Setting up LDAP authentication for crew machines

Introduction

Systems provides a LDAP (Lightweight Directory Access Protocol) cluster which can be used to authenticate CCIS users. This document will show how to convert a vanilla Ubuntu machine into one where CCIS users can login.

Install libpam-ldap

```
sudo apt-get install libpam-ldap nscd
```

PAM (Pluggable Authentication Modules) is an API for authentication. The package libpam-ldapd provides the LDAP module for PAM.

Running the above line will pop-up a ncurses window asking for the ldap URI.

Question	Answer
LDAP URI	`ldap://cluster.ldap.ccs.neu.edu`
Distinguished name of search base	`dc=ccs,dc=neu,dc=edu`
LDAP version	3
Make local root Database admin	No
Does your LDAP require login?	No

Edit `/etc/ldap.conf`

Add this:

```
ssl start_tls
tls_checkpeer no
```

Edit `/etc/nsswitch.conf`

A sample `/etc/nsswitch.conf` looks like:

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat
group:          compat
shadow:         compat

hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

You need to have these lines instead.

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
netgroup:       ldap
```

Traditionally (before NIS), a machine only had to look at its `/etc/passwd` to authenticate a user. With the rise of NIS (and later LDAP) as a centralized mechanism of authentication, the `/etc/nsswitch.conf` was designated to specify the **search order**.

The line `passwd: files ldap` tells the system to look at the file `/etc/passwd` first, then LDAP.

Enable `/etc/security/access.conf`

`/etc/pam.d/sshd` should have these lines:

```
# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account  required     pam_access.so
```

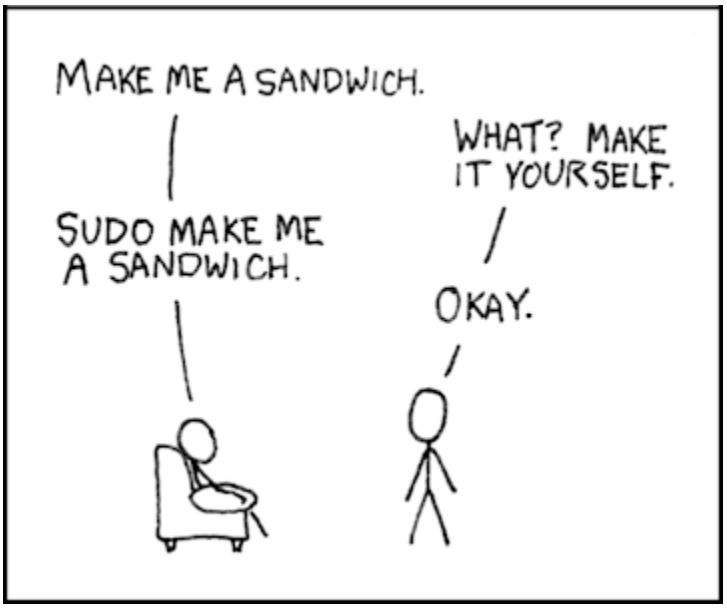
Uncomment (or add) the line: `account required pam_access.so`.

`/etc/security/access.conf`

Our standard configuration looks like:

```
+ : (systems) (elders) (crew) : ALL
- : ALL : ALL
```

sudo - `/etc/sudoers`



The command `sudo` allows non-root users to run certain (or all) commands as root.

Add the netgroup elders and systems (required) and add additional lines for crewbies.

Run

```
sudo visudo
```

to edit the sudoers file.

```
%elders      ALL=(ALL) ALL
%systems     ALL=(ALL) ALL
somecrewbie1 ALL=(ALL) ALL
somecrewbie2 ALL=(ALL) ALL
```