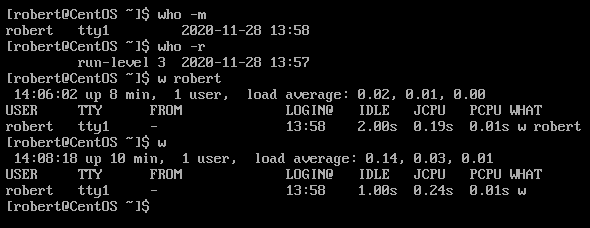
Take a snapshot of users every hour (Use a cron job for this) to see if there is any suspicious adding/removing of users

**who -m** : provides which user is currently logged in

**who -r** : display the current privileges from the user

**w** : provides a list of who is logged in and what they are doing.

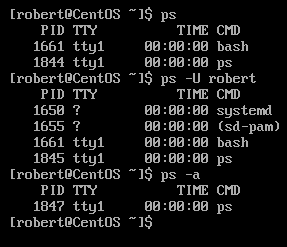
**w user** : narrow the list to a specific user to see what the user is doing



**ps** : (processes status) display the processes of the current shell

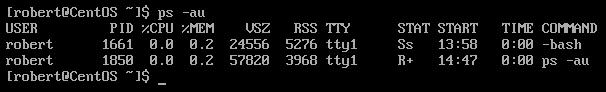
**ps -U username**: display the processes being run by a specific user

**ps -a** : display all processes ran by every user on the system



We can snapshot what other users are doing with ps

Note: **-a** list all process ran by all users, **-x** list all processes started at boot and **-u** will add colums with additional information.

****

Let us create a script to take a snapshot of users every hour and monitor what they are doing.

vi filename.sh

#!/bin/bash

ps -au | more

Save the script and exit

Run **crontab -e** in the command line to create a new cron job rule.

|  |  |
| --- | --- |
| Special string | Meaning |
| @reboot | Run once, at startup. |
| @yearly | Run once a year, “0 0 1 1 \*”. |
| @annually | (same as @yearly) |
| @monthly | Run once a month, “0 0 1 \* \*”. |
| @weekly | Run once a week, “0 0 \* \* 0”. |
| @daily | Run once a day, “0 0 \* \* \*”. |
| @midnight | (same as @daily) |
| @hourly | Run once an hour, “0 \* \* \* \*”. |

In the editor type the following according to your credentials **@hourly /home/user/filename.sh** once typed save and exit.Cron will run the script once an hour and the script would take a snapshot of what users are doing in the system. This a good way to monitor users’ activities within a system.

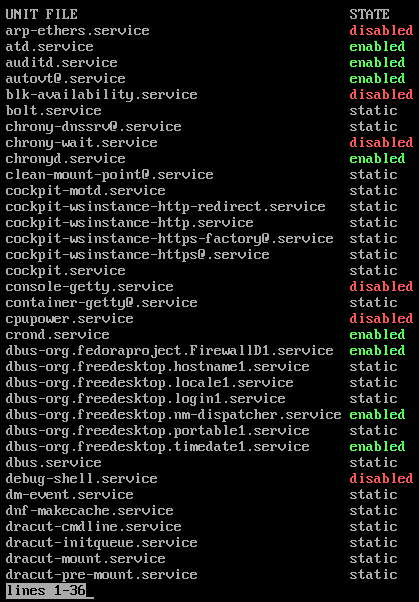
Write a document that will show how to control what daemons run on boot and how to change that.  assume your audience is technically inclined, but not an expert.

What is daemon in Linux?

A daemon in Linux, and in any UNIX-like system, is a process that runs in the background and is autonomous, so it does not need interaction from a system user to start up and function.

Daemons are useful for running programs independent of a user session, processes that start automatically when the system boots, services that listen to perform their tasks when they are called.

**systemctl list-unit-files --type service** : List all services and check if they are enabled or disable.



**systemctl enable name.service** : Enables a service

**systemctl disable name.service** : Disable a service

**systemctl status name.service** : Checks if a service is enabled



Find out how to boot into emergency mode for both your servers.  Write a one page (or less) document on how to do that. Include 1 paragraph executive summary on why you might want to.

What is emergency mode?

Emergency mode is just a raw shell. No services are started, no mounts are mounted, and no sockets are established. Emergency mode is good for debugging purposes.

The biggest advantage of emergency mode over single-user mode is that the init files are not loaded. If init is corrupt or not working, you can still mount file systems to recover data that might have been lost during a reinstall.

**How to Boot Into Emergency Mode in Ubuntu Server and CentOS**

1. Restart the server while holding down the “**SHIFT**” key in the keyboard**.** The GNU GRUB menu would appear.

****

1. Select the option “**Ubuntu**” and the press the “**e**” key to edit.



1. Use the arrow key to scroll down the page and find the line that start with the word “Linux” and append the string “**systemd.unit=rescue.target**” at the end of it.



After adding the above string, hit **Ctrl-x** or **F10** to boot into emergency mode

If successful, a message would appear “ You are in emergency mode”. From here we can start running commands to troubleshoot the server.

****

Press “**Ctrl + d**” to boot back to normal mode or user mode. Alternatively, type **systemctl default** or **exit**.

**Note:** CentOS users can follow the sameprocess to boot in emergency mode.

References

Ostechnix. “Boot Into Rescue Mode Or Emergency Mode In Ubuntu 20.04 / 18.04.” *OSTechNix*, 15 May 2020, ostechnix.com/how-to-boot-into-rescue-mode-or-emergency-mode-in-ubuntu-18-04/.

Skenlon. “An Introduction to Linux User Account Monitoring.” *Enable Sysadmin*, Red Hat, Inc., 28 Jan. 2020, www.redhat.com/sysadmin/monitor-users-linux.

Vanney, Ivan. “Using Ps Command on Linux.” *Linux Hint*, 1 Jan. 1968, linuxhint.com/ps\_command\_linux-2/.