the DHCP Server role, you need to configure a DHCP scope.

1. **Complete DHCP Configuration**:

   - 

     Post-deployment Configura...

     Configuration required for DHCP Server at SW2022DHCP-NACH

     Complete DHCP configuration

   - In the "Add Roles and Features Wizard" results page, click the **"Complete DHCP configuration"** link.
   - Alternatively, click the yellow warning flag in Server Manager and select "Complete DHCP configuration".
   - Click **"Next"** on the "Description" page.
   - Ensure the administrator account is selected for authorization. Click **"Commit"**.
   - Click **"Close"**.

2. **Open DHCP Console**:

   - In Server Manager, click on **"Tools"** > **"DHCP"**.

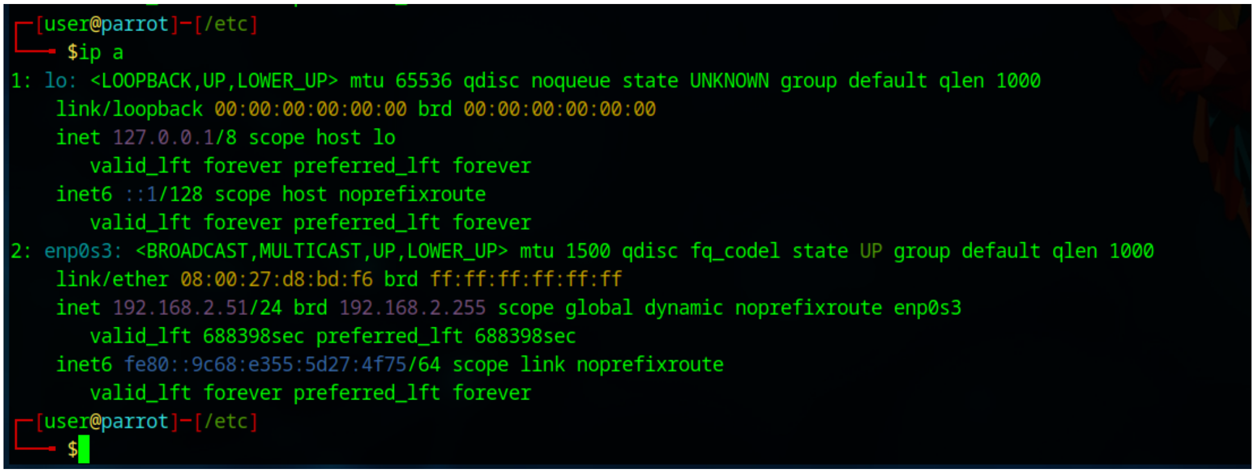
3. **Authorize the DHCP Server**:

   - In the DHCP console, you might see a red down arrow on your server name. Right-click on your server name and select **"Authorize"**.
   - Right-click again and select **"Refresh"**. The arrow should turn green.

4. **Create a New Scope**:
    - Expand your server name, then right-click on **"IPv4"** and select **"New Scope..."**.
    - Click **"Next"** on the "Welcome to the New Scope Wizard" page.
5. **Scope Name**:
    - Enter a **"Name"** for your scope (e.g., lan_network) and an optional **"Description"**.
    - Click **"Next"**.
6. **IP Address Range**:
    - Enter the **"Start IP address"**: 192.168.2.50
    - Enter the **"End IP address"**: 192.168.2.100
    - The **"Length/Subnet mask"** will automatically populate based on the IP range (e.g., 255.255.255.0 for a /24 network).
    - Click **"Next"**.
7. **Add Exclusions and Delay (Optional)**:
    - You can exclude specific IP addresses from the range if needed (e.g., for static assignments). For this guide, click **"Next"**.
8. **Lease Duration**:
    - Set the **"Lease duration"** (e.g., 8 days is common).
    - Click **"Next"**.
9. **Configure DHCP Options**:
    - Select **"Yes, I want to configure these options now"**.
    - Click **"Next"**.
10. **Router (Default Gateway)**:
    - Enter the **"IP address"** for your default gateway: 192.168.2.1
    - Click **"Add"**.
    - Click **"Next"**.

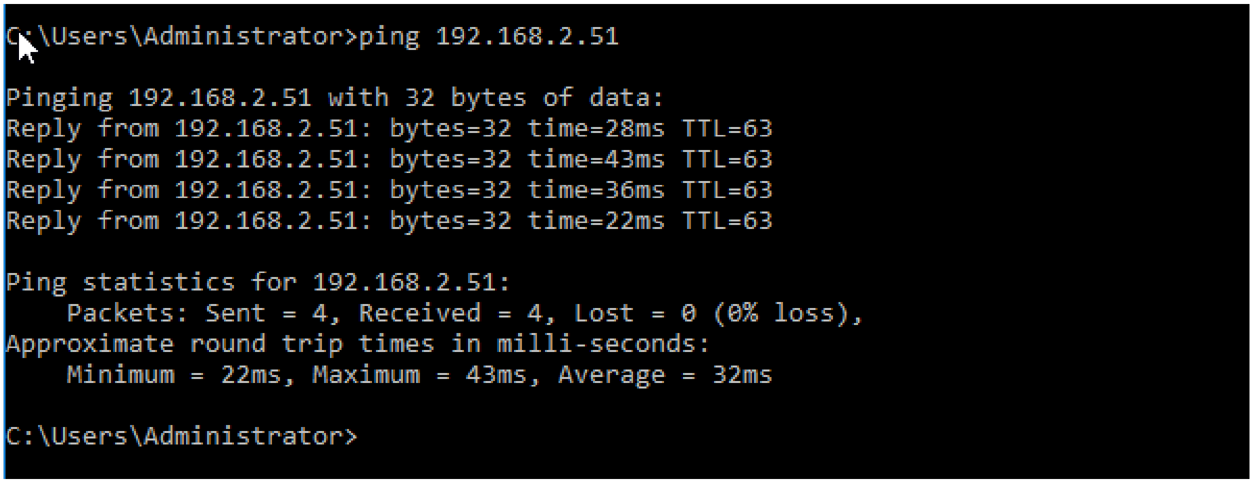
11. **Domain Name and DNS Servers**:
    - The **"Parent domain"** should be your Active Directory domain name.
    - Enter the **"IP address"** for your DNS server: 192.168.10.10
    - Click **"Add"**.
    - Click **"Next"**.
12. **WINS Servers (Optional)**:
    - If you don't use WINS, click **"Next"**.
13. **Activate Scope**:
    - Select **"Yes, I want to activate this scope now"**.
    - Click **"Next"**.
14. **Completing the New Scope Wizard**:
    - Click **"Finish"**.

Test DHCP from a Client

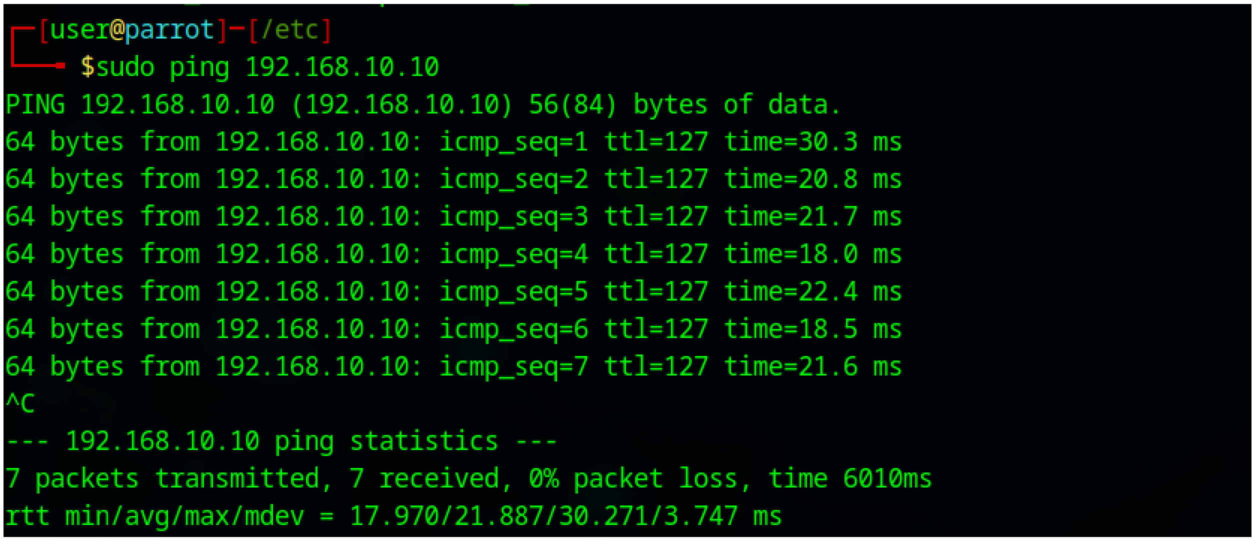


```
┌─[user@parrot]─[/etc]
└──╼ $ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d8:bd:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.51/24 brd 192.168.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 688398sec preferred_lft 688398sec
    inet6 fe80::9c68:e355:5d27:4f75/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
┌─[user@parrot]─[/etc]
└──╼ $
```

As we shown above the parrot client get ip 192.168.2.51 from the windows dhcp server



```
C:\Users\Administrator>ping 192.168.2.51

Pinging 192.168.2.51 with 32 bytes of data:
Reply from 192.168.2.51: bytes=32 time=28ms TTL=63
Reply from 192.168.2.51: bytes=32 time=43ms TTL=63
Reply from 192.168.2.51: bytes=32 time=36ms TTL=63
Reply from 192.168.2.51: bytes=32 time=22ms TTL=63

Ping statistics for 192.168.2.51:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 43ms, Average = 32ms

C:\Users\Administrator>
```



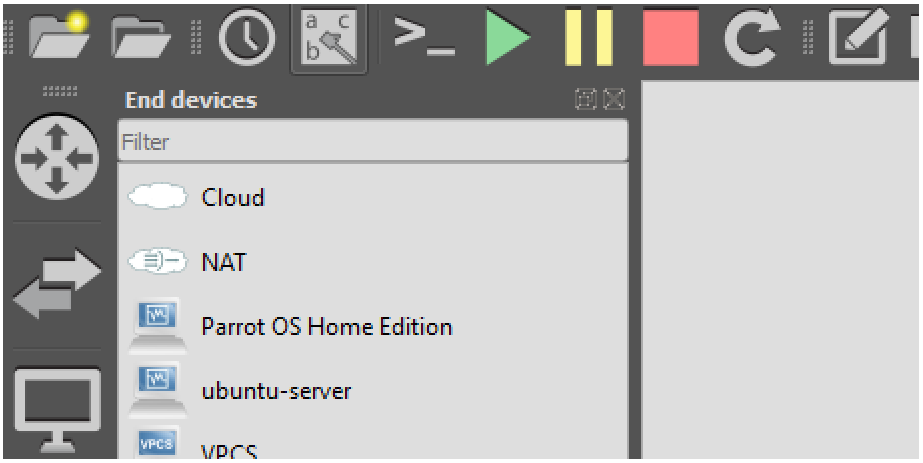
```
┌─[user@parrot]─[/etc]
└──╼ $sudo ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
64 bytes from 192.168.10.10: icmp_seq=1 ttl=127 time=30.3 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=127 time=20.8 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=127 time=21.7 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=127 time=18.0 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=127 time=22.4 ms
64 bytes from 192.168.10.10: icmp_seq=6 ttl=127 time=18.5 ms
64 bytes from 192.168.10.10: icmp_seq=7 ttl=127 time=21.6 ms
^C
--- 192.168.10.10 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 17.970/21.887/30.271/3.747 ms
```

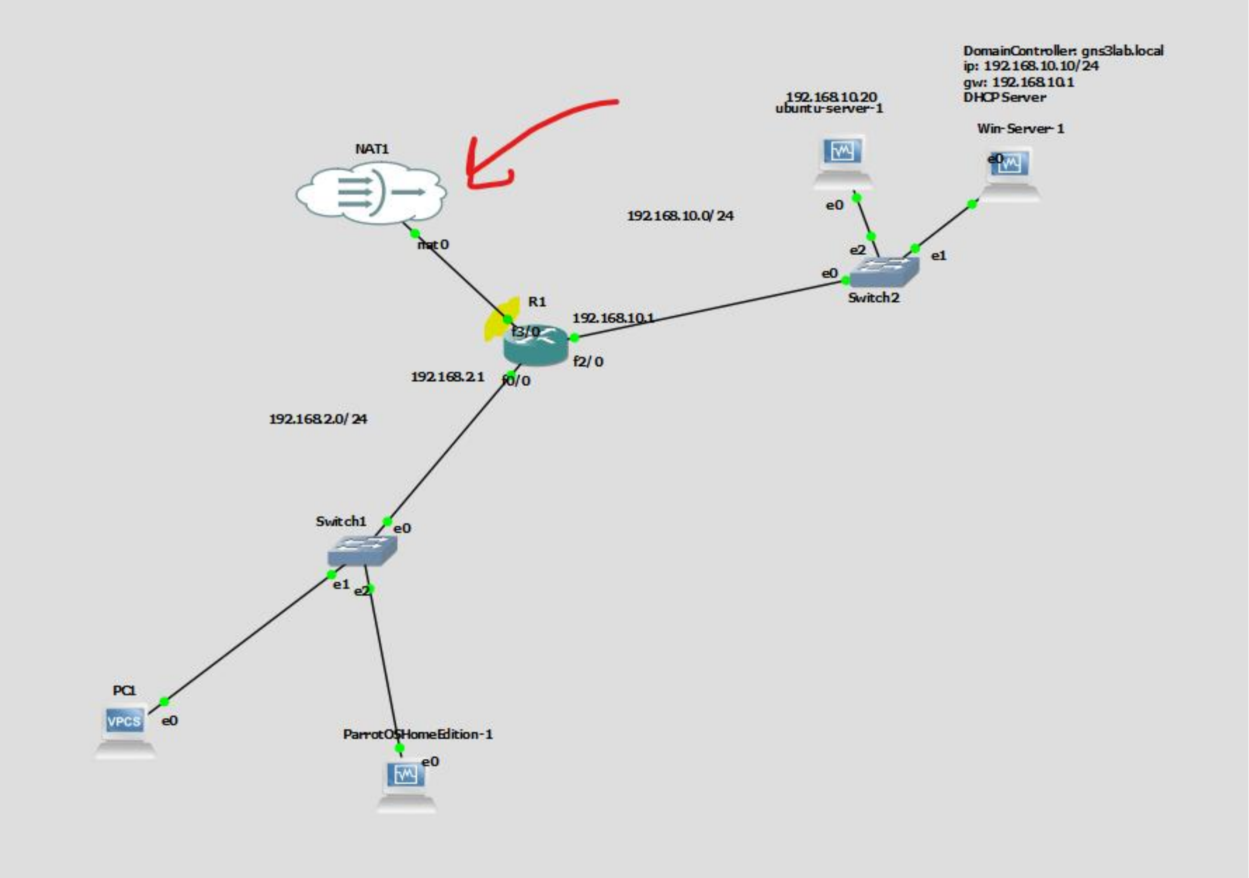
Check the connectivity between clients and windows server.

Part 3: Ubuntu Linux Server Configuration (Apache & SSH)

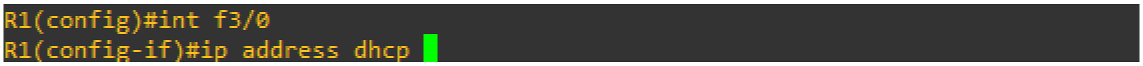
Before we configure Apache & SSH services lets connect our gns3 network to access internet connection using nat.

1. First deploy a NAT cloud from the left.

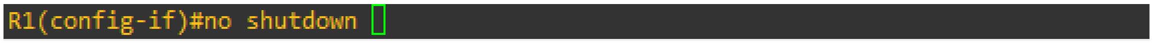




Now let's configure our router to route the Internet traffic inside and outside the LAN.

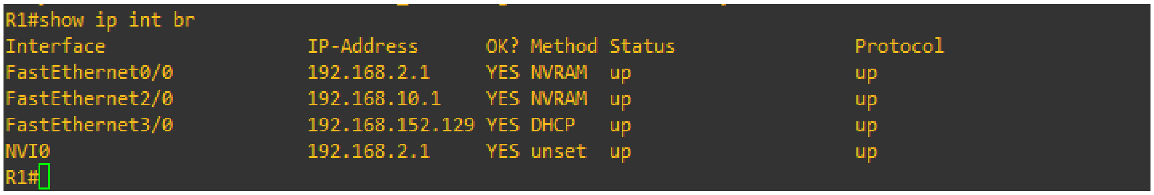


```
R1(config)#int f3/0
R1(config-if)#ip address dhcp
```



```
R1(config-if)#no shutdown
```

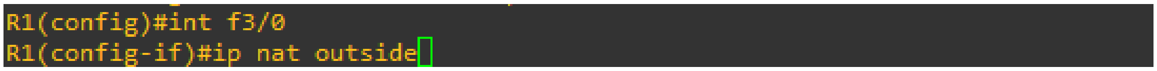
The interface f3/0 will get automatic DHCP from the NAT cloud.



```
R1#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.2.1     YES NVRAM  up                    up
FastEthernet2/0            192.168.10.1    YES NVRAM  up                    up
FastEthernet3/0            192.168.152.129 YES DHCP   up                    up
NVI0                       192.168.2.1     YES unset  up                    up
R1#
```

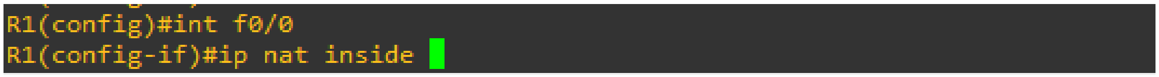
As shown in the image above the f3/0 get a DHCP ip (12.168.152.129).

Now we need to configure the inside-outside NAT interfaces.



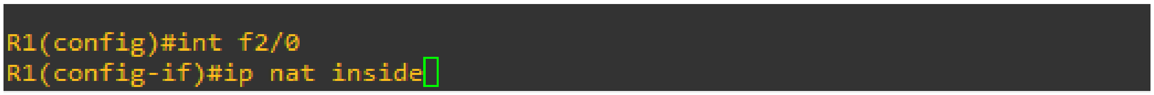
```
R1(config)#int f3/0
R1(config-if)#ip nat outside
```

Interface f3/0



```
R1(config)#int f0/0
R1(config-if)#ip nat inside
```

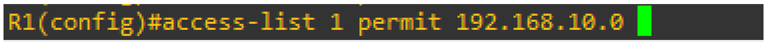
Interface f0/0



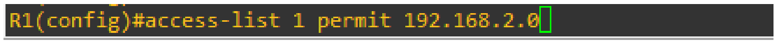
```
R1(config)#int f2/0
R1(config-if)#ip nat inside
```

Interface f2/0

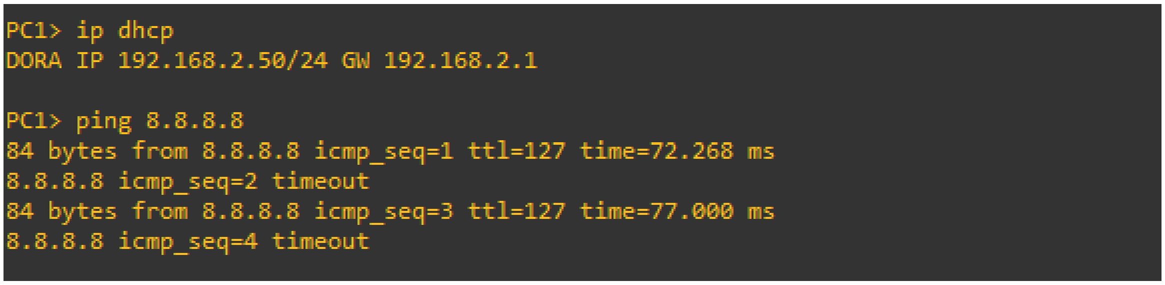
Then let’s permit our networks (192.168.10.0 & 192.168.2.0)



```
R1(config)#access-list 1 permit 192.168.10.0
```



```
R1(config)#access-list 1 permit 192.168.2.0
```



```
PC1> ip dhcp
DORA IP 192.168.2.50/24 GW 192.168.2.1

PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=127 time=72.268 ms
8.8.8.8 icmp_seq=2 timeout
84 bytes from 8.8.8.8 icmp_seq=3 ttl=127 time=77.000 ms
8.8.8.8 icmp_seq=4 timeout
```

This prove that now we have an internet connection.

Now let's dive throw ubuntu server to configure the apache2 and ssh services. First of all, we need to install the two services:

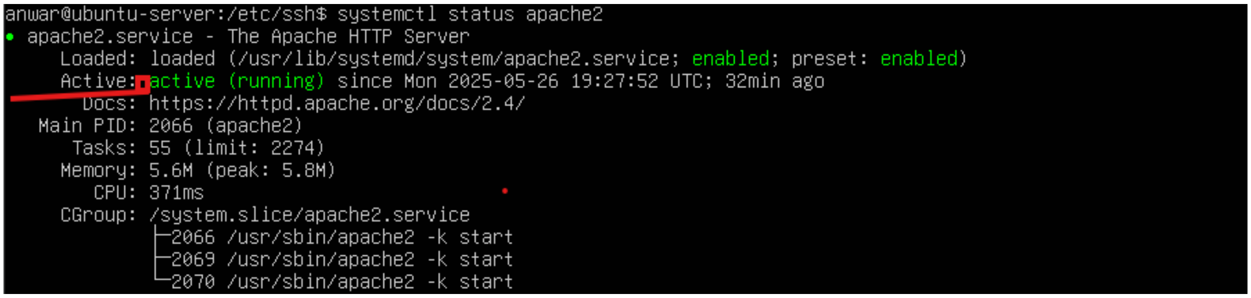
$sudo apt install apache2 -y

$sudo apt install ssh -y

After installing apache2 and ssh, let's begin with apache2 configurations.

To work the apache service we just need to start the service.

$sudo systemctl start apache2

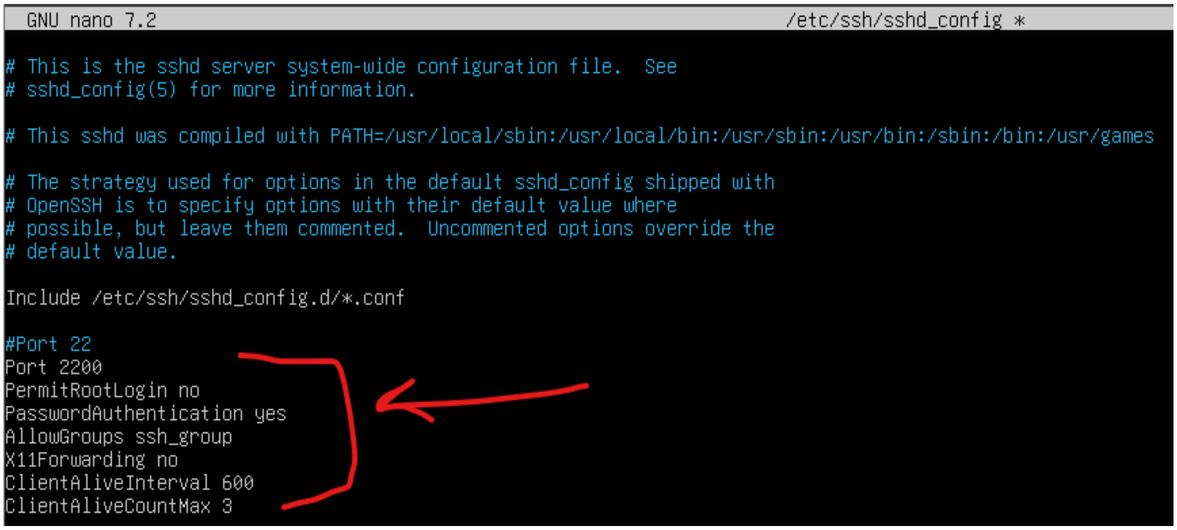


```
anwar@ubuntu-server:/etc/ssh$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-05-26 19:27:52 UTC; 32min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2066 (apache2)
      Tasks: 55 (limit: 2274)
     Memory: 5.6M (peak: 5.8M)
        CPU: 371ms
     CGroup: /system.slice/apache2.service
             ├─2066 /usr/sbin/apache2 -k start
             ├─2069 /usr/sbin/apache2 -k start
             └─2070 /usr/sbin/apache2 -k start
```

It must be active (running).

That enough to run apache2 service. Now let's configure the SSH service.

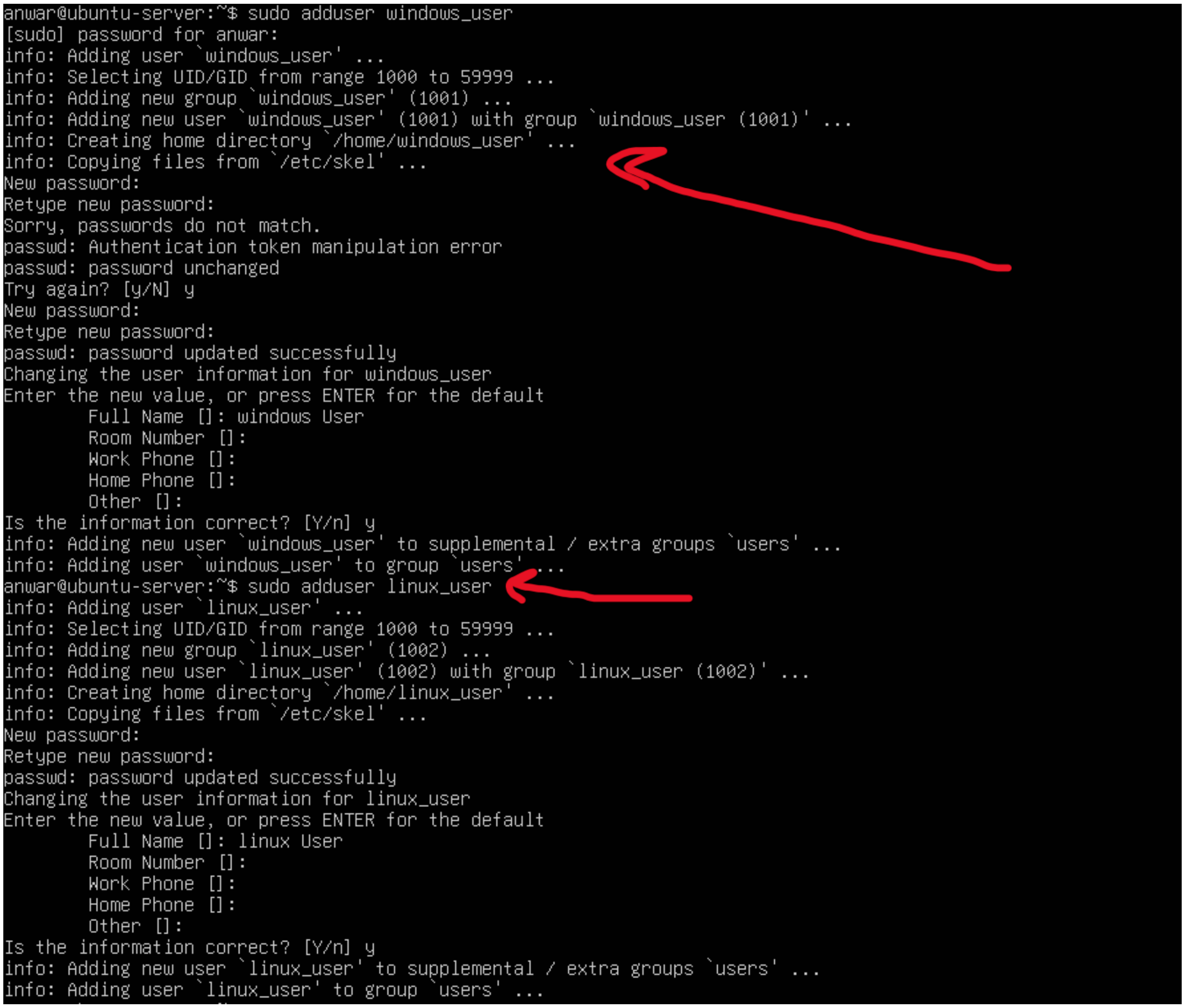
To configure the SSH we need to modify the /etc/ssh/sshd_config.



```
  GNU nano 7.2                                                        /etc/ssh/sshd_config *

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
Port 2200
PermitRootLogin no
PasswordAuthentication yes
AllowGroups ssh_group
X11Forwarding no
ClientAliveInterval 600
ClientAliveCountMax 3
```

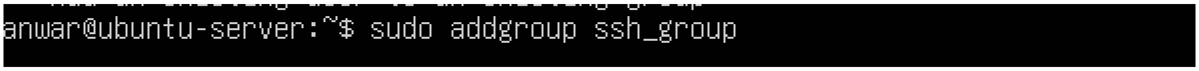
Now save and exit from the file.

Now, we should create a two users (linux_user, and windows_user) and create a group named ssh_group. Finally, assign the two users into the ssh_group and put the needed permissions.



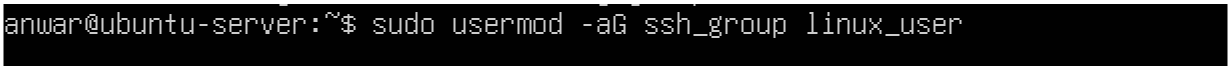
```
anwar@ubuntu-server:~$ sudo adduser windows_user
[sudo] password for anwar:
info: Adding user `windows_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `windows_user' (1001) ...
info: Adding new user `windows_user' (1001) with group `windows_user (1001)' ...
info: Creating home directory `/home/windows_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for windows_user
Enter the new value, or press ENTER for the default
        Full Name []: windows User
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `windows_user' to supplemental / extra groups `users' ...
info: Adding user `windows_user' to group `users' ...
anwar@ubuntu-server:~$ sudo adduser linux_user
info: Adding user `linux_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `linux_user' (1002) ...
info: Adding new user `linux_user' (1002) with group `linux_user (1002)' ...
info: Creating home directory `/home/linux_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for linux_user
Enter the new value, or press ENTER for the default
        Full Name []: linux User
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `linux_user' to supplemental / extra groups `users' ...
info: Adding user `linux_user' to group `users' ...
```

Add the allowed group. Note(The allowed group mentioned in the ssh configuration file as mentioned above).

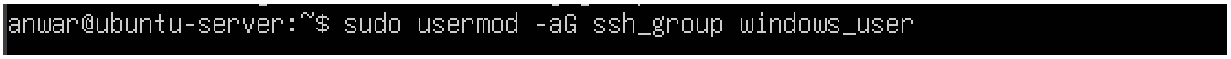


```
anwar@ubuntu-server:~$ sudo addgroup ssh_group
```

Assign the two users into this group.

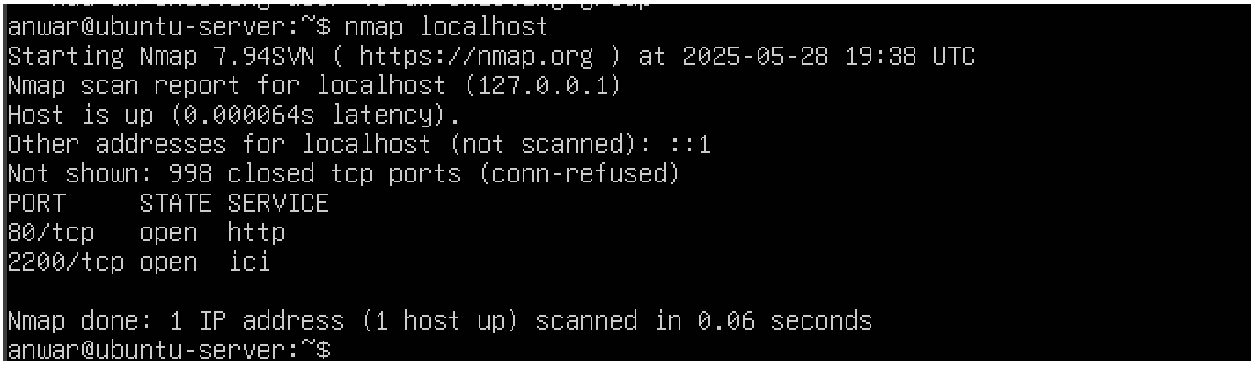


```
anwar@ubuntu-server:~$ sudo usermod -aG ssh_group linux_user
```



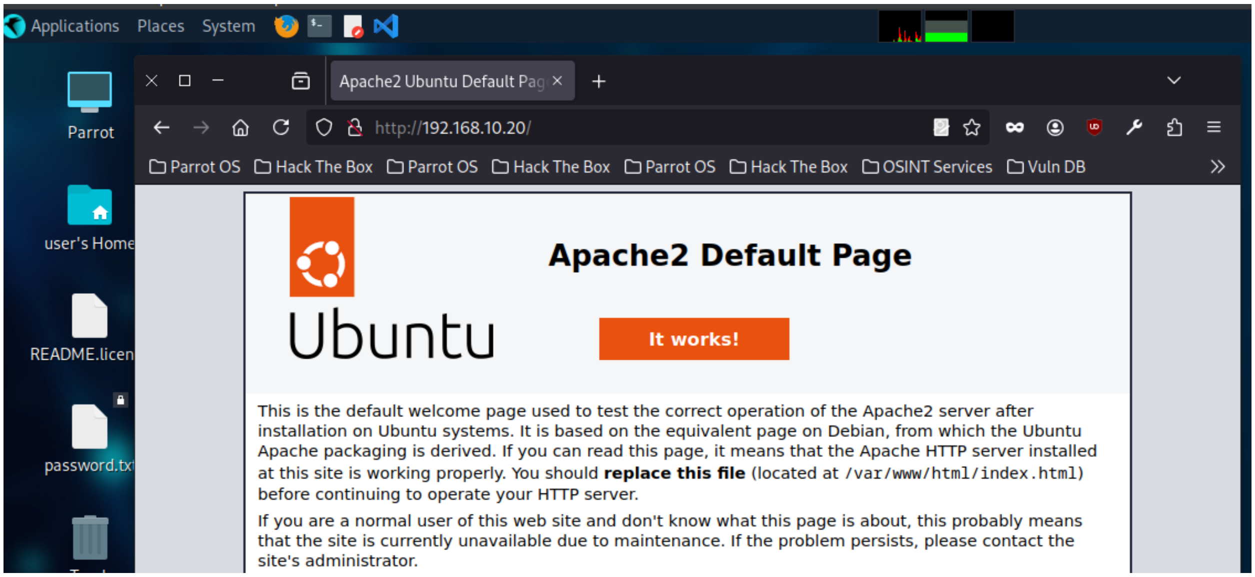
```
anwar@ubuntu-server:~$ sudo usermod -aG ssh_group windows_user
```

Now let’s check if the two services are running on ubuntu server. (Using nmap)



```
anwar@ubuntu-server:~$ nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-28 19:38 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000064s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
2200/tcp open  ici

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
anwar@ubuntu-server:~$
```

Let’s test our two services.

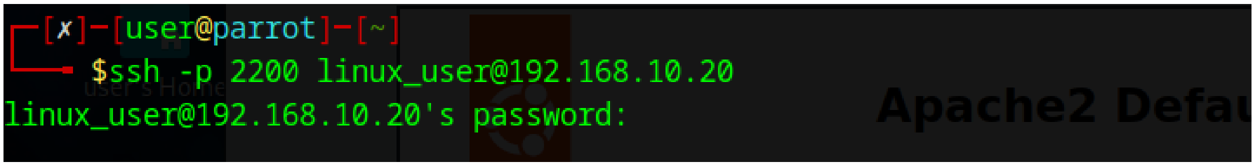


Apache2 Default Page

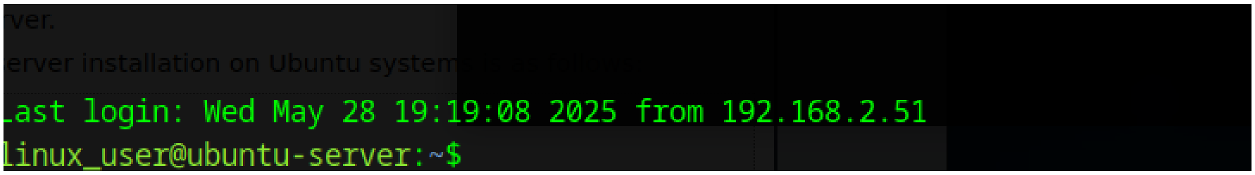
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

As shown above, The Linux client can visit the webpage that hosted on ubuntu server.



```
┌─[✗]─[user@parrot]─[~]
└──╼ $ssh -p 2200 linux_user@192.168.10.20
linux_user@192.168.10.20's password:
```



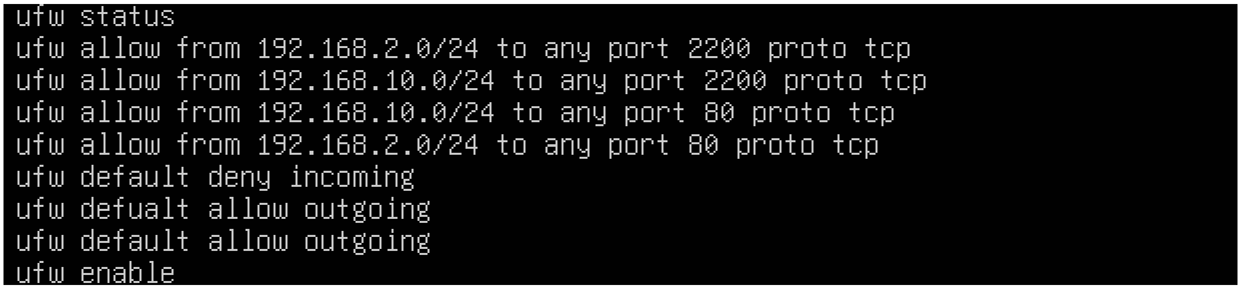
```
Last login: Wed May 28 19:19:08 2025 from 192.168.2.51
linux_user@ubuntu-server:~$
```

As shown above the linux user can connect to the ubuntu server as linux_user.

Part 4: Network Security & Testing

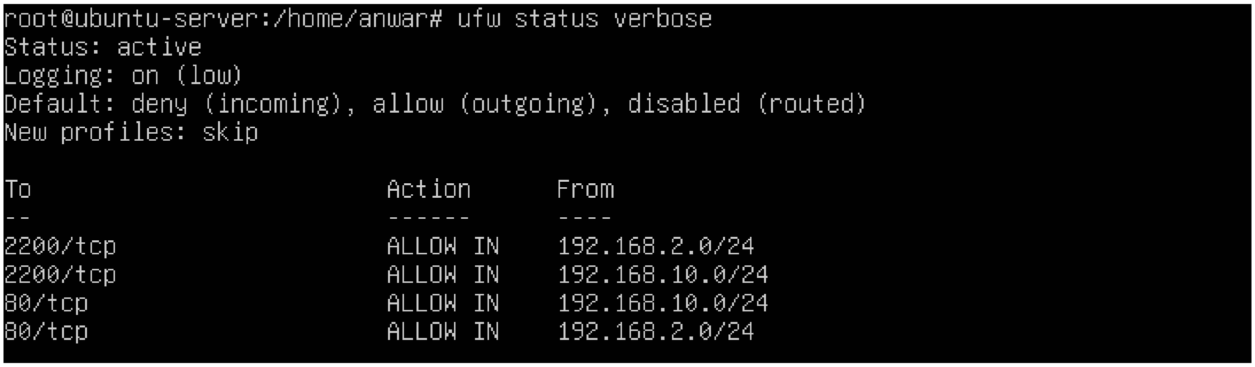
Configure Firewall Rules (Windows & Linux)

Ubuntu server using ufw and modsecurity (OWASP web application firewall as a software) configurations .



```
ufw status
ufw allow from 192.168.2.0/24 to any port 2200 proto tcp
ufw allow from 192.168.10.0/24 to any port 2200 proto tcp
ufw allow from 192.168.10.0/24 to any port 80 proto tcp
ufw allow from 192.168.2.0/24 to any port 80 proto tcp
ufw default deny incoming
ufw defualt allow outgoing
ufw default allow outgoing
ufw enable
```

Add these rules to only allow 192.168.2.0 and 192.168.10.0 to access port 2200 (ssh) and port 80 (http-service) and deny any at the end.

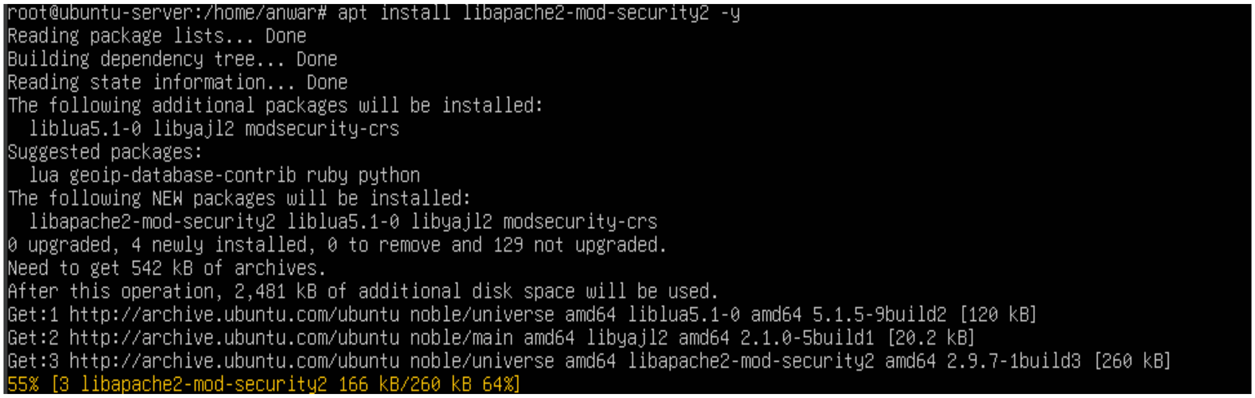


```
root@ubuntu-server:/home/anwar# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
2200/tcp                   ALLOW IN    192.168.2.0/24
2200/tcp                   ALLOW IN    192.168.10.0/24
80/tcp                     ALLOW IN    192.168.10.0/24
80/tcp                     ALLOW IN    192.168.2.0/24
```

Ensure that the rules are ALLOW IN and configured correctly.

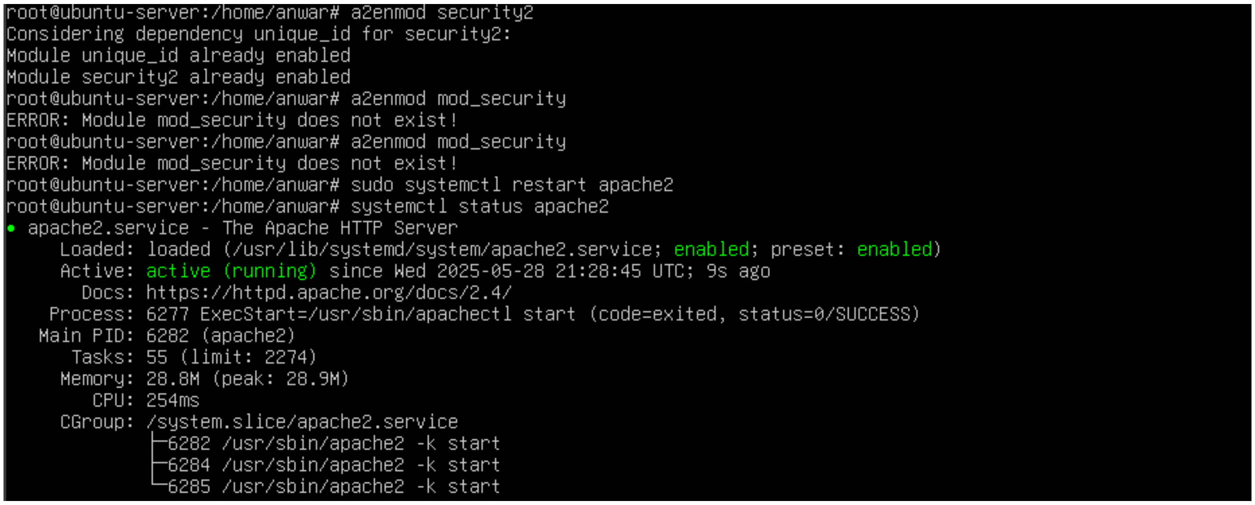
Now let's enhanced our security on the ubuntu server by applying the ModSecurity CRS as a Web Application Firewall (WAF).

First, we need to install the modsecurity CRS .



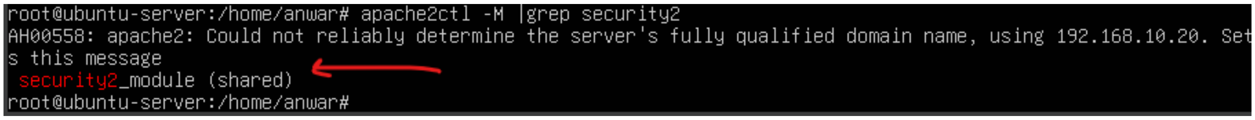
```
root@ubuntu-server:/home/anwar# apt install libapache2-mod-security2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  liblua5.1-0 libyajl2 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby python
The following NEW packages will be installed:
  libapache2-mod-security2 liblua5.1-0 libyajl2 modsecurity-crs
0 upgraded, 4 newly installed, 0 to remove and 129 not upgraded.
Need to get 542 kB of archives.
After this operation, 2,481 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 liblua5.1-0 amd64 5.1.5-9build2 [120 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libyajl2 amd64 2.1.0-5build1 [20.2 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/universe amd64 libapache2-mod-security2 amd64 2.9.7-1build3 [260 kB]
55% [3 libapache2-mod-security2 166 kB/260 kB 64%]
```

Apply the security2 module.



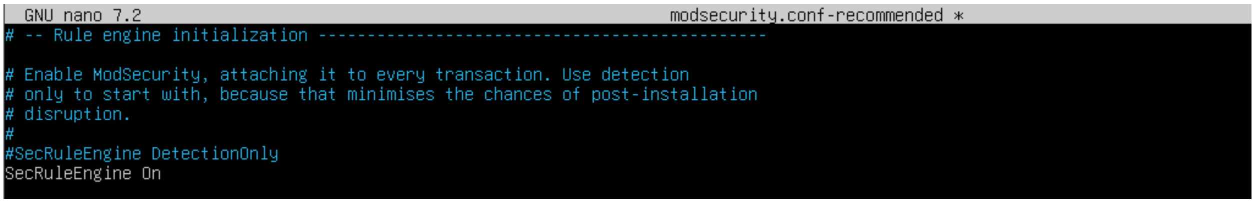
```
root@ubuntu-server:/home/anwar# a2enmod security2
Considering dependency unique_id for security2:
Module unique_id already enabled
Module security2 already enabled
root@ubuntu-server:/home/anwar# a2enmod mod_security
ERROR: Module mod_security does not exist!
root@ubuntu-server:/home/anwar# a2enmod mod_security
ERROR: Module mod_security does not exist!
root@ubuntu-server:/home/anwar# sudo systemctl restart apache2
root@ubuntu-server:/home/anwar# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-05-28 21:28:45 UTC; 9s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 6277 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 6282 (apache2)
      Tasks: 55 (limit: 2274)
     Memory: 28.8M (peak: 28.9M)
        CPU: 254ms
     CGroup: /system.slice/apache2.service
             ├─6282 /usr/sbin/apache2 -k start
             ├─6284 /usr/sbin/apache2 -k start
             └─6285 /usr/sbin/apache2 -k start
```

Restart the apache2 service and check the apache2 status.



```
root@ubuntu-server:/home/anwar# apache2ctl -M |grep security2
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 192.168.10.20. Set
s this message
 security2_module (shared)
root@ubuntu-server:/home/anwar#
```

Security2_module should appear means that security2 are enabled successfully.

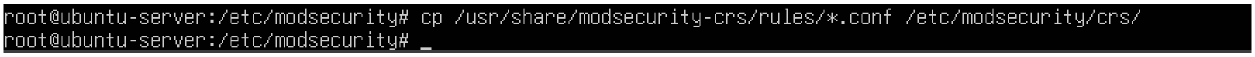


```
  GNU nano 7.2                                            modsecurity.conf-recommended *
# -- Rule engine initialization ----------------------------------------------

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
#SecRuleEngine DetectionOnly
SecRuleEngine On
```

Configure the core configuration file /etc/modsecurity/mod_security.conf.

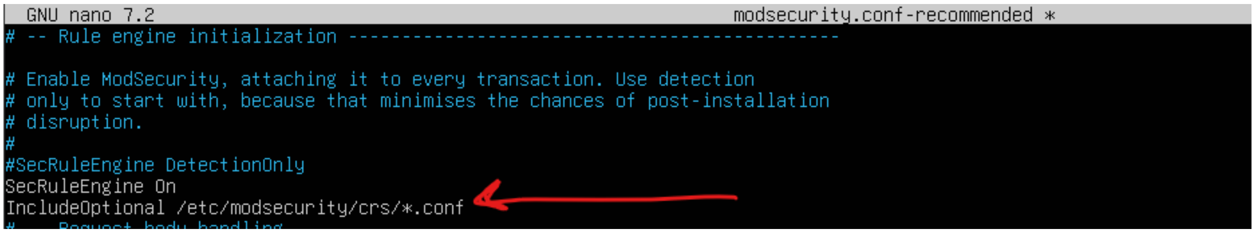
Change the SecRuleEngine from DetectionOnly to On, As shown above.

Next, we should copy all the core rule set (crs) into the crs configuration file.



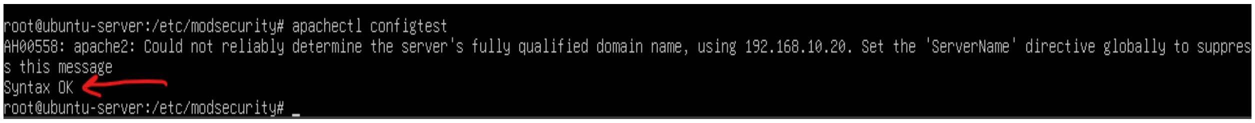
```
root@ubuntu-server:/etc/modsecurity# cp /usr/share/modsecurity-crs/rules/*.conf /etc/modsecurity/crs/
root@ubuntu-server:/etc/modsecurity# _
```

Copy all the .conf files from rules folder to /etc/modsecurity/crs/ folder.



```
  GNU nano 7.2                                            modsecurity.conf-recommended *
# -- Rule engine initialization ----------------------------------------------

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
#SecRuleEngine DetectionOnly
SecRuleEngine On
IncludeOptional /etc/modsecurity/crs/*.conf
# -- Request body handling
```

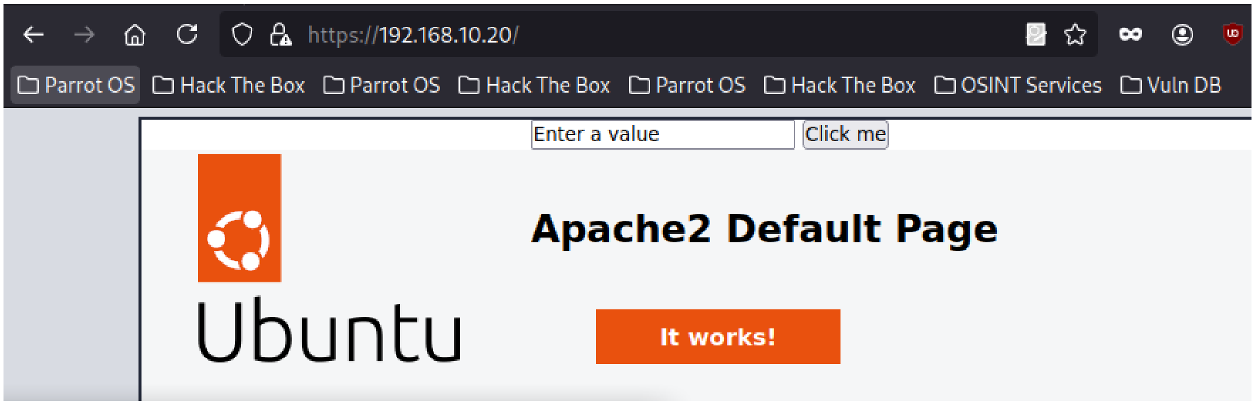
This will tell modsecurity core configuration file to check all the .conf files (rules) on every HTTP request that recieved.



```
root@ubuntu-server:/etc/modsecurity# apachectl configtest
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 192.168.10.20. Set the 'ServerName' directive globally to suppres
s this message
Syntax OK
root@ubuntu-server:/etc/modsecurity# _
```

Check if the configurations syntax are OK.

Then restart the apache2 service.

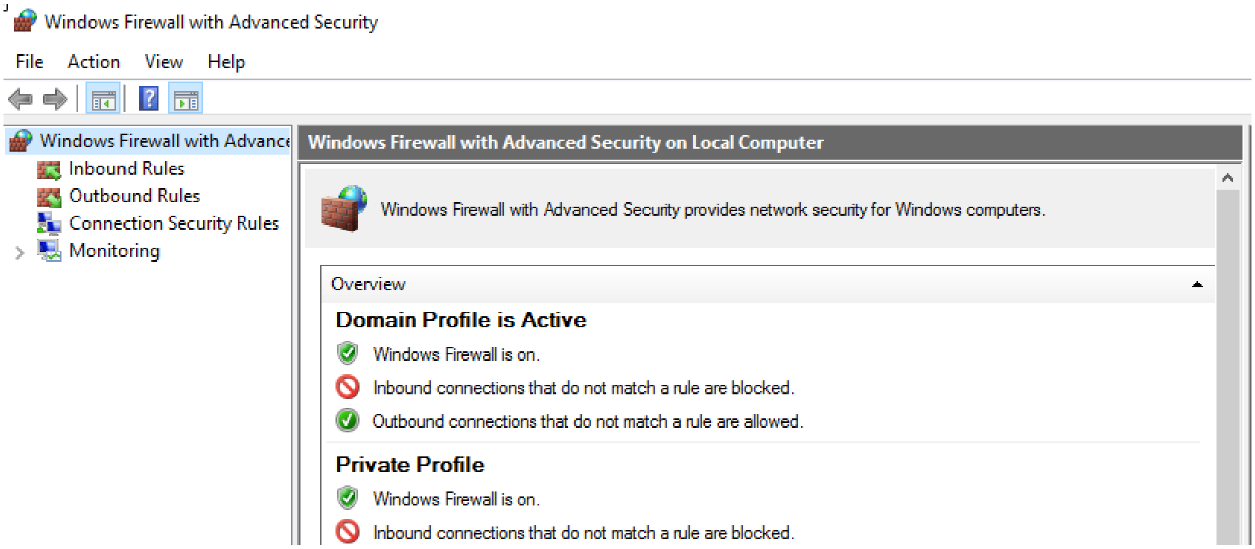


Apache2 Default Page

It works!

Configure apache HTTPS by adding ssl-cert as an open-source certificate generator for web servers.

Now let’s add rules to the windows server firewall.


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Overview

Windows Firewall with Advanced Security provides network security for Windows computers.

Domain Profile is Active

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

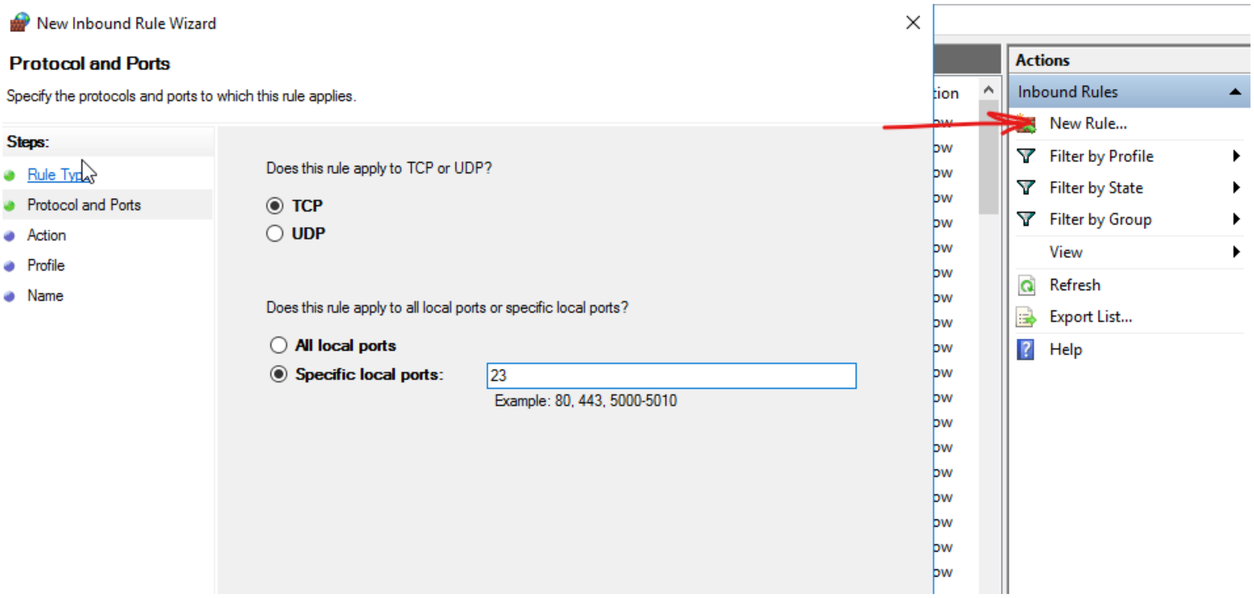
Outbound connections that do not match a rule are allowed.

Private Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Press Windows+R and write wf.msc.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

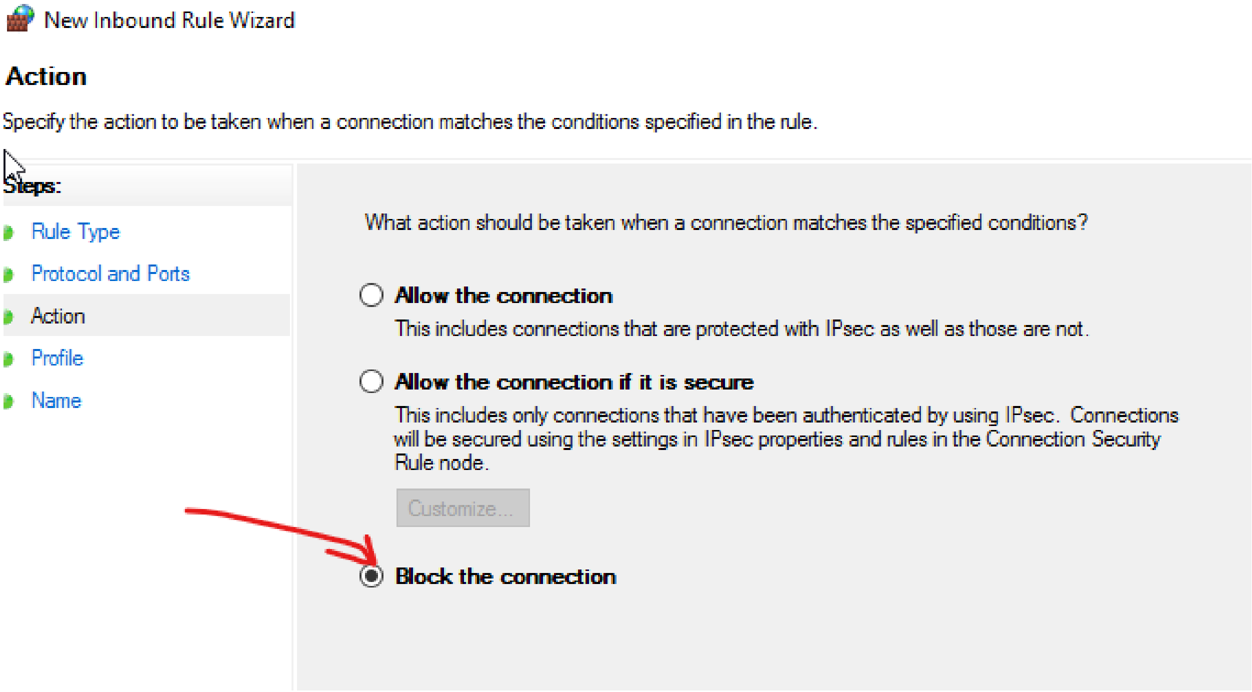
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 23

Example: 80, 443, 5000-5010

Add a rule rule> select block by Port > specific the port to block.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

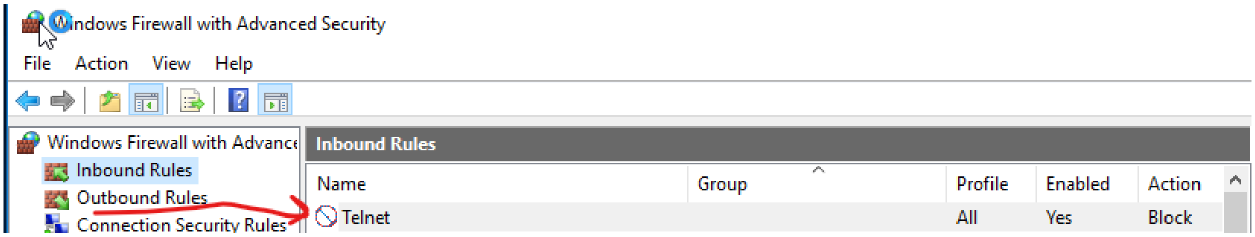
What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

Check the block the connection radio button.

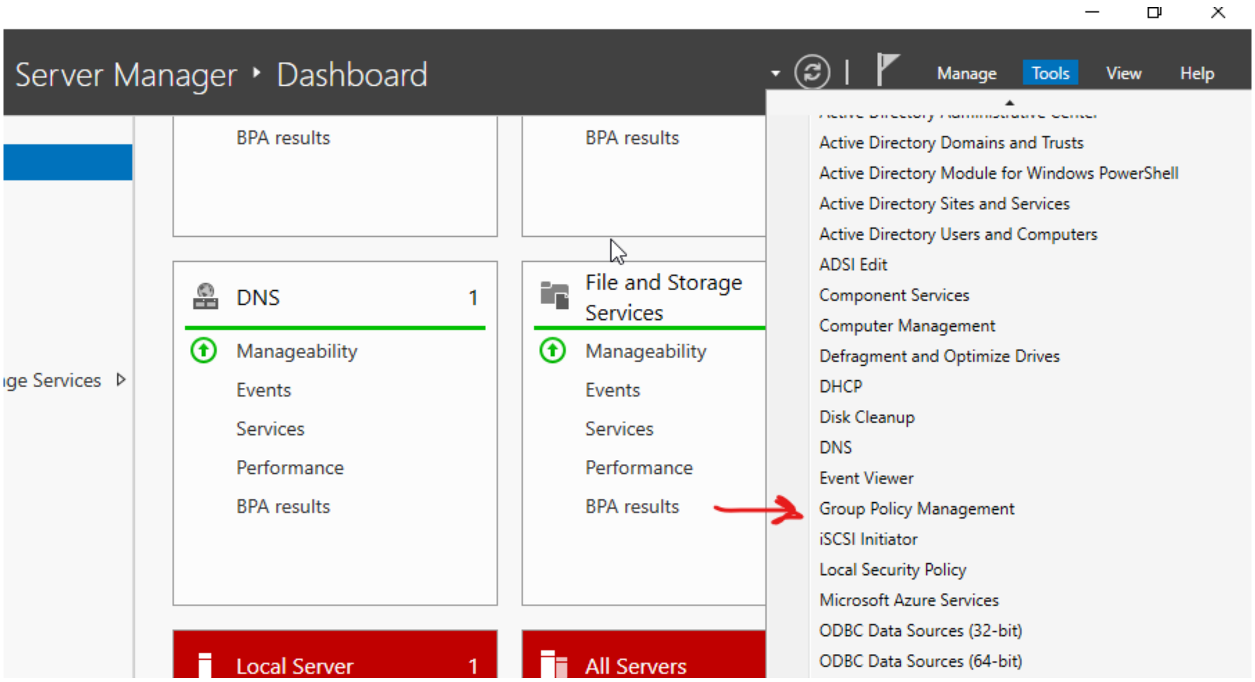


Windows Firewall with Advanced Security

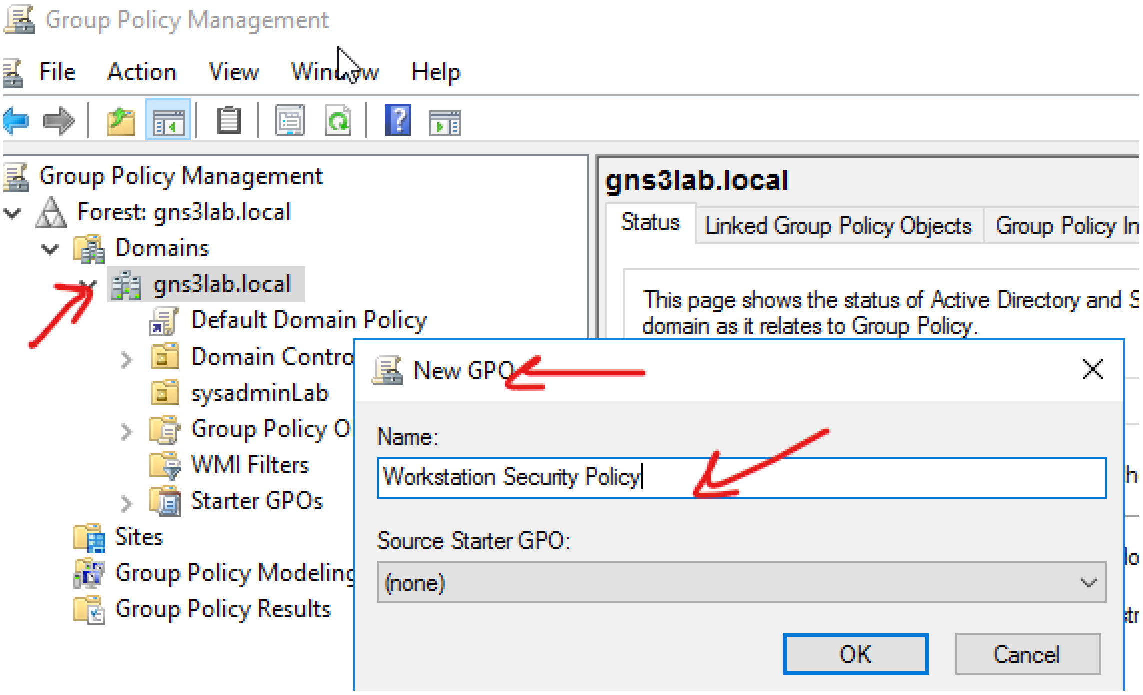
Inbound Rules

Name	Group	Profile	Enabled	Action
Telnet		All	Yes	Block

Windows Server: Group Policy Implementation



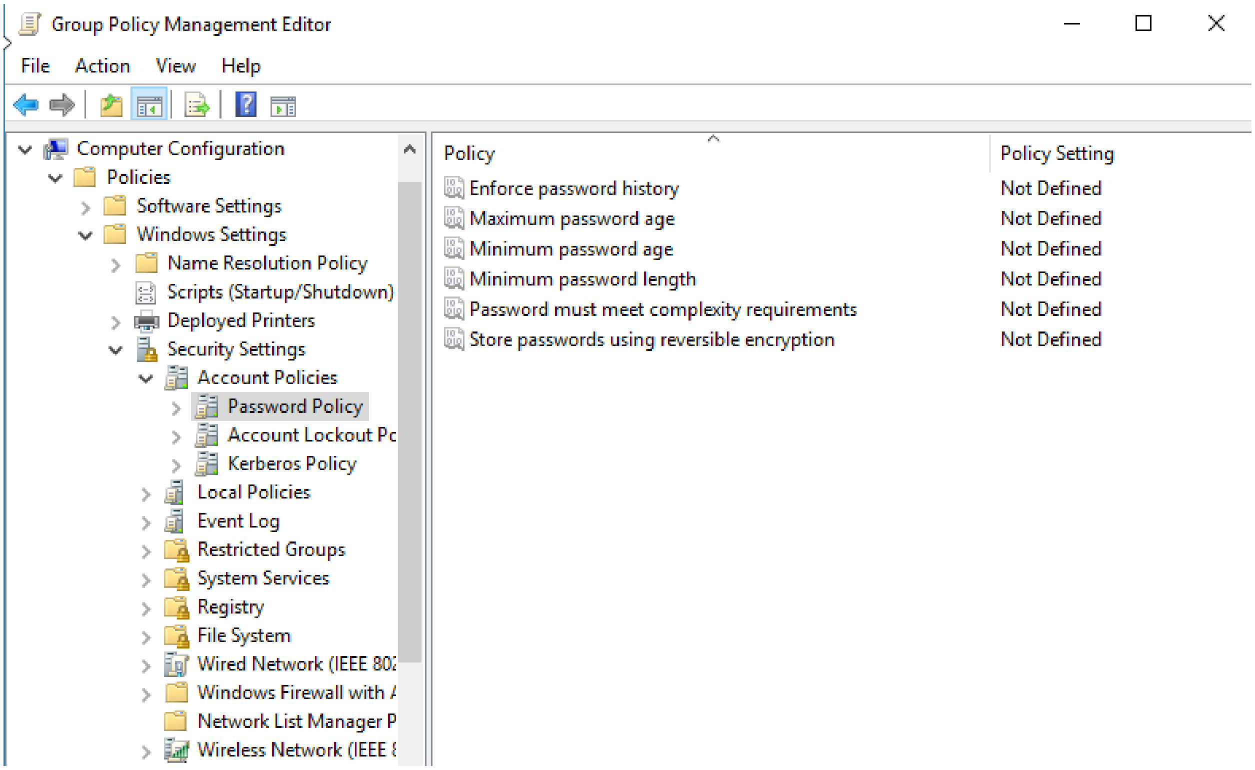
Server Manager > Tools > Group Policy Management.



Name: Workstation Security Policy

Source Starter GPO: (none)

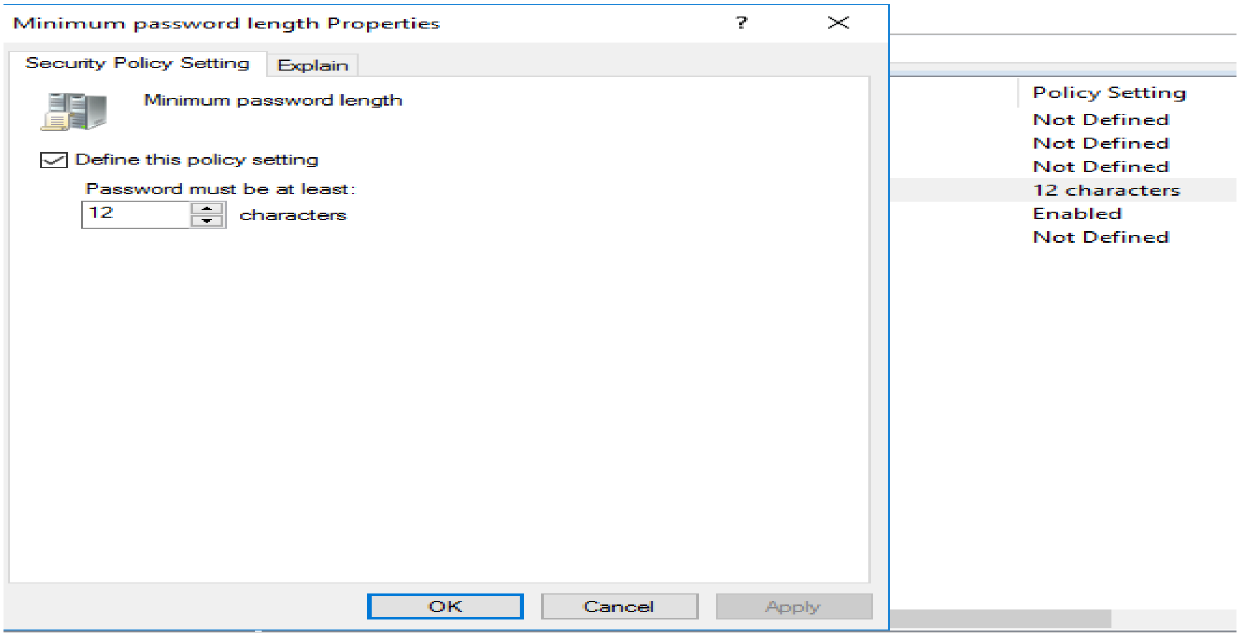
Domains > gns3lab.local > right click > new.



Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy

Put a minimum password length



Minimum password length

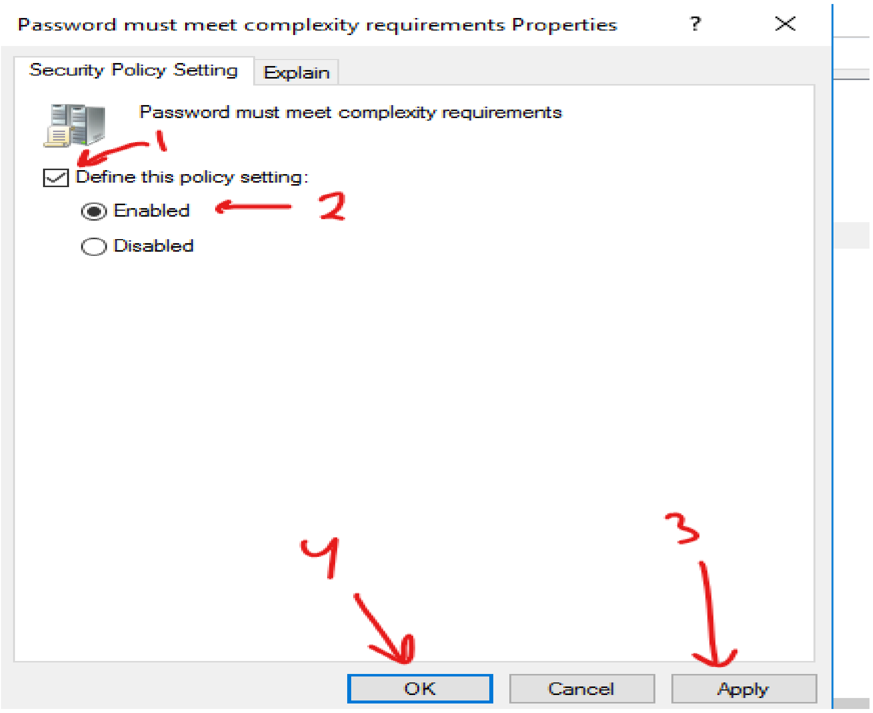
☑ Define this policy setting

Password must be at least:

12 characters

Policy Setting
Not Defined
Not Defined
Not Defined
12 characters
Enabled
Not Defined

Enabled password complexity.



Password must meet complexity requirements Properties

Security Policy Setting | Explain

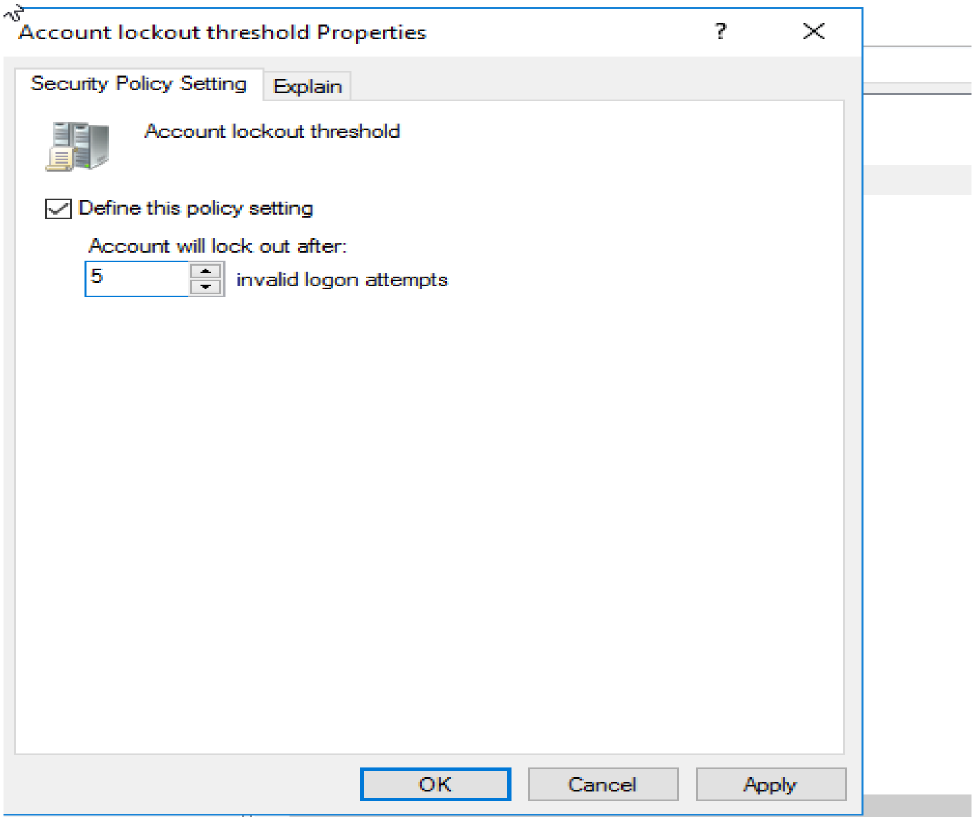
Password must meet complexity requirements

☑ Define this policy setting:

● Enabled

○ Disabled

Put the lockout after 5 failed attempts.



Account lockout threshold Properties

Security Policy Setting | Explain

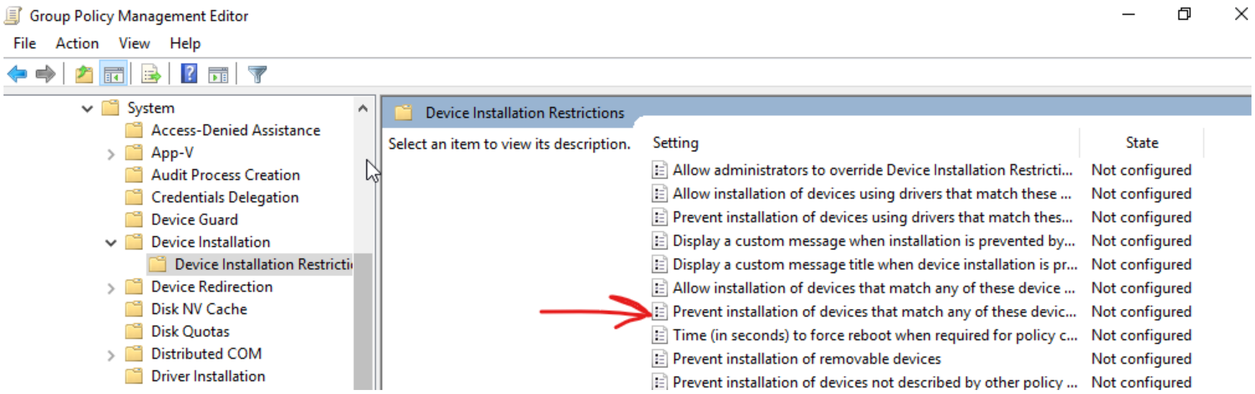
Account lockout threshold

☑ Define this policy setting

Account will lock out after:

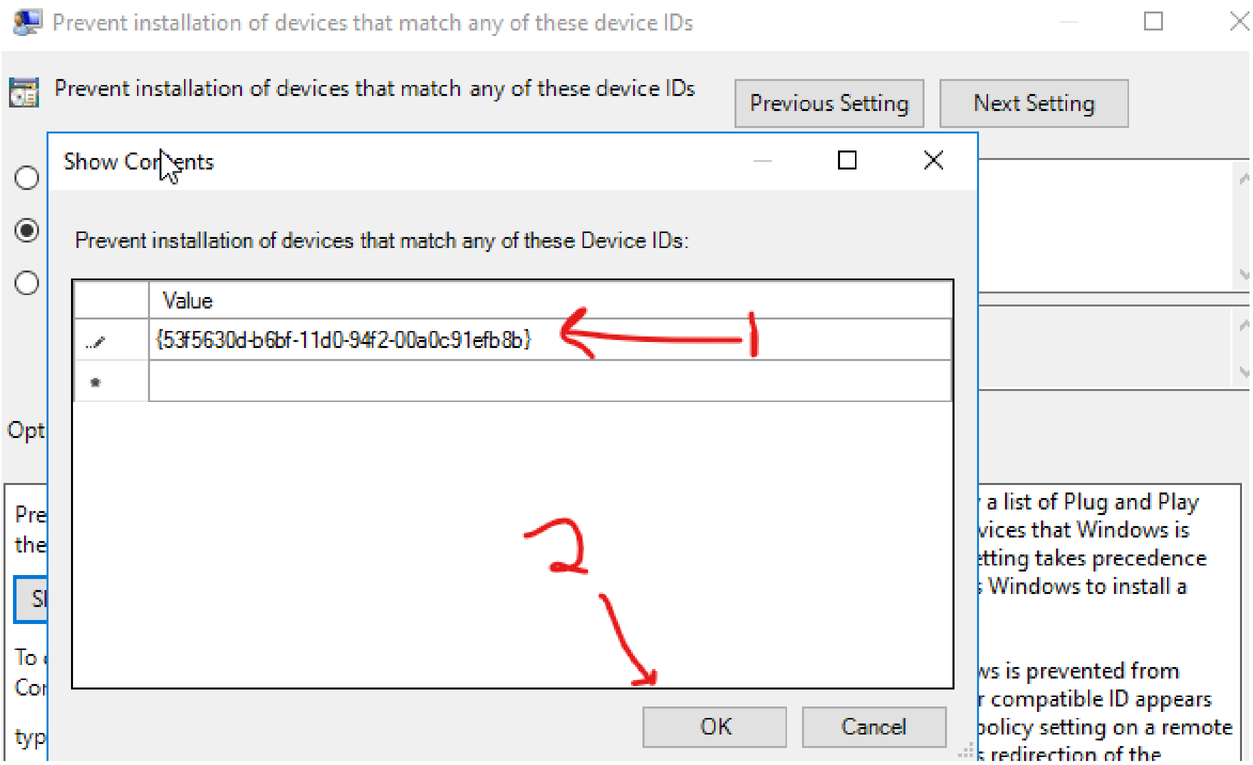
5 invalid logon attempts

Disable USB storage devices via Device Installation Restrictions:



Setting	State
Allow administrators to override Device Installation Restricti...	Not configured
Allow installation of devices using drivers that match these ...	Not configured
Prevent installation of devices using drivers that match thes...	Not configured
Display a custom message when installation is prevented by...	Not configured
Display a custom message title when device installation is pr...	Not configured
Allow installation of devices that match any of these device ...	Not configured
Prevent installation of devices that match any of these devic...	Not configured
Time (in seconds) to force reboot when required for policy c...	Not configured
Prevent installation of removable devices	Not configured
Prevent installation of devices not described by other policy ...	Not configured

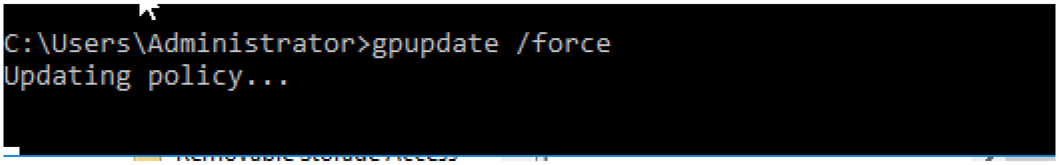
Computer Configuration > Policies > Administrative Templates > System > Device Installation > Device Installation Restrictions



Prevent installation of devices that match any of these Device IDs:

	Value
	{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
*	

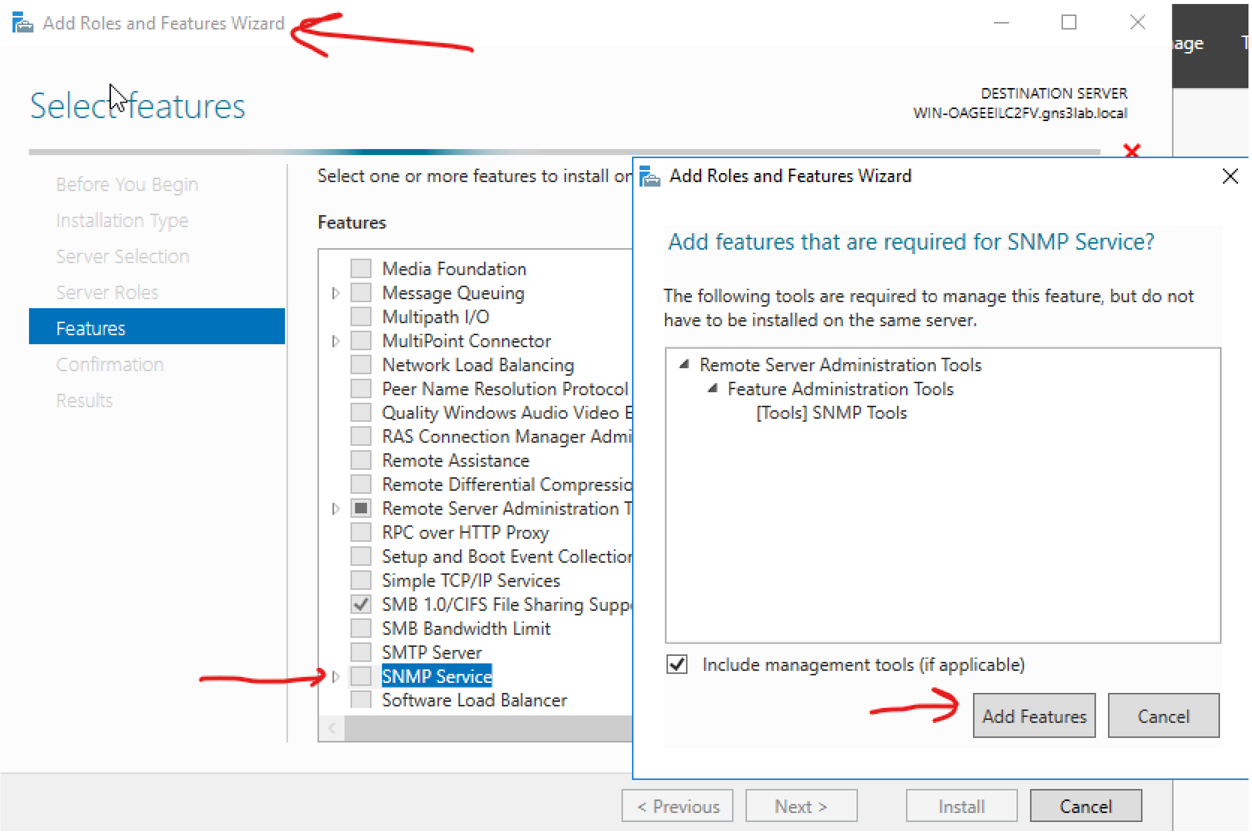
This drive match the ID for the USB's.



```
C:\Users\Administrator>gpupdate /force
Updating policy...
```

Finally, update the policies to refresh the server.

Install SNMP Service via Server Manager



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-OAGEEILC2FV.gns3lab.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more features to install on

Features

- □ Media Foundation
- □ Message Queuing
- □ Multipath I/O
- □ MultiPoint Connector
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video E
- □ RAS Connection Manager Admi
- □ Remote Assistance
- □ Remote Differential Compressio
- ■ Remote Server Administration T
- □ RPC over HTTP Proxy
- □ Setup and Boot Event Collection
- □ Simple TCP/IP Services
- ☑ SMB 1.0/CIFS File Sharing Supp
- □ SMB Bandwidth Limit
- □ SMTP Server
- □ SNMP Service
- □ Software Load Balancer

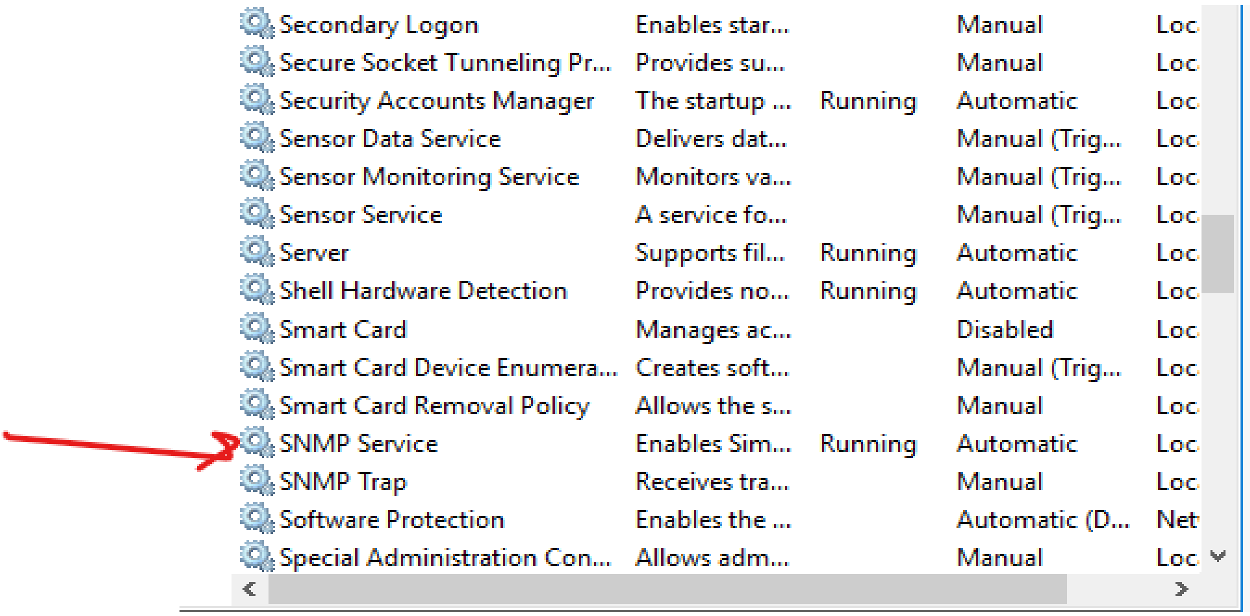
Add Roles and Features Wizard

Add features that are required for SNMP Service?

The following tools are required to manage this feature, but do not have to be installed on the same server.

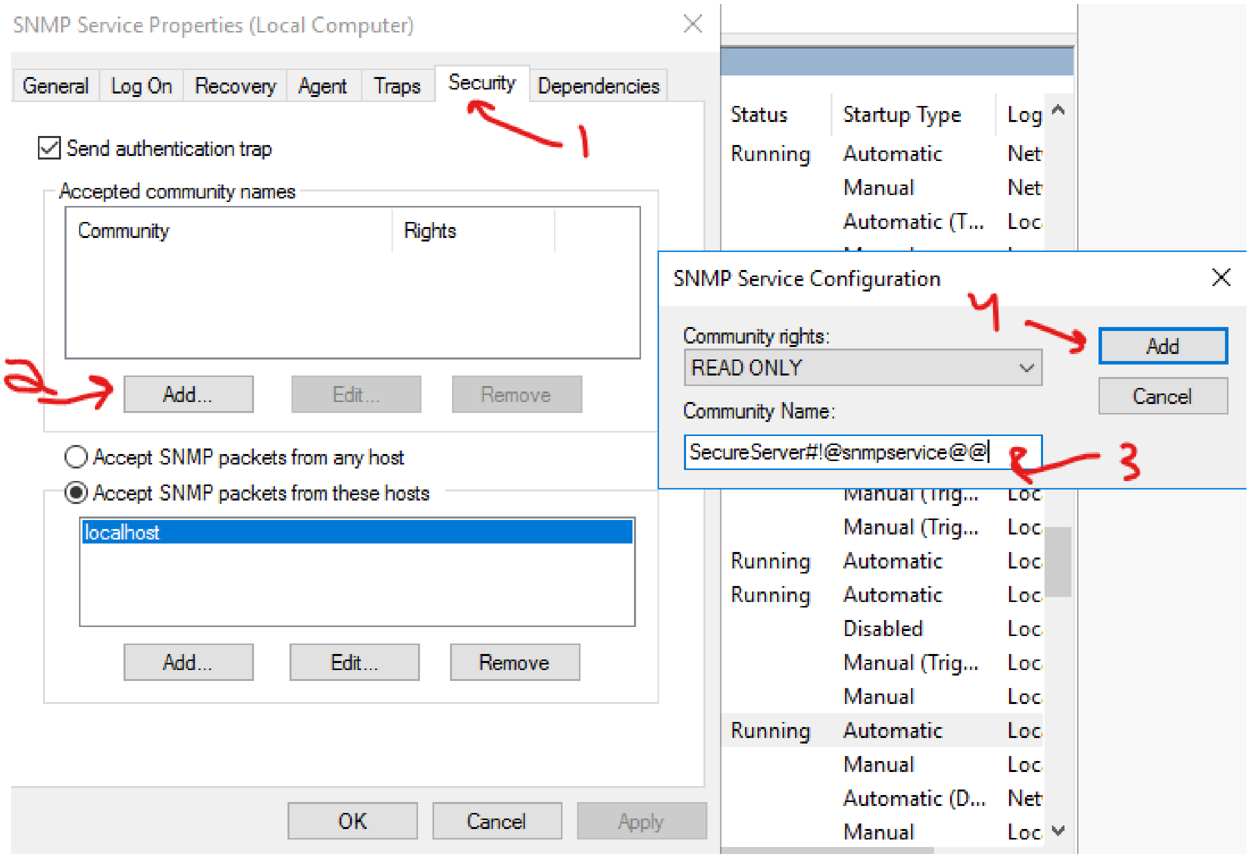
- Remote Server Administration Tools
  - Feature Administration Tools
    - [Tools] SNMP Tools

☑ Include management tools (if applicable)



Secondary Logon	Enables star...		Manual	Loc
Secure Socket Tunneling Pr...	Provides su...		Manual	Loc
Security Accounts Manager	The startup ...	Running	Automatic	Loc
Sensor Data Service	Delivers dat...		Manual (Trig...	Loc
Sensor Monitoring Service	Monitors va...		Manual (Trig...	Loc
Sensor Service	A service fo...		Manual (Trig...	Loc
Server	Supports fil...	Running	Automatic	Loc
Shell Hardware Detection	Provides no...	Running	Automatic	Loc
Smart Card	Manages ac...		Disabled	Loc
Smart Card Device Enumera...	Creates soft...		Manual (Trig...	Loc
Smart Card Removal Policy	Allows the s...		Manual	Loc
SNMP Service	Enables Sim...	Running	Automatic	Loc
SNMP Trap	Receives tra...		Manual	Loc
Software Protection	Enables the ...		Automatic (D...	Net
Special Administration Con...	Allows adm...		Manual	Loc

Double click on it.



☑ Send authentication trap

Accepted community names

Community	Rights

○ Accept SNMP packets from any host

● Accept SNMP packets from these hosts

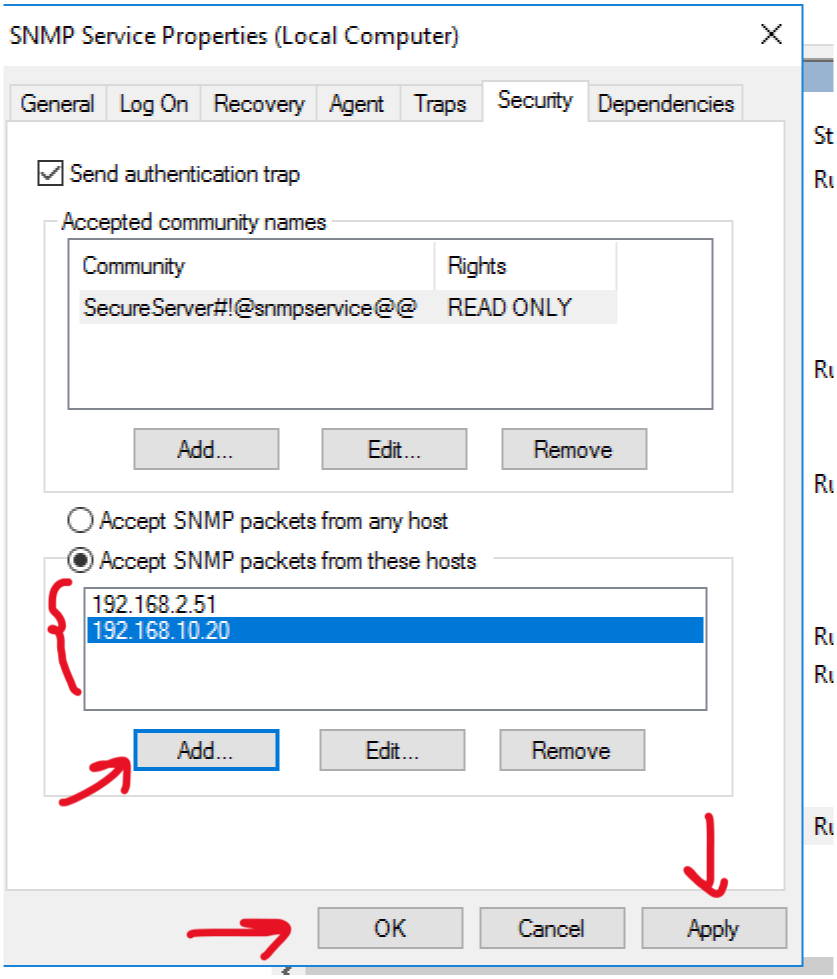
localhost

Community rights: READ ONLY

Community Name: SecureServer#!@snmpservice@@

The community's name is our complex string.

Set Allowed Management Stations



SNMP Service Properties (Local Computer)

☑ Send authentication trap

Accepted community names

Community	Rights
SecureServer#!@snmpservice@@	READ ONLY

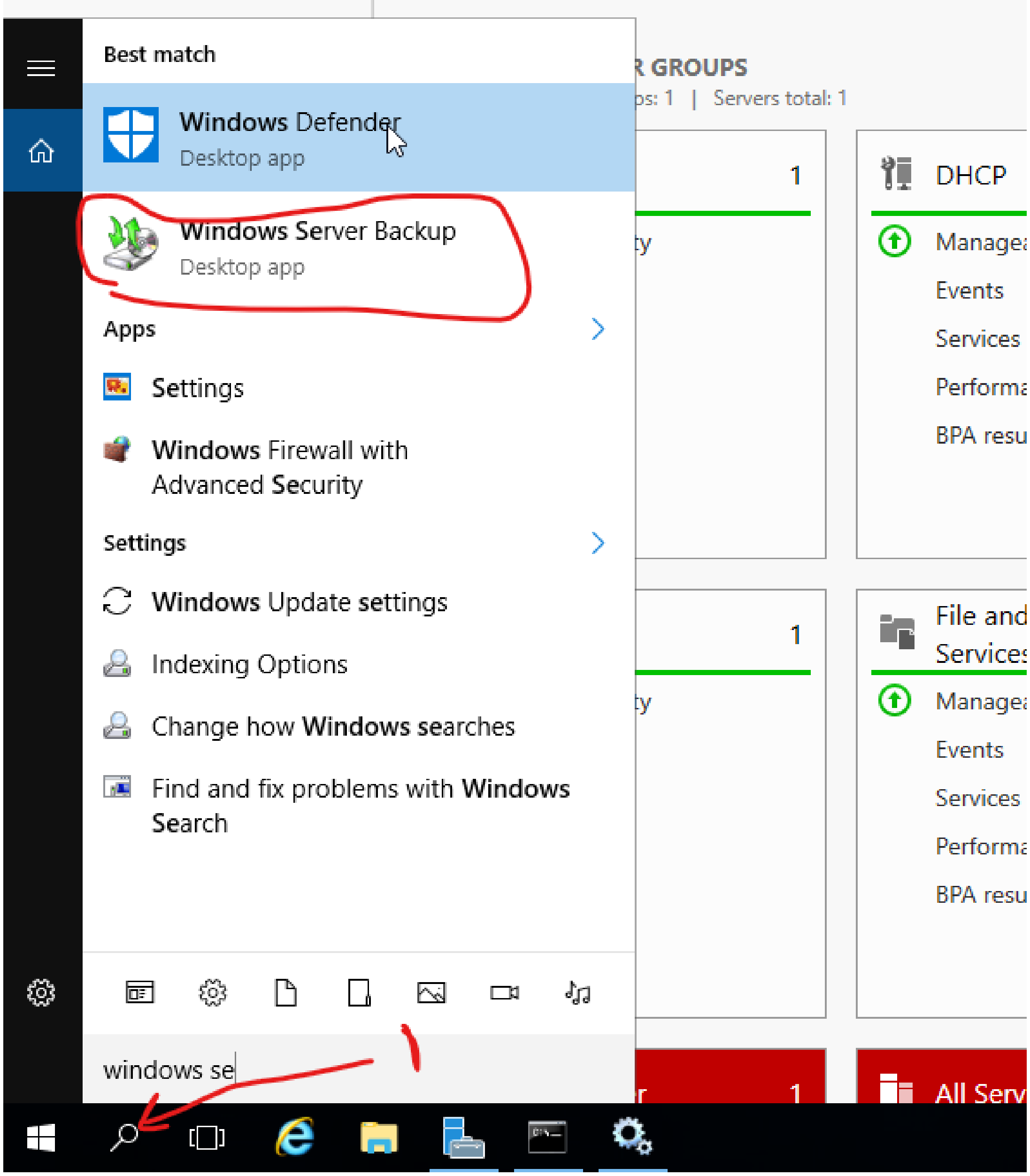
○ Accept SNMP packets from any host

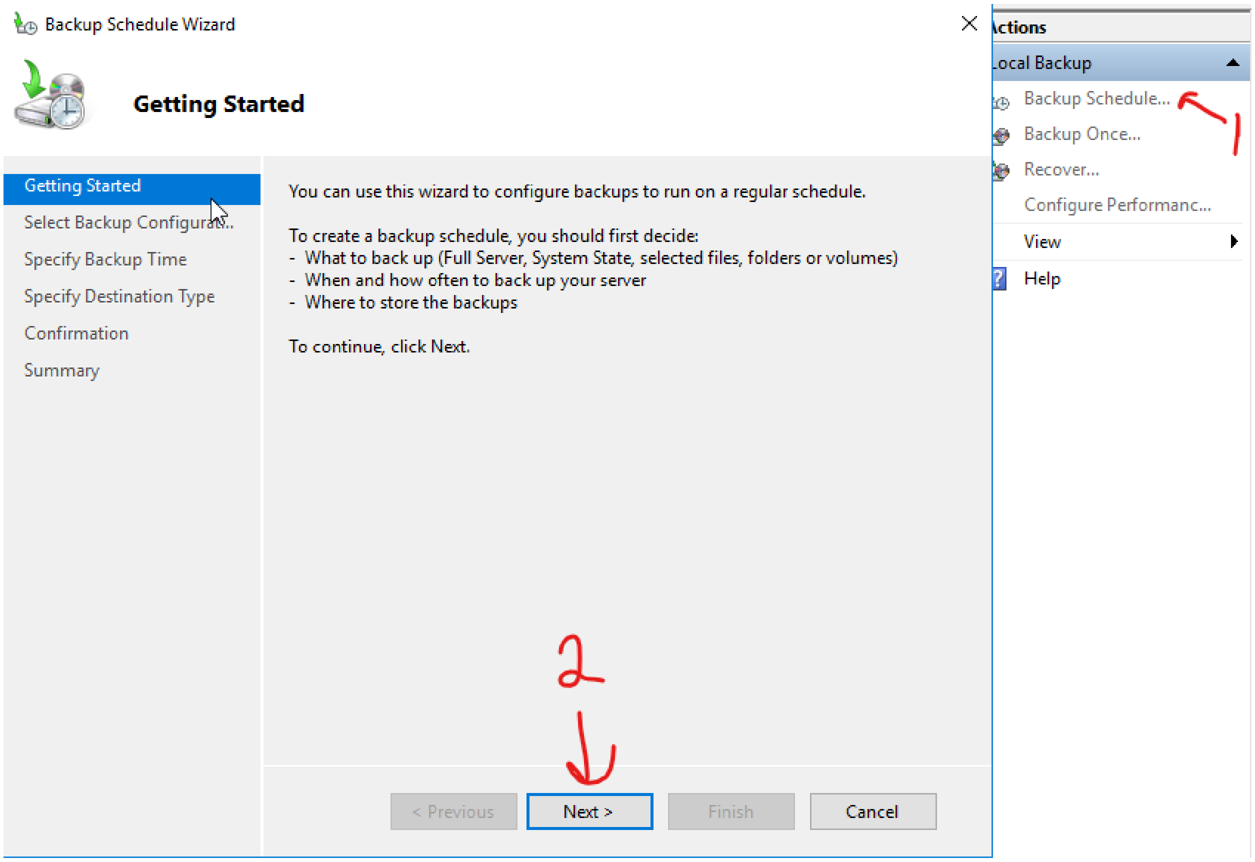
● Accept SNMP packets from these hosts

192.168.2.51
192.168.10.20

Automated Backup Solution

Manage> **Add Roles and Features**.> **Next**.> **Select features** page, scroll down and check the box next to **Windows Server Backup**.> Once the installation is complete, click **Close.**



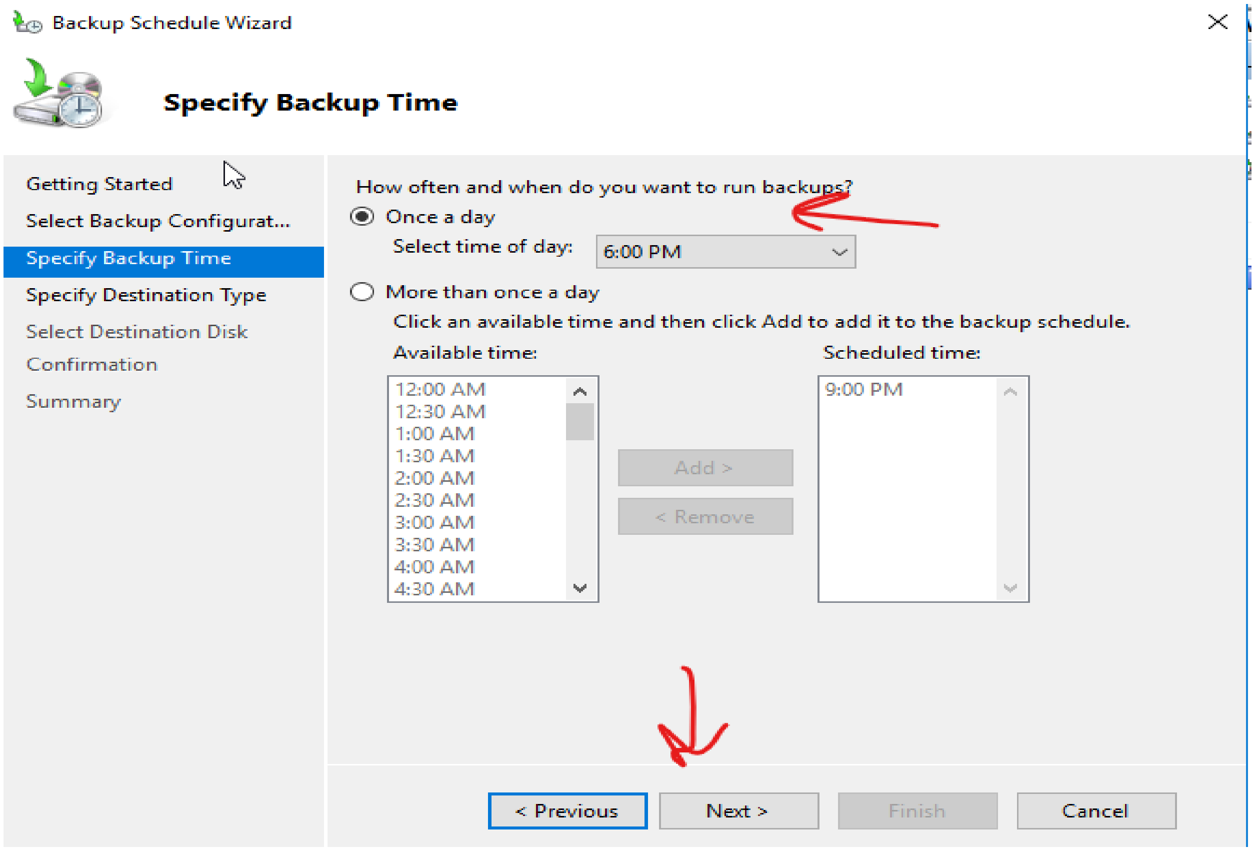


Getting Started

You can use this wizard to configure backups to run on a regular schedule.

To create a backup schedule, you should first decide:
- What to back up (Full Server, System State, selected files, folders or volumes)
- When and how often to back up your server
- Where to store the backups

To continue, click Next.



Specify Backup Time

How often and when do you want to run backups?

● Once a day

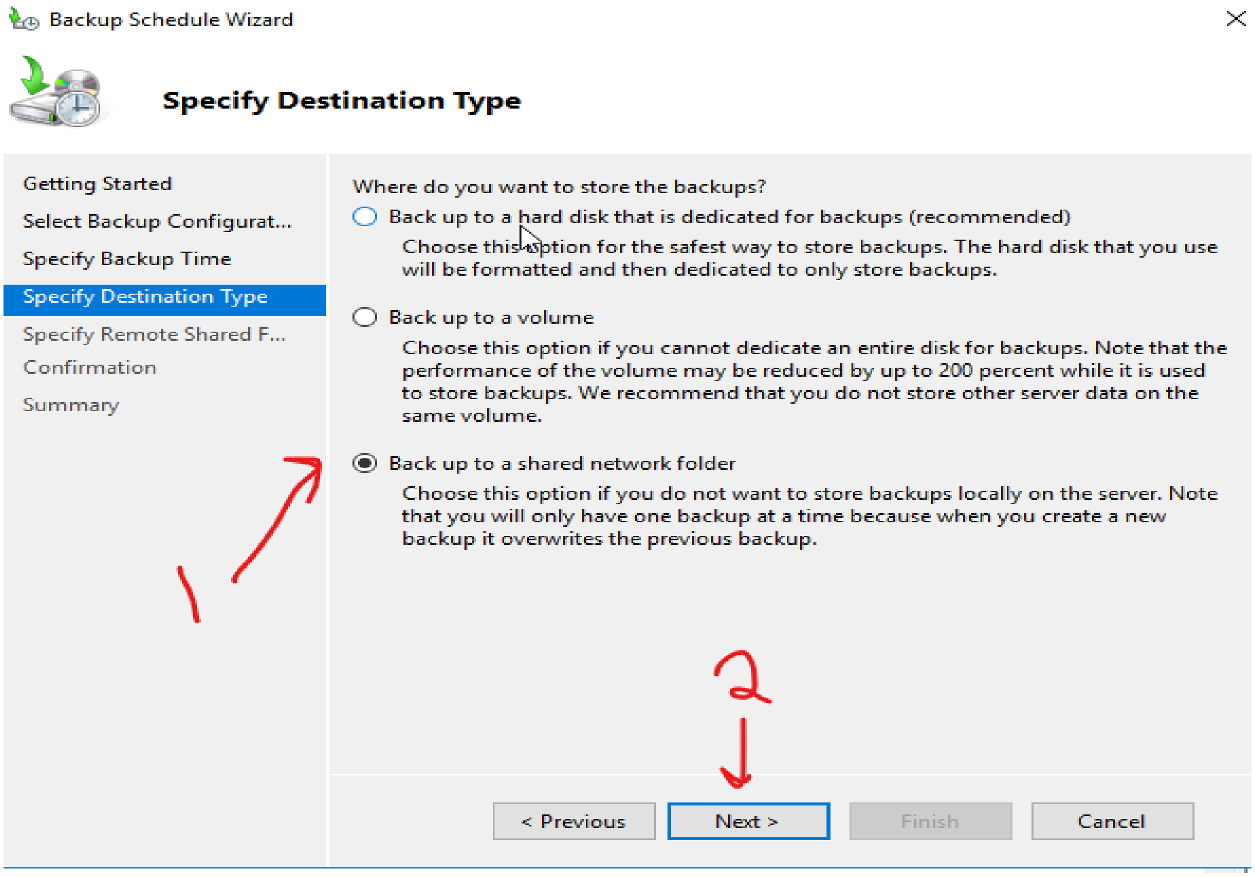
Select time of day: 6:00 PM

○ More than once a day

Click an available time and then click Add to add it to the backup schedule.

Available time: 12:00 AM, 12:30 AM, 1:00 AM, 1:30 AM, 2:00 AM, 2:30 AM, 3:00 AM, 3:30 AM, 4:00 AM, 4:30 AM

Scheduled time: 9:00 PM



Backup Schedule Wizard

Specify Destination Type

Where do you want to store the backups?

○ Back up to a hard disk that is dedicated for backups (recommended)

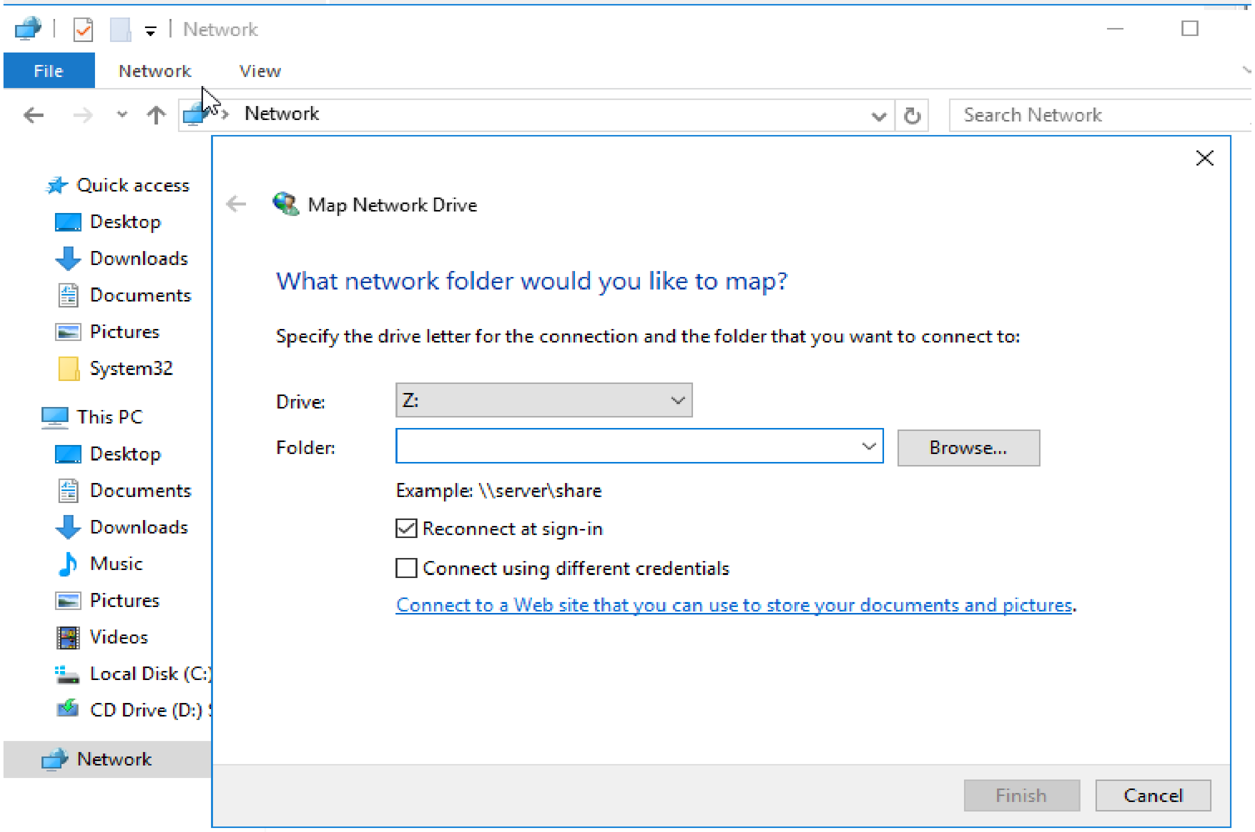
Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.

○ Back up to a volume

Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.

● Back up to a shared network folder

Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z:

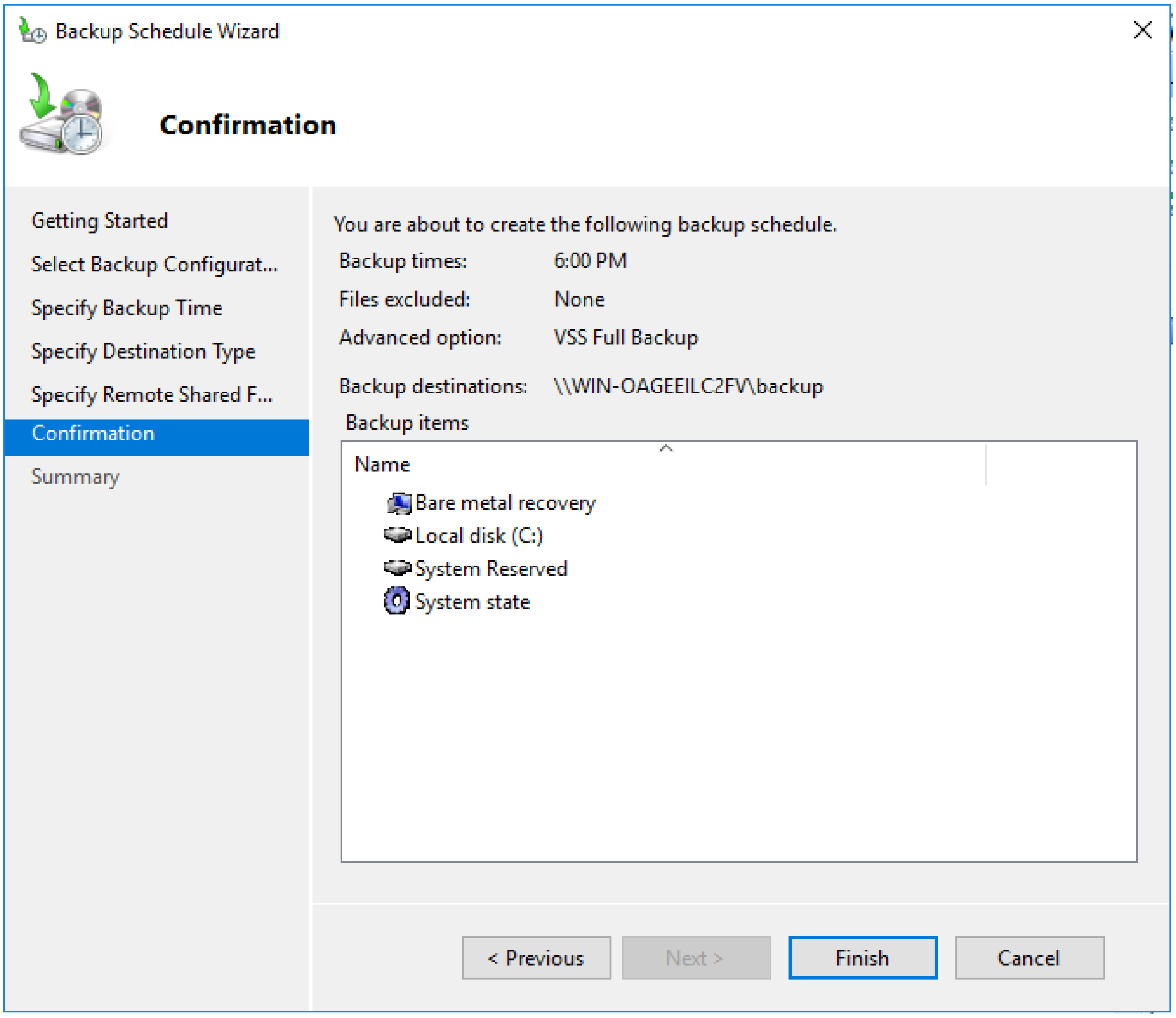
Folder:

Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.



Confirmation

You are about to create the following backup schedule.

Backup times: 6:00 PM

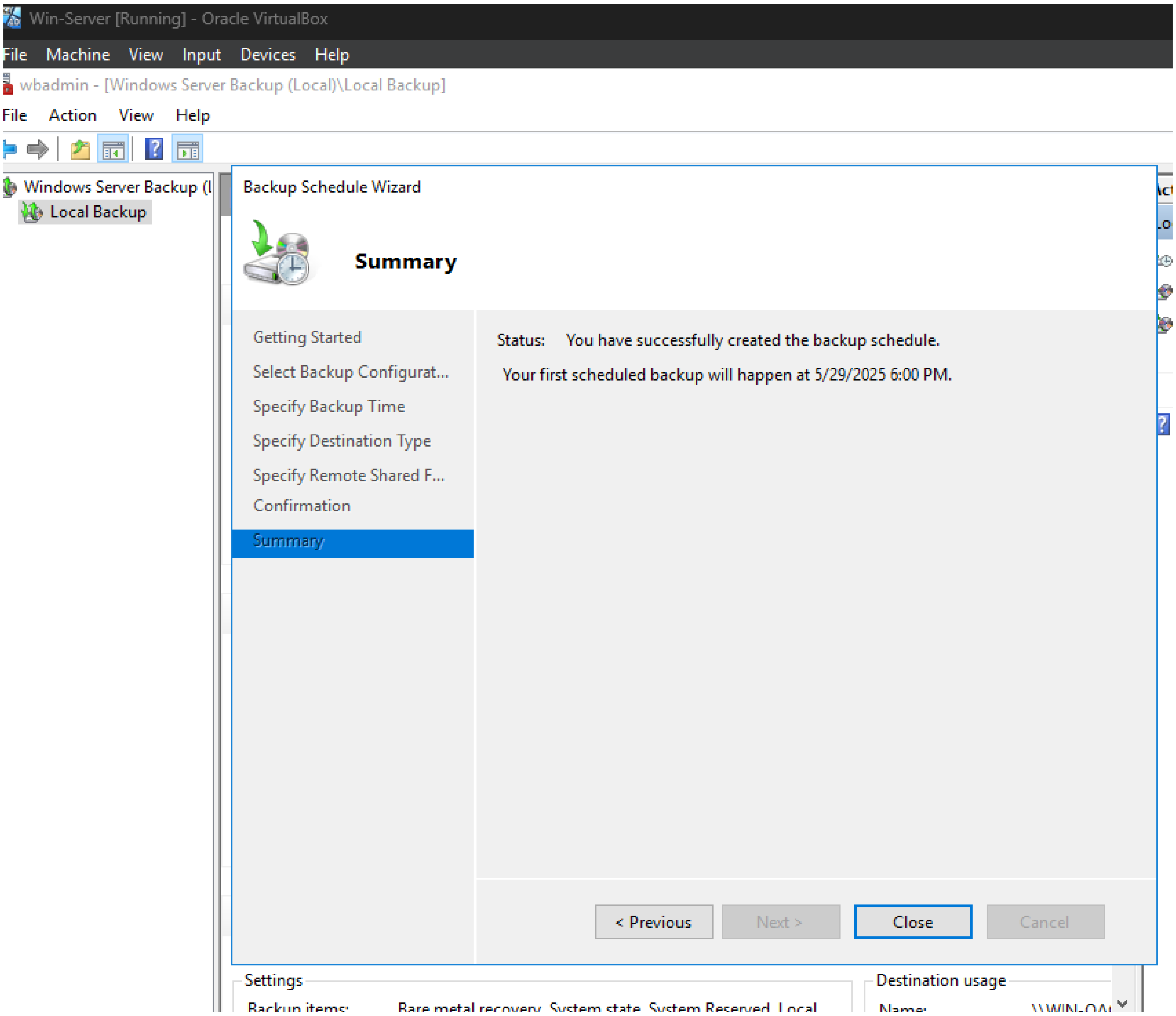
Files excluded: None

Advanced option: VSS Full Backup

Backup destinations: \\WIN-OAGEEILC2FV\backup

Backup items

Name
Bare metal recovery
Local disk (C:)
System Reserved
System state



Status: You have successfully created the backup schedule.

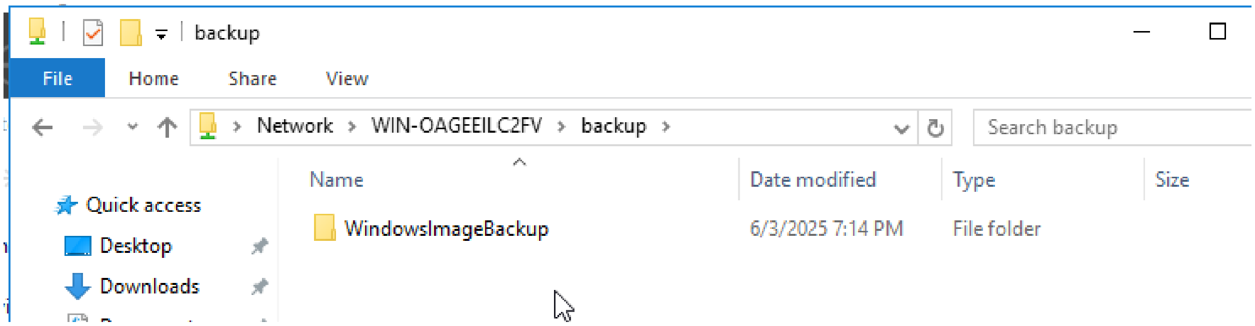
Your first scheduled backup will happen at 5/29/2025 6:00 PM.

Settings

Backup items: Bare metal recovery, System state, System Reserved, Local

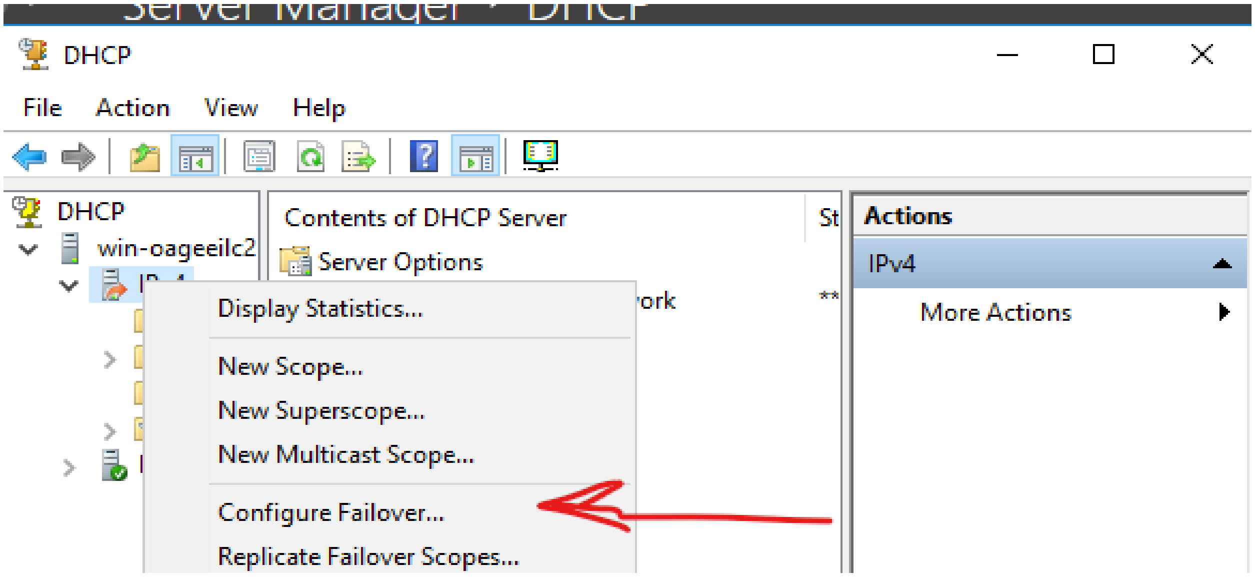
Destination usage

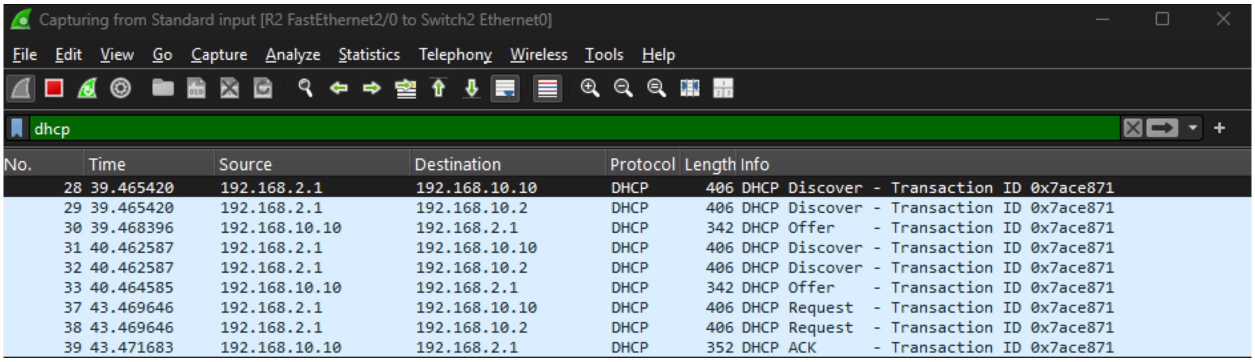
Name: \\WIN-OA



Name	Date modified	Type	Size
WindowsImageBackup	6/3/2025 7:14 PM	File folder	

DHCP Failover:




Capturing from Standard input [R2 FastEthernet2/0 to Switch2 Ethernet0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.   Time        Source          Destination     Protocol Length Info
   28 39.465420   192.168.2.1     192.168.10.10   DHCP      406 DHCP Discover - Transaction ID 0x7ace871
   29 39.465420   192.168.2.1     192.168.10.2    DHCP      406 DHCP Discover - Transaction ID 0x7ace871
   30 39.468396   192.168.10.10   192.168.2.1     DHCP      342 DHCP Offer    - Transaction ID 0x7ace871
   31 40.462587   192.168.2.1     192.168.10.10   DHCP      406 DHCP Discover - Transaction ID 0x7ace871
   32 40.462587   192.168.2.1     192.168.10.2    DHCP      406 DHCP Discover - Transaction ID 0x7ace871
   33 40.464585   192.168.10.10   192.168.2.1     DHCP      342 DHCP Offer    - Transaction ID 0x7ace871
   37 43.469646   192.168.2.1     192.168.10.10   DHCP      406 DHCP Request  - Transaction ID 0x7ace871
   38 43.469646   192.168.2.1     192.168.10.2    DHCP      406 DHCP Request  - Transaction ID 0x7ace871
   39 43.471683   192.168.10.10   192.168.2.1     DHCP      352 DHCP ACK      - Transaction ID 0x7ace871
```