Linux Authentication to UTEP Domain Running RHEL/COS 7.X

NOTE:

Make sure you have the Admin tools install on your Windows Desktop in order to manage your OU. For Windows 10 click here.

Before you join a Linux Server to the UTEP domain, make sure that the Linux OU exists already in RADC OU or your corresponding OU. All physical or virtual servers managed in the RADC must be under the this OU, see figure below.

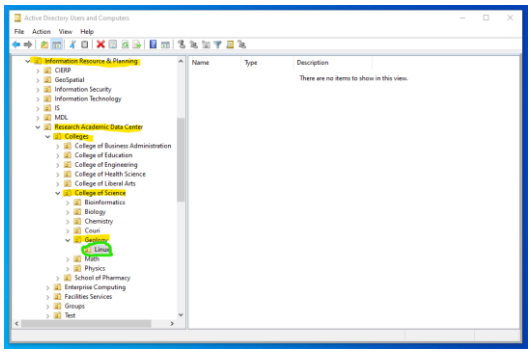

Figure 1 Existence of Linux OU on Department

1) SSH with an account that has access to login to the Linux machine. You must have sudo access or have the root password to complete the setup.

2) If the machine was not pre-configured by RADC staff you must install the packages and meet some requirements first.

   a. Install packages to bind to UTEP.EDU, use *sudo* or *su* – to install.
      i. # yum install realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-common-tools ntpdate ntpd
   b. In order for realm to work properly you must sync the clock to UTEP.EDU. Backup your /etc/ntp.conf
      i. # cp /etc/ntp.conf /etc/ntp.conf_*YYYYMMDD*
      ii. # mount lus:/lus/repos /mnt
      iii. # cp /mnt/ntp7.conf /etc/ntp.conf
      iv. # systemctl enable ntpd
      v. # systemctl restart ntpd
      vi. # ntpq –p

```
[root@[redacted]sssd]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*[redacted].utep 198.50.238.156   3 u  385  512  377    0.266  -10.533   0.746
+[redacted].utep 69.89.207.199    3 u  307  512  377    0.256   -9.616   1.103
+[redacted].utep 108.61.73.244    3 u  368  512  377    0.284   -9.083   0.900
-[redacted].utep 108.61.73.244    3 u  293  512  377    0.287   -6.937   5.532
```

Figure 2 Connection to UTEP time server.

3) If the Linux machine was configured by RADC staff all the packages are pre-install and pre-configured.

   a. Join to the UTEP domain (automatic process – script based):
      i. If running CentOS 7.x or higher use the script to join.

> If your LINUX OU exists, but when you run the script ***realm-setup.sh*** and your department is not listed! Run the manual setup and request to radcadmin@utep.edu to add your department.

      ii. Check the /etc/sssd/sssd.conf_UTEP exists first.
         1. # cp /mnt/sssd7.conf_v2 /etc/sssd/sssd.conf_UTEP
      iii. # ./mnt/realm-setup.sh
         1. Choose the department that this machine belongs to. If you do not see your department or research group, press "***ctrl + c***" and exit the script. Either run the manual process or request to radcadmin@utep.edu to update the script.
         2. You will be prompted to use your UTEP credentials to join UTEP.EDU. If successful, the script will exit gracefully.
         3. # umount /mnt
         4. Skip to step 4

   b. Join to the UTEP domain (manual process):
      i. Check the /etc/sssd/sssd.conf_UTEP exists first.
         1. # cp /mnt/sssd7.conf_v2 /etc/sssd/sssd.conf_UTEP
      ii. Replace the username with an actual UTEP account.
         1. # realm join --user=*username*@utep.edu utep.edu
      iii. If successful, the command will exit gracefully.
      iv. # umount /mnt
      v. You must connect to a system where you have the Admin tools installed to manage UTEP.EDU, and create the Linux OU based on the type of equipment joined.
         1. Open the AD Users and Computers, search for your computer and make sure that your server is locate on the following OU:

> **Servers only:**
> - Utep.edu\Information Resource & Planning\Research Academic Data Center\Colleges*Your-College**Your-Department*\Linux.
>
> **Workstations only:**
> - Utep.edu\Academic Affairs\Colleges*Your-College**Your-Department*\Linux.

4) Replace the generic sssd.conf configuration with UTEP based sssd.conf. The UTEP template include access to the system(s) by RADC Staff only and must base for all sssd customizations.
   a. RADC Staff access only:
      i. # cd /etc/sssd
      ii. # cp sssd.conf_UTEP sssd.conf
      iii. # systemctl restart sssd

iv. # systemctl status sssd

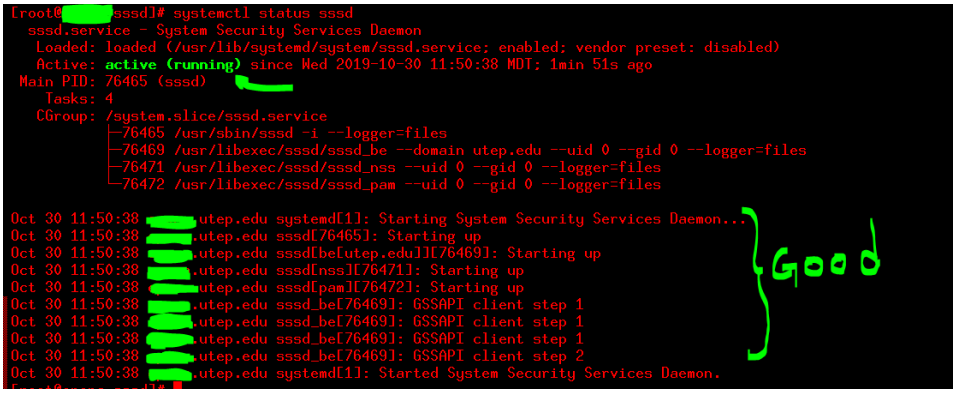

Figure 3 Successful integration to UTEP domain.

b. Customizing the sssd.conf for your Department.
   i. The configuration has been documented, please retain the RADC groups and append the corresponding UTEP security groups that you plan to use to restrict access to the server/workstation. This configuration is located at the end of the file.

```
###############################################################
# ACL based on access_provider = simple
# Only one simple_allow_groups is process. The last line will
# supercede previous groups.  To allow multiple groups you must
# include them in a single line separated by commas.
#simple_allow_groups = group1@utep.edu
#simple_allow_groups = group1@utep.edu, group2@utep.edu
#
# The following three groups (RADC *) are required for proper
# administration of Linux machines by the RADC group.  However,
# only  RADC Linux Sudo is part of the sudoers file.

simple_allow_groups = RADC SysAdmin@utep.edu, RADC Linux Sudo@utep.edu, RADC SysOps@utep.edu
```

Figure 4 /etc/sssd/sssd.conf

   ii. Once you finished customizing the sssd.conf, make a backup of configuration.
      1. # cp sssd.conf sssd.conf_*YourDEPT*
      2. # systemctl restart sssd
      3. # systemctl status sssd

> Note:
> The only difference between the files sssd.conf_*YourDEPT* & sssd.conf_UTEP should be the security groups.

5) Check that the service is working and that is binding to UTEP.EDU
   a. # systemctl status sssd
   b. Refer to Figure 3 Successful integration to UTEP domain.
6) Test with an account that has never logged in
   a. # realm list –all (You should see your security groups)
   b. # id username (It should pull information from AD)

7) Setup sudo file to use UTEP.EDU groups

a. Make a copy of the EXAMPLE file located in /etc/sudoers.d/. If there is now at the end of this document, there is template that you can copy.
   i. # cp –p /etc/sudoers.d/EXAMPLE /etc/sudoers.d/*YourDEPT*
   ii. # visudo –f /etc/sudoers.d/*YourDEPT*
   iii. Add to your sudo file the @utep.edu groups that will have access. See the figure below for examples, especially when dealing with spaces in the name group.

```
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
radcadmin       ALL=(ALL)       ALL

## Allow any member from the RADC Linux Administrator@utep.edu to run all commands
%RADC\ Linux\ Sudo@utep.edu     ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel ALL=(ALL)      NOPASSWD: ALL
radcadmin ALL=(ALL)     NOPASSWD: EMERGENCY
radcadmin ALL=(ALL)     NOPASSWD: CONFIGURE_REMOTE
```

Figure 5 Adding special access to the organization sudo file.

   iv. All Domain groups must end with @utep.edu
   v. Local groups still work in the same away.
   vi. Exit the edit mode
      1. [ESC]:wq (If there are not errors in the syntax, it exit editing mode)
   vii. To test your sudo access, you must log off or open a new SSH connections then performed the following command:
      1. # sudo su - (if given administrator access).

8) All done

Sudo Template Example:

```
################################################################
## Defined ALIAS commands below
################################################################
## Containers
# Cmnd_Alias CONTAINERS = /bin/systemctl start docker, /bin/systemctl stop docker, /bin/systemctl restart
docker, /bin/systemctl status docker

## Apache config to start & stop service
# Cmnd_Alias APACHE = /sbin/apachectl

## Redis config
# Cmnd_Alias REDIS = /bin/systemctl start redis, /bin/systemctl stop redis, /bin/systemctl restart redis,
/bin/systemctl status redis

################################################################
## Allow any member from AD to run any commands anywhere
##
## <<<<<<<<<<<<<<< WARNING WARNING WARNING >>>>>>>>>>>>>>>
## This is give full admni rights to the whole
## machine.  Only Administrator should use a syntax below
## which is an example for give access to MINERS users
## group.
##
## %RADC\ Linux\ Sudo@utep.edu   ALL=(ALL)      ALL
################################################################


################################################################
## Special accesss to run ALIAS command or
## other command go here
################################################################
## Give JDOE access to the apachectl command
# JDOE ALL=(ALL) APACHE
# JDOE ALL=CONTAINERS
# JDOE ALL=REDIS
```