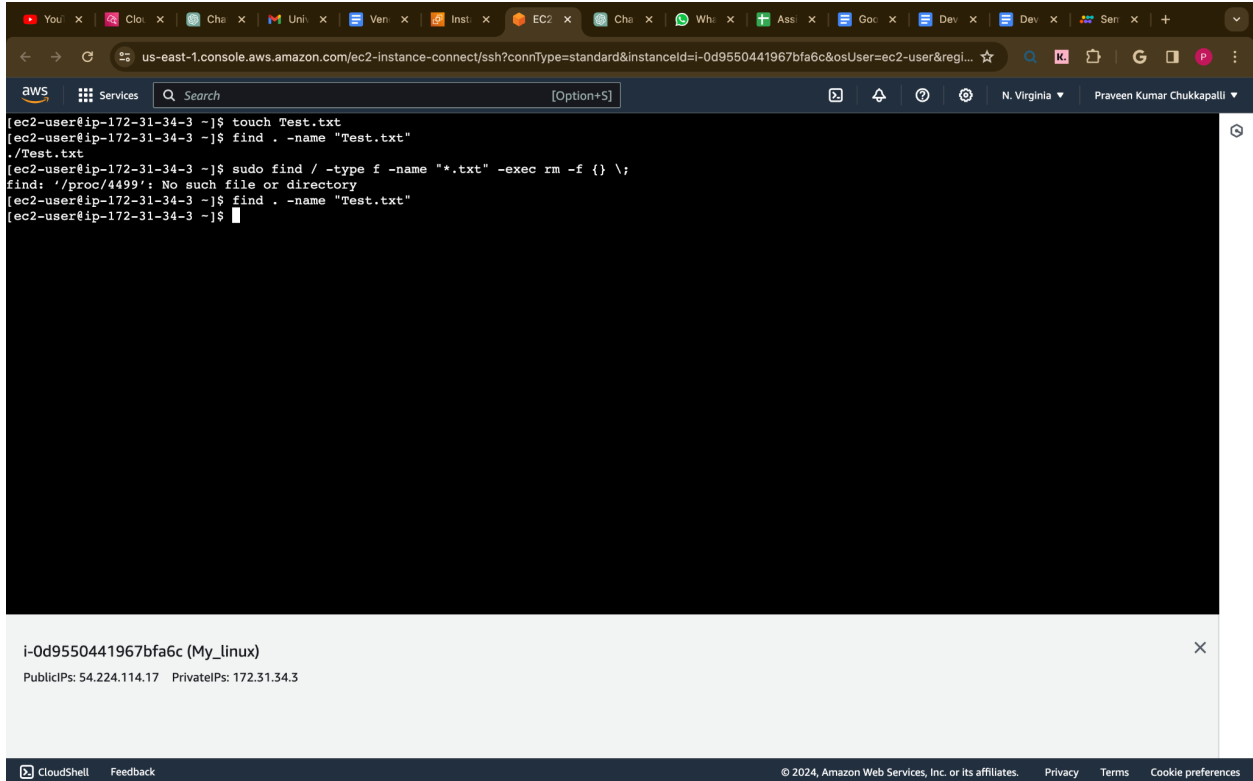


# Devops Assignment- 5

Praveen Kumar Chukkapalli

1) Find all files in entire machine ending with .txt and remove them



```
[ec2-user@ip-172-31-34-3 ~]$ touch Test.txt
[ec2-user@ip-172-31-34-3 ~]$ find . -name "Test.txt"
./Test.txt
[ec2-user@ip-172-31-34-3 ~]$ sudo find / -type f -name "*.txt" -exec rm -f {} \;
find: '/proc/4499': No such file or directory
[ec2-user@ip-172-31-34-3 ~]$ find . -name "Test.txt"
[ec2-user@ip-172-31-34-3 ~]$
```

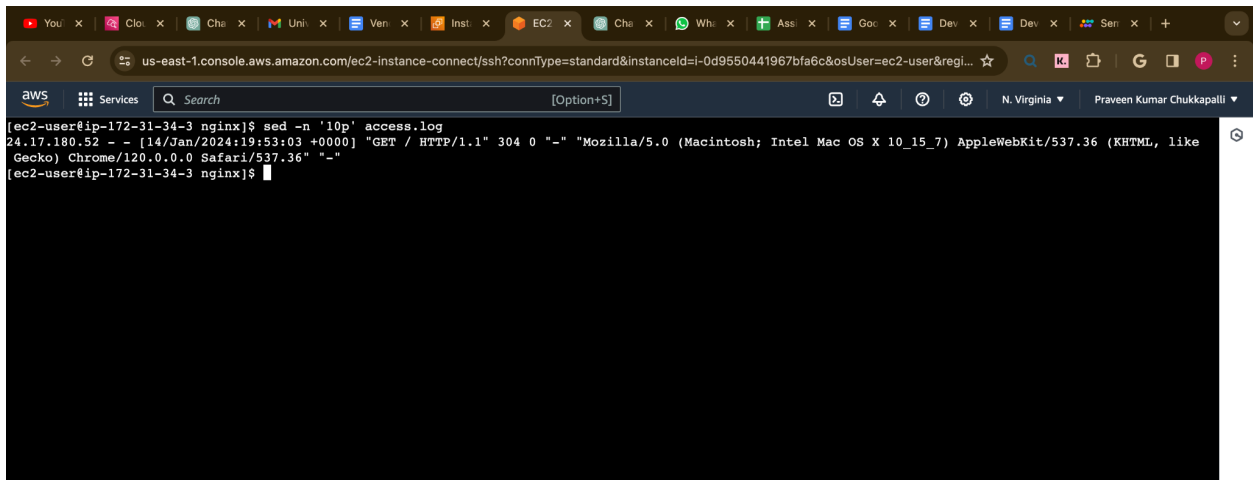
i-Od9550441967bfa6c (My\_linux)

PublicIPs: 54.224.114.17 PrivateIPs: 172.31.34.3

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

2) Find 10th record of var/log/audit/access.log file

I can't access the audit directory in AWS linux OS, so i printed out the 10th record of nginx access.log



```
[ec2-user@ip-172-31-34-3 nginx]$ sed -n '10p' access.log
24.17.180.52 - - [14/Jun/2024:19:53:03 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36" "-"
[ec2-user@ip-172-31-34-3 nginx]$
```

# Devops Assignment- 5

Praveen Kumar Chukkapalli

## 3) Get only today's logs from access.log file

```
[ec2-user@ip-172-31-34-3 nginx]$ awk -v date="$(date +%d/%b/%Y)" ' $0 ~ date' access.log
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "\x16\x03\x01\x00{\x01\x00\x00w\x03\x03Rv\xB6-\xFA_\xFFz\xE2\x16\xCC\x87^\xF0\xB7\xB0,$\x98\x1D\xA1eA\x15
K\x8A" /\xD1\x903\x00\x00\x1A\xC0/\xC0+\xC0\x11\xC0\x07\xC0\x13\xC0\x09\xC0\x14\xC0" 400 157 "-" "-" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "\x16\x03\x01\x00{\x01\x00\x00w\x03\x03\x0E\x12\x92T\xEC\x04\x99\x1F\x97c\x95FC\xCF;\x9F\xAB\xDA\xBA\xE3\
\x18\x1D\x82\x09Bv\x03\xAD\x00\x00\x1A\xC0/\xC0+\xC0\x11\xC0\x07\xC0\x13\xC0\x09\xC0\x14\xC0" 400 157 "-" "-" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET / HTTP/1.1" 200 615 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
ecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /form.html HTTP/1.1" 404 3650 "-" "curl/8.1.2" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /upl.php HTTP/1.1" 404 3650 "-" "Mozilla/5.0" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "\x16\x03\x01\x00{\x01\x00\x00w\x03\x03\x0E\x12\x92T\xEC\x04\x99\x1F\x97c\x95FC\xCF;\x9F\xAB\xDA\xBA\xE3\
\xB4\xCCA\xFF\xF86\x8BN\x16\xE72\xB3\x00\x00\x1A\xC0/\xC0+\xC0\x11\xC0\x07\xC0\x13\xC0\x09\xC0\x14\xC0" 400 157 "-" "-" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /geoip/ HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /favicon.ico HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
HTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /1.php HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /bundle.js HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
ML, like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /files/ HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /systembc/password.php HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:39 +0000] "GET /password.php HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
104.248.127.93 - - [15/Jan/2024:00:01:40 +0000] "GET /info.php HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
L, like Gecko) Chrome/108.0.0.0 Safari/537.36" "-"
135.125.246.110 - - [15/Jan/2024:00:09:00 +0000] "GET /.env HTTP/1.1" 404 3650 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/81.0.4044.129 Safari/537.36" "-"
135.125.246.110 - - [15/Jan/2024:00:09:00 +0000] "POST / HTTP/1.1" 405 559 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
rome/81.0.4044.129 Safari/537.36" "-"
87.236.176.15 - - [15/Jan/2024:00:13:14 +0000] "GET / HTTP/1.1" 200 615 "-" "Mozilla/5.0 (compatible; InternetMeasurement/1.0; +https://internet-measur
```

i-0d9550441967bfa6c (My\_linux)

PublicIPs: 54.224.114.17 PrivateIPs: 172.31.34.3

## 4) Get all ports which are running ( Occupied Ports)

```
[ec2-user@ip-172-31-34-3 nginx]$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                  :::*                    LISTEN
udp        0      0 127.0.0.1:323           0.0.0.0:*               *
udp        0      0 172.31.34.3:68          0.0.0.0:*               *
udp6       0      0 :::1:323                :::*                    *
udp6       0      0 fe80::cd2:9dff:fea8:546 :::*                    *

[ec2-user@ip-172-31-34-3 nginx]$ systemctl start nginx
Failed to start nginx.service: Access denied
See system logs and 'systemctl status nginx.service' for details.
[ec2-user@ip-172-31-34-3 nginx]$ sudo systemctl start nginx
[ec2-user@ip-172-31-34-3 nginx]$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::80                  :::*                    LISTEN
tcp6       0      0 :::22                  :::*                    LISTEN
udp        0      0 127.0.0.1:323           0.0.0.0:*               *
udp        0      0 172.31.34.3:68          0.0.0.0:*               *
udp6       0      0 :::1:323                :::*                    *
udp6       0      0 fe80::cd2:9dff:fea8:546 :::*                    *
```