Security Server Provision & Setup Ubuntu Desktop 22.04

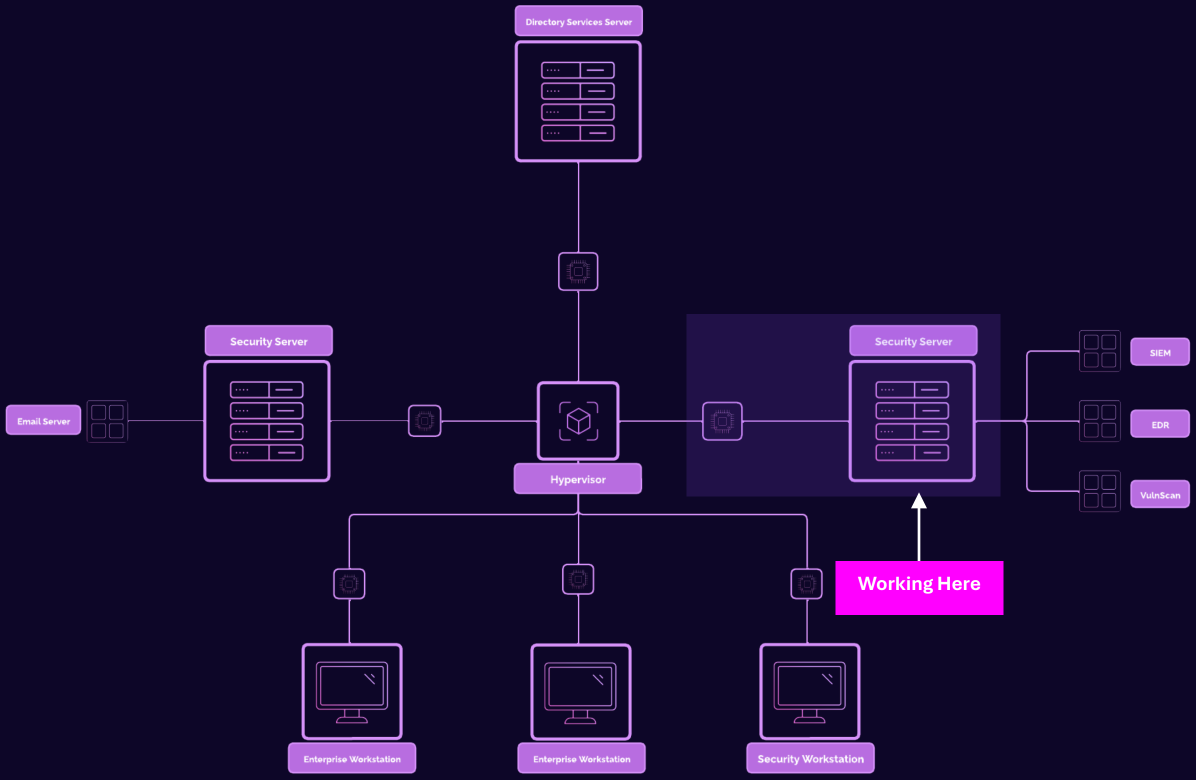
>projectsecurity_

Table of Contents

Prerequisites

1. Virtualbox installed.
2. Virtual Machine with Ubuntu 22.04 ISO has been configured and provisioned (the ISO should be attached to the new VM).
3. Windows Server 2025 with AD Directory Services (ADDS) configured.

Network Topology



Security Server Overview

A dedicated security server is critical for ensuring the performance, security, and scalability of your monitoring and analysis stack. Here’s why:

Performance Isolation Running resource-intensive tools on a dedicated server prevents performance degradation caused by competing workloads on shared resources. Each application demands significant CPU, RAM, and disk I/O to function efficiently.

Enhanced Security: Security tools process sensitive data, including logs and vulnerability scans. A dedicated server minimizes the attack surface by isolating these critical processes from unrelated systems.

Centralized Management: A dedicated server simplifies monitoring and management, providing a single point for handling logs, alerts, and vulnerability data, which improves efficiency and reduces administrative overhead.

We will be using a few closed and open-source security tools to monitor, detect, and prevent our simulated "attacks".

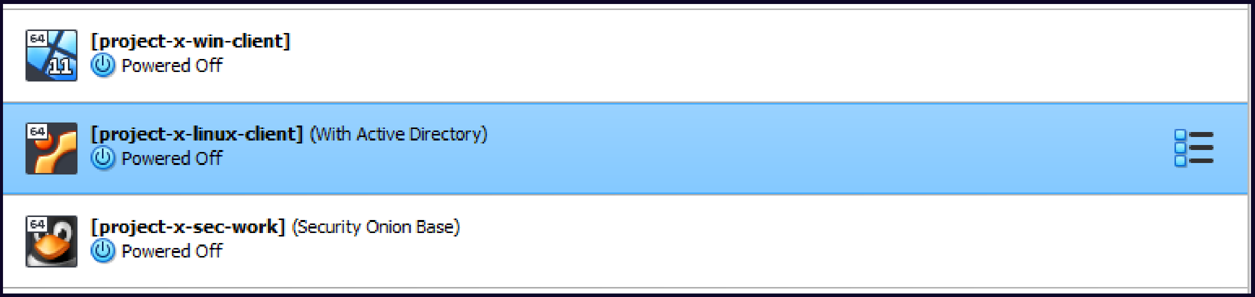
Instead of duplicating our steps, we are going to "Clone" the Ubuntu Desktop 22.04 workstation client. We will make a few configuration changes to the Security Server.

You are welcomed to repeat the steps in the Ubuntu 22.04 Desktop guide if you want extra practice with provisioning VMs.

Setup Security Server

Step 1

Navigate to the `[project-x-linux-client]` Virtual Machine. Make sure the Virtual Machine is powered off.

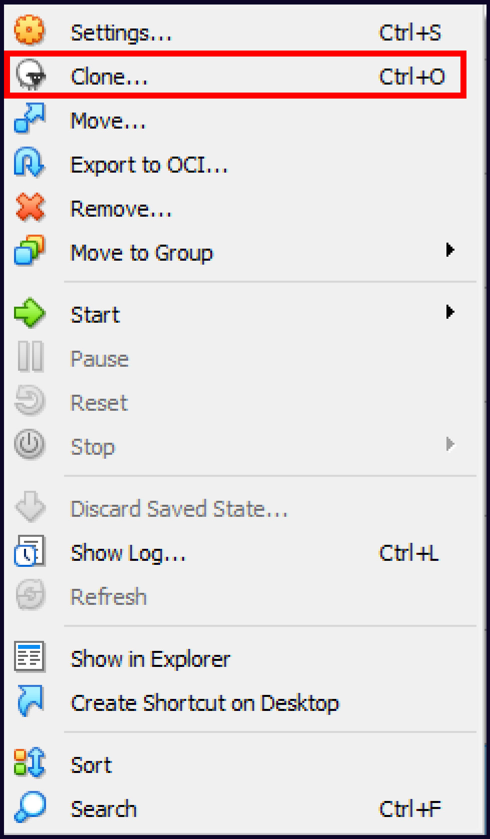


[project-x-win-client]
Powered Off

[project-x-linux-client] (With Active Directory)
Powered Off

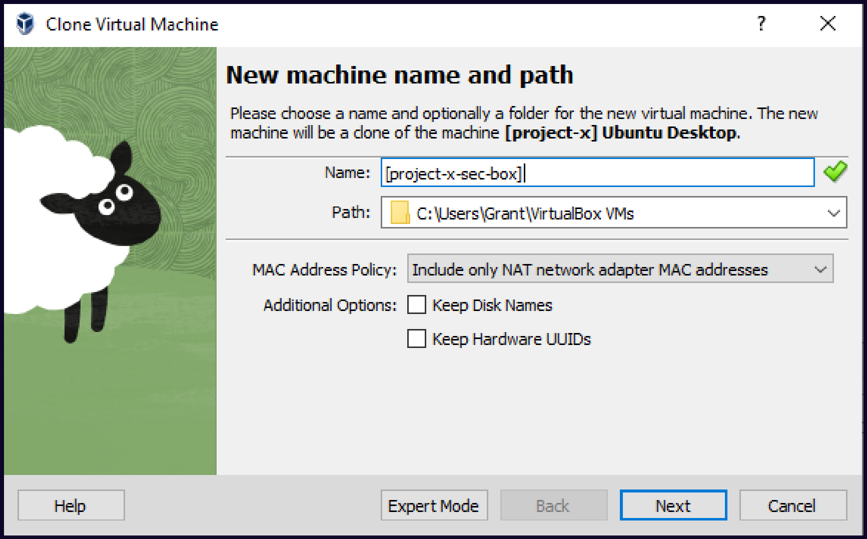
[project-x-sec-work] (Security Onion Base)
Powered Off

Right-click the Virtual Machine → Select "Clone".



Name the new machine `[project-x-sec-box]`. Select "Next".

👉 Refer to the "Project Overview" guide for more information on default hostnames.



New machine name and path

Please choose a name and optionally a folder for the new virtual machine. The new machine will be a clone of the machine **[project-x] Ubuntu Desktop**.

Name: [project-x-sec-box] ✓

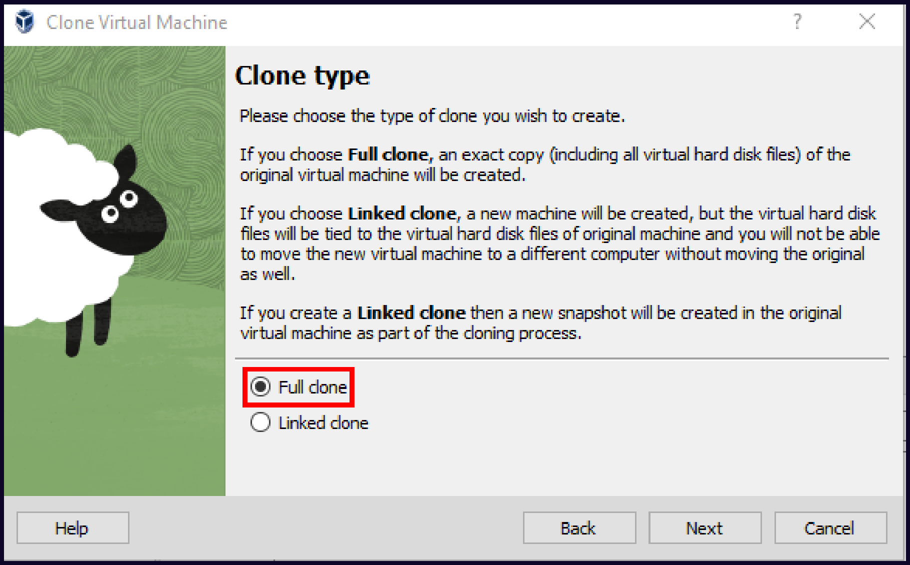
Path: C:\Users\Grant\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: □ Keep Disk Names

□ Keep Hardware UUIDs

Ensure "Full Clone" is selected.



Clone Virtual Machine

Clone type

Please choose the type of clone you wish to create.

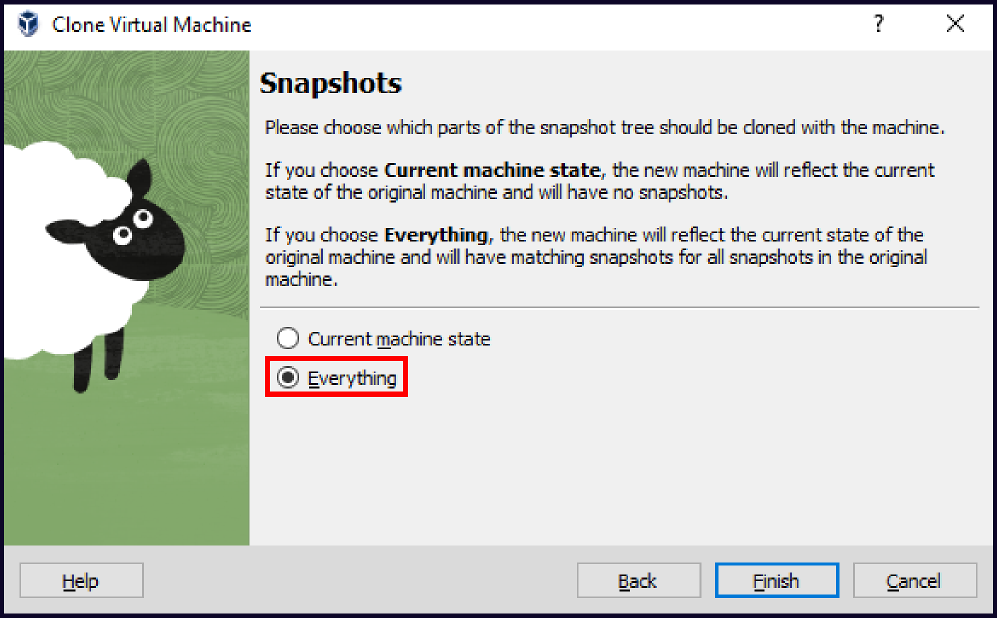
If you choose **Full clone**, an exact copy (including all virtual hard disk files) of the original virtual machine will be created.

If you choose **Linked clone**, a new machine will be created, but the virtual hard disk files will be tied to the virtual hard disk files of original machine and you will not be able to move the new virtual machine to a different computer without moving the original as well.

If you create a **Linked clone** then a new snapshot will be created in the original virtual machine as part of the cloning process.

● Full clone
○ Linked clone

Select "Everything". This will include our original snapshot, which we would like, just in case.



Clone Virtual Machine

Snapshots

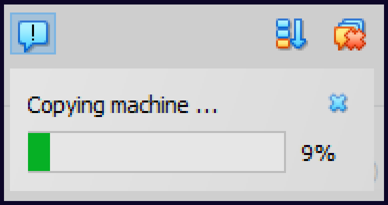
Please choose which parts of the snapshot tree should be cloned with the machine.

If you choose **Current machine state**, the new machine will reflect the current state of the original machine and will have no snapshots.

If you choose **Everything**, the new machine will reflect the current state of the original machine and will have matching snapshots for all snapshots in the original machine.

○ Current machine state
● Everything

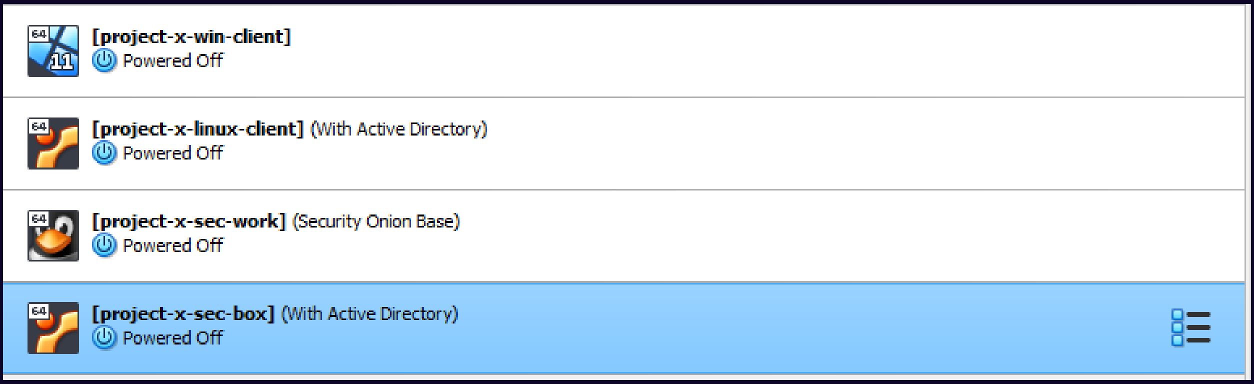
Wait until the new machine is cloned.



Copying machine ...

9%

You should now see a fully cloned Virtual Machine, titled `[project-x-sec-box]`.



[project-x-win-client]
Powered Off

[project-x-linux-client] (With Active Directory)
Powered Off

[project-x-sec-work] (Security Onion Base)
Powered Off

[project-x-sec-box] (With Active Directory)
Powered Off

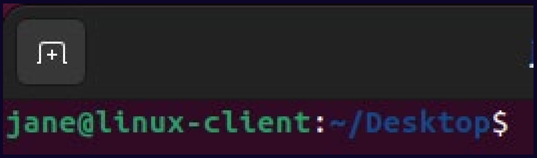
Power on the machine.

Change Hostname + Account

Let's adjust a few configuration settings to make this the Security Server.

Step 1 – Change Hostname

Right now, the hostname is `linux-client` as we have a fully cloned copy of the Ubuntu Linux 22.04 Desktop workstation.



```
jane@linux-client:~/Desktop$
```

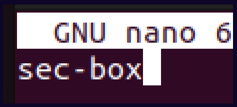
Open a new terminal.

Adjust the `/etc/hostname` configuration:

```
sudo nano /etc/hostname
```

Type in the password for `jane` (`@password123!`)

Replace `linux-client` on line 1 with `sec-box`. Save + Exit out of configuration.

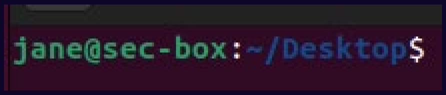


```
  GNU nano 6
sec-box
```

Reboot the machine with:

```
reboot
```

See the changes reflected when opening a new terminal.



```
jane@sec-box:~/Desktop$
```

Step 2 – Change Account

Let's provision a new account with sudo privileges.

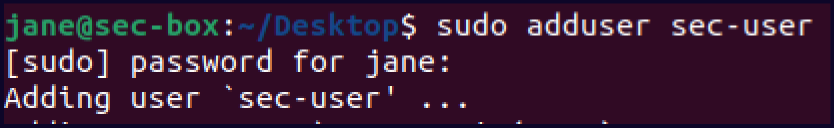
👉 Refer to the "Project Overview" guide for more default usernames and passwords.

Open a new terminal.

Type in adduser:

```
sudo adduser sec-user
```

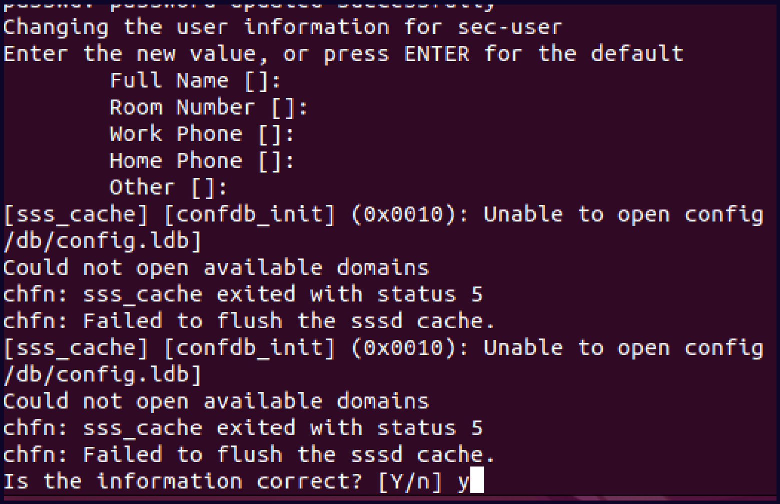
You will be prompted for jane's password, use the default password of (@password123!)



```
jane@sec-box:~/Desktop$ sudo adduser sec-user
[sudo] password for jane:
Adding user `sec-user' ...
```

Enter sec-user's password with the default

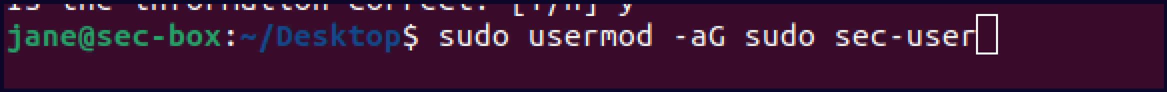
Hit "Enter" for all the user information, then y.



```
Changing the user information for sec-user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
[sss_cache] [confdb_init] (0x0010): Unable to open config
/db/config.ldb]
Could not open available domains
chfn: sss_cache exited with status 5
chfn: Failed to flush the sssd cache.
[sss_cache] [confdb_init] (0x0010): Unable to open config
/db/config.ldb]
Could not open available domains
chfn: sss_cache exited with status 5
chfn: Failed to flush the sssd cache.
Is the information correct? [Y/n] y
```

Use the following command to grant sudo privileges.

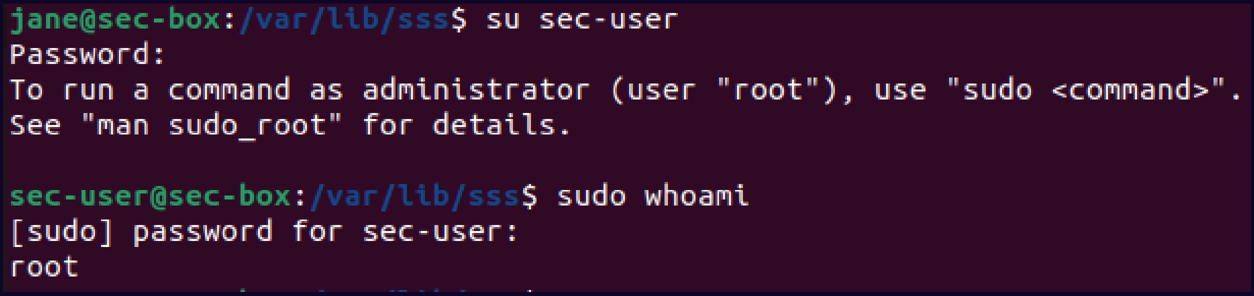
```
sudo usermod -aG sudo sec-user
```



```
jane@sec-box:~/Desktop$ sudo usermod -aG sudo sec-user
```

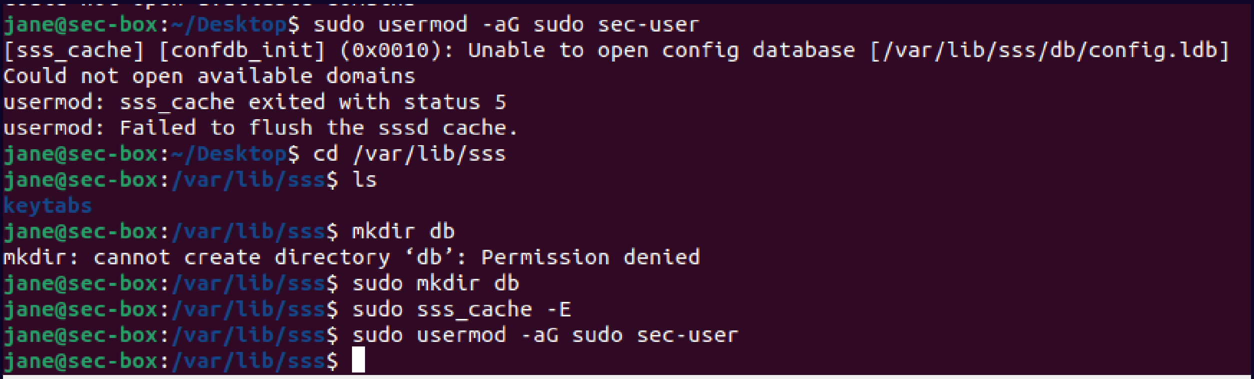
Switch to sec-user account. Issue a sudo whoami to confirm root privileges.

```
su sec-user

sudo whoami
```



```
jane@sec-box:/var/lib/sss$ su sec-user
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

sec-user@sec-box:/var/lib/sss$ sudo whoami
[sudo] password for sec-user:
root
```

💡 If you get the following error (from the previous guide), do the following.



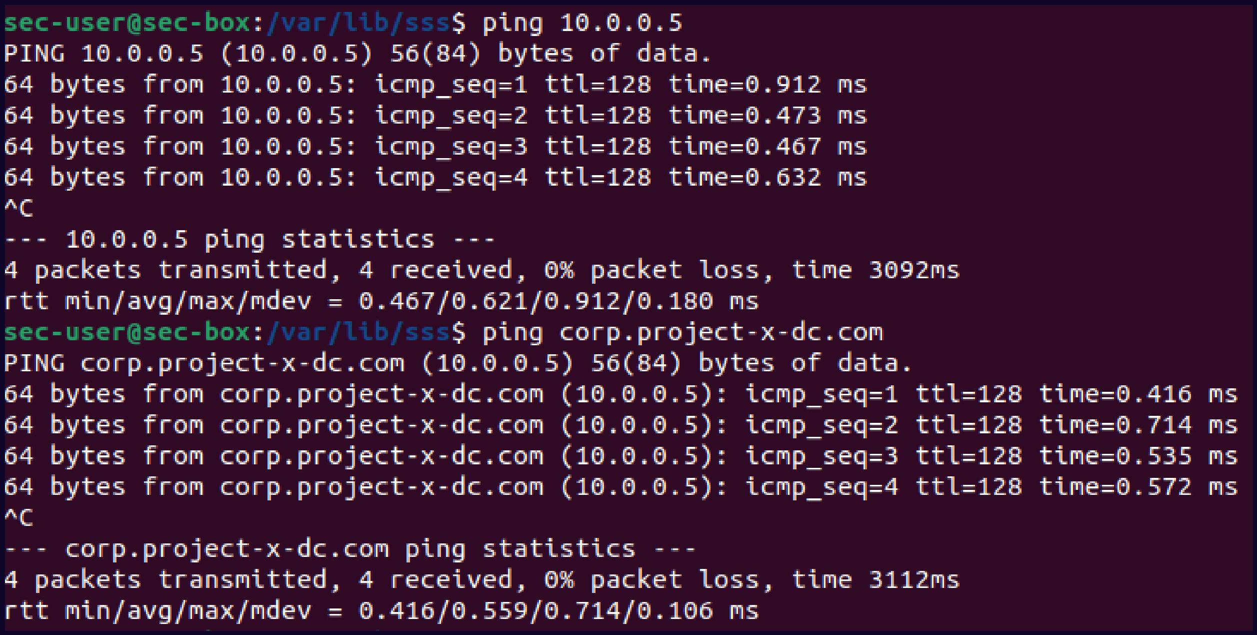
```
jane@sec-box:~/Desktop$ sudo usermod -aG sudo sec-user
[sss_cache] [confdb_init] (0x0010): Unable to open config database [/var/lib/sss/db/config.ldb]
Could not open available domains
usermod: sss_cache exited with status 5
usermod: Failed to flush the sssd cache.
jane@sec-box:~/Desktop$ cd /var/lib/sss
jane@sec-box:/var/lib/sss$ ls
keytabs
jane@sec-box:/var/lib/sss$ mkdir db
mkdir: cannot create directory ‘db’: Permission denied
jane@sec-box:/var/lib/sss$ sudo mkdir db
jane@sec-box:/var/lib/sss$ sudo sss_cache -E
jane@sec-box:/var/lib/sss$ sudo usermod -aG sudo sec-user
jane@sec-box:/var/lib/sss$ 
```

Connect to Active Directory

Based on our previous configuration steps conducted in on `[project-x-linux-client]`, we should have the necessary dependencies to automatically join the `corp.project-x-dc.com` domain.

Step 1

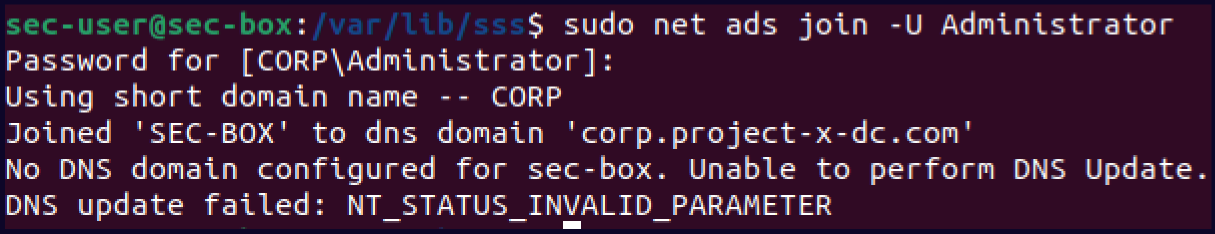
Verify you can ping 10.0.0.5 and corp.project-x-dc.com.



```
sec-user@sec-box:/var/lib/sss$ ping 10.0.0.5
PING 10.0.0.5 (10.0.0.5) 56(84) bytes of data.
64 bytes from 10.0.0.5: icmp_seq=1 ttl=128 time=0.912 ms
64 bytes from 10.0.0.5: icmp_seq=2 ttl=128 time=0.473 ms
64 bytes from 10.0.0.5: icmp_seq=3 ttl=128 time=0.467 ms
64 bytes from 10.0.0.5: icmp_seq=4 ttl=128 time=0.632 ms
^C
--- 10.0.0.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3092ms
rtt min/avg/max/mdev = 0.467/0.621/0.912/0.180 ms
sec-user@sec-box:/var/lib/sss$ ping corp.project-x-dc.com
PING corp.project-x-dc.com (10.0.0.5) 56(84) bytes of data.
64 bytes from corp.project-x-dc.com (10.0.0.5): icmp_seq=1 ttl=128 time=0.416 ms
64 bytes from corp.project-x-dc.com (10.0.0.5): icmp_seq=2 ttl=128 time=0.714 ms
64 bytes from corp.project-x-dc.com (10.0.0.5): icmp_seq=3 ttl=128 time=0.535 ms
64 bytes from corp.project-x-dc.com (10.0.0.5): icmp_seq=4 ttl=128 time=0.572 ms
^C
--- corp.project-x-dc.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3112ms
rtt min/avg/max/mdev = 0.416/0.559/0.714/0.106 ms
```

Join the domain with:

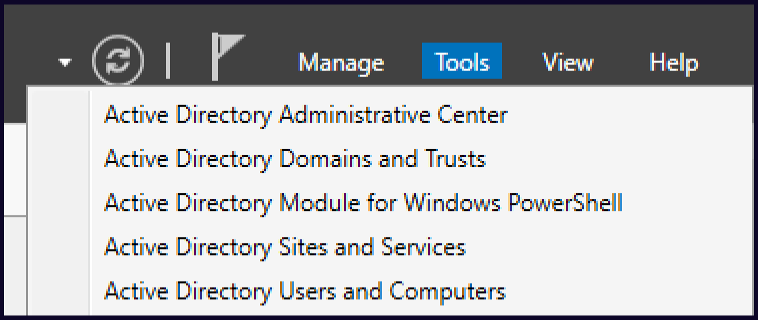
```
sudo net ads join -U Administrator
```



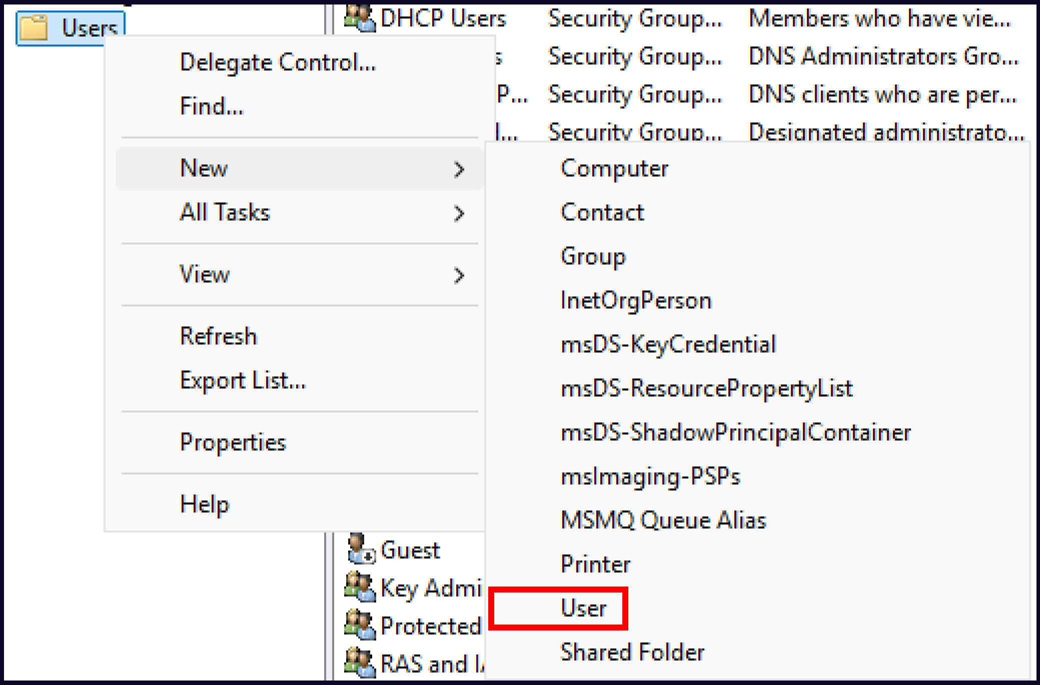
```
sec-user@sec-box:/var/lib/sss$ sudo net ads join -U Administrator
Password for [CORP\Administrator]:
Using short domain name -- CORP
Joined 'SEC-BOX' to dns domain 'corp.project-x-dc.com'
No DNS domain configured for sec-box. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
```

Let's create sec-user's AD account in our Domain Controller.

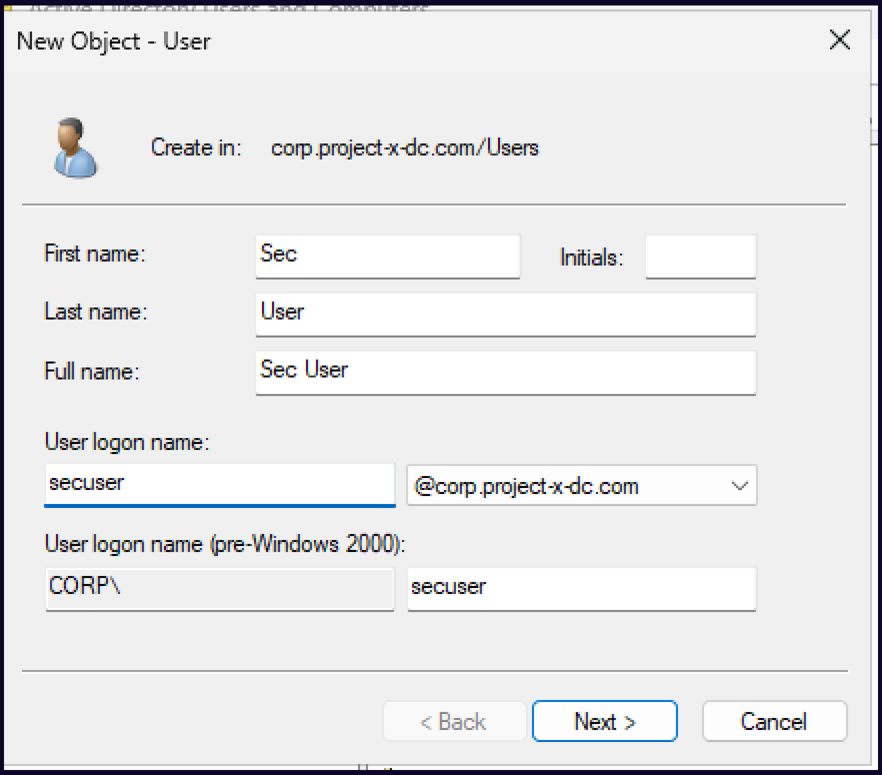
Go to Server Manager, then on the top right "Tools" → "Active Directory Users and Computers".


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers

Navigate to the "Users" folder. Right-click, then go to "New" → "User".


Users
DHCP Users Security Group... Members who have vie...
Security Group... DNS Administrators Gro...
Security Group... DNS clients who are per...
Security Group... Designated administrato...
Delegate Control...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder
Guest
Key Admi
Protected
RAS and I

Add the following information. Make sure `secuser` username is `secuser@corp.project-x-dc.com`.



New Object - User

Create in: corp.project-x-dc.com/Users

First name: Sec

Initials:

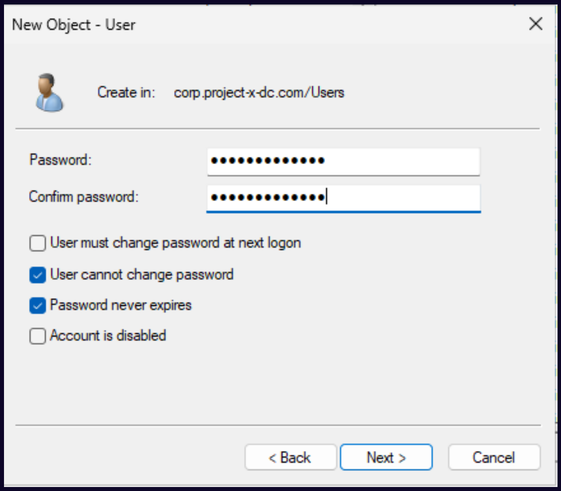
Last name: User

Full name: Sec User

User logon name: secuser @corp.project-x-dc.com

User logon name (pre-Windows 2000): CORP\ secuser

Set secuser password (`@password123!`). Refer to the Project Overview for default passwords if needed.



New Object - User

Create in: corp.project-x-dc.com/Users

Password: •••••••••••••

Confirm password: •••••••••••••

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

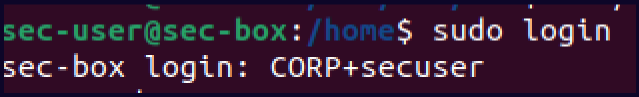
□ Account is disabled

Clear the winbind cache by restarting the service, then see the changes reflected.

```
sudo systemctl restart winbind

wbinfo -u
```

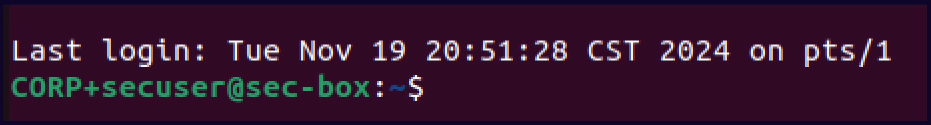
Then login with:

```
sudo login
```



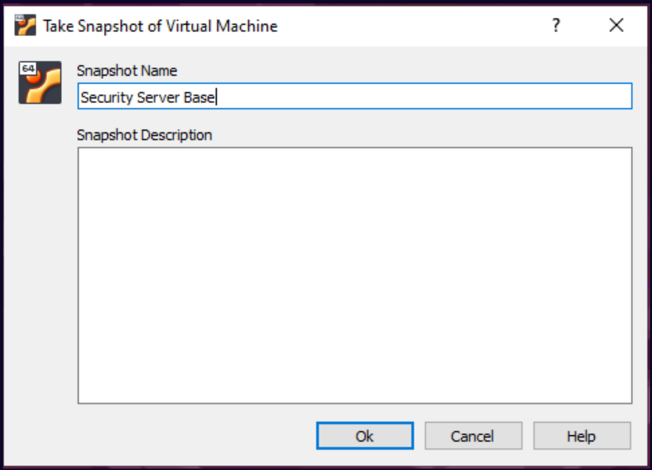
```
sec-user@sec-box:/home$ sudo login
sec-box login: CORP+secuser
```

Success!



```
Last login: Tue Nov 19 20:51:28 CST 2024 on pts/1
CORP+secuser@sec-box:~$
```

📷 Take Snapshot!



Take Snapshot of Virtual Machine

Snapshot Name: Security Server Base

Snapshot Description:

›projectsecurity_