Project Overview: Building a Home Lab Environment for Active Directory and Cybersecurity Practice

Objective:

The primary objective of this project is to create a comprehensive home lab environment that simulates a real-world Active Directory (AD) setup. This lab will be incredibly beneficial for both my blue team (defensive cybersecurity) and red team (offensive cybersecurity) practices, as well as for anyone like me who is interested in gaining hands-on experience with IT administration and cybersecurity tools.

Project Components:

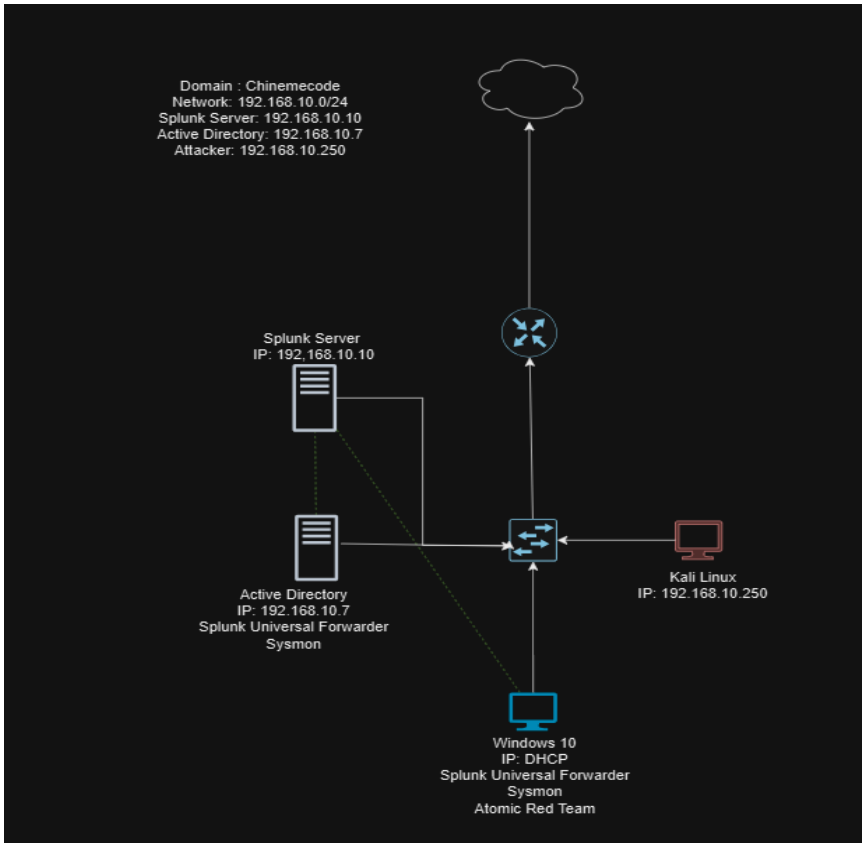
1. Active Directory Setup:
    - I'm using Windows Server 2022 to establish an Active Directory environment. This setup will allow me to learn more about AD administration and domain management.
    - I'll be creating and managing domain users and integrating a target Windows PC into the domain.
2. Security Information and Event Management (SIEM):
    - I'll be installing and configuring Splunk to ingest and analyze telemetry data from the Windows Server and target machine. This will help me detect security incidents and create alerts, dashboards, and reports based on the data I collect.
3. Red Teaming:
    - I'll use Kali Linux as my attacking machine to perform a brute force attack on the Active Directory domain. This exercise will help me understand attack techniques and the corresponding telemetry.
    - Additionally, I'll run Atomic Red Team to perform further attack scenarios, giving me more insight into potential security threats and how to detect them.

Learning Outcomes:

- Active Directory Administration: By the end of this project, I expect to have a solid understanding of how Active Directory works, including user management, domain configuration, and system integration.
- Splunk Proficiency: I'll learn how to install, configure, and use Splunk as a SIEM tool to monitor and analyze security data. I plan to delve into creating custom alerts, dashboards, and reports.
- Cybersecurity Techniques: This project will give me hands-on experience with both offensive and defensive cybersecurity techniques. I'll simulate attacks using Kali Linux and analyze the telemetry in Splunk.
- Problem-Solving Skills: I aim to enhance my ability to troubleshoot issues that arise during the setup and configuration of various systems, building my confidence in my technical skills.

Project Design:

- Diagram Creation: Before starting the technical setup, I'll create a diagram of my lab environment. This diagram will serve as a visual guide, helping me conceptualize the network layout and the flow of data. It's also a valuable tool for interviews and discussions about my project.



Tools and Technologies:

- Windows Server 2022: Used to set up the Active Directory environment.
- Windows 10 pro: The target machine that I'll integrate into the Active Directory domain.
- Kali Linux: The attacking machine I'll use for red team exercises.
- Splunk/ubuntu sever: The SIEM tool I'll rely on for monitoring, alerting, and reporting based on security data.
- VirtualBox: The virtualization platform I'll use to create and manage my lab environment.

The VM Set up and configuration

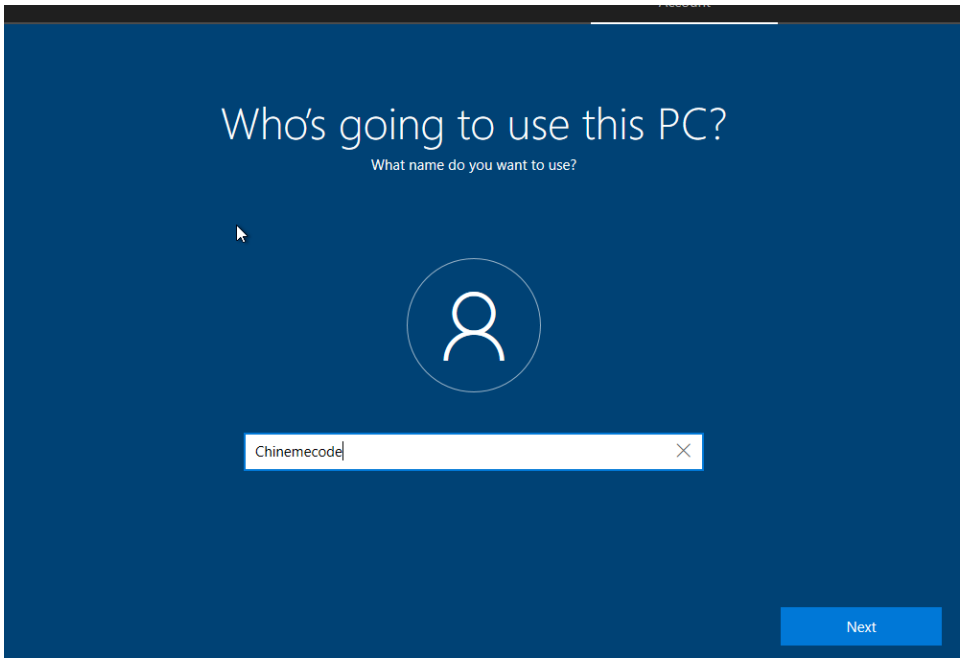
I will be hosting 4 of my VM's on my virtual box and the other two in the cloud.

VirtualBox: **Kali Linux**

-username: kali

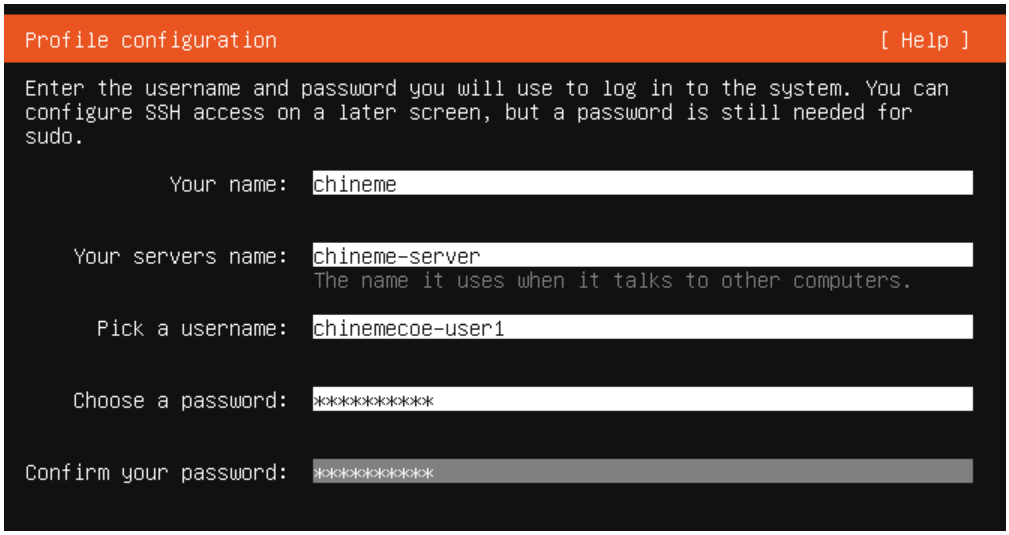
-Password: kali

Windows 10 Pro



- Password: Umea228822

Ubuntu Server:



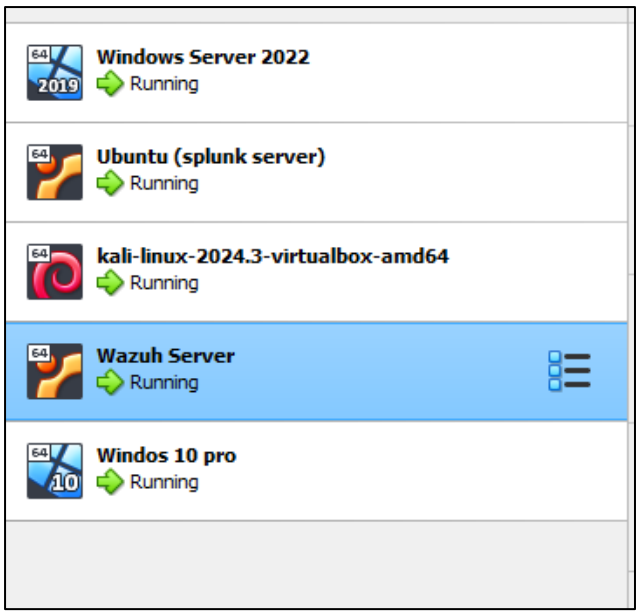
Password: Umea228822

Windows server 2022

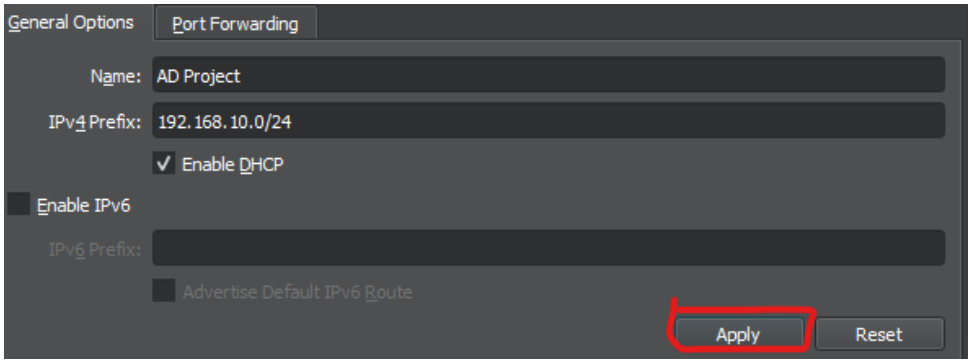
Username: Administrator

Password: Umea228822

The necessary Operating system I needed for this project.



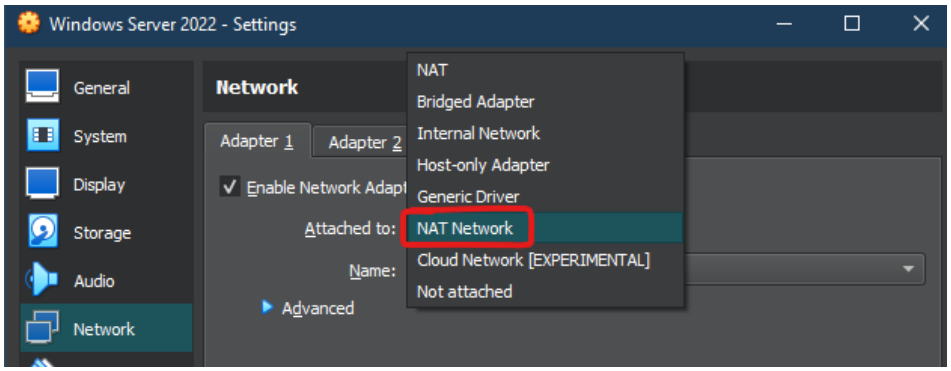
I have to create a NAT network so my VMs can all be connected to each other internally



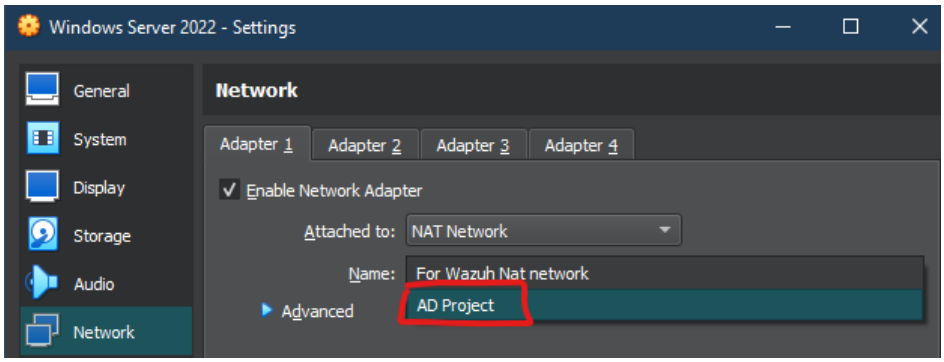
Change the network setting of all of them

Here are the steps to do that

1. Click on the VM you want to change the network setting
2. Click on setting
3. Click on Network
4. Then go to Attached To and you find **Nat network**



5. Then go to Name and click on **AD Project**



Configuring Static IP on Ubuntu Server

As part of the Active Directory lab environment, a static IP address was configured on the Ubuntu server to ensure consistent communication within the network. This process involved modifying the network configuration file using netplan. Below are the steps taken to achieve this:

1. **Open the Network Configuration File:**
   - Used the nano text editor to modify the netplan configuration file located at /etc/netplan/00-installer-config.yaml.
2. **Specify Network Interface:**
   - Defined the network interface (enp0s3 in this case).
3. **Set Static IP Address:**
   - Assigned a static IP address (192.168.10.10/24) to the network interface.
   - Disabled dhcp4 to ensure that the server does not receive an IP address from a DHCP server.
4. **Configure Nameserver:**
   - Configured the nameserver to use Google's public DNS (8.8.8.8) to resolve domain names.
5. **Define Routes:**
   - Added a default route with 102.168.10.1 as the gateway for network traffic.
6. **Save and Apply Changes:**
   - Saved the configuration file and applied the changes using the command sudo netplan apply.

```
  GNU nano 6.2                    /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.10/24]
      nameservers:
          addresses: [8.8.8.8]
      routes:
          - to: default
            via: 102.168.10.1
  version: 2
```

Outcome:

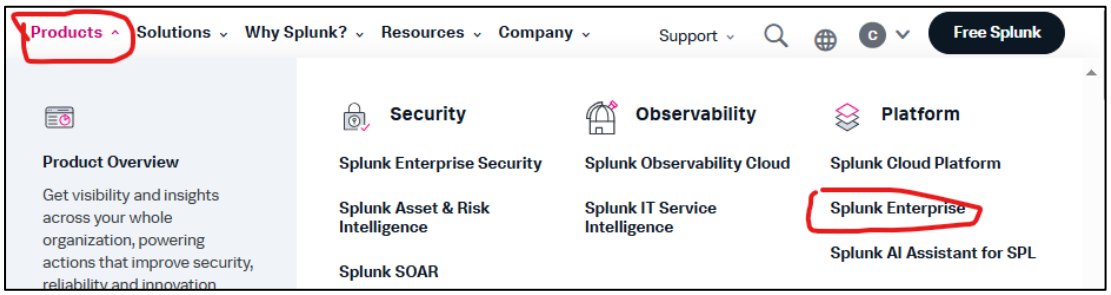
- The Ubuntu server now has a static IP address (192.168.10.10), allowing for reliable network communication and easy access within the Active Directory lab setup.

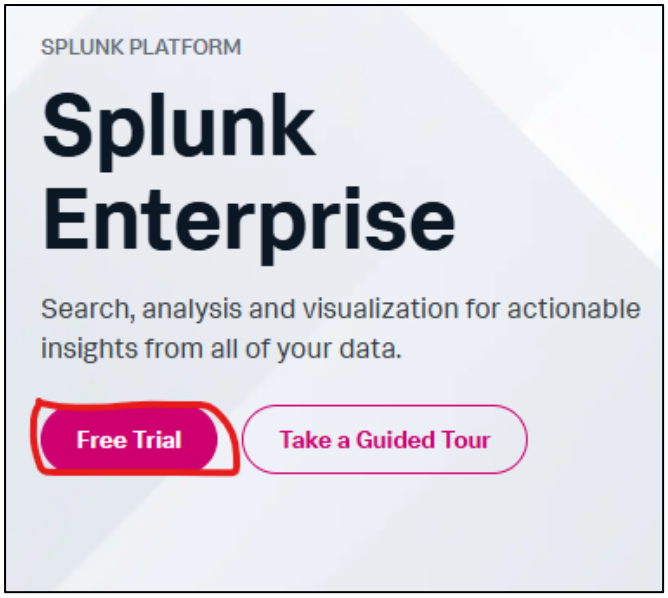
```
chinemecoe-user1@chineme-server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default q
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
0
    link/ether 08:00:27:0e:5b:d1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.10/24 brd 192.168.10.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.10.4/24 metric 100 brd 192.168.10.255 scope global secondary dynam
       valid_lft 466sec preferred_lft 466sec
    inet6 fe80::a00:27ff:fe0e:5bd1/64 scope link
       valid_lft forever preferred_lft forever
chinemecoe-user1@chineme-server:~$
```

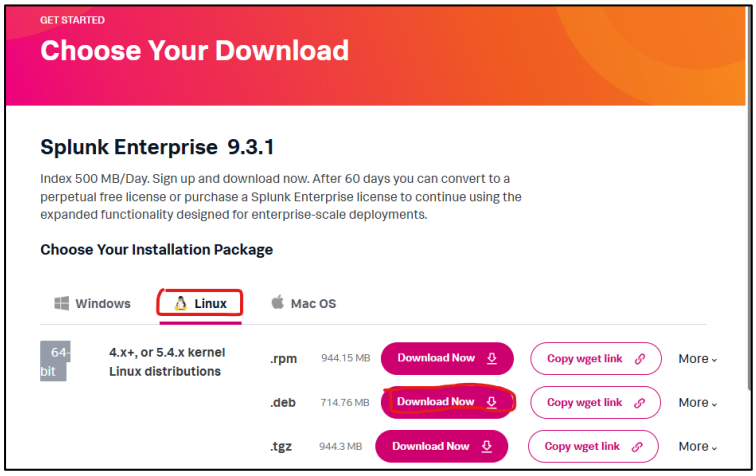
Now we head over to

```
adduser: The user `sandra' does not exist.
chinemecoe-user1@chineme-server:~$ sudo apt-get install virtualbox-guest-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  virtualbox-guest-x11
The following NEW packages will be installed:
  virtualbox-guest-utils
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 1,042 kB of archives.
After this operation, 6,128 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 virtualbox-guest
4 6.1.50-dfsg-1~ubuntu1.22.04.3 [1,042 kB]
Fetched 1,042 kB in 1s (1,518 kB/s)
Selecting previously unselected package virtualbox-guest-utils.
(Reading database ... 94652 files and directories currently installed.)
Preparing to unpack .../virtualbox-guest-utils_6.1.50-dfsg-1~ubuntu1.22.04.3_amd64.deb ...
Unpacking virtualbox-guest-utils (6.1.50-dfsg-1~ubuntu1.22.04.3) ...
Setting up virtualbox-guest-utils (6.1.50-dfsg-1~ubuntu1.22.04.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/virtualbox-guest-utils.servic
stemd/system/virtualbox-guest-utils.service.
[  259.521664] vboxsf: Unknown parameter 'tag'
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
chinemecoe-user1@chineme-server:~$
```

Head to Splunk on your host computer and download Splunk for .deb Linux file and save it where you like. I saved mine in my downloads.








```
chinemecoe-user1@chineme-server:~$ sudo adduser chinemecoe-user1 vboxsf
Adding user `chinemecoe-user1' to group `vboxsf' ...
Adding user chinemecoe-user1 to group vboxsf
Done.
chinemecoe-user1@chineme-server:~$ mkdir share
chinemecoe-user1@chineme-server:~$ ls
share
chinemecoe-user1@chineme-server:~$ _
```

```
chinemecoe-user1@chineme-server:~/share$ sudo mount -t vboxsf -o uid=1000 Downloads share/_
```

```
chinemecoe-user1@chineme-server:~/share$ cd share/
```

```
chinemecoe-user1@chineme-server:~/share$ ls -la
```

to print out everything in that directory

I was able to locate the file I downloaded

```
-amd64
-rwxrwxrwx 1 chinemecoe-user1 root    3346104649 Sep 15 00:22  kali-linux-2024.3-virtualbox
-amd64.7z
-rwxrwxrwx 1 chinemecoe-user1 root      39731395 Sep 16 00:26  Mantooth.E01
-rwxrwxrwx 1 chinemecoe-user1 root       2062398 Sep 16 03:00 'mantooth findings  2 df.pdf'
-rwxrwxrwx 1 chinemecoe-user1 root      19463448 Sep 15 00:18  MediaCreationTool_22H2.exe
-rwxrwxrwx 1 chinemecoe-user1 root        340071 Sep 17 14:34 'Opt Form.pdf'
-rwxrwxrwx 1 chinemecoe-user1 root    4945863680 Sep 17 14:07  remnux-v7-focal-virtualbox.o
va
-rwxrwxrwx 1 chinemecoe-user1 root    5044094976 Sep 14 17:52  SERVER_EVAL_x64FRE_en-us.iso
-rwxrwxrwx 1 chinemecoe-user1 root        787391 Sep 18 03:34  solar.png
-rwxrwxrwx 1 chinemecoe-user1 root     749476896 Sep 19 03:19  splunk-9.3.1-0b8d769cb912-li
nux-2.6-amd64.deb
-rwxrwxrwx 1 chinemecoe-user1 root    2136926208 Sep 14 05:12  ubuntu-22.04.5-live-server-a
md64.iso
-rwxrwxrwx 1 chinemecoe-user1 root      25397512 Sep 14 03:09  VC_redist.x64.exe
-rwxrwxrwx 1 chinemecoe-user1 root      13867304 Sep 14 17:24  VC_redist.x86.exe
-rwxrwxrwx 1 chinemecoe-user1 root     110252592 Sep 14 17:43  VirtualBox-7.0.20-163906-Win
.exe
-rwxrwxrwx 1 chinemecoe-user1 root     110639152 Sep 14 02:26  VirtualBox-7.1.0-164728-Win.
exe
-rwxrwxrwx 1 chinemecoe-user1 root    4893900800 Sep 15 00:31  Windows.iso
drwxrwxrwx 1 chinemecoe-user1 root         12288 Sep 15 23:48  winhex
-rwxrwxrwx 1 chinemecoe-user1 root       4587388 Sep 15 23:48  winhex.zip
chinemecoe-user1@chineme-server:~/share$ sudo dpkg -i splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 94666 files and directories currently installed.)
Preparing to unpack splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb ...
Unpacking splunk (9.3.1) ...
Setting up splunk (9.3.1) ...
complete
```

Now that Splunk is done downloading

We are going to login as a Splunk user, and this is the script for doing that

```
chinemecoe-user1@chineme-server:/opt/splunk$ sudo -u splunk bash
splunk@chineme-server:~$ _
```

To start running Splunk on the ubuntu server this is the way

```
splunk@chineme-server:~/bin$ ./splunk start
```

Creating an administrator username and password

Username = chinemecoe-user1

Password = Umea228822

```
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]:
Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: chinemecoe-user1
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password: _
```

```
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://chineme-server:8000

splunk@chineme-server:~/bin$ exxit
exxit: command not found
splunk@chineme-server:~/bin$ exit
exit
chinemecoe-user1@chineme-server:/opt/splunk$ cd bin
chinemecoe-user1@chineme-server:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
chinemecoe-user1@chineme-server:/opt/splunk/bin$ _
```

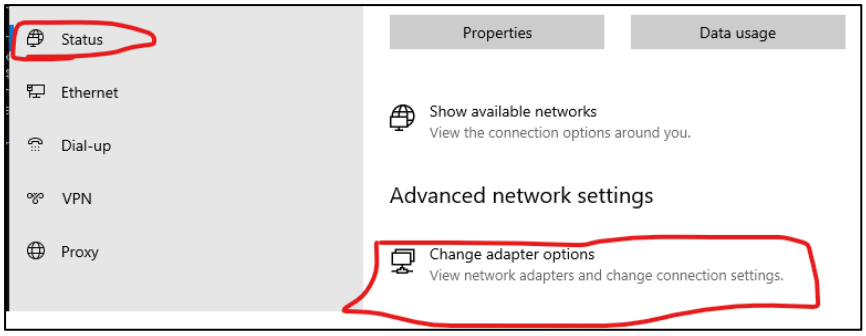
The last one was to make sure that the user Splunk boots when the ubuntu Splunk server is restarted.

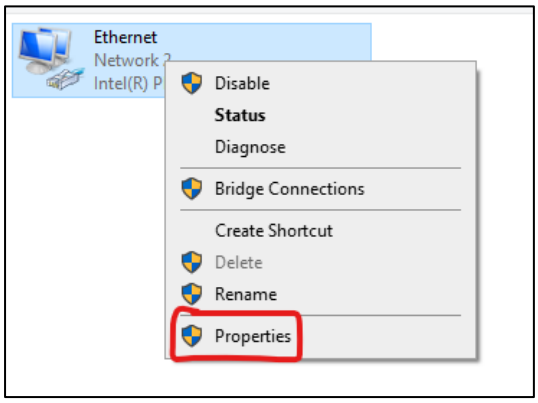
Let's install Sysmon and Splunk on windows 10 pro

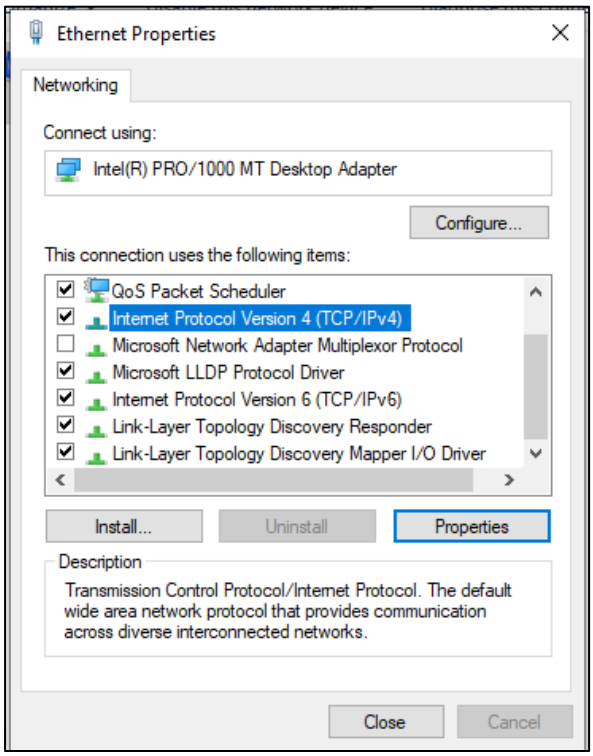
Steps I used to configure my windows target machine Ip address to be static instead of dynamic

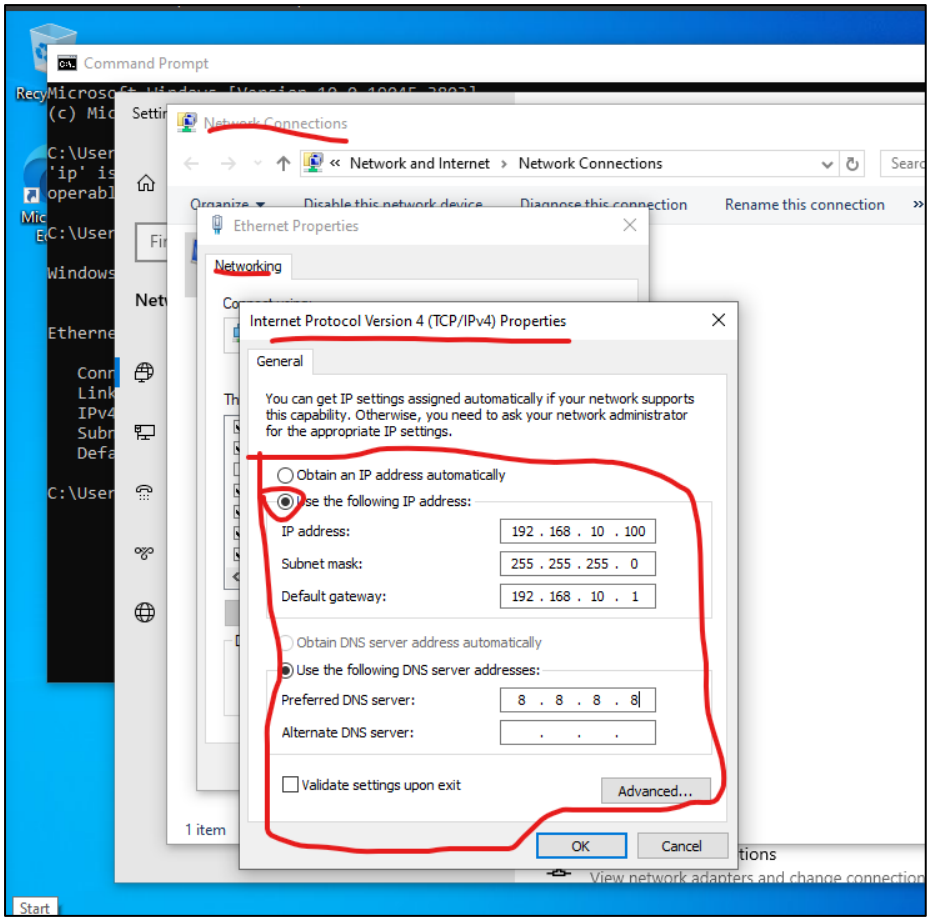
Firstly, rename computer

Restart the computer and check if the PC name change


Status
Ethernet
Dial-up
VPN
Proxy
Properties
Data usage
Show available networks
View the connection options around you.
Advanced network settings
Change adapter options
View network adapters and change connection settings.


Ethernet
Network 2
Intel(R) P
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

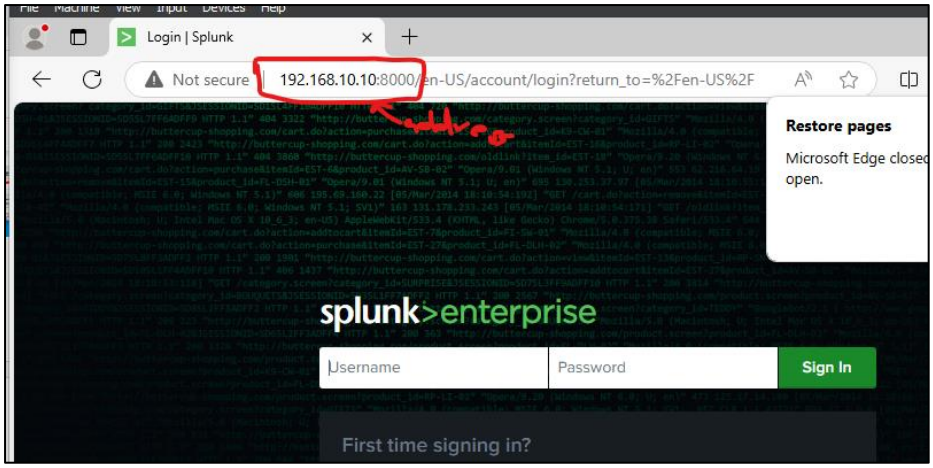

Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
Configure...
This connection uses the following items:
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Link-Layer Topology Discovery Responder
Link-Layer Topology Discovery Mapper I/O Driver
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Close
Cancel



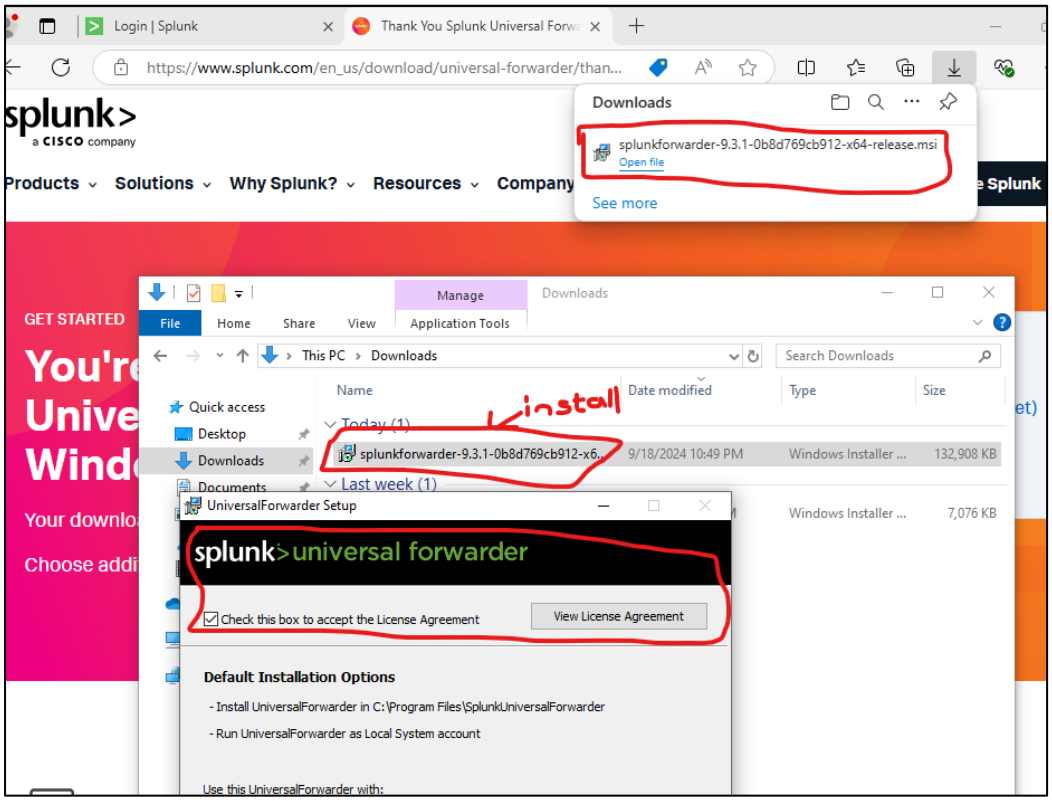

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c847:32a5:b24f:40fb%6
   IPv4 Address. . . . . . . . . . . : 192.168.10.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1

C:\Users\Chinemecode>
```

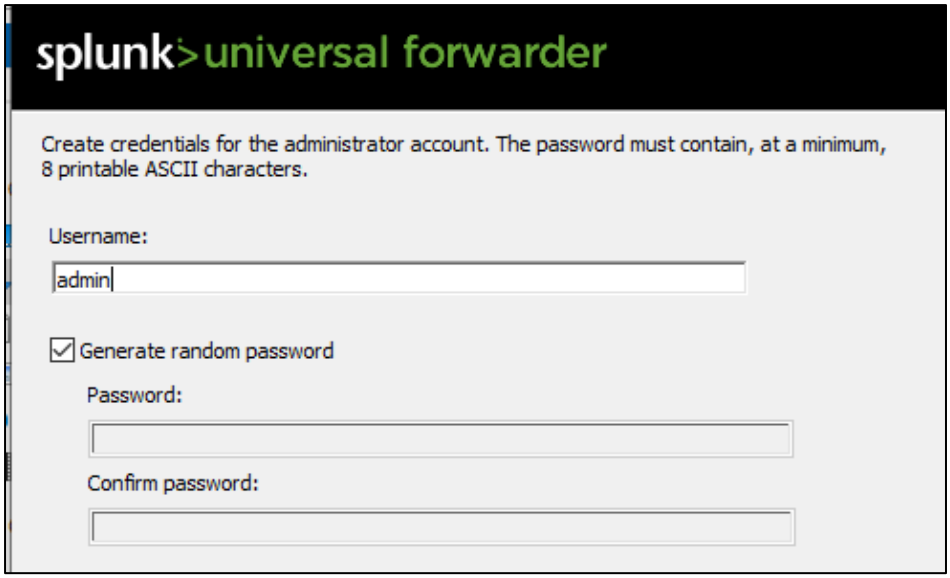
Let see if the Splunk is up

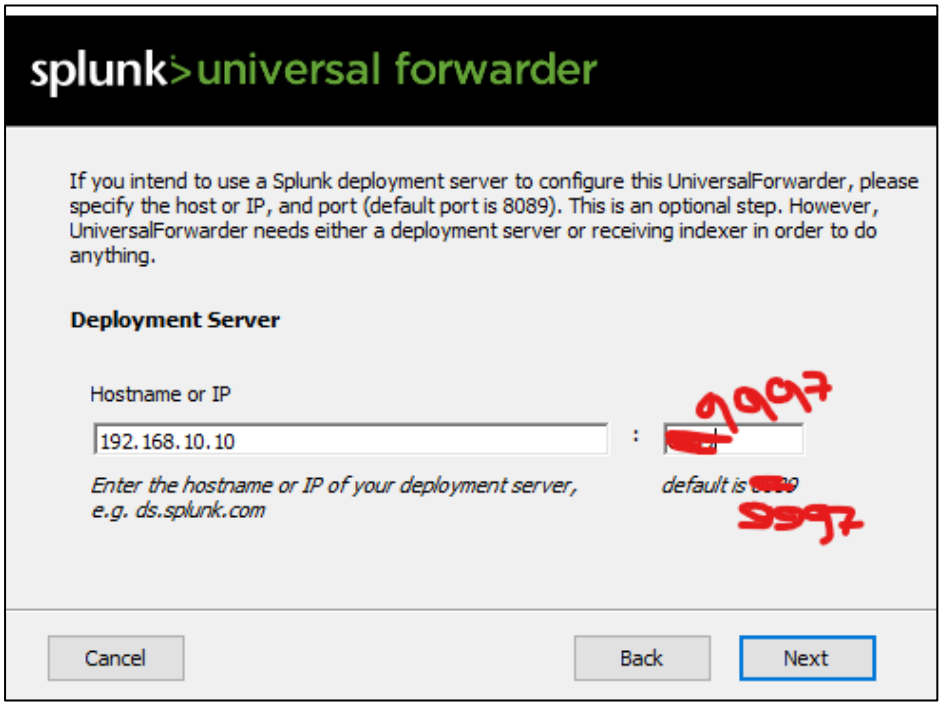
We can do this by heading to a browser and typing in the ip address of the Splunk server which is 192.168.10.10:8000. Splunk always listens on port 8000.

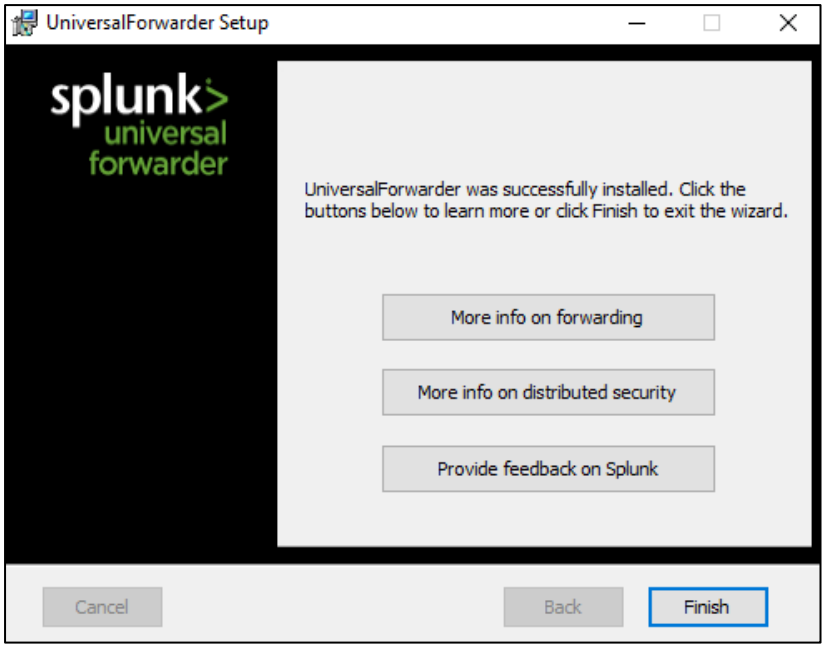

Login | Splunk
Not secure
192.168.10.10:8000/en-US/account/login?return_to=%2Fen-US%2F
Restore pages
Microsoft Edge closed open.
splunk>enterprise
Username
Password
Sign In
First time signing in?


Products
Solutions
Why Splunk?
Resources
Company
Support
Product Overview
Get visibility and insights across your whole organization, powering actions that improve security, reliability and innovation velocity.
MORE FROM SPLUNK
Pricing
Free Trials & Downloads
Product Tours


Login | Splunk
Thank You Splunk Universal Forw
https://www.splunk.com/en_us/download/universal-forwarder/than...
splunk>
a CISCO company
Products
Solutions
Why Splunk?
Resources
Company
Downloads
splunkforwarder-9.3.1-0b8d769cb912-x64-release.msi
Open file
See more
GET STARTED
Manage
Downloads
File
Home
Share
View
Application Tools
This PC > Downloads
Search Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Today (1)
install
splunkforwarder-9.3.1-0b8d769cb912-x6...
9/18/2024 10:49 PM
Windows Installer ...
132,908 KB
Last week (1)
Windows Installer ...
7,076 KB
UniversalForwarder Setup
splunk>universal forwarder
Check this box to accept the License Agreement
View License Agreement
Default Installation Options
- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account
Use this UniversalForwarder with:

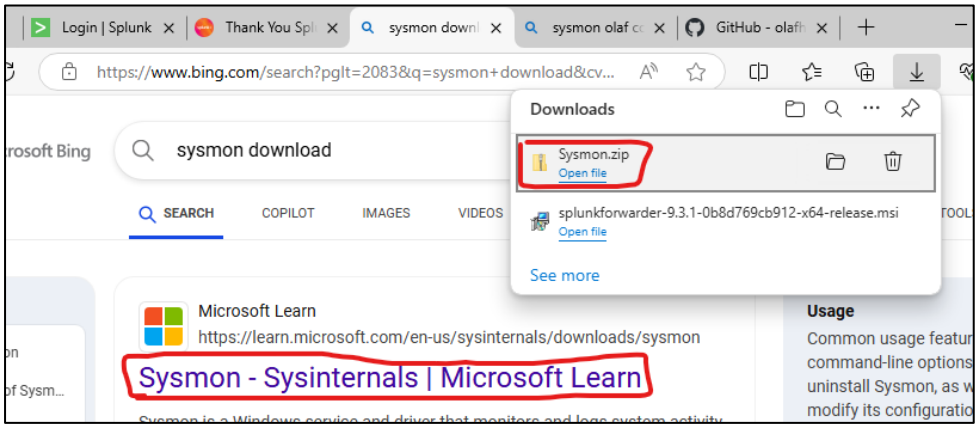

splunk>universal forwarder
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.
Username:
admin
Generate random password
Password:
Confirm password:


splunk>universal forwarder
If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.
Deployment Server
Hostname or IP
192.168.10.10
:
9997
Enter the hostname or IP of your deployment server, e.g. ds.splunk.com
default is
9997
Cancel
Back
Next



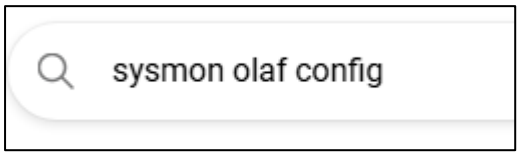
I am going to install Sysmon on the windows 10 pro as well

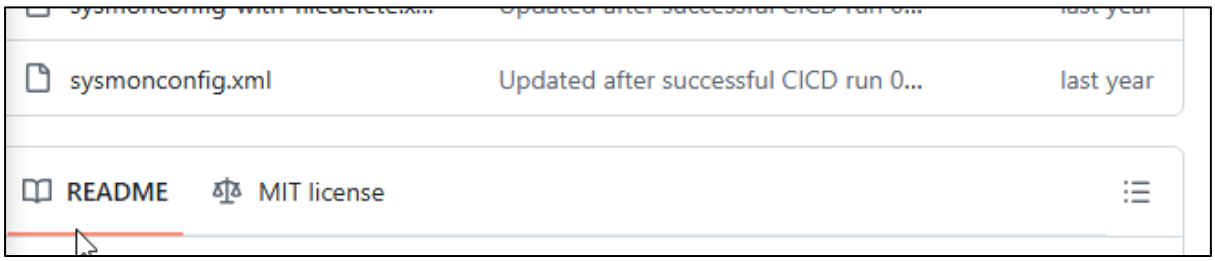
Here are the steps to do so



We will be using Olaf Sysmon config and it's on GitHub.
https://github.com/olafhartong/sysmon-modular

Scroll down and download this .xml file

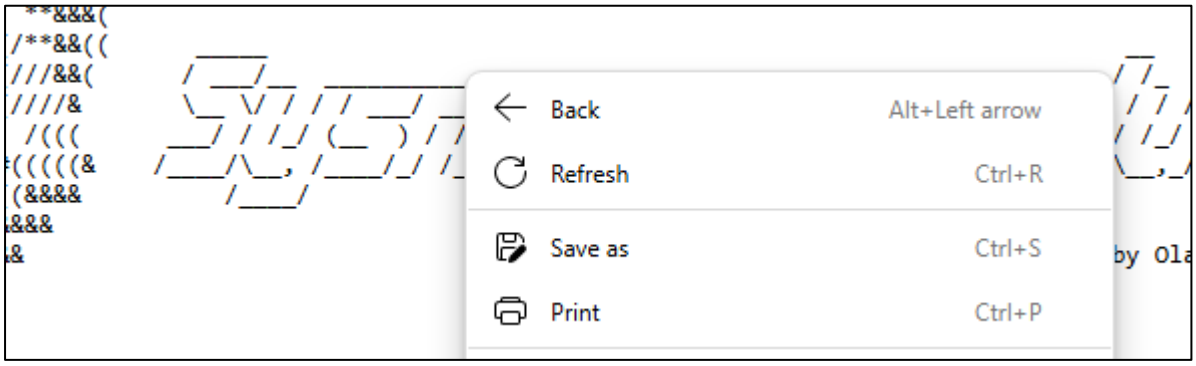




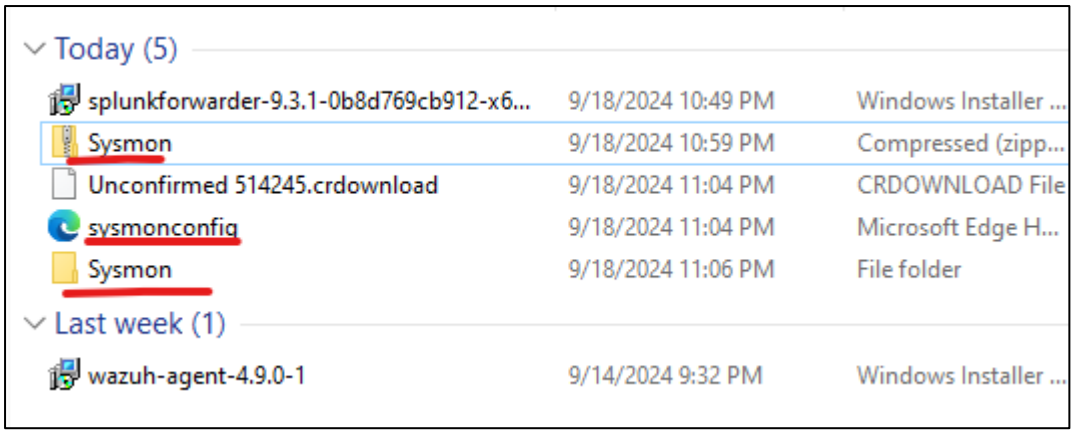
Click on it and go ahead and click on raw

Then right click and click on save as

Save it to your downloads



Ater you are done saving the file, extract your Sysmon file

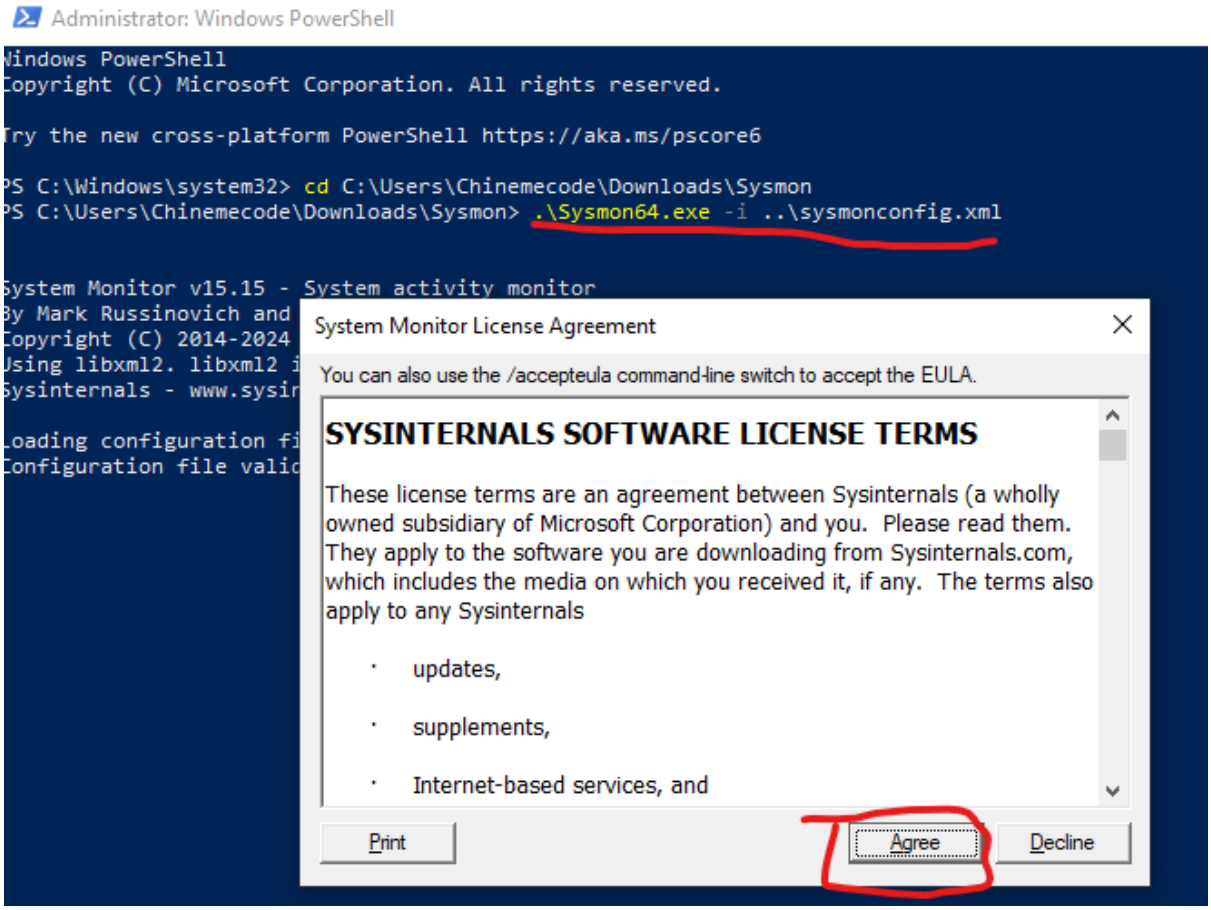


Open the extracted file and copy the path.

Then go to wiodws and open powershell as privileged

Type in the following command and hit enter for Sysmon to install

-i indicate specification of a configuration file



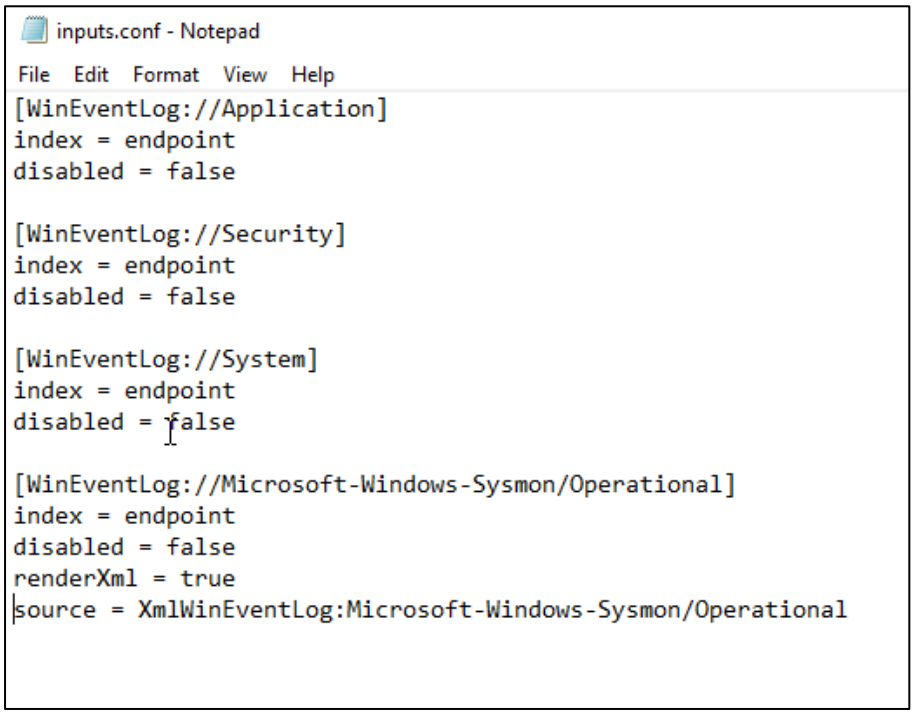
Configuring Splunk Universal Forwarder for Event Monitoring

In this step of the Active Directory project, we configure the Splunk Universal Forwarder to send specific event data to our Splunk server for monitoring and analysis. This involves editing the inputs.conf file, which tells the forwarder which data sources to monitor and forward.

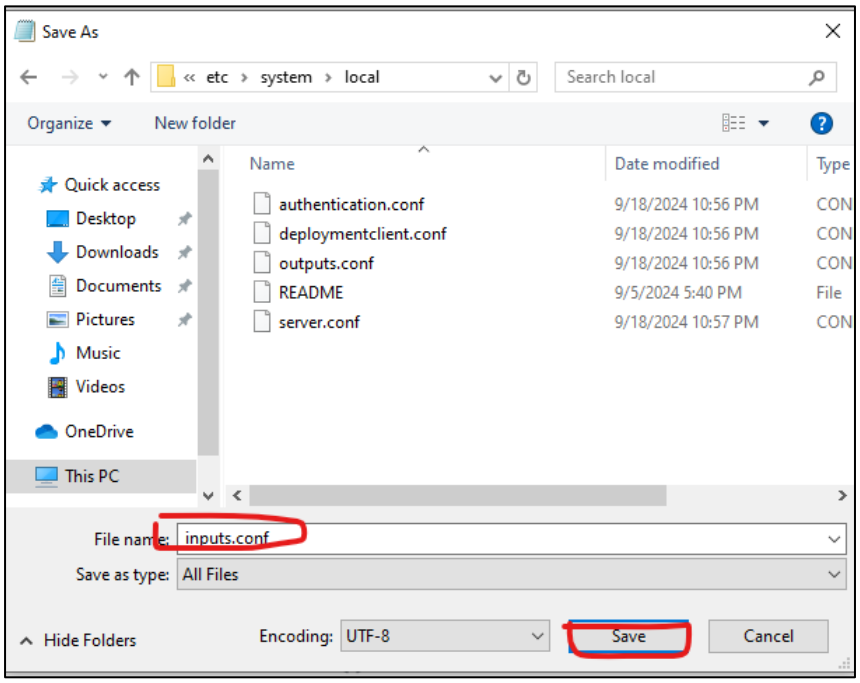
Steps for Configuring the Splunk Forwarder:

1. **Locate the inputs.conf File:**
    - The inputs.conf file is crucial for specifying what data the Splunk Forwarder should send to the Splunk server.
    - It is initially located in the following directory:
        - C:\Program Files\SplunkUniversalForwarder\etc\system\default\inputs.conf
2. **Do Not Edit the Default File:**
    - It is important **not** to edit the inputs.conf file in the default directory. Editing this file can cause configuration issues and may make it difficult to revert to the default settings if mistakes are made.
    - Instead, create a new inputs.conf file in the local directory:
        - C:\Program Files\SplunkUniversalForwarder\etc\system\local\

3. **Create a New inputs.conf File:**
    - Right-clicking in the local directory may not allow file creation due to administrative restrictions.
    - To overcome this, open **Notepad** (or your preferred text editor) with **administrative privileges**:
        - Search for "Notepad" in the Start Menu, right-click, and select "Run as administrator."
    - Copy the content for the new inputs.conf file, which specifies the types of events (e.g., application, security, system) the forwarder should monitor and the index to which they should be sent.
4. **Copy and Paste Configuration:**
    - The contents of the new inputs.conf file should include instructions for the Splunk Forwarder on which events to monitor and where to send them.
    - Ensure to paste the provided content into the newly created inputs.conf file in the local directory.
    - The configuration directs the Splunk Forwarder to push events related to application, security, and system logs to the specified Splunk server.
5. **Specify the Index:**
    - In the configuration file, make sure to define the correct index. For this setup, the events are sent to an index named **"endpoint"**.
    - **Important:** The specified index (**"endpoint"**) must exist on the Splunk server. If the server does not have an index with this name, it will **not receive** the forwarded events.

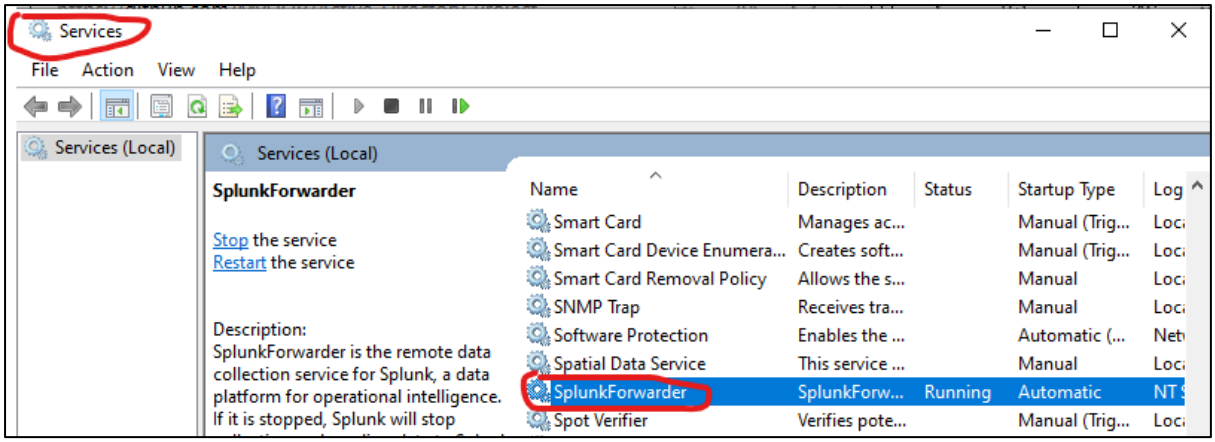


1. **Save the inputs.conf File:**
    - The new inputs.conf file, which defines the types of events to forward to the Splunk server, was saved in the following location:
        - C:\Program Files\SplunkUniversalForwarder\etc\system\local\
    - **File Creation:** The file was saved using Notepad running with administrative privileges.
    - When saving the file:
        - **File Name:** Entered as inputs.conf.
        - **Save As Type:** Changed to "All Files."
        - **Extension:** Used .conf to indicate it is a configuration file.



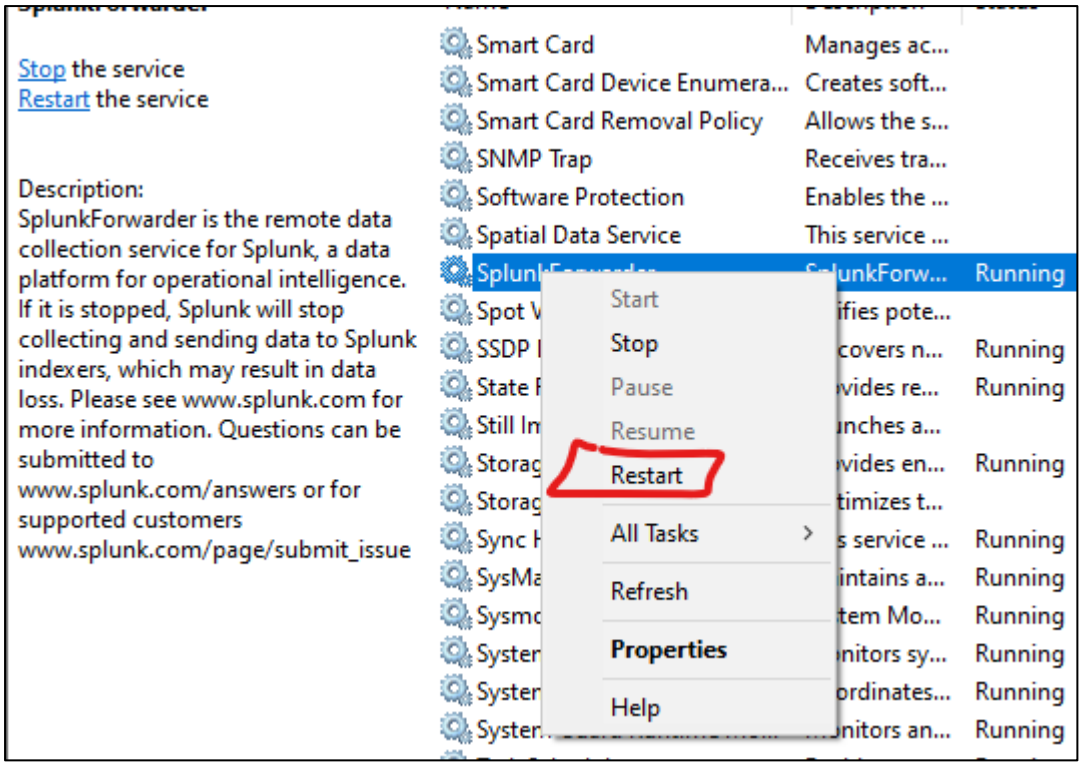
2. **Restart Splunk Universal Forwarder Service:**
    - After updating the inputs.conf file, it is **crucial** to restart the Splunk Universal Forwarder service to apply the changes.
    - To restart the service:

1. Open **Services** on the Windows machine as an administrator.
2. Locate the **SplunkForwarder** service.



3. **Log On As:** If the service is running under the NT SERVICE\SplunkForwarder account, change it to run as the **Local System Account** for proper permission to collect logs:

- Double-click the SplunkForwarder service.
- Navigate to the **Log On** tab.
- Select **Local System Account** and click **Apply**.
- Restart the service to apply the new logon settings.

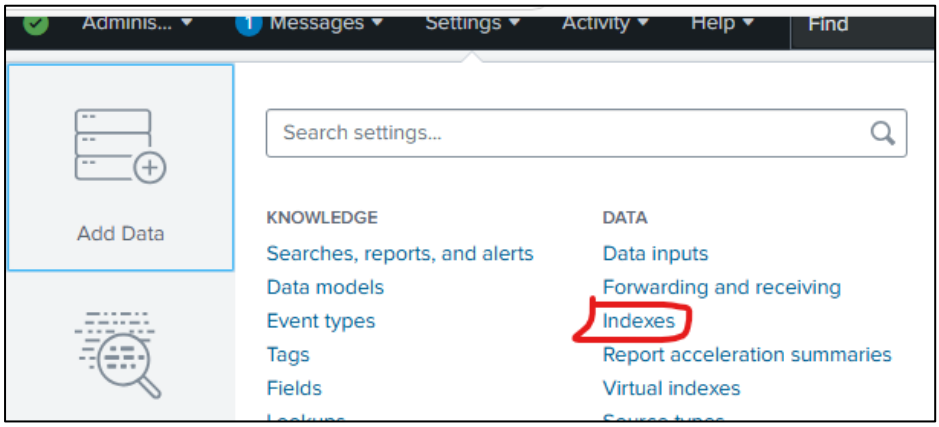


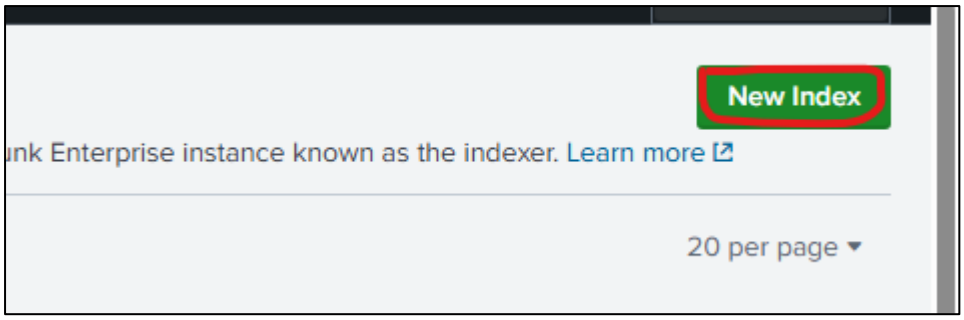
4. If prompted with warnings about stopping the service, proceed by clicking **OK** and start the service again.

3. **Configure the Splunk Server to Receive Data:**

   - Access the Splunk web portal using the credentials created during the Splunk server installation (e.g., username: chinemecoe-user1, Password: Umea228822).

- Navigate to **Settings** > **Indexes**:
  - Check if the **"endpoint"** index (as specified in inputs.conf) exists. If it does not:

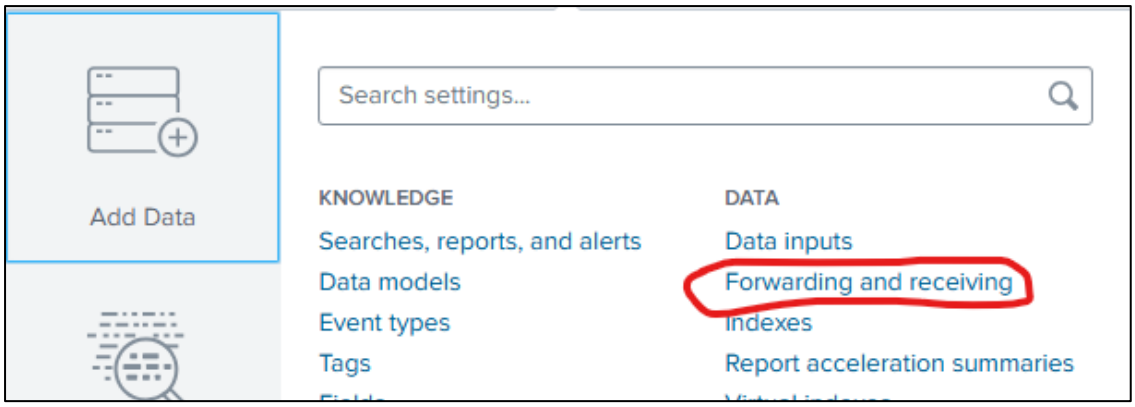




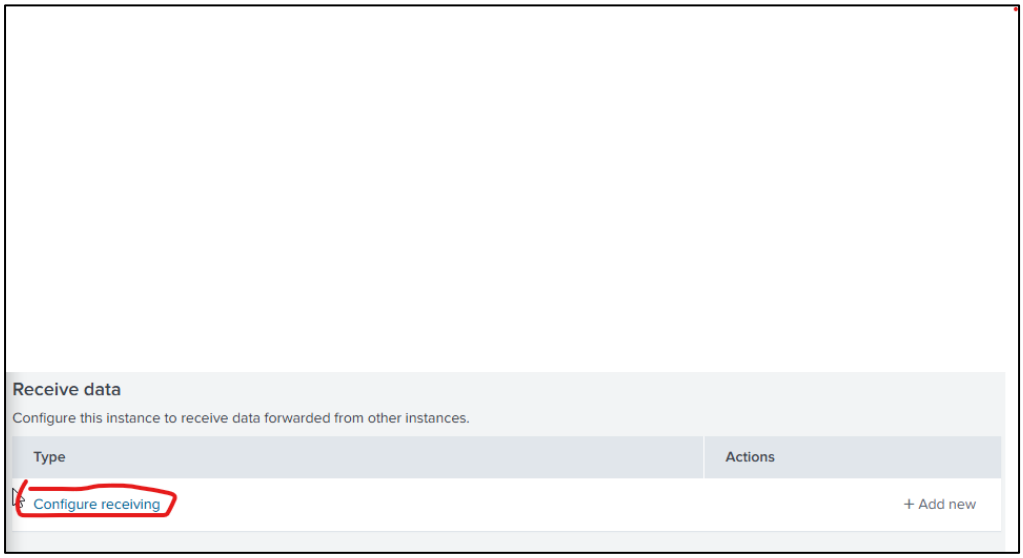
1. Click on **New Index**.
2. Name the new index "endpoint" and click **Save**.

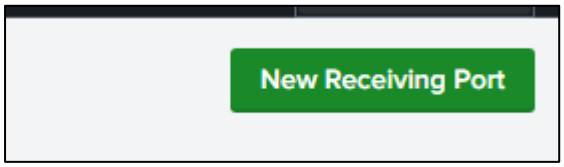
3. Verify the index is created by scrolling through the list of indexes.

- Enable data receiving:
  - Go to **Settings** > **Forwarding and Receiving**.

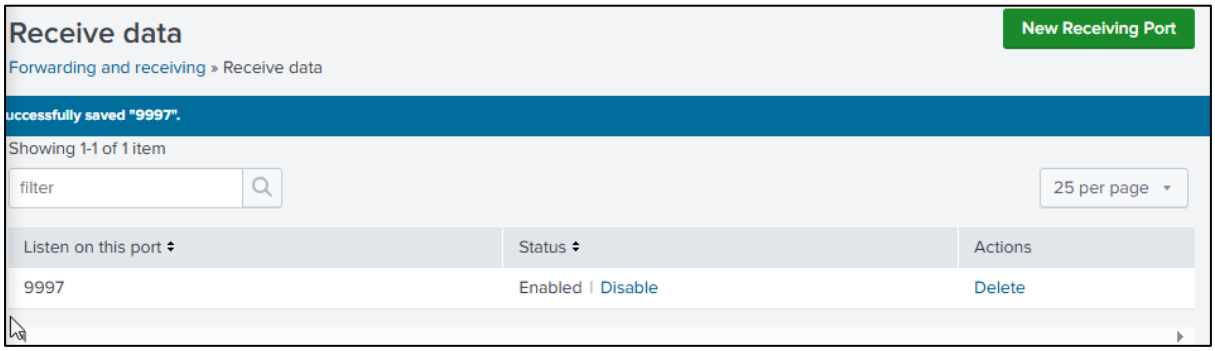


  - Under **Receive Data**, select **Configure Receiving**.

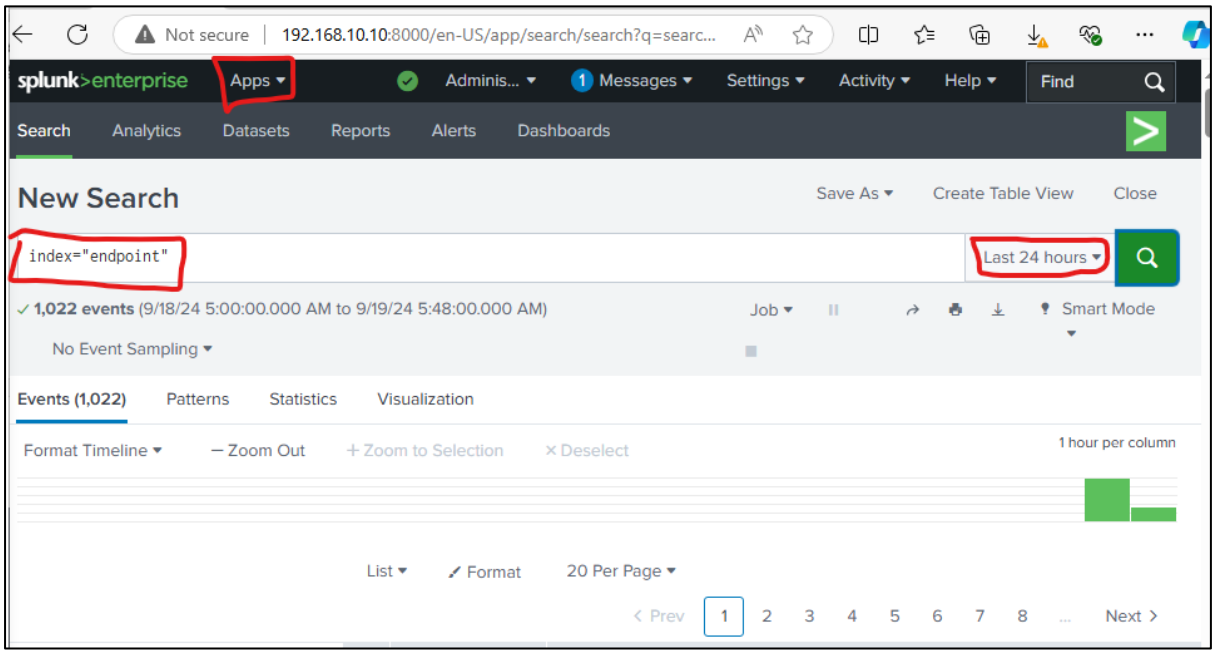


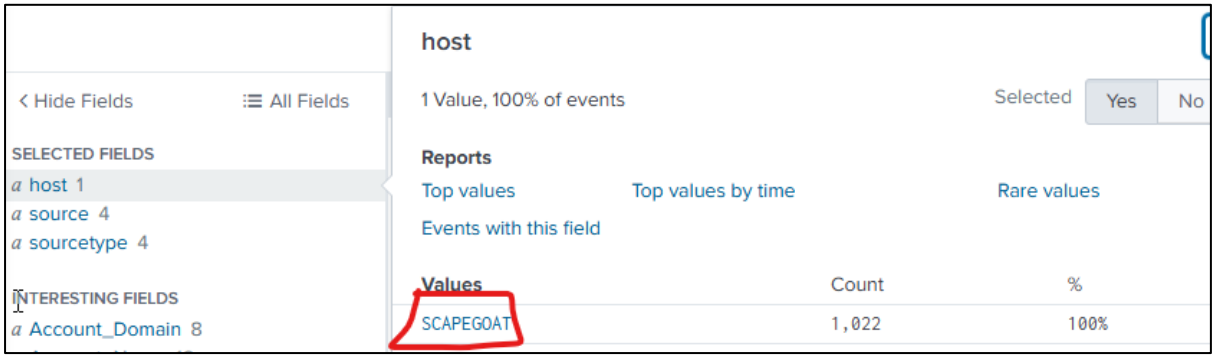


  - Add a new receiving port (**9997**), as previously configured in the forwarder.

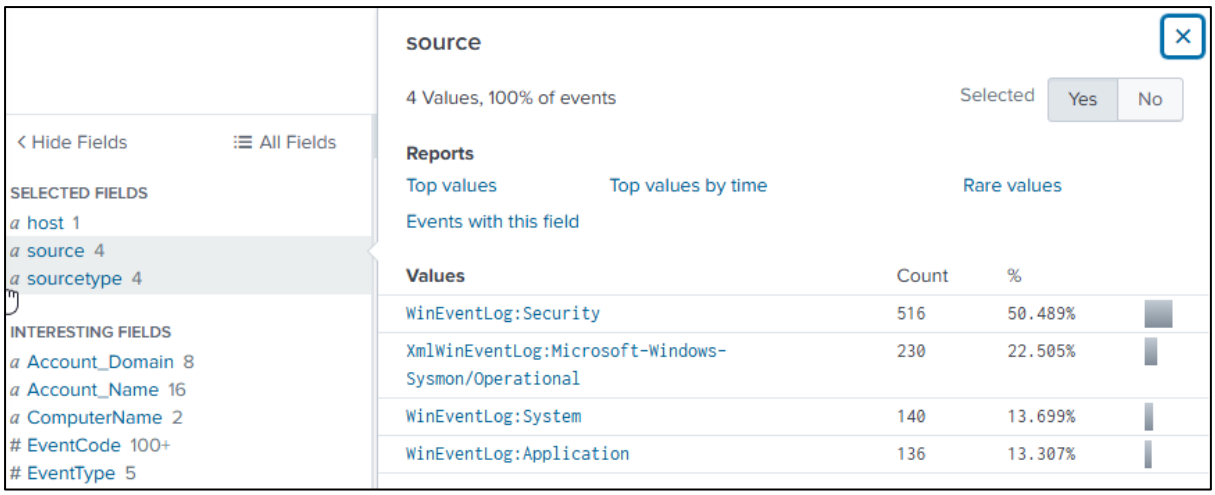


4. **Verify Data Ingestion in Splunk:**
    - After setting up the receiver and confirming the index, go to the **Search & Reporting** app in Splunk.
    - Run a search query to verify incoming data:
        - Use the search query: index=endpoint.
        - Check the time frame (e.g., "Last 24 hours") and click **Search**.
    - **Expected Results:** A list of events should appear, indicating successful data forwarding from the target machines.

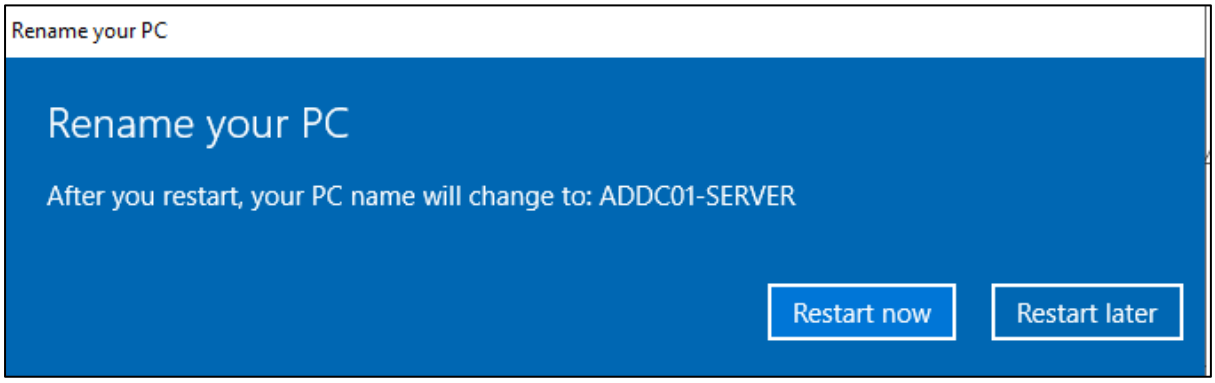


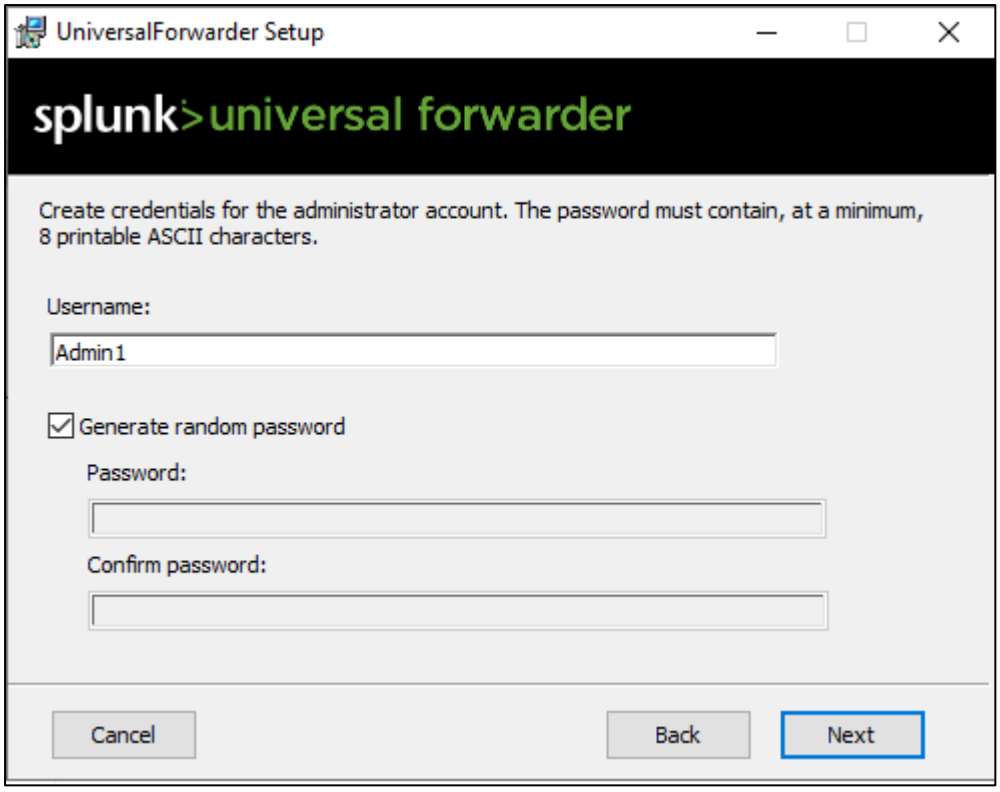


    - Confirm that the source types (application, security, system, sysmon) are present, as specified in the inputs.conf file.

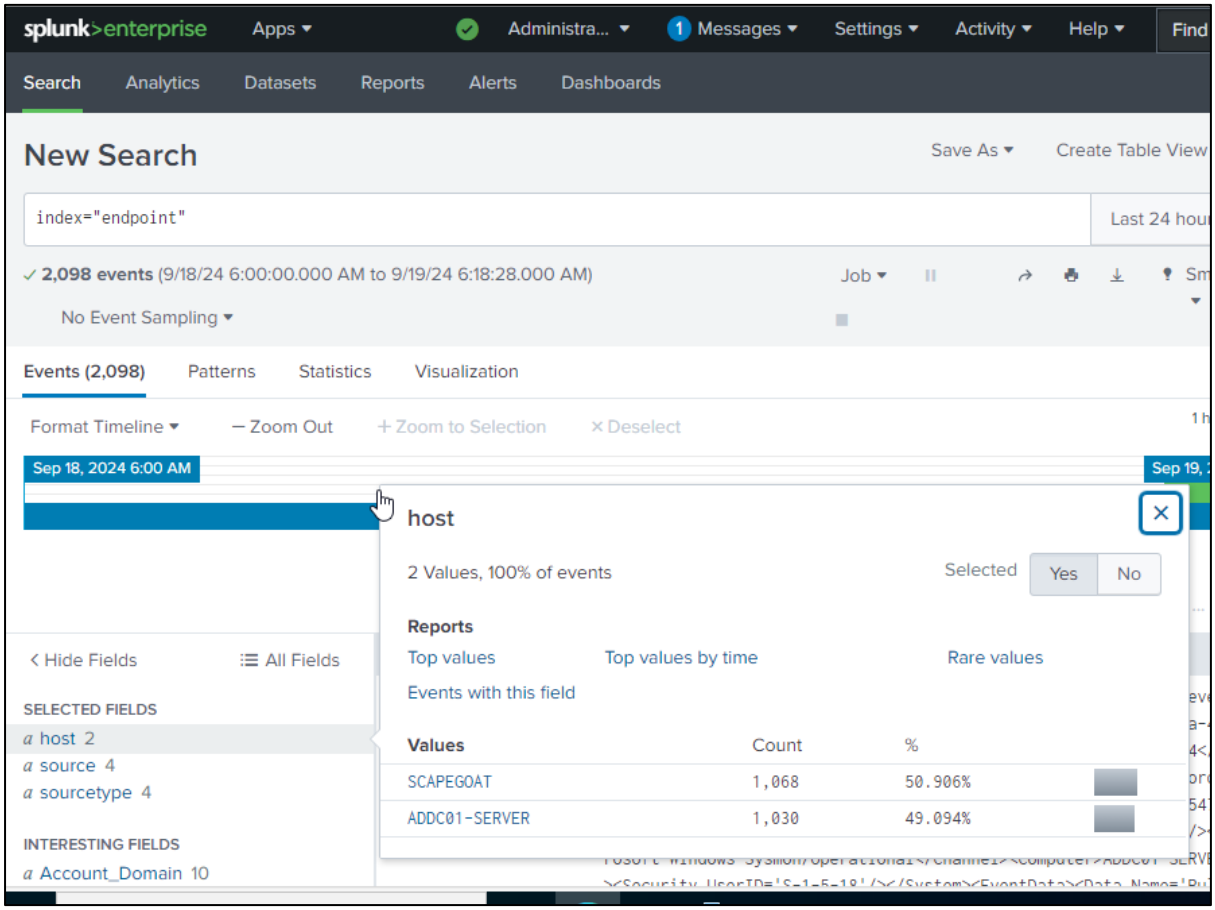


5. **Install and Configure Sysmon:**
   - Ensure Sysmon is installed and running on the target machines. The Splunk Universal Forwarder and the updated inputs.conf file should now collect and forward logs generated by Sysmon.
6. **Change Computer Name (Optional):**
   - To reflect proper naming conventions in the Active Directory environment, the server's computer name was changed to ADDC01:
     - Right-click on **This PC** > **Properties** > **Rename this PC**.
     - Enter the new name and restart the server to apply changes.





I was able to follow the same step for the windows 10 and I was able to get my windows server (ADDC01) up and running



Key Reminders:

- **Restart After Updates:** Whenever you update the inputs.conf file, remember to restart the Splunk Universal Forwarder service for the changes to take effect.
- **Permissions:** Ensure the SplunkForwarder service runs as **Local System Account** to avoid permission-related issues when collecting logs.
- **Verification:** Regularly check the Splunk web portal to ensure logs are being forwarded and indexed correctly.

Outcome:

With these steps, the Splunk Universal Forwarder and Sysmon are now properly installed, configured, and communicating with the Splunk server. Logs are forwarded to the "endpoint" index, allowing for real-time analysis and monitoring.

Part 4: Installing and Configuring Active Directory, Promoting to Domain Controller, and Adding Target Machines

In this part of the project, the focus is on setting up and configuring Active Directory (AD) on the Windows Server, promoting it to a domain controller, and integrating target machines into the newly created domain. This setup provides the foundation for managing network resources and users effectively.

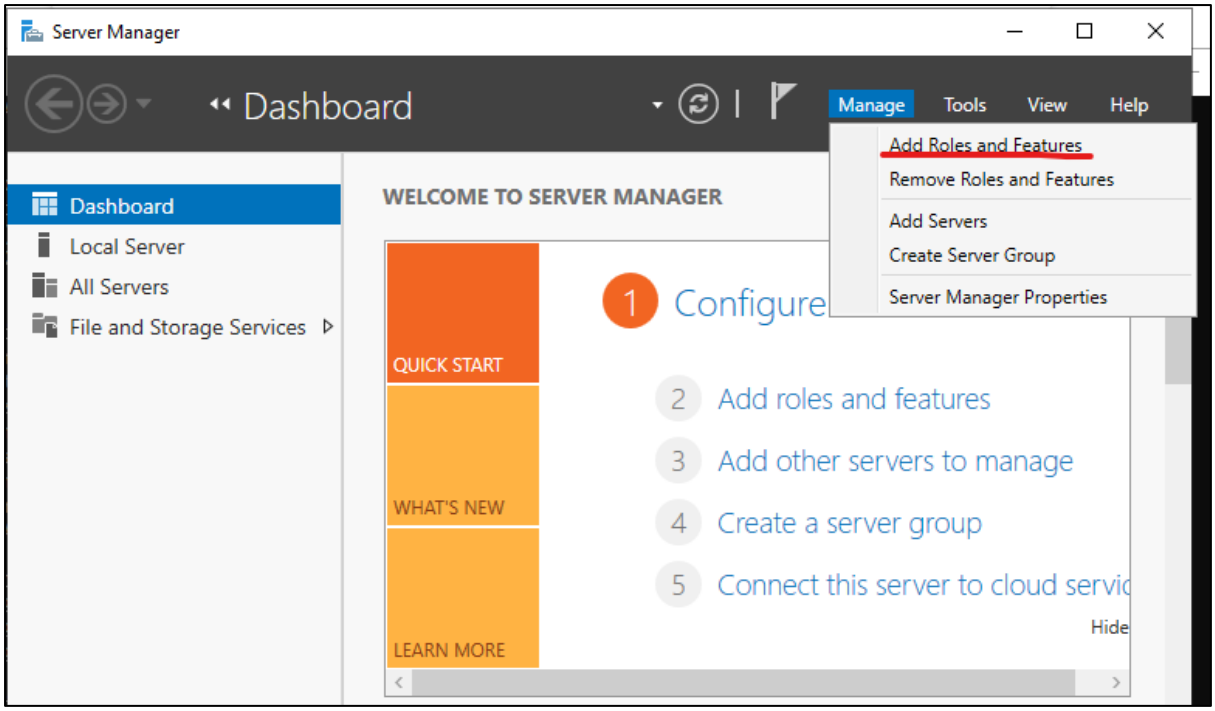
Steps Involved:

1. Setting a Static IP Address on Windows Server:

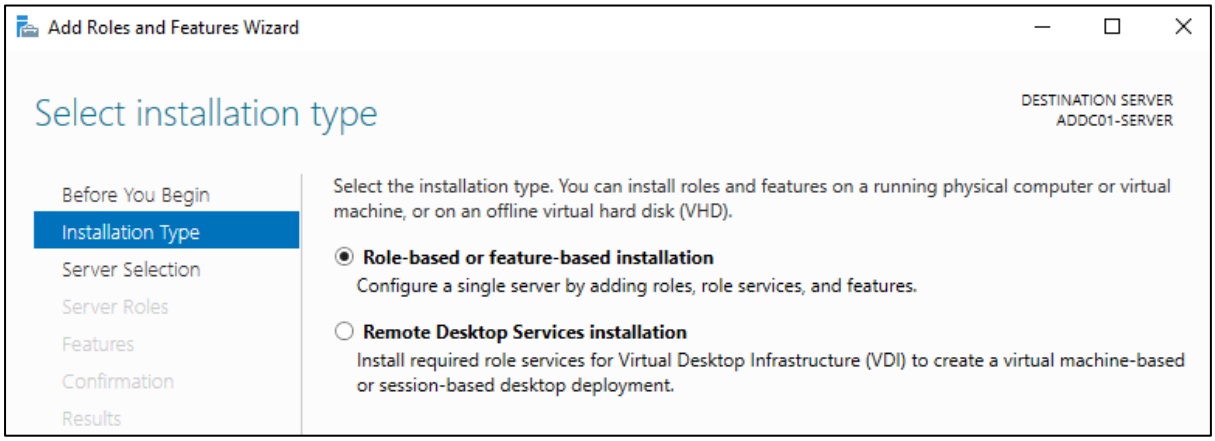
- Open **Network and Internet Settings** by right-clicking the network icon on the bottom-right of the screen.
- Select **Change Adapter Options**.
- Right-click the network interface and select **Properties**.
- Double-click on **Internet Protocol Version 4 (TCP/IPv4)**.
- Choose **Use the following IP address** and configure the network settings:
    - **IP Address:** 192.168.10.7
    - **Subnet Mask:** 255.255.255.0
    - **Default Gateway:** 192.168.10.1
    - **DNS Server:** 8.8.8.8 (Google's DNS)
- Confirm changes by clicking **OK**.
- Open **Command Prompt** (cmd) and run ipconfig to verify the IP address. Optionally, ping external servers (e.g., google.com) and internal servers (e.g., the Splunk server) to confirm connectivity.

2. Installing Active Directory Domain Services (AD DS):

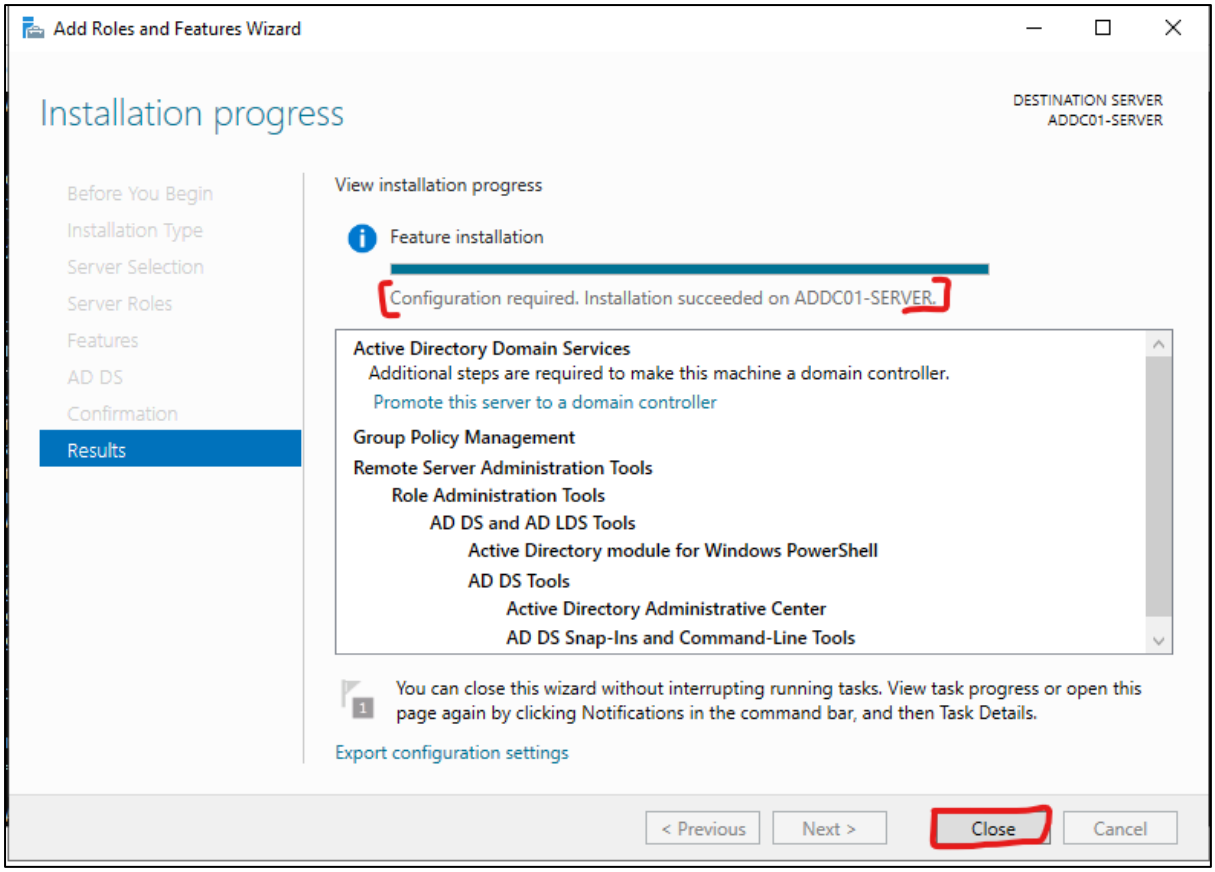
- Open **Server Manager** and click on **Manage** > **Add Roles and Features**.



- Select **Role-based or feature-based installation**.

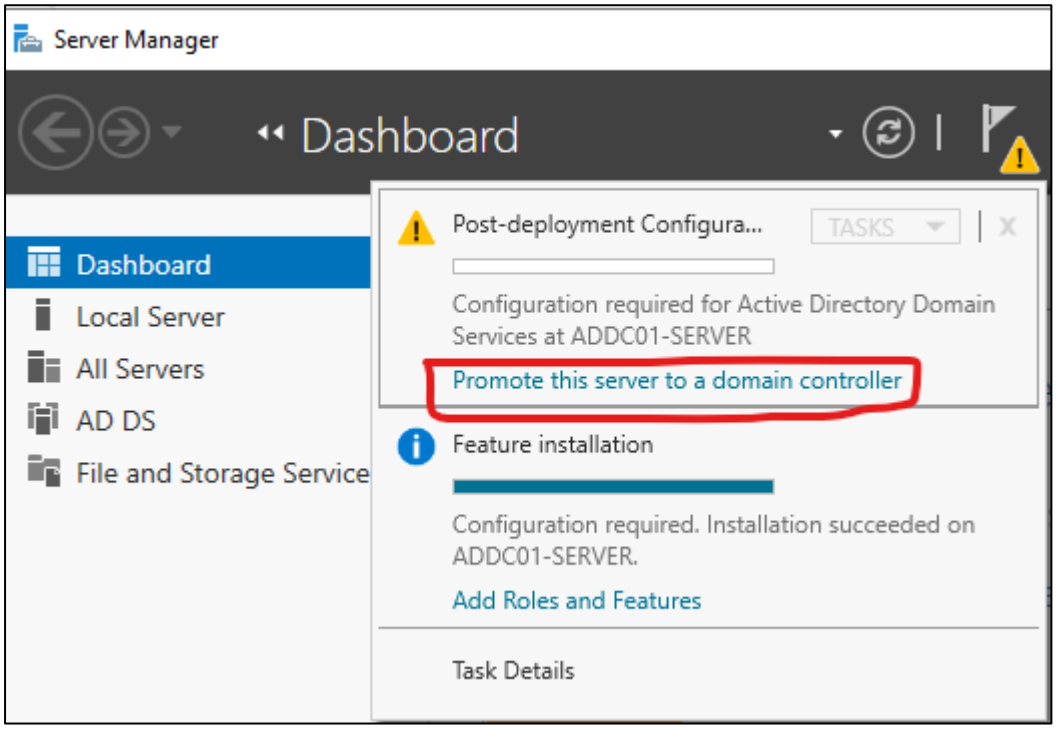


- Choose **Active Directory Domain Services (AD DS)** and click **Add Features**.
- Continue clicking **Next** and then **Install**. This process may take a few minutes to complete.
- After installation, look for a notification indicating "Installation succeeded" for AD DS.

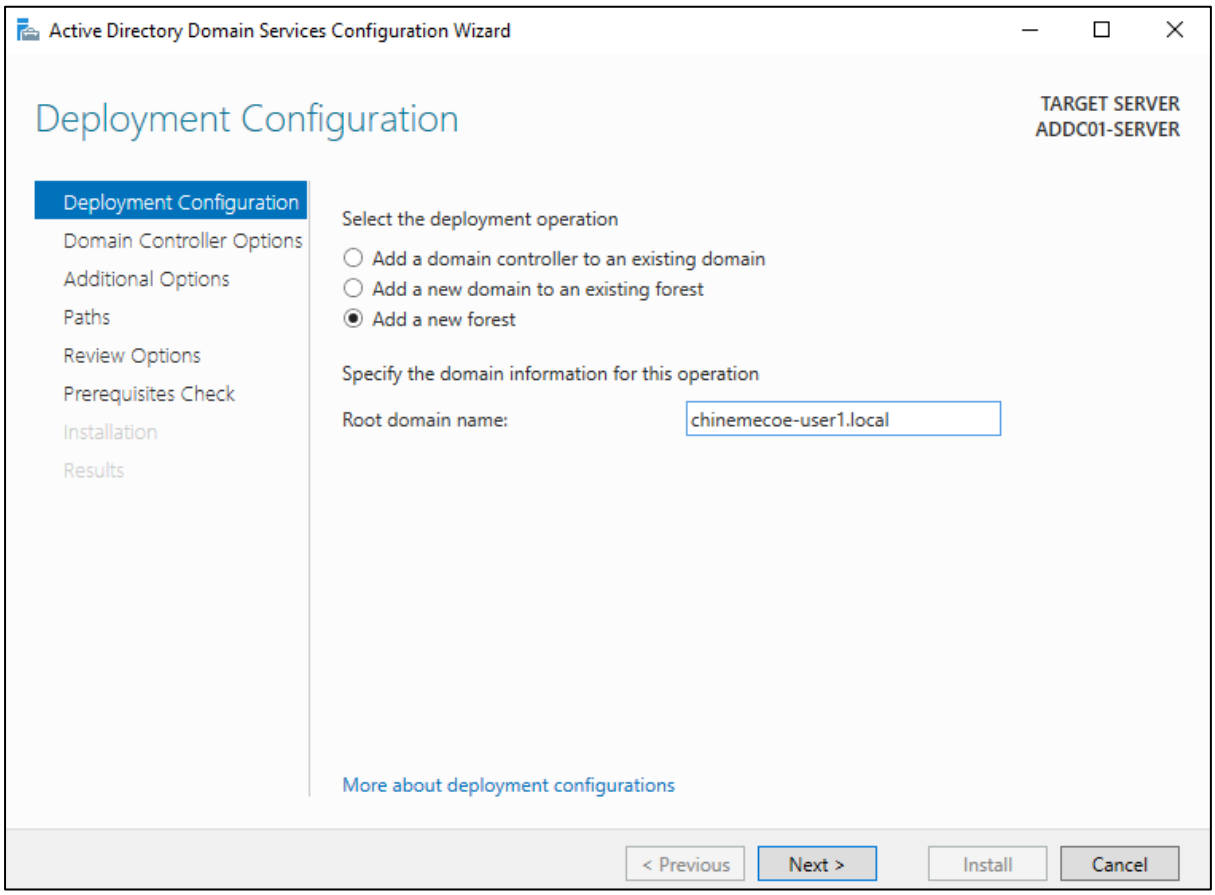


3. Promoting the Server to a Domain Controller:

- In **Server Manager**, click on the flag icon beside **Manage** and select **Promote this server to a domain controller**.



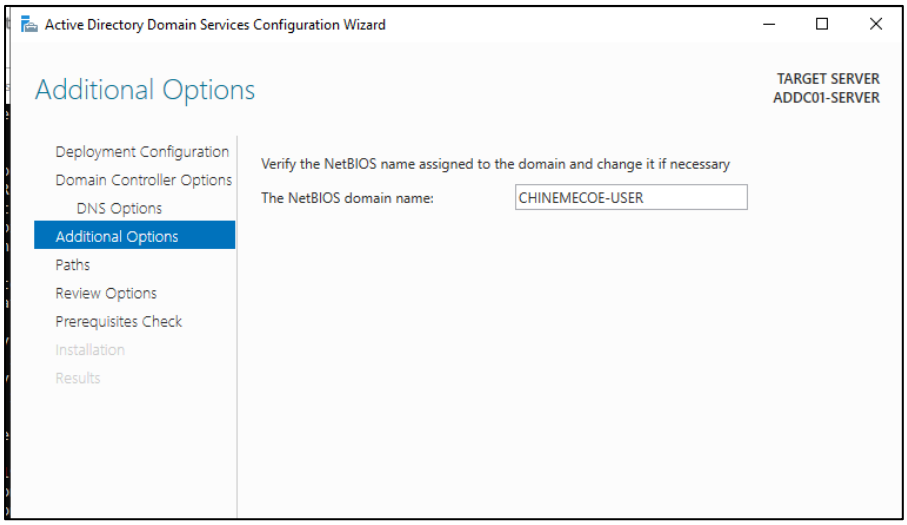
- Choose **Add a new forest** and provide the **Domain Name** (e.g., chinemecoe-username1.local). A top-level domain is required (e.g., .local).

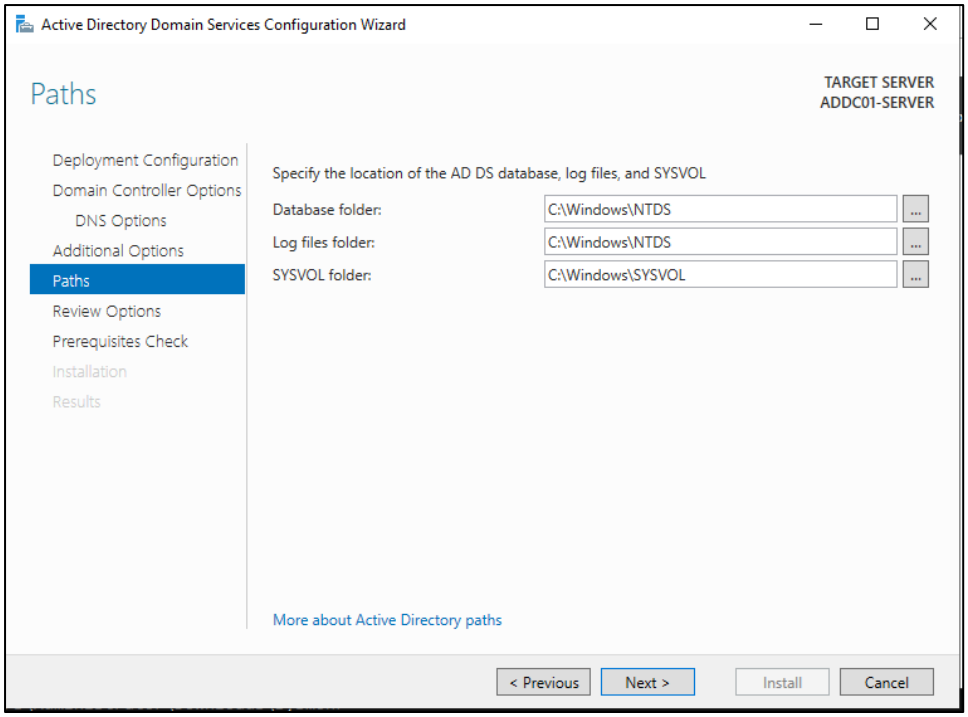


- Set a password for the Directory Services Restore Mode (DSRM).

Password: Umea228822

- Review the **NTDS.DIT** file location (a critical file for Active Directory that stores database and password hashes) and proceed with the default paths.

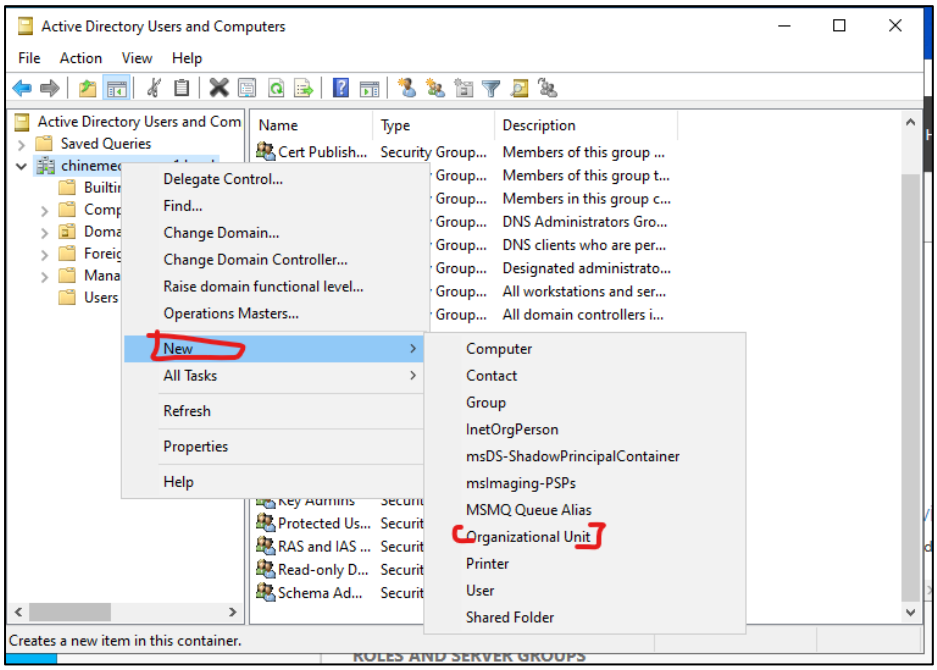




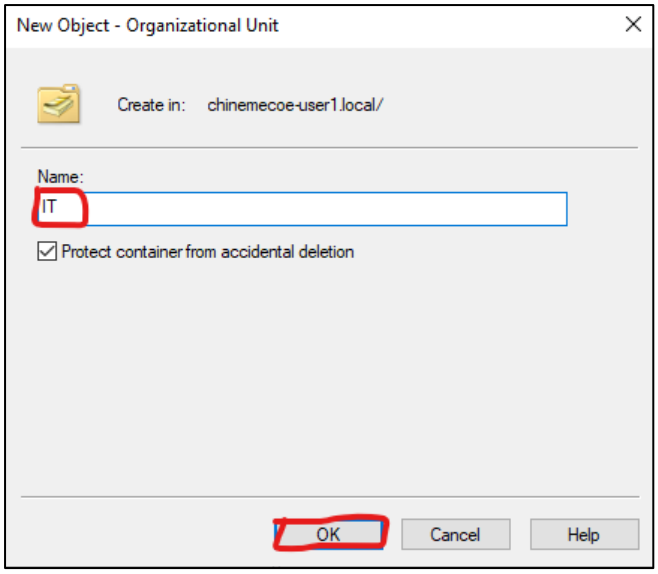
- Click **Install** to promote the server. The system will automatically restart upon completion.

4. Creating Users and Organizational Units (OUs):

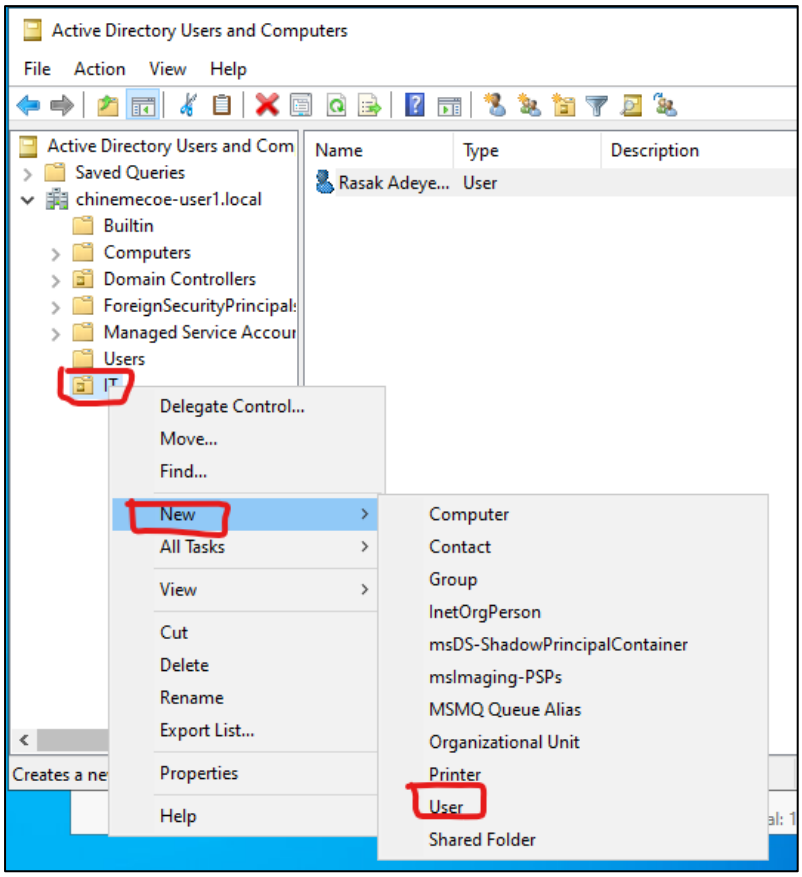
- Open **Active Directory Users and Computers** from the **Tools** menu in **Server Manager**.
- **Create Organizational Units (OUs):**
  - Right-click the domain, select **New** > **Organizational Unit**.

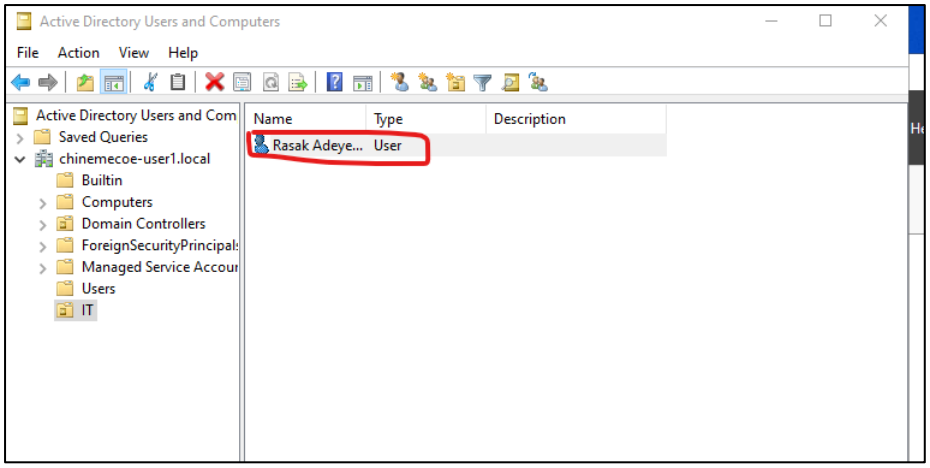


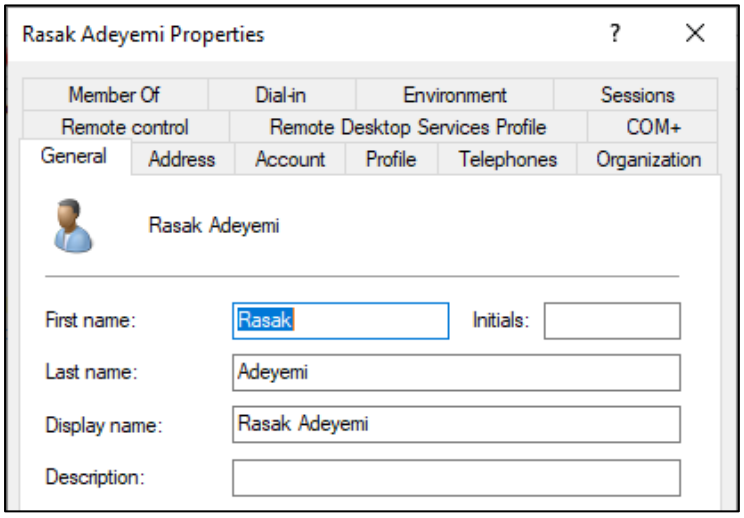
  - Name the OU (e.g., IT, HR) and click **OK**.

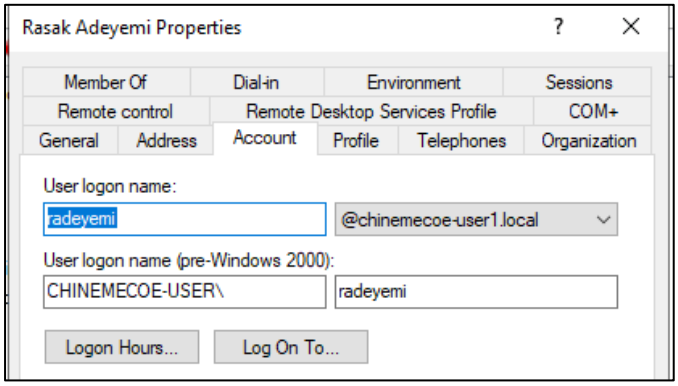


- **Create Users:**
  - Right-click the newly created OU (e.g., IT) and select **New** > **User**.
  - Provide user details (e.g., First Name: Rasak, Last Name: Adeyemi, Username: radeyemi).
  - Password: Umea228822

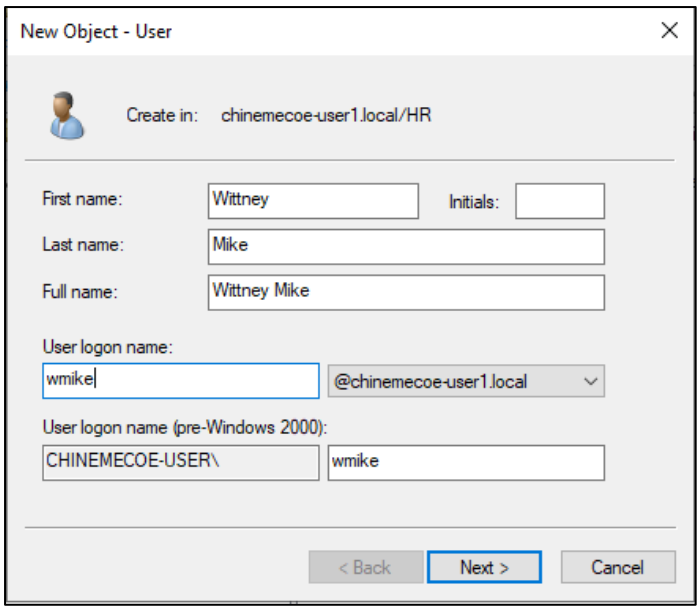








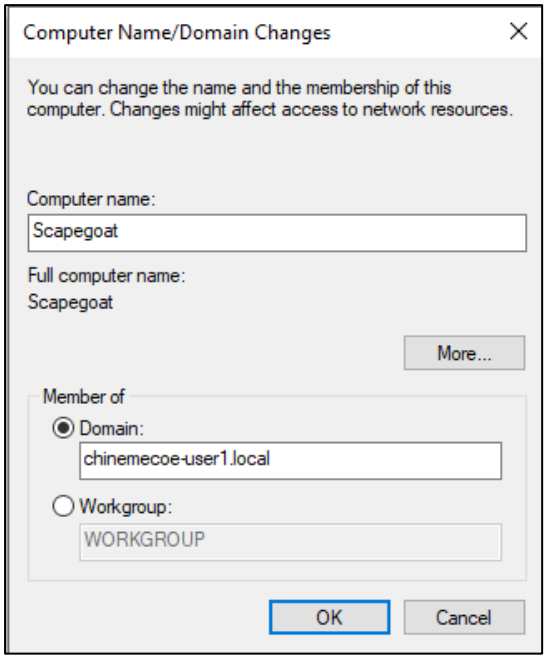
- Set a password and configure account settings (e.g., uncheck "User must change password at next logon" for lab environments).
- Repeat the process to create additional users as needed (e.g., Wittney for the HR OU).



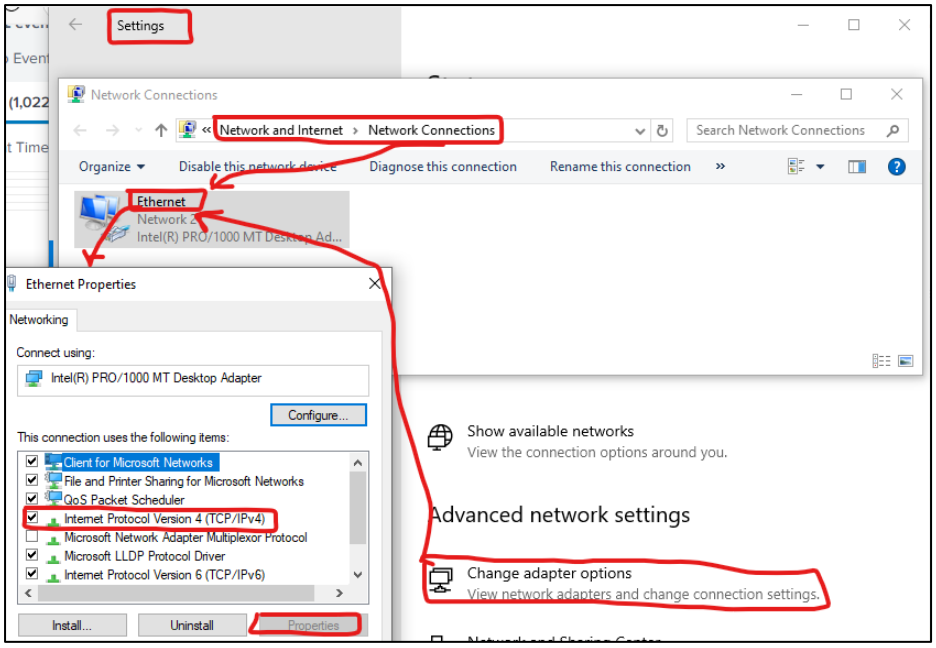
The password is the same as the guy from IT

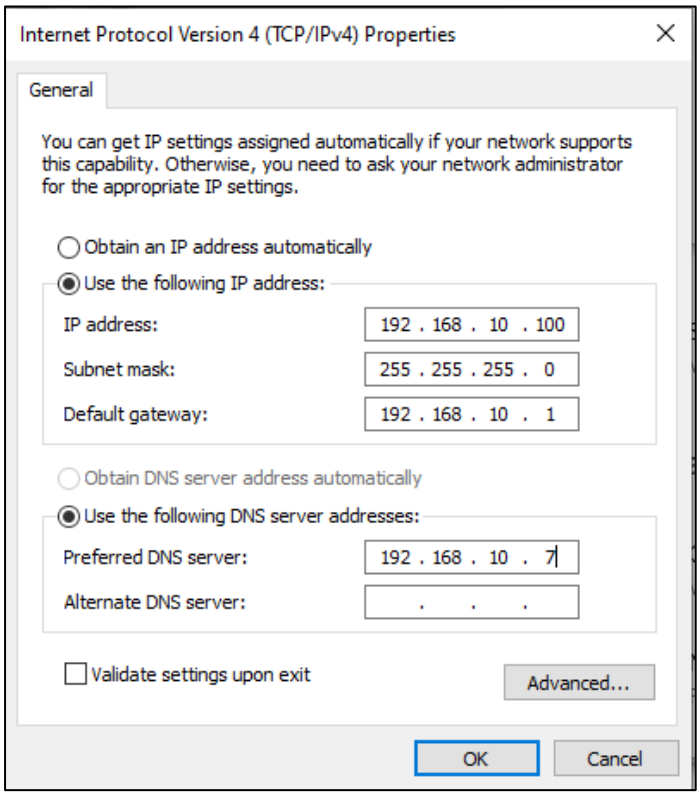
5. Adding Scapegoat Machine to the Domain:

- On the target Windows machine:
    1. Search for **This PC**, right-click, and select **Properties**.
    2. Click on **Advanced System Settings**, go to the **Computer Name** tab, and click **Change**.
    3. Select **Domain** and enter the domain name (e.g., chinemecoe-user1.local).

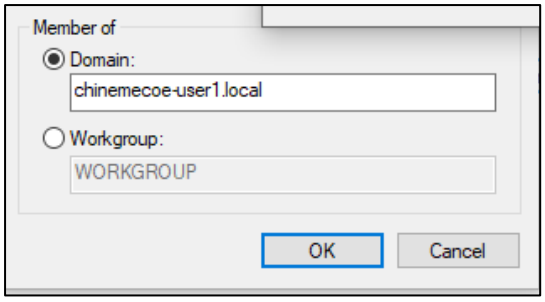


    4. If an error occurs stating that the domain controller could not be contacted, update the target machine's DNS server to point to the domain controller's IP address (192.168.10.7).

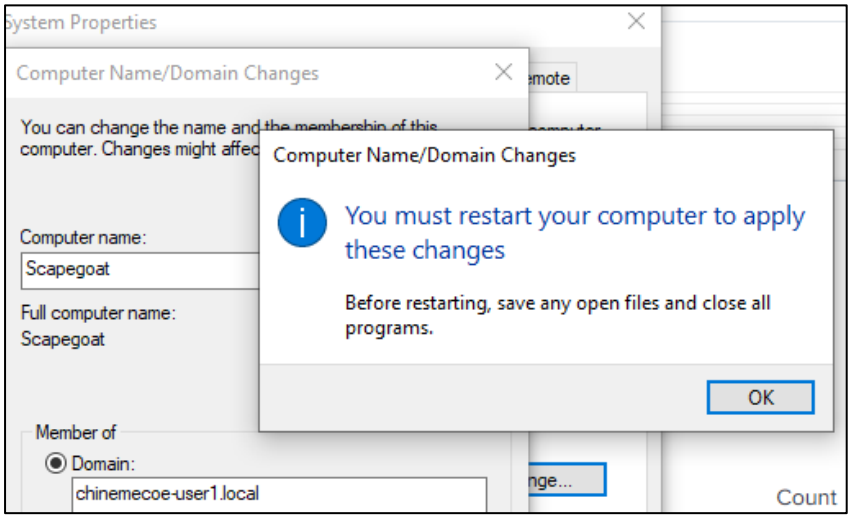




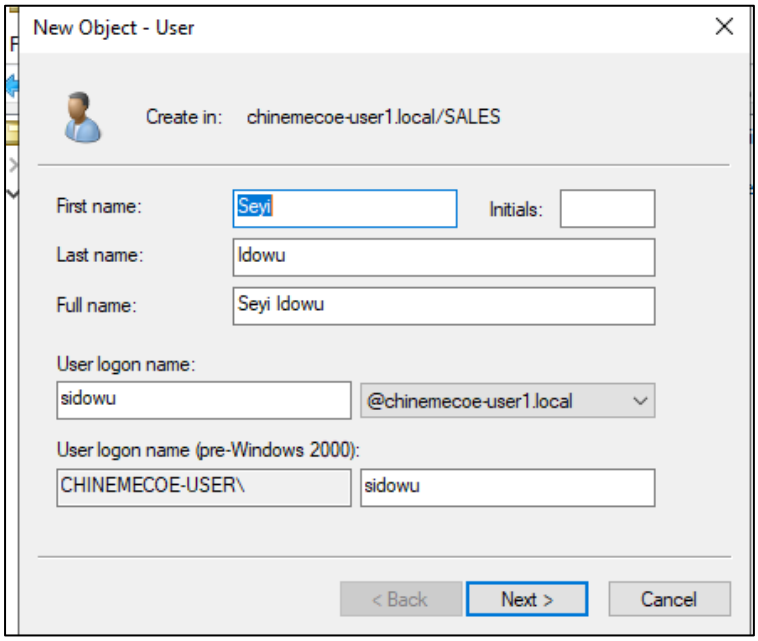
- After updating the DNS:
    - Use ipconfig /all in the command prompt to verify the DNS settings.
- Retry joining the domain using the domain administrator's credentials (e.g., Administrator).

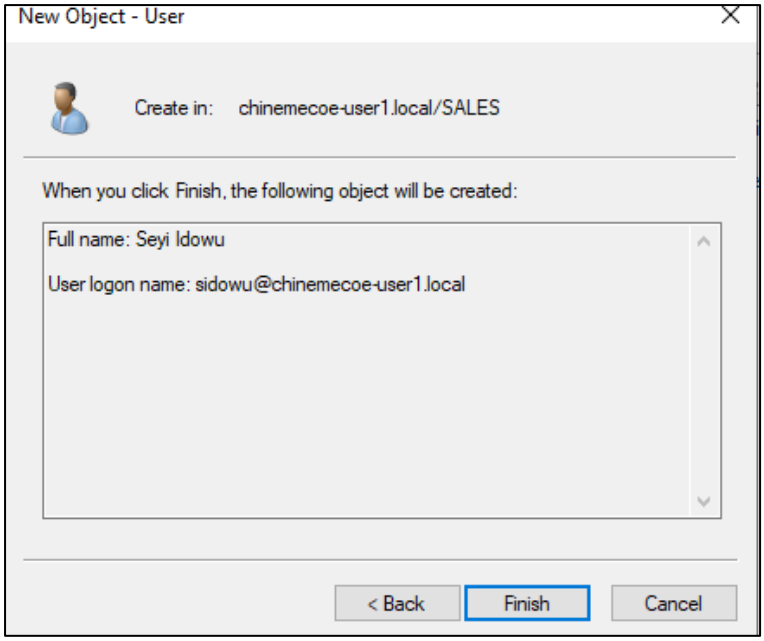


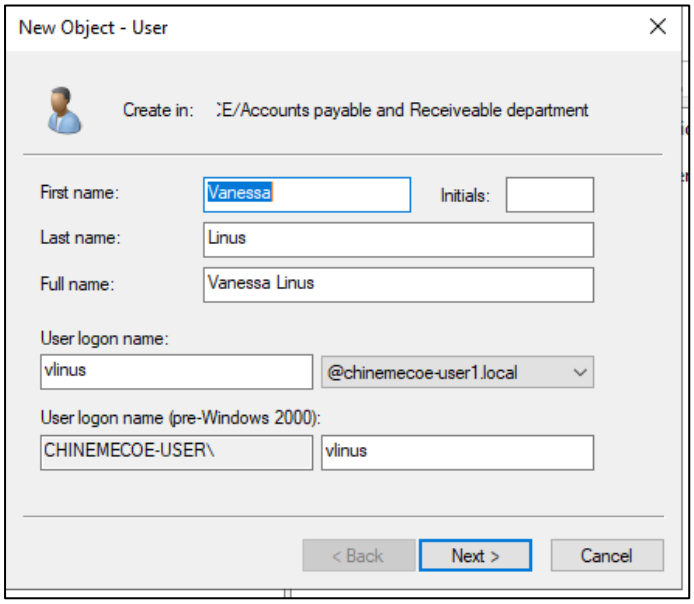
- Restart the target machine as prompted to complete the process.

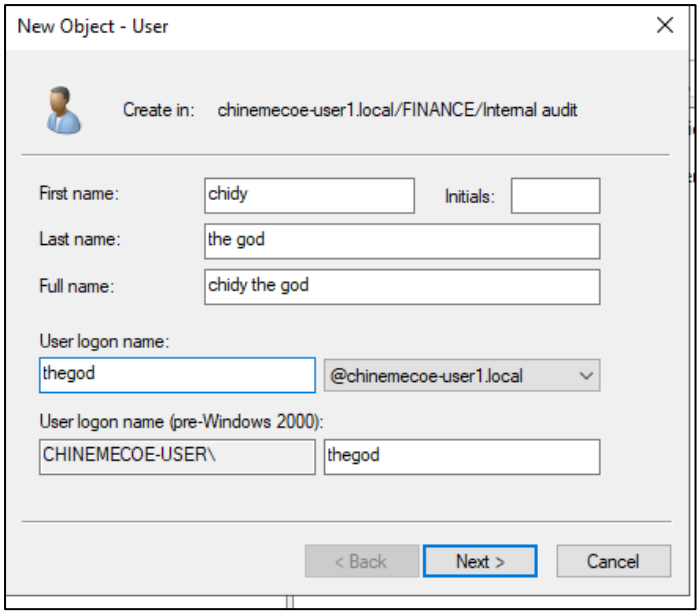


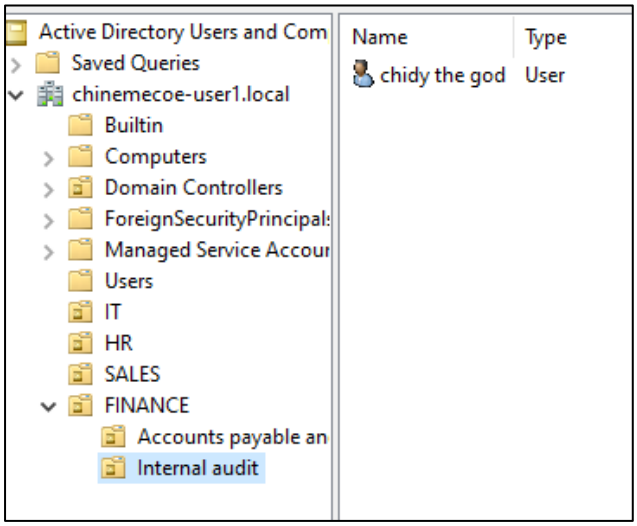
- Log in to the machine using the domain user account (e.g., wmike).




New Object - User
Create in: chinemecoe-user1.local/SALES
When you click Finish, the following object will be created:
Full name: Seyi Idowu
User logon name: sidowu@chinemecoe-user1.local
< Back
Finish
Cancel


New Object - User
Create in: :E/Accounts payable and Receiveable department
First name:
Vanessa
Initials:
Last name:
Linus
Full name:
Vanessa Linus
User logon name:
vlinus
@chinemecoe-user1.local
User logon name (pre-Windows 2000):
CHINEMECOE-USER\
vlinus
< Back
Next >
Cancel





Key Considerations:

- **Security:** The ntds.dit file on the domain controller is a critical target for attackers, as it contains all information related to Active Directory, including password hashes. Monitor access to this file closely.
- **Permissions:** Ensure that only authorized users are added to groups and use Organizational Units (OUs) to mimic real-world departmental structures.
- **DNS Configuration:** Proper DNS settings are vital for communication within the domain. Target machines must point to the domain controller's IP address for DNS resolution.

Next Steps:

With Active Directory set up and a domain controller in place, the target machines have been successfully joined to the domain. Moving forward, the project will focus on:

- Using **Kali Linux** to perform a brute force attack on the domain to simulate a real-world cybersecurity scenario.

- Setting up **Atomic Red Team** on the target machine to generate telemetry data for analysis in Splunk.

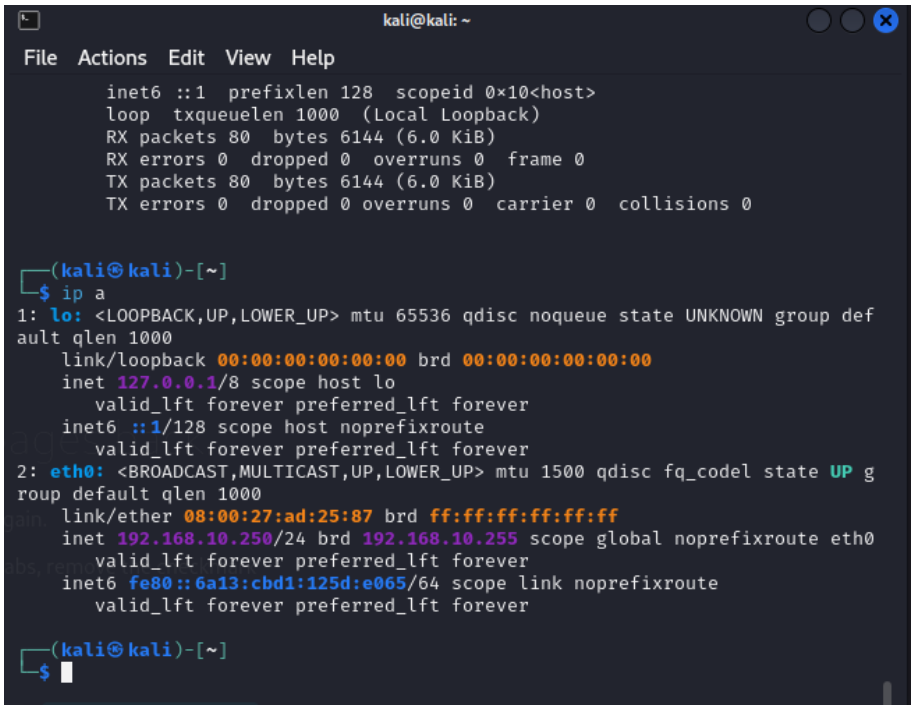
Part 5: Performing a Brute Force Attack and Setting Up Atomic Red Team for Telemetry in Splunk

In this final phase of the Active Directory project, we use Kali Linux to conduct a brute force attack against the Active Directory environment and set up Atomic Red Team to generate telemetry data for analysis in Splunk. This provides a practical understanding of attack detection, event logging, and how to leverage tools for both offensive and defensive cybersecurity activities.

Steps Involved:

1. Preparing Kali Linux for the Attack:

- **Set Up a Static IP Address:**
  - Right-click the Ethernet icon on Kali Linux and select **Edit Connections**.
  - Choose the active connection (e.g., Wired Connection 1), click the cog icon, and go to the **IPv4 Settings** tab.
  - Change the method to **Manual** and set the IP address:
    - **IP Address:** 192.168.1.250
    - **Netmask:** /24
    - **Gateway:** 192.168.10.1
    - **DNS Server:** 8.8.8.8
  - Save changes, disconnect, and reconnect the network interface to apply the new IP configuration.



- **Update and Upgrade Kali Linux:**
    - Open a terminal and run:

sudo apt-get update

sudo apt-get upgrade -y

- **Create a Project Directory:**
    - Create a directory to store all necessary files for the attack:

mkdir ~/Desktop/AD-project

- **Install Crowbar (Brute Force Tool):**
    - Install the crowbar tool for the brute force attack:

sudo apt-get install crowbar

- **Unzip the RockYou Wordlist:**
    - Kali Linux comes with a popular wordlist located in /usr/share/wordlists/rockyou.txt.gz.
    - Unzip the file using:

sudo gunzip /usr/share/wordlists/rockyou.txt.gz

    - Copy the unzipped wordlist to the project directory:

cp /usr/share/wordlists/rockyou.txt ~/Desktop/ad-project/

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass       dnsmap.txt     john.lst    nmap.lst        wfuzz
dirb        fasttrack.txt  legion      rockyou.txt.gz  wifite.txt
dirbuster   fern-wifi      metasploit  sqlmap.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo gunzip rockyou.txt.gz

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ ls
amass       dnsmap.txt     john.lst    nmap.lst     wfuzz
dirb        fasttrack.txt  legion      rockyou.txt  wifite.txt
dirbuster   fern-wifi      metasploit  sqlmap.txt

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cp rockyou.txt ~/Desktop/AD-project

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cd ~/Desktop/AD-project

┌──(kali㉿kali)-[~/Desktop/AD-project]
└─$
```

2. Setting Up the Attack:

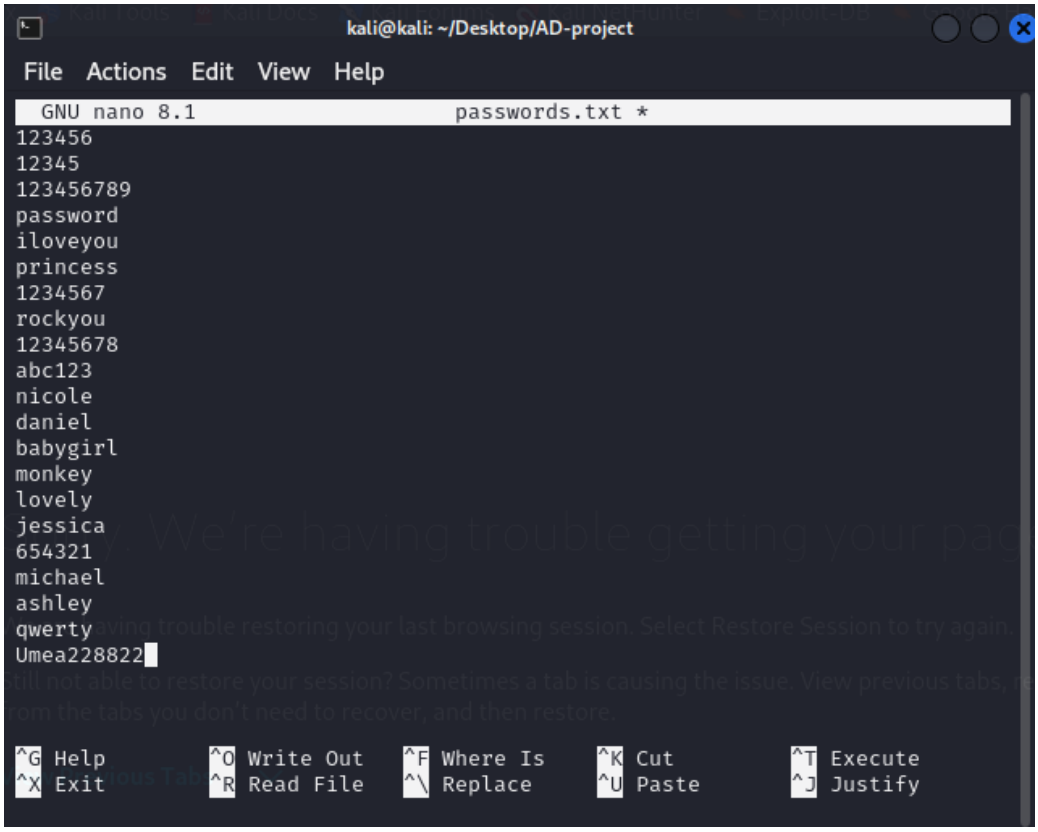
- **Limit the Wordlist for Demo Purposes:**
  - Use the first 20 lines of the rockyou.txt wordlist for the attack and save it to a new file called passwords.txt:

head -n 20 ~/Desktop/ad-project/rockyou.txt > ~/Desktop/ad-project/passwords.txt

- **Modify the Wordlist:**
  - Open the passwords.txt file and add a known "secure" password for the attack:

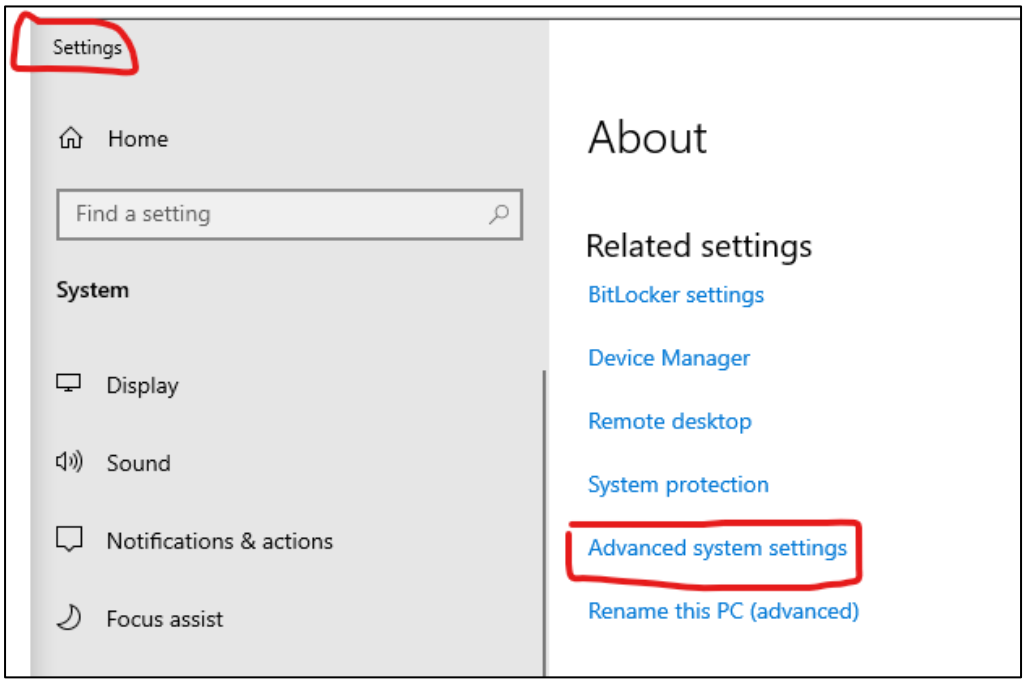
nano ~/Desktop/ad-project/passwords.txt

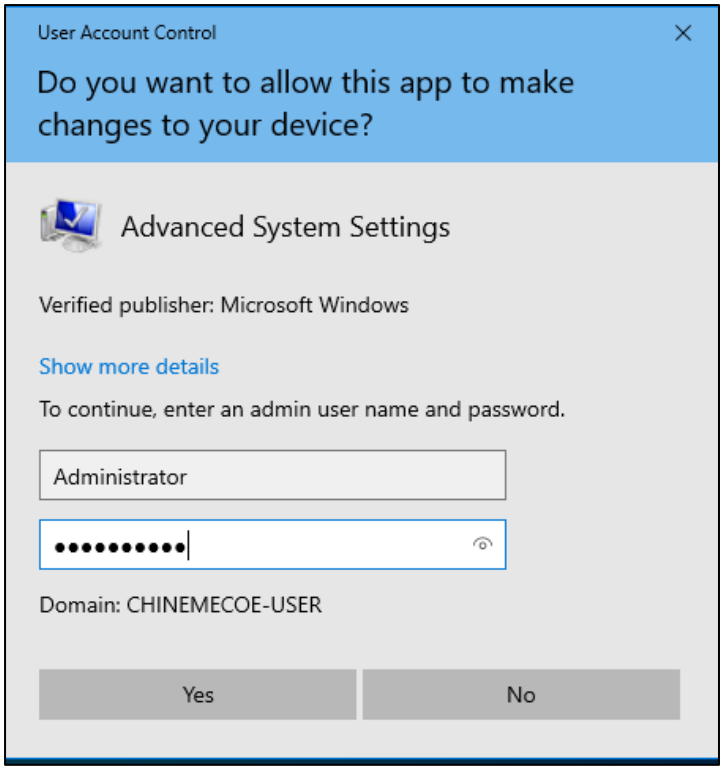
  - Save and exit.



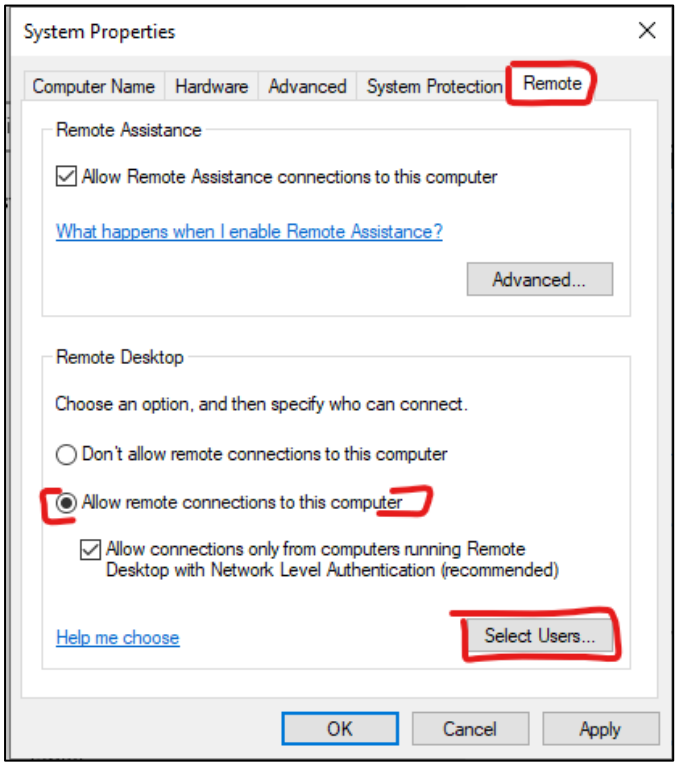
3. Enable Remote Desktop on the Target Machine:

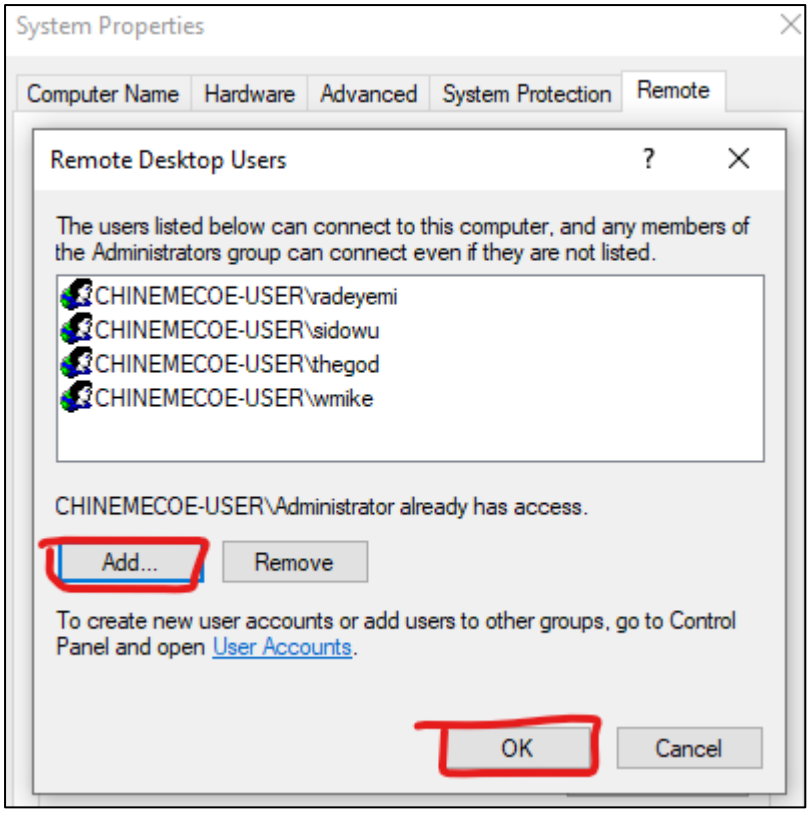
- On the target Windows machine:
    - Search for **This PC**, open **Properties**, and click on **Advanced System Settings**.

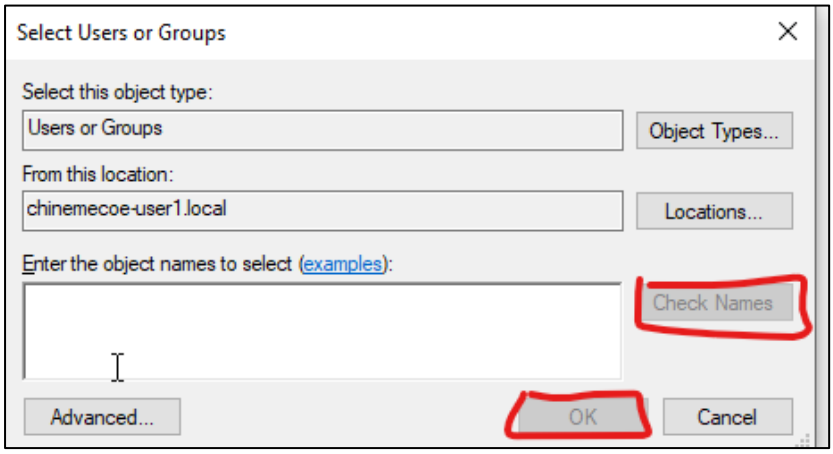




- Go to the **Remote** tab and select **Allow remote connections to this computer**.
- Add users to allow remote access (e.g., wmike, radeyemi, sidowu, thegod).



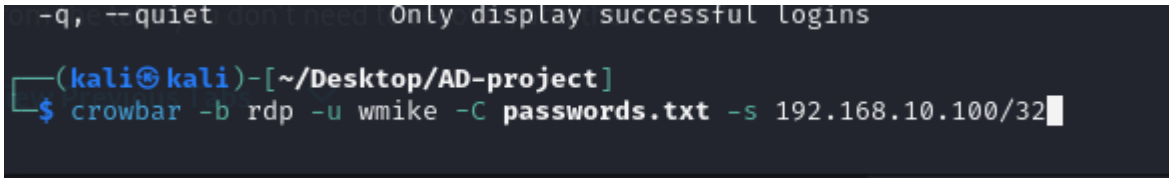




4. Perform the Brute Force Attack:

- **Run the Crowbar Tool:**
  - Clear the screen in Kali Linux and use crowbar to attempt a brute force attack on the target machine's Remote Desktop Protocol (RDP):

crowbar -b rdp -u TSmith -C ~/Desktop/ad-project/passwords.txt -s 192.168.10.10/32

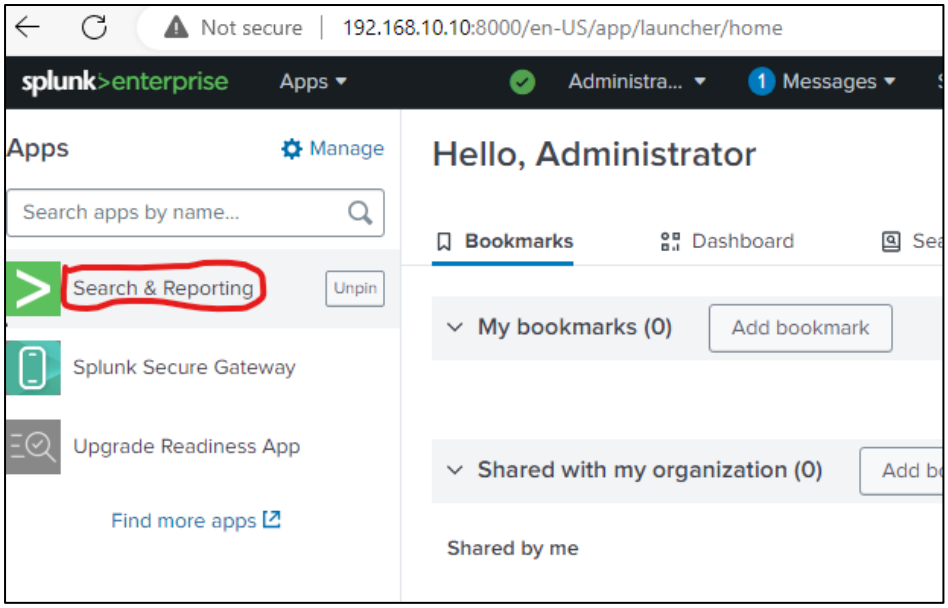


- The tool will iterate through the passwords in passwords.txt. If successful, you will see an RDP login success message.

```
┌──(kali㉿kali)-[~/Desktop/AD-project]
└─$ crowbar -b rdp -u wmike -C passwords.txt -s 192.168.10.100/32
2024-09-19 04:26:48 START
2024-09-19 04:26:48 Crowbar v0.4.2
2024-09-19 04:26:48 Trying 192.168.10.100:3389
2024-09-19 04:26:54 RDP-SUCCESS : 192.168.10.100:3389 - wmike:Umea228822
2024-09-19 04:26:54 STOP
```

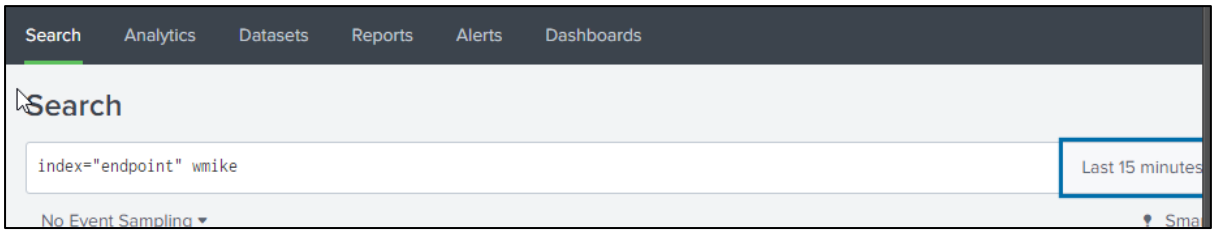
5. Analyzing the Attack in Splunk:

- **Search for Failed Login Attempts:**



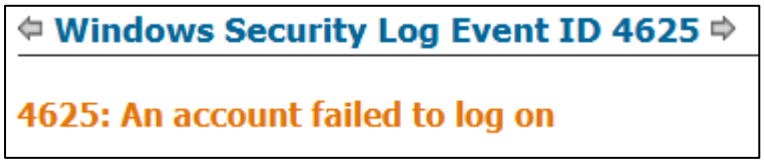
- In Splunk, open **Search & Reporting** and filter events for the target machine and user (wmike):

index=endpoint wmike



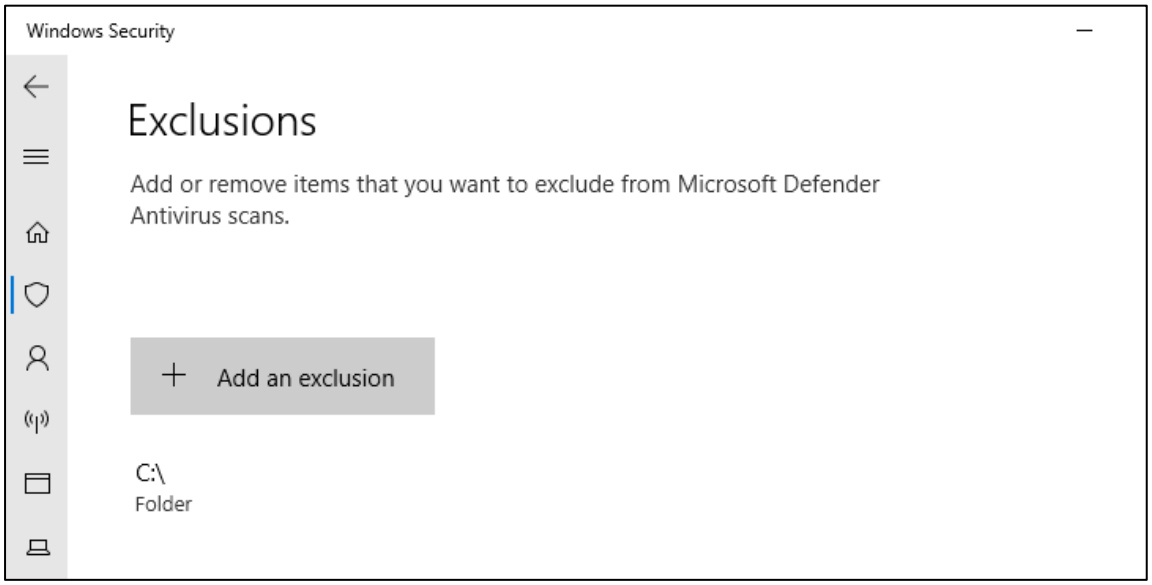
- Look for **Event ID 4625**, which indicates a failed login attempt. If you see multiple attempts within a short period, it signals potential brute force activity.

- **Search for Successful Login:**
  - Look for **Event ID 4624**, which represents a successful login attempt. Cross-reference the IP address and workstation name in the event details to verify the source of the login.



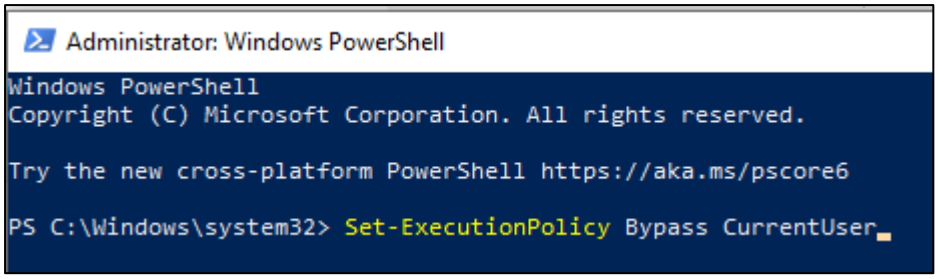
6. Setting Up Atomic Red Team for Telemetry Generation:

- **Disable Microsoft Defender:** (To avoid interference with Atomic Red Team)
  - Open **Windows Security** and navigate to **Virus & Threat Protection** > **Manage Settings**.
  - Add an exclusion for the entire C:\ drive.



- **Install Atomic Red Team:**
    - Open **PowerShell** as an administrator and change the execution policy:

Set-ExecutionPolicy Bypass -Scope CurrentUser



    - Download and install Atomic Red Team using the command provided in the Atomic Red Team documentation.

- **Run a Test:**
    - Navigate to the Atomic Red Team directory (C:\AtomicRedTeam) and select a technique to test. For example, create a local user:

Invoke-AtomicTest T1116.001

- **Verify in Splunk:**
    - Search for logs in Splunk related to the test (e.g., newly created users) to ensure visibility and detection capabilities.

Key Considerations:

- **Permissions:** Only conduct brute force attacks and telemetry generation in a controlled lab environment with machines you own or have permission to test.
- **Splunk Alerts:** Use the information gathered to create alerts for suspicious activities, such as multiple failed login attempts (Event ID 4625) or the creation of unexpected user accounts.
- **Atomic Red Team:** Use Atomic Red Team to identify gaps in monitoring and visibility, enhancing your understanding of what activities your current security setup can detect.

Outcome:

By completing this phase, you now have a simulated understanding of common attack techniques (e.g., brute force attacks) and how to set up monitoring for these events in Splunk. Using tools like Atomic Red Team provides invaluable insights into the effectiveness of your security defenses and helps improve your detection capabilities.