



Provision & Setup Ubuntu Server 22.04

>pr0jectsecurity_

Table of Contents

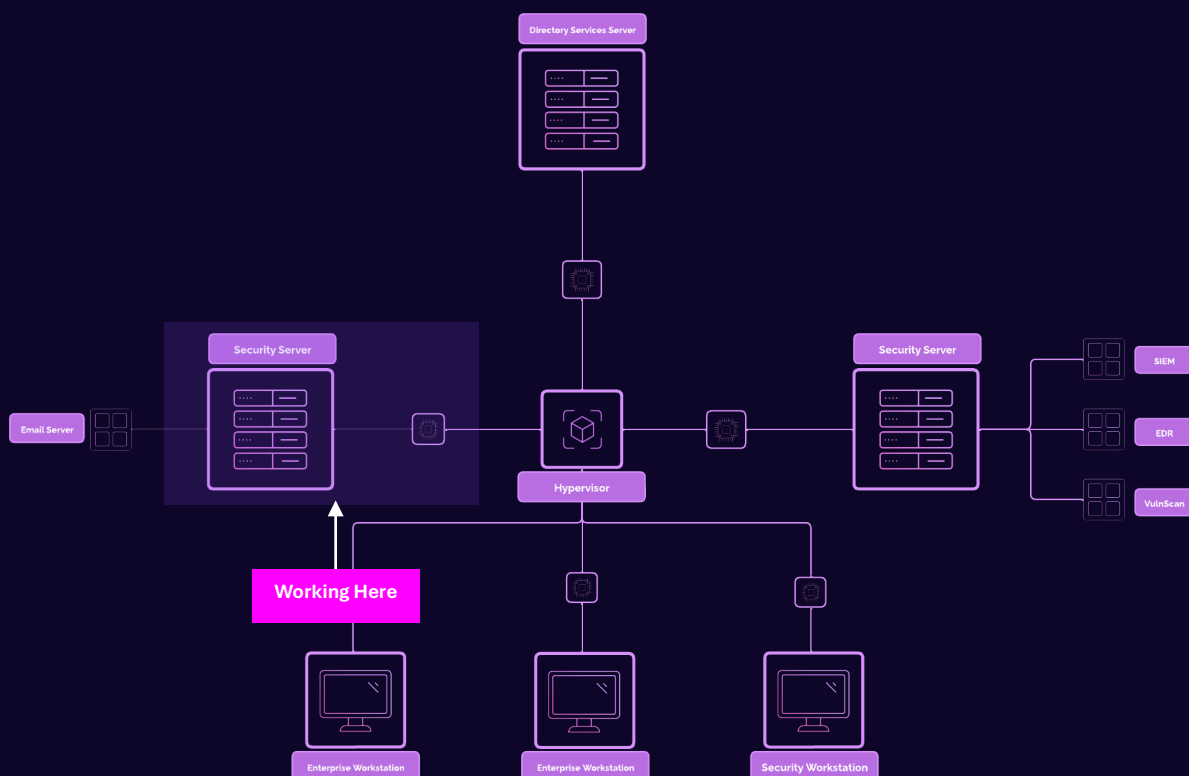
Table of Contents	2
Prerequisites	4
Network Topology	4
Email Security Server Overview	4
Overview.....	4
Security Implications	5
Setup Security Server	6
Step 1	6
Connect Ubuntu Desktop to Active Directory	17
Realmd + SSSD	18
Step 1	18
Step 2	19
Step 3	19
Step 4	20
Step 5	20
Samba Winbind	20
Step 1	20
Step 2	21
Step 3	21
Step 4	22
Step 5	22
Step 6	23
Step 7	24
Step 8	24
Step 9	24
Step 10	24

Step 11	24
Step 12	26
Step 13	26

Prerequisites

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

Network Topology



Email Security Server Overview

Overview

An **email server** is a system designed to send, receive, store, and manage email communication for users. It uses protocols such as SMTP (Simple Mail Transfer Protocol) for sending emails, and IMAP (Internet Message Access Protocol) or POP3 (Post Office Protocol) for receiving and managing email messages.

We will be configuring Postfix as a Mail Transfer Agent (MTA), which is used for sending and routing emails on Linux servers.

Email servers are much less common today than they were 20+ years ago. Running an email server requires expertise with configuring DNS records, securing against spam, developing a good reputation via IP address for email delivery, and more. With the emergence of third-party application such as Gmail, Microsoft 365, and ProtonMail (for personal use), these managed services provide scalable, secure email without having to manage the infrastructure of an email server.

Why are we configuring an email server in this project then?

It provides good insight into how email works and why it's important to secure your email gateways.

This guide will be used to set up the underlying Operating System, Ubuntu 22.04 Server LTS, and connection through Active Directory. Additional guides will be provided for configuring Postfix.

Security Implications

While running an email server like Postfix on Ubuntu Server 22.04 gives you control, it also introduces several security considerations:

Common Threats

1. **Open Relay Exploitation:** If improperly configured, your server can be used by spammers to send large volumes of email, damaging your IP reputation.
2. **Brute Force Attacks:** Attackers often attempt to compromise accounts via brute force or credential stuffing.
3. **Spam and Phishing:** Attackers may spoof your domain or use your server for phishing campaigns.
4. **Data Breaches:** Poorly secured servers can expose sensitive emails and user credentials.
5. **Malware Delivery:** Your server could inadvertently become a vehicle for spreading malware if attachments are not scanned.

Setup Security Server

Step 1

Press “Enter”.

```
GNU GRUB  version 2.06

*Try or Install Ubuntu Server
Ubuntu Server with the HWE kernel
Test memory

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 25s.
```

Select language.

```
Willkommen! Bienvenue! Welcome! Добро пожаловать! Welkom! [ Help ]

Use UP, DOWN and ENTER keys to select your language.

[ Asturianu ]
[ Bahasa Indonesia ]
[ Català ]
[ Deutsch ]
[ English ]
[ English (UK) ]
[ Español ]
[ Français ]
[ Galego ]
[ Hrvatski ]
[ Latviski ]
[ Lietuviškai ]
[ Magyar ]
[ Nederlands ]
[ Norsk bokmål ]
[ Occitan ]
[ Polski ]
[ Português ]
[ Suomi ]
[ Svenska ]
[ Čeština ]
[ Ελληνικά ]
[ Беларуская ]
[ Русский ]
[ Српски ]
[ Українська ]
```

Continue without updating.

Installer update available

[Help]

Version 24.10.1 of the installer is now available (24.08.1 is currently running).

You can read the release notes for each version at:

<https://github.com/canonical/subiquity/releases>

If you choose to update, the update will be downloaded and the installation will continue from here.

[Update to the new installer]
[Continue without updating]
[Back]

Select "Ubuntu Server".

Choose the type of installation

[Help]

Choose the base for the installation.

☒ Ubuntu Server

The default install contains a curated set of packages that provide a comfortable experience for operating your server.

☐ Ubuntu Server (minimized)

This version has been customized to have a small runtime footprint in environments where humans are not expected to log in.

Additional options

☐ Search for third-party drivers

This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers should not be installed on systems that will be used for FIPS or the real-time kernel.

[Done]

[Back]

Leave default Network configuration → Leave Proxy Page empty.

Network configuration

[Help]

Configure at least one interface this server can use to talk to other machines, and which preferably provides sufficient access for updates.

NAME	TYPE	NOTES
[enp0s3	eth	- ▶]
DHCPv4 10.0.2.15/24		
08:00:27:07:b3:69 / Intel Corporation / 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)		
[Create bond ▶]		

[Done]

[Back]

Leave “Mirror” configuration empty → “Done”

If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address: `http://us.archive.ubuntu.com/ubuntu/`

You may provide an archive mirror to be used instead of the default.

This mirror location passed tests.

```
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Fetched 255 kB in 1s (327 kB/s)
Reading package lists...
```

[Done]
[Back]

Select “Use an entire disk”. Press the “Tab” key until selecting “Done.”

Guided storage configuration

[Help]

Configure a guided storage layout, or create a custom one:

☒ Use an entire disk

[VBOX_HARDDISK_VB170497d3-63d1286b local disk 25.000G ▼]

☒ Set up this disk as an LVM group

☐ Encrypt the LVM group with LUKS

Passphrase:

Confirm passphrase:

☐ Also create a recovery key

The key will be stored as
~/recovery-key.txt in the live system and
will be copied to /var/log/installer/ in
the target system.

☐ Custom storage layout

[Done]

[Back]

Leave Storage Configuration as default.

Storage configuration

[Help]

FILE SYSTEM SUMMARY

MOUNT POINT	SIZE	TYPE	DEVICE TYPE
[/	11.496G	new ext4	new LVM logical volume ▶]
[/boot	2.000G	new ext4	new partition of local disk ▶]

AVAILABLE DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	22.996G ▶]
free space		11.500G ▶

[Create software RAID (md) ▶]

[Create volume group (LVM) ▶]

USED DEVICES

DEVICE	TYPE	SIZE
[ubuntu-vg (new)	LVM volume group	22.996G ▶]
ubuntu-lv new, to be formatted as ext4, mounted at /		11.496G ▶

[VBOX_HARDDISK_VB170497d3-63d1286b local disk 25.000G ▶]

partition 1 new, BIOS grub spacer 1.000M ▶

partition 2 new, to be formatted as ext4, mounted at /boot 2.000G ▶

partition 3 new, PV of LVM volume group ubuntu-vg 22.997G ▶

[Done]

[Reset]

[Back]

Arrow to “Continue”.

```
Storage configuration [ Help ]

FILE SYSTEM SUMMARY

MOUNT POINT      SIZE      TYPE      DEVICE TYPE
[ /               11.496G   new ext4  new LVM logical volume ► ]
[ /boot           2.000G   new ext4  new partition of local disk ► ]

AVAILABLE DEVICES

Confirm destructive action

Selecting Continue below will begin the installation process and
result in the loss of data on the disks selected to be formatted.

You will not be able to return to this or a previous screen once the
installation has started.

Are you sure you want to continue?

[ No ]
[ Continue ]

partition 2  new, to be formatted as ext4, mounted at /boot      2.000G ►
partition 3  new, PV of LVM volume group ubuntu-vg              22.997G ►

[ Done ]
[ Reset ]
[ Back ]
```

Enter in the server's hostname, username, and password.

👉 Refer to the “**Project Overview**” guide for more information on default usernames and passwords.

Profile configuration [Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on a later screen, but a password is still needed for sudo.

Your name:

Your servers name: The name it uses when it talks to other computers.

Pick a username:

Choose a password:

Confirm your password:

[Done]

Select “Skip for now” for the Ubuntu Pro → Select “Install OpenSSH server”. Use the Tab key until selecting “Done”.

SSH configuration

[Help]

You can choose to install the OpenSSH server package to enable secure remote access to your server.

☒ Install OpenSSH server

☐ Allow password authentication over SSH

[Import SSH key ►]

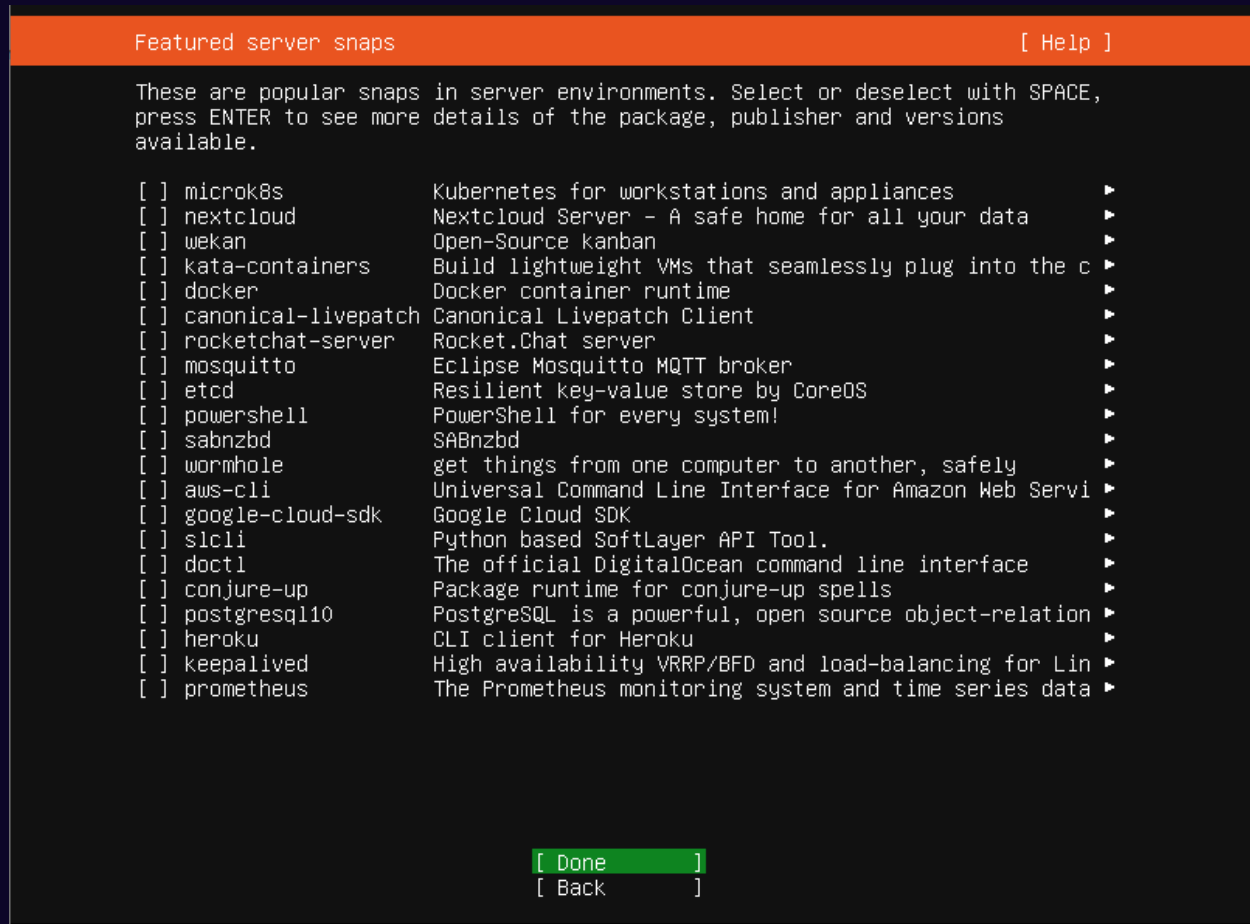
AUTHORIZED KEYS

No authorized key

[Done]

[Back]

Use the Tab key until selecting “Done”.



Wait for the OS to install, press “enter for a reboot”.


```
Installing system [ Help ]

executing curtin install curthooks step
curtin command install
configuring installed system
  running 'curtin curthooks'
  curtin command curthooks
    configuring apt configuring apt
    installing missing packages
    Installing packages on target system: ['grub-pc']
    configuring iscsi service
    configuring raid (mdadm) service
    configuring NVMe over TCP
    installing kernel
    setting up swap
    apply networking config
    writing etc/fstab
    configuring multipath
    updating packages on target system
    configuring pollinate user-agent on target
    updating initramfs configuration
    configuring target system bootloader
    installing grub to target devices
    copying metadata from /cdrom
final system configuration
calculating extra packages to install
installing openssh-server
retrieving openssh-server
curtin command system-install
unpacking openssh-server -
curtin command system-install /

[ View full log ]
```

Success!

```
Ubuntu 22.04.5 LTS project-x-email-svr tty1
project-x-email-svr login: _
```

Connect Ubuntu Desktop to Active Directory

👉 Switch the Network from “NAT Network” → Bridged.

👉 Refer to [this](#) guide if you would like to insert VirtualBox Guest Additions (for copy/paste controls).

Connecting Ubuntu (and Debian-based systems) to Active Directory can be accomplished in a couple ways. The easiest way is to connect Ubuntu to Active Directory with **realmd** and

SSSD (System Security Services Daemon). **Samba Winbind** can also be used to join Linux systems if **realmd** / **SSSD** is not working.

! Currently **realmd** and **SSSD** integration do not work for Windows Server 2025 and Debian/Ubuntu-based systems.

About SSSD / Realmd

- **System Security Services Daemon (SSSD):** A service on Linux systems that provides a central access point for identity management and authentication. When connecting a Linux system to Active Directory (AD), SSSD allows for the integration by acting as an intermediary between the Linux system and AD needing to know what files should be edited.
- **realmd:** A tool that simplifies the process of joining Linux machines to AD domains. It automates the discovery, configuration, and enrollment of Linux systems in Active Directory, making it easier to integrate Linux systems into existing AD environments. **Realmd** is especially useful for administrators because it manages the complexities of setting up Kerberos, configuring LDAP settings, and ensuring proper authentication protocols.
- **realmd** is a tool that automates domain joining and manages configurations for **sssd**, which provides caching, more flexible configuration options, and better performance.

About Samba Winbind

- **Samba Winbind:** A component of the Samba suite that allows Linux systems to authenticate users against Windows Active Directory (AD) and integrate with Windows network environments. Is a more direct integration, especially useful for legacy systems and environments where tight compatibility with Windows protocols is necessary. It's often preferred when working in older Windows Server environments or where native Samba compatibility is crucial.

Realmd + SSSD

Step 1

Open a new terminal session.

Update the system with:

```
sudo apt update
```

Step 2

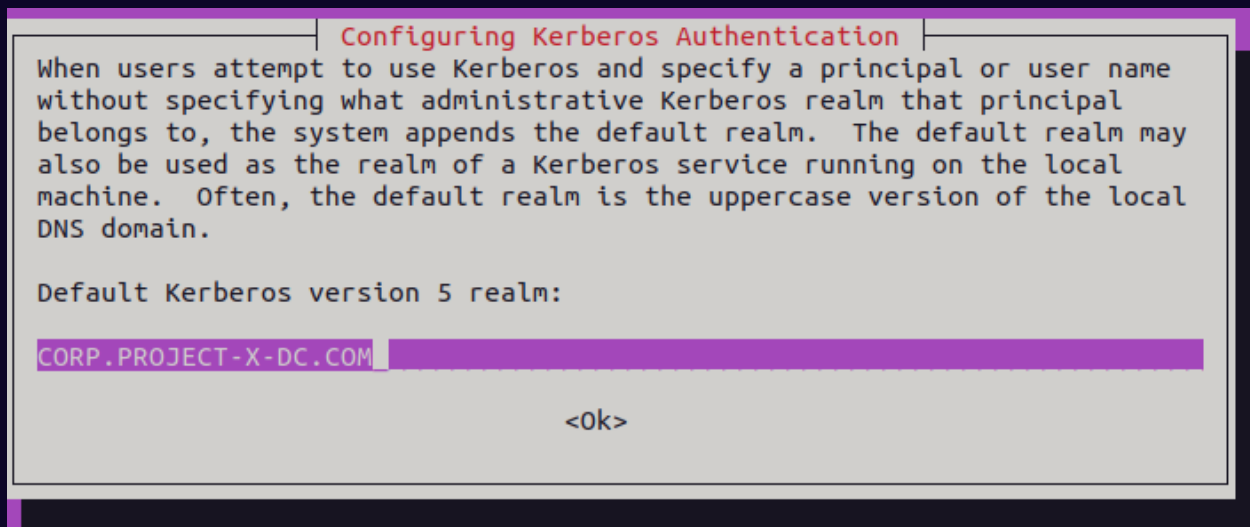
Adding the following under the [Time] block.

```
sudo nano /etc/systemd/timesyncd.conf
```

```
[Time]
NTP=corp.project-x-dc.com
#FallbackNTP=ntp.ubuntu.com
RootDistanceMaxSec=30
```

Install the necessary packages:

```
sudo apt install realmd sssd sssd-tools samba-common krb5-user
packagekit libnss-sss libpam-sss adcli samba-common-bin
```



Step 3

Use the realm command to discover the domain.

```
jane@linux-client:~$ sudo realm discover corp.project-x-dc.com
corp.project-x-dc.com
type: kerberos
realm-name: CORP.PROJECT-X-DC.COM
domain-name: corp.project-x-dc.com
configured: no
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: libnss-sss
required-package: libpam-sss
required-package: adcli
required-package: samba-common-bin
```

Step 4

Enter the following command, enter the Administrator password:

```
sudo realm join --verbose --user=Administrator corp.project-x-
dc.com
```

Step 5

If no output is shown in the console, then the VM has been connected.

Enter the following command to confirm:

```
realm list
```

Samba Winbind

Step 1

Open a new terminal session.

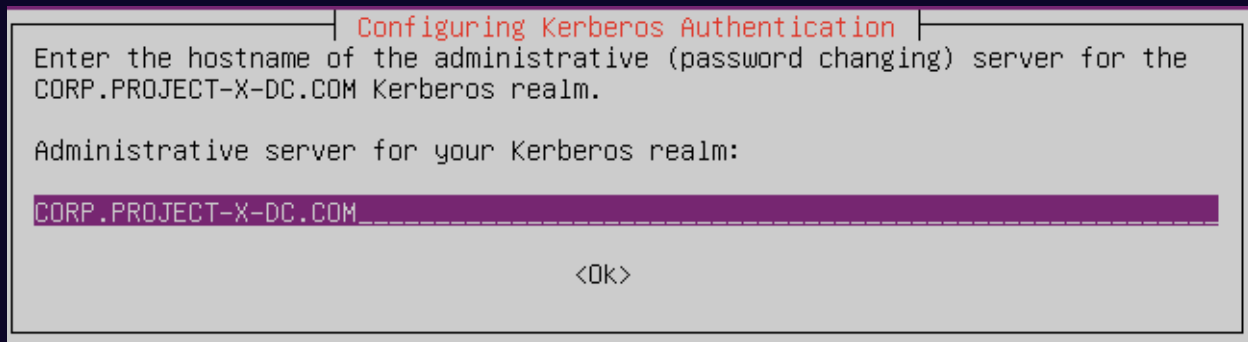
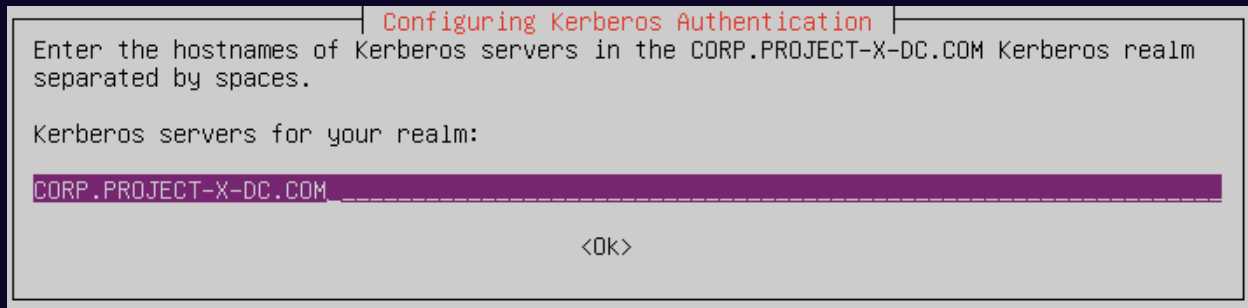
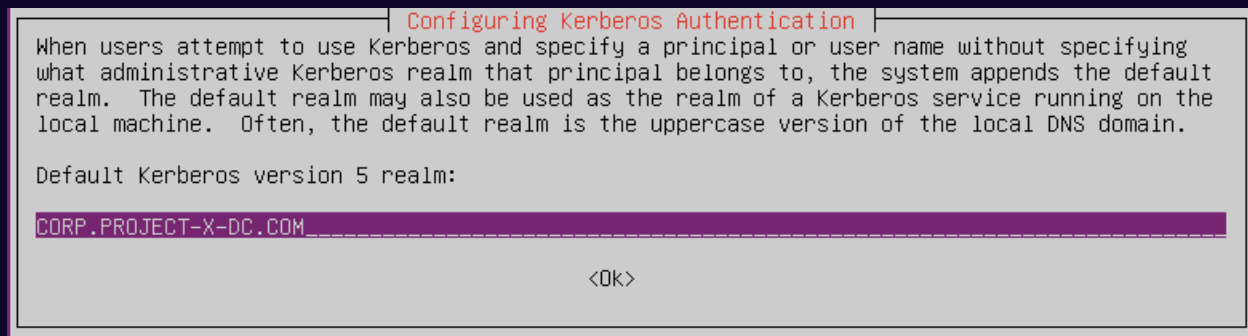
Update the system with:

```
sudo apt update
```

Install the necessary packages (note that **krb5-user** is installed this time):

```
sudo apt -y install winbind libpam-winbind libnss-winbind krb5-
config krb5-user samba-dsdb-modules samba-vfs-modules
```

Add CORP.PROJECT-X-DC.COM for the two Kerberos Authentication pages.



Step 2

Move the smb.conf.org file:

```
mv /etc/samba/smb.conf /etc/samba/smb.conf.org
```

Step 3

```
sudo nano /etc/samba/smb.conf
```

Replace realm and workgroup with the following:

```
[global]

kerberos method = secrets and keytab

realm = CORP.PROJECT-X-DC.COM

workgroup = CORP
```

```
security = ads
template shell = /bin/bash
winbind enum groups = Yes
winbind enum users = Yes
winbind separator = +
idmap config * : rangesize = 1000000
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
```

Step 4

Confirm passwd and group have winbind set as a value.

```
sudo nano /etc/nsswitch.conf
```

Add if needed.

```
passwd:      files systemd winbind
group:       files systemd winbind
shadow:      files
gshadow:     files
```

Step 5

On Ubuntu, every user that has an interactive logon to the system needs a home directory. For domain users, we need to set this before a user is able to successfully logon and start working.

Issue the following command

```
sudo pam-auth-update
```

Scroll down up to the point where it states:” Create *home directory on login*“. Use the space bar to select, tab to “OK” and hit enter.

Package configuration

PAM configuration

Pluggable Authentication Modules (PAM) determine how authentication, authorization, and password changing are handled on the system, as well as allowing configuration of additional actions to take when starting user sessions.

Some PAM module packages provide profiles that can be used to automatically adjust the behavior of all PAM-using applications on the system. Please indicate which of these behaviors you wish to enable.

PAM profiles to enable:

☐ [*] SSS authentication

☐ [*] Register user sessions in the systemd control group ...

☒ [*] Create home directory on login

<Ok>

<Cancel>

Kudos to [Michael Waterman](#) for the screenshot!

Step 6

Change DNS settings to refer to AD.

```
sudo nano /etc/resolv.conf
```

```
nameserver 10.0.0.5
nameserver 127.0.0.53
options edns0 trust-ad
search localdomain
```

Add corp.project-x-dc.com to /etc/hosts:

```
sudo nano /etc/hosts
```

```
GNU nano 6.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 email-svr
10.0.0.5 corp.project-x-dc.com
# the following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

👉 Change Network settings from Bridged → NAT Network (project-x-network).

Step 7

Join the domain with Administrator:

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

Step 8

Restart winbind:

```
systemctl restart winbind
```

Step 9

Get Active Directory services information listing.

```
net ads info
```

Step 10

List all available users.

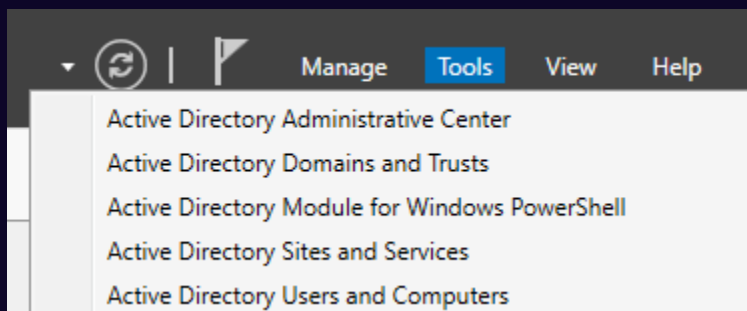
```
wbinfo -u
```

```
email-svr@email-svr:~$ wbinfo -u
CORP+administrator
CORP+guest
CORP+krbtgt
CORP+johnd
CORP+janed
CORP+secuser
```

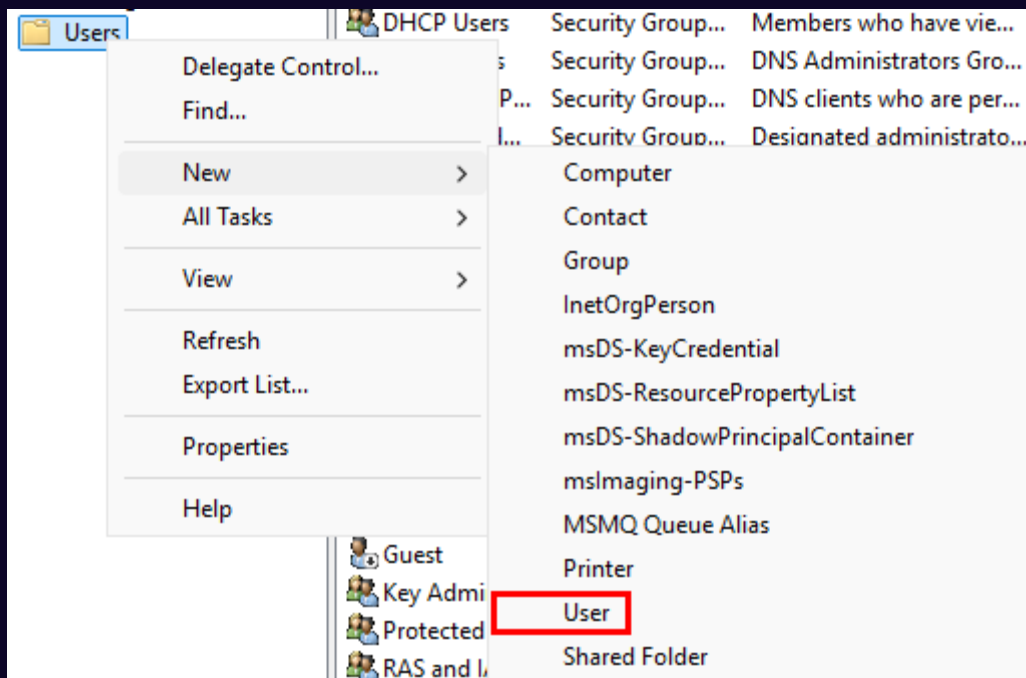
Step 11

Let's create email-svr's AD account in our Domain Controller.

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



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



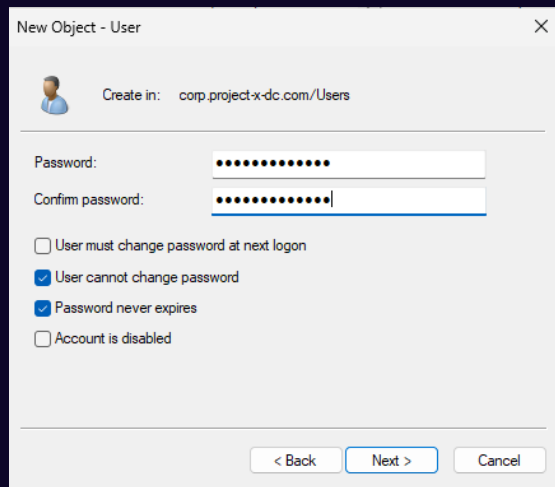
Add the following information.

emailsvr@corp.project-x-dc.com

The 'New Object - User' dialog box is shown. The 'Create in' field is set to 'corp.project-x-dc.com/Users'. The 'First name' field contains 'Email', and the 'Full name' field also contains 'Email'. The 'User logon name' field is filled with 'email-svr' and the domain dropdown is set to '@corp.project-x-dc.com'. The 'User logon name (pre-Windows 2000)' field is filled with 'CORP\email-svr'. The 'Next >' button is highlighted.

Set email-svr's password (@password123!).

👉 Refer to the “Project Overview” guide for more information on default usernames and passwords.



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

```
sudo systemctl restart winbind
```

```
wbinfo -u
```

```
email-svr@email-svr:~$ wbinfo -u
CORP+administrator
CORP+guest
CORP+krbtgt
CORP+johnd
CORP+janed
CORP+secuser
CORP+email-svr
```

Step 12

Login as email-svr (CORP+email-svr):

```
sudo login
```

```
email-svr@email-svr:~$ sudo login
email-svr login: CORP+email-svr
```

Step 13

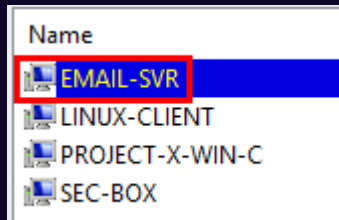
Issue an `id` command to view status:

```
id
```

Success!

```
Creating directory '/home/CORP/email-svr'.
CORP+email-svr@email-svr:~$ id
uid=2001120(CORP+email-svr) gid=2000513(CORP+domain users) groups=2000513(CORP+domain users),2001120
(CORP+email-svr)
CORP+email-svr@email-svr:~$ _
```

Going back to the Server Manager, we should see “LINUX-CLIENT” under the “Computers” folder.



 **Take Snapshot!**

