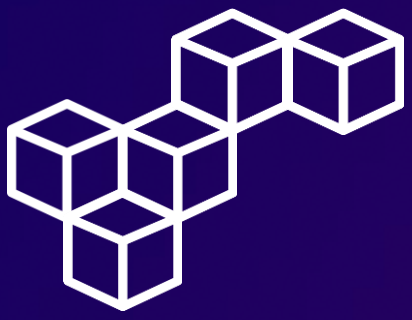
AWS re:Start

LAB

Managing Processes

WEEK 2

aws re/start



Overview

Managing processes in Linux involves using various commands and utilities to monitor and control program execution. Tools like ps and top provide real-time insights into running processes, including resource usage and status, facilitating efficient troubleshooting and resource optimization. Additionally, utilities like pstree visualize process relationships, helping administrators understand process hierarchies and dependencies.

Furthermore, Linux offers scheduling tools such as at and cron for executing tasks at specific times or intervals. With crontab, administrators can automate tasks, ensuring timely execution of critical processes and maintenance routines without manual intervention. This comprehensive set of process management tools enables Linux administrators to maintain system stability, optimize resource utilization, and streamline task execution for efficient system operation.

Note: This lab was made using Windows Subsystem for Linux.

Topics covered

- Create a new log file for process listings
- Use the top command
- Establish a repetitive task that runs your previous auditing commands once a day

Task 1

Use SSH to connect to an Amazon Linux EC2 instance

Initial Preparations

In the AWS Management Console, select the EC2 instance and make note of the **Public IPv4 address**.

Download the **private key file** labsuser.pem. Change to the Downloads directory and modify the permissions on the key to be read-only (r--------).

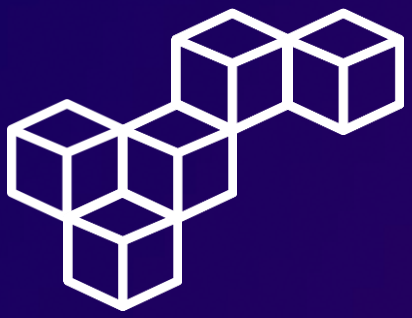
Connect to the instance using SSH

Establish a connection to the EC2 instance using the ssh command, the key and the instance's public IPv4 address.

```
support@HP-Pavilion-Laptop:~/Downloads$ ssh -i labsuser.pem ec2-user@52.38.114.107
The authenticity of host '52.38.114.107 (52.38.114.107)' can't be established.
ED25519 key fingerprint is SHA256:LfMKWqB/dOln6tFNMJQlWDEsynx2vW/RN/mkq8Bwxu8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '52.38.114.107' (ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-10-202 ~]$
```

aws re/start



Task 2

Create List of Processes

Create a log file from the ps command

Using the tee command, create a log file named **processes.csv** from the ps -aux command output and filter out any process containing the root user with the grep -v command.

```
[ec2-user@ip-10-0-10-202 companyA]$ sudo ps -aux | grep -v root | sudo tee SharedFolders/processes.csv
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
rpc       1707  0.0  0.3  67256  3356 ?        Ss   15:07   0:00 /sbin/rpcbind -w
dbus      1709  0.0  0.4  58248  4072 ?        Ss   15:07   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork
 --nopidfile --systemd-activation
libstor+  1713  0.0  0.1  12628  1904 ?        Ss   15:07   0:00 /usr/bin/lsmd -d
rngd      1724  0.0  0.4  96344  4716 ?        Ss   15:07   0:00 /sbin/rngd -f --fill-watermark=0 --exclude=jitter
chrony    1726  0.0  0.3 120184  3084 ?        S    15:07   0:00 /usr/sbin/chronyd -F 2
postfix   2148  0.0  0.7  90396  6772 ?        S    15:07   0:00 pickup -l -t unix -u
postfix   2149  0.0  0.7  90468  6848 ?        S    15:07   0:00 qmgr -l -t unix -u
ec2-user  2892  0.0  0.4 150760  4400 ?        S    15:09   0:00 sshd: ec2-user@pts/0
ec2-user  2893  0.0  0.4 126840  4124 pts/0    Ss   15:09   0:00 -bash
[ec2-user@ip-10-0-10-202 companyA]$
```

Review the log file

Validate your work by typing cat SharedFolders/processes.csv.

```
[ec2-user@ip-10-0-10-202 companyA]$ cat SharedFolders/processes.csv
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
rpc       1707  0.0  0.3  67256  3356 ?        Ss   15:07   0:00 /sbin/rpcbind -w
dbus      1709  0.0  0.4  58248  4072 ?        Ss   15:07   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork
 --nopidfile --systemd-activation
libstor+  1713  0.0  0.1  12628  1904 ?        Ss   15:07   0:00 /usr/bin/lsmd -d
rngd      1724  0.0  0.4  96344  4716 ?        Ss   15:07   0:00 /sbin/rngd -f --fill-watermark=0 --exclude=jitter
chrony    1726  0.0  0.3 120184  3084 ?        S    15:07   0:00 /usr/sbin/chronyd -F 2
postfix   2148  0.0  0.7  90396  6772 ?        S    15:07   0:00 pickup -l -t unix -u
postfix   2149  0.0  0.7  90468  6848 ?        S    15:07   0:00 qmgr -l -t unix -u
ec2-user  2892  0.0  0.4 150760  4400 ?        S    15:09   0:00 sshd: ec2-user@pts/0
ec2-user  2893  0.0  0.4 126840  4124 pts/0    Ss   15:09   0:00 -bash
[ec2-user@ip-10-0-10-202 companyA]$
```

Task 3

List the processes using the top command

The top command

Run the top command to display the system performance and the processes and threads active in the system. Observe the output of the command. Notice how many tasks are running.

```
[ec2-user@ip-10-0-10-202 companyA]$ top
top - 15:18:40 up 11 min,  1 user,  load average: 0.00, 0.02, 0.00
Tasks:  86 total,   1 running,  47 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :   966808 total,   368604 free,    72652 used,   525552 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   751880 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
    1 root      20   0  123504   5372   3896 S   0.0  0.6   0:01.09 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
    4 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kworker/0:0H
    6 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 mm_percpu_wq
    7 root      20   0       0      0      0 S   0.0  0.0   0:00.04 ksoftirqd/0
    8 root      20   0       0      0      0 I   0.0  0.0   0:00.04 rcu_sched
    9 root      20   0       0      0      0 I   0.0  0.0   0:00.00 rcu_bh
   10 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 migration/0
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/0
   12 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/0
   13 root      20   0       0      0      0 S   0.0  0.0   0:00.00 cpuhp/1
   14 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/1
   15 root      rt   0       0      0      0 S   0.0  0.0   0:00.21 migration/1
   16 root      20   0       0      0      0 S   0.0  0.0   0:00.02 ksoftirqd/1
   18 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kworker/1:0H
   20 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
   21 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 netns
   25 root      20   0       0      0      0 I   0.0  0.0   0:00.09 kworker/u4:2
  117 root      20   0       0      0      0 S   0.0  0.0   0:00.00 khungtaskd
  150 root      20   0       0      0      0 S   0.0  0.0   0:00.00 oom_reaper
  201 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 writeback
  205 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kcompactd0
  206 root      25   5       0      0      0 S   0.0  0.0   0:00.00 ksmd
  207 root      39  19       0      0      0 S   0.0  0.0   0:00.00 khugepaged
  208 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 crypto
  209 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kintegrityd
  210 root       0 -20       0      0      0 I   0.0  0.0   0:00.00 kblockd
```

To quit top, press q. You can also run the top -hv command to find the usage and version information.

Task 4

Create a Cron Job

Edit the crontab file

Enter the command sudo crontab -e to edit the crontab file with the Vim text editor.

```
[ec2-user@ip-10-0-10-202 companyA]$ sudo crontab -e
no crontab for root - using an empty one
crontab: installing new crontab
[ec2-user@ip-10-0-10-202 companyA]$
```

Create a cron job

Create a cron job that creates an audit file with ##### in order to cover all .csv files.

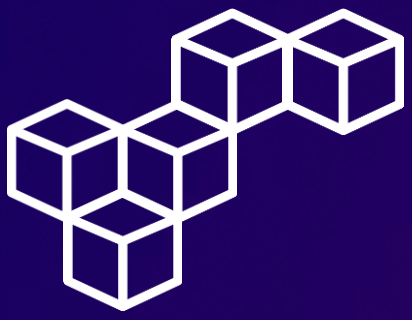
```
SHELL=/bin/bash
PATH=/usr/bin:/bin:/usr/local/bin
MAILTO=root
0 * * * * ls -la $(find .) | sed -e 's/..csv/#####.csv/g' > /home/ec2-user/companyA/SharedFolders/filteredAudit.csv
-- INSERT --                                                                    1,1           All
```

Inspect the crontab file

To validate your work, enter the command sudo crontab –l.

```
[ec2-user@ip-10-0-10-202 companyA]$ sudo crontab -l
SHELL=/bin/bash
PATH=/usr/bin:/bin:/usr/local/bin
MAILTO=root
0 * * * * ls -la $(find .) | sed -e 's/..csv/#####.csv/g' > /home/ec2-user/companyA/SharedFolders/filteredAudit.csv
[ec2-user@ip-10-0-10-202 companyA]$
```

aws re/start



Conclusions

The ps command

The ps command offers a detailed view of currently running processes, making it instrumental for system administrators to monitor system activity, identify resource-intensive processes, and troubleshoot issues effectively.

The top command

The top command provides real-time monitoring of system processes and their resource consumption, enabling administrators to assess system performance, identify bottlenecks, and optimize resource allocation for improved system efficiency.

The kill command

The kill command plays a crucial role in managing processes by allowing administrators to terminate processes gracefully or forcefully as needed, ensuring system stability and efficient resource utilization.

The crontab command

Crontab is a powerful tool for managing scheduled tasks in Unix/Linux systems, providing administrators with the ability to automate repetitive tasks, schedule system maintenance, and execute critical processes at specified times for streamlined system management and improved productivity.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru