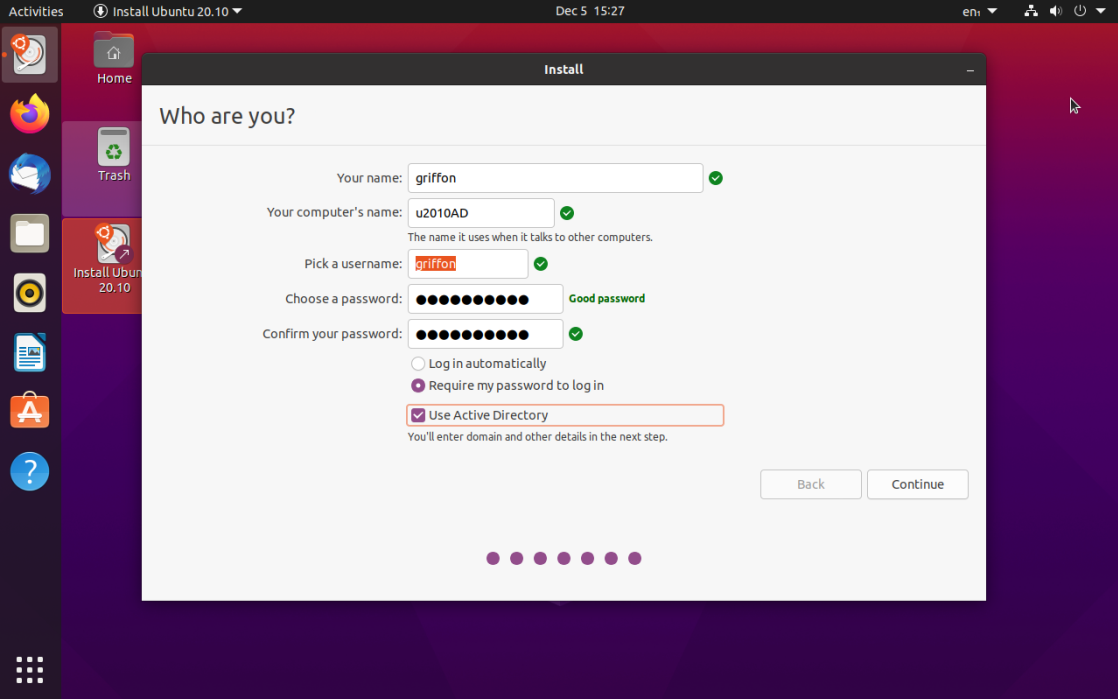
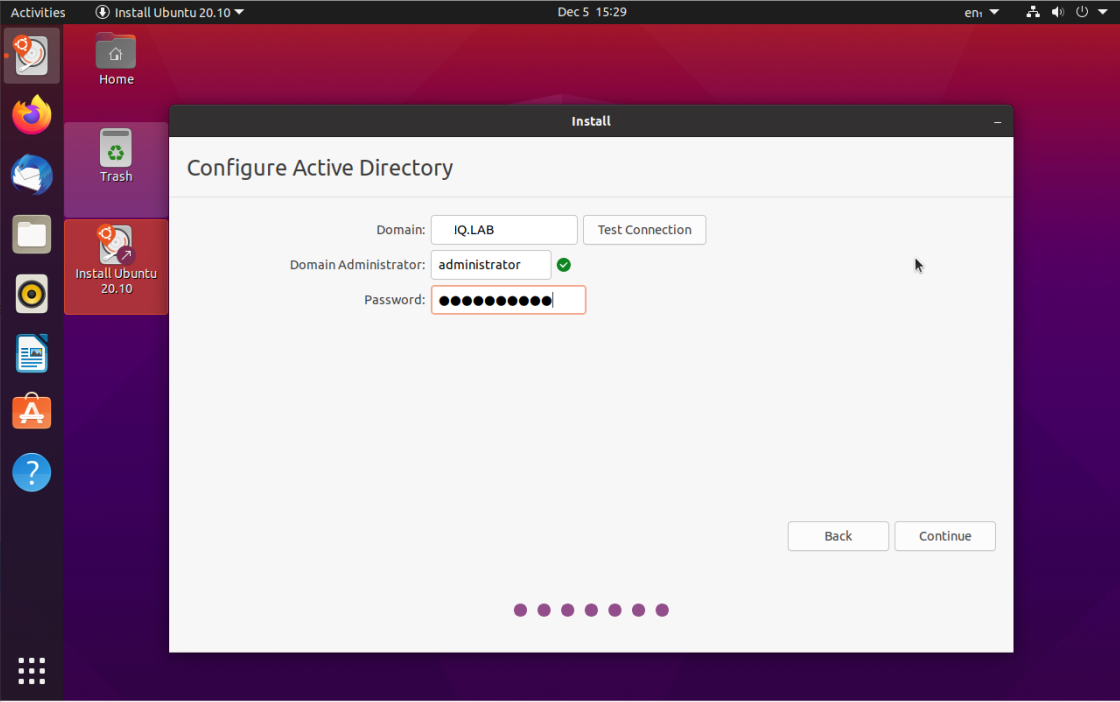
lDetail the joining of AD by ubuntu machines. Starts with latest ubuntu (21.10)

During install, make sure to click the box “Use Active Directory”.



On the next screen, input “UCDENVER.PVT” as the domain. The domain administrator & pass are your own university account with the privilege of adding computers to domains.

sey

Then reboot

IF you don’t do the above, you can do it thru terminal with the following command:

**Realm -vvv join -U YourUsername UCDENVER.PVT**

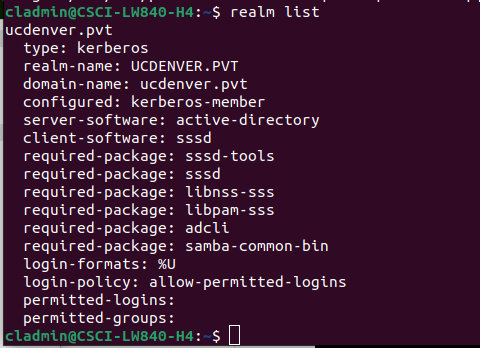
(If the above command gives any error and doesn’t work, the problem is either the hostname of the computer does not exist as an object in AD, or that you need to add permissions to the object for your username. You can right-click properties, go to “Managed By” tab and add your username, and/or go to security tab and add yourself with full control.)

On the above comment, do not put the domain on your username (eg [YourUsername@UCDENVER.PVT](mailto:YourUsername@UCDENVER.PVT))

Next, open terminal & check if you are joined to the domain (called realms in Ubuntu):

**Realm list**

This will list the realm you are part of. You should see this:



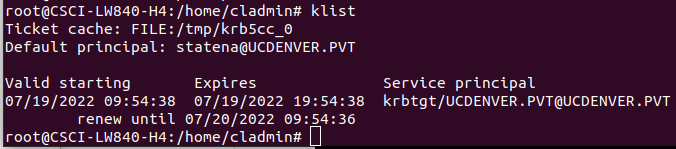
You can further test domain connectivity by getting a Kerberos ticket:

**Sudo apt install krb5-user** (to install the tools)

**kinit** [**YourUsername**](mailto:YourUsername@UCDENVER.PVT) (you will be prompted to enter your password. Should not need @UCDENVER.PVT at the end of your username)

then run:

**klist**



Run script (and buttons to press) using sudo ./ADconnection.sh

(make sure perl is installed)

chmod +x ADConnection.sh

./ADConnection etc)

Afterwards, install the rest:

**sudo snap install office365webdesktop –beta**

**apt-get install openssh-server**

Using /var/log/auth.log | tail grep (or just down arrow) to see tail end of file when having issues

**How to get AD to work with Ubuntu 21.10**

Use linux active directory script. Or possibly just setup domain join at installation, above files, and ssh

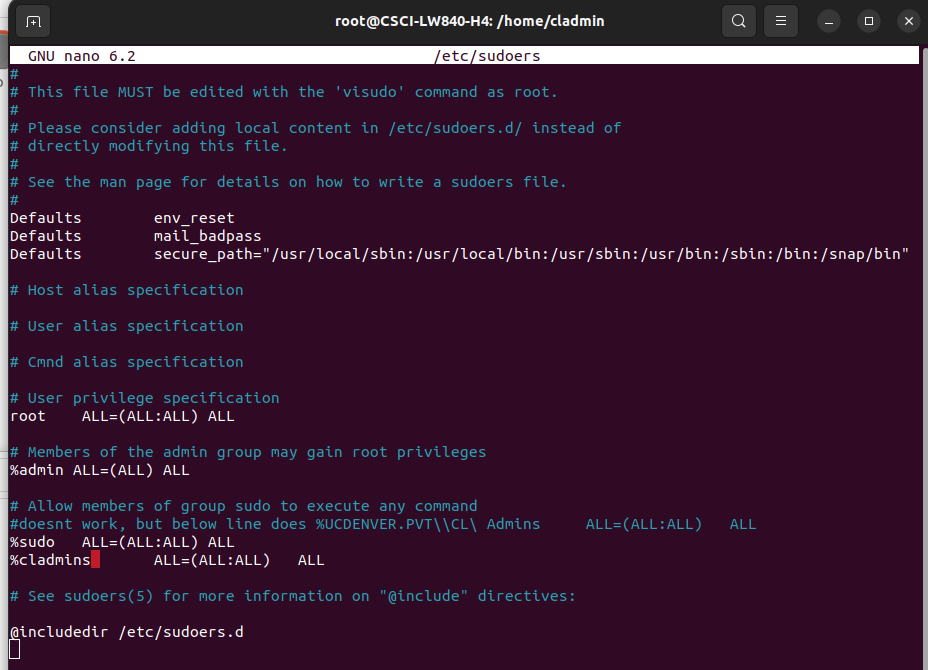
Login local and remote works.

6-29-2022

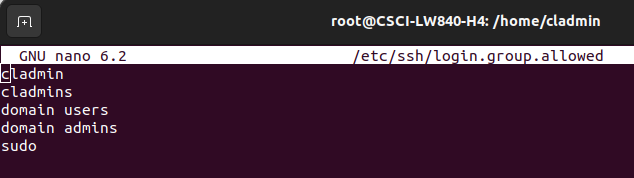
DO NOT USE AllowGroups in sshd\_config, just use PAM

Make sure /etc/pam.d/common-auth has the below line:

auth required pam\_listfile.so onerr=fail item=group sense=allow file=/etc/ssh/login.group.allowed



and login.group.allowed should mirror this:



cladmin (for actual local cladmin account)

cladmins (for all networked cl admin accounts /techs)

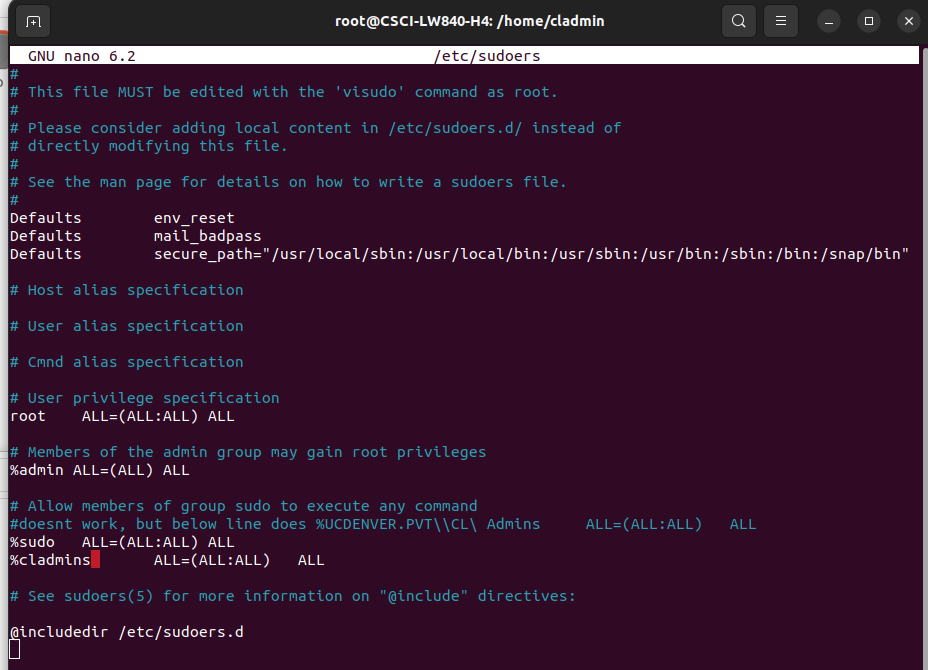
domain users (for all students )

domain admins (never know)

sudo (all those in sudo group can login)

and for sudo only cladmins in /etc/sudoers

%cladmins ALL=(ALL:ALL) ALL



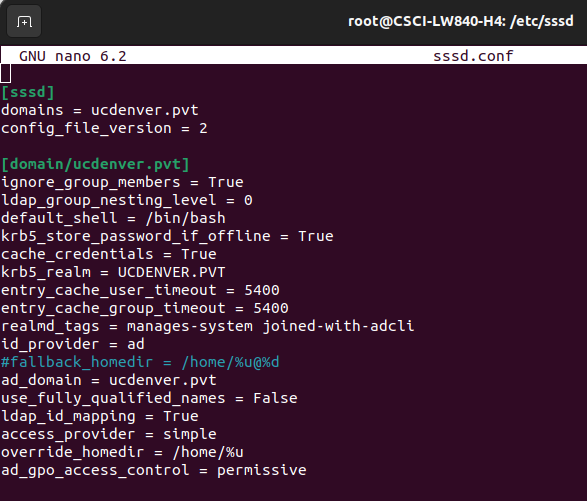
Next update to latest Ubuntu as well as upgrade all software..

And try with latest ubuntu: works with latest 22.04 LTS

Important to add the below 2 lines to sssd.conf to hasten ssh logins:

ignore\_group\_members = True

ldap\_group\_nesting\_level = 0



both disable looking up nested groups (groups within groups for permissions)

and to restart ssd properly: systemctl daemon-reload;systemctl restart sssd

to remove the users from showing (in this case cladmin, staten, and anyone else who will login in the future) and make them type it manually like our windows pcs, do the below:

Then run the commands below:

sudo nano /etc/gdm3/greeter.dconf-defaults

When the file opens, un-comment (**#**) the highlighted line in the file as shown below and save.

# Login manager options

# =====================

[org/gnome/login-screen]

#logo='/usr/share/images/vendor-logos/logo-text-version-128.png'

# - Disable user list

disable-user-list=true

# - Disable restart buttons

# disable-restart-buttons=true

# - Show a login welcome message

sssd.conf

[sssd]

domains = ucdenver.pvt

config\_file\_version = 2

[domain/ucdenver.pvt]

ignore\_group\_members = True

ldap\_group\_nesting\_level = 0

default\_shell = /bin/bash

krb5\_store\_password\_if\_offline = True

cache\_credentials = True

krb5\_realm = UCDENVER.PVT

entry\_cache\_user\_timeout = 5400

entry\_cache\_group\_timeout = 5400

realmd\_tags = manages-system joined-with-adcli

id\_provider = ad

#fallback\_homedir = /home/%u@%d

ad\_domain = ucdenver.pvt

use\_fully\_qualified\_names = False

ldap\_id\_mapping = True

access\_provider = simple

override\_homedir = /home/%u

ad\_gpo\_access\_control = permissive

/etc/ssh/ssh\_config:

# This is the ssh client system-wide configuration file. See

# ssh\_config(5) for more information. This file provides defaults for

# users, and the values can be changed in per-user configuration files

# or on the command line.

# Configuration data is parsed as follows:

# 1. command line options

# 2. user-specific file

# 3. system-wide file

# Any configuration value is only changed the first time it is set.

# Thus, host-specific definitions should be at the beginning of the

# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options. For a comprehensive

# list of available options, their meanings and defaults, please see the

# ssh\_config(5) man page.

Include /etc/ssh/ssh\_config.d/\*.conf

Host \*

# ForwardAgent no

# ForwardX11 no

# ForwardX11Trusted yes

# PasswordAuthentication yes

# HostbasedAuthentication no

# GSSAPIAuthentication no

# GSSAPIDelegateCredentials no

# GSSAPIKeyExchange no

# GSSAPITrustDNS no

# BatchMode no

# CheckHostIP yes

# AddressFamily any

# ConnectTimeout 0

# StrictHostKeyChecking ask

# IdentityFile ~/.ssh/id\_rsa

# IdentityFile ~/.ssh/id\_dsa

# IdentityFile ~/.ssh/id\_ecdsa

# IdentityFile ~/.ssh/id\_ed25519

# Port 22

# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc

# MACs hmac-md5,hmac-sha1,umac-64@openssh.com

# EscapeChar ~

# Tunnel no

# TunnelDevice any:any

# PermitLocalCommand no

# VisualHostKey no

# ProxyCommand ssh -q -W %h:%p gateway.example.com

# RekeyLimit 1G 1h

# UserKnownHostsFile ~/.ssh/known\_hosts.d/%k

SendEnv LANG LC\_\*

HashKnownHosts yes

GSSAPIAuthentication yes