

Network & System Tools + Compression & Archiving + Text Process Tools Assignment

Assignment Objective

You will simulate a real-world Linux system administrator or DevOps engineer role by:

- Setting up user and group permissions
- Running real-time network & system diagnostics
- Performing data compression and decompression
- Using powerful text processing tools like `grep` and `awk` in combination.

You must **capture and document** command outputs as if working in a production or staging server environment.

Industry Scenario

You are a junior system administrator in a company called **CloudOps Ltd.**. Your manager has asked you to:

1. Set up proper **user and group permissions** for the network team.
2. Run **network and system diagnostics** to check connectivity and performance.
3. Archive and compress **log files** for backup.
4. Use `grep` and `awk` to **extract meaningful data** from logs.

Assignment Tasks

Part 1: User & Group Permissions

Task 1.1 — Create users & groups

```
ubuntu@ip-172-31-24-202:~$ sudo groupadd network_team
ubuntu@ip-172-31-24-202:~$ sudo useradd -m -G network_team alice
ubuntu@ip-172-31-24-202:~$ sudo useradd -m -G network_team bob
ubuntu@ip-172-31-24-202:~$
```

1.2 — Set directory permissions

- Create a shared directory /opt/network_data.
- Set group ownership to network_team.
- Give group members **read/write/execute** access.

```
ubuntu@ip-172-31-24-202:~$ sudo chown root:network_team /opt/network_data/
ubuntu@ip-172-31-24-202:~$ sudo chmod 770 /opt/network_data/
ubuntu@ip-172-31-24-202:~$ sudo mkdir /opt/network_data|
```

Expected Output:

Run `ls -ld /opt/network_data` and capture permissions: `drwxrwx--- 2 root`

```
ubuntu@ip-172-31-24-202:~$ ls -ld /opt/network_data/
drwxrwx--- 2 root network_team 4096 May 13 17:54 /opt/network_data/
ubuntu@ip-172-31-24-202:~$
```

Part 2: Network Tools & Real-Time Checks

Task 2.1 — Check connectivity to google.com

```
ubuntu@ip-172-31-24-202:~$ ping -c 4 google.com
PING google.com (142.250.74.142) 56(84) bytes of data.
64 bytes from arnlls11-in-f14.1e100.net (142.250.74.142): icmp_seq=1 ttl=113 time=3.89 ms
64 bytes from arnlls11-in-f14.1e100.net (142.250.74.142): icmp_seq=2 ttl=113 time=4.22 ms
64 bytes from arnlls11-in-f14.1e100.net (142.250.74.142): icmp_seq=3 ttl=113 time=3.90 ms
64 bytes from arnlls11-in-f14.1e100.net (142.250.74.142): icmp_seq=4 ttl=113 time=3.93 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 3.889/3.983/4.215/0.134 ms
ubuntu@ip-172-31-24-202:~$
```

Ping: used to check connectivity of a host.

-c 4 : sends exactly 4 packets to test.

```
ubuntu@ip-172-31-24-202:~$ traceroute google.com
traceroute to google.com (142.250.74.142), 30 hops max, 60 byte packets
 1  240.3.96.8 (240.3.96.8)  3.510 ms  240.3.96.12 (240.3.96.12)  4.605 ms  240.3.96.9 (240.3.96.9)  3.481 ms
 2  240.3.96.22 (240.3.96.22)  3.710 ms  3.698 ms  240.3.96.27 (240.3.96.27)  3.574 ms
 3  240.3.96.28 (240.3.96.28)  3.625 ms  240.3.96.54 (240.3.96.54)  3.030 ms  240.3.96.52 (240.3.96.52)  3.044 ms
 4  * * *
 5  173.194.124.194 (173.194.124.194)  4.608 ms  3.827 ms  4.581 ms
 6  142.250.236.117 (142.250.236.117)  4.042 ms  2.664 ms  2.916 ms
 7  142.251.48.43 (142.251.48.43)  3.377 ms  142.251.48.45 (142.251.48.45)  2.900 ms  142.251.48.43 (142.251.48.43)  4.821 ms
 8  arnlls11-in-f14.1e100.net (142.250.74.142)  4.636 ms  3.870 ms  3.853 ms
ubuntu@ip-172-31-24-202:~$ |
```

Traceroute: maps the path that packet takes from sender to receiver.

Here:

- Limit Maximum number of hops(routers) = 30
- Packets size =30

- Each line represents a hop with hop number(sequential count), IP, and RTT.

```
ubuntu@ip-172-31-24-202:~$ mtr --report google.com
Start: 2025-05-13T18:03:11+0000
HOST: ip-172-31-24-202          Loss%   Snt    Last    Avg    Best   Wrst StDev
 1.|-- 240.3.96.12            0.0%    10    3.9    3.9    3.9    4.0   0.1
 2.|-- 240.3.96.24            0.0%    10    3.7    3.7    3.7    3.8   0.0
 3.|-- 240.3.96.56            0.0%    10    3.7    3.8    3.7    5.4   0.5
 4.|-- ???                   100.0    10    0.0    0.0    0.0    0.0   0.0
 5.|-- 173.194.124.194        0.0%    10    3.8    3.7    3.6    3.8   0.1
 6.|-- 192.178.44.87          0.0%    10    4.9    4.8    4.7    5.0   0.1
 7.|-- 142.251.48.43          0.0%    10    4.0    4.0    4.0    4.1   0.0
 8.|-- arn11s11-in-f14.1e100.net 0.0%    10    4.0    4.0    3.9    4.0   0.0
ubuntu@ip-172-31-24-202:~$
```

Combines traceroute and ping to show the path to google.com with continuous statistics.

Here:

- Loss%: Packet loss at each hop.
- Snt: Packets sent (10).
- Last/Avg/Best/Wrst: Latency metrics in milliseconds.
- StDev: Jitter (consistency of latency).

Task 2.2 — Check open ports & listening services

```
ubuntu@ip-172-31-24-202:~$ sudo netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp      0      0 127.0.0.53:53           0.0.0.0:*          LISTEN
tcp      0      0 127.0.0.54:53           0.0.0.0:*          LISTEN
tcp6     0      0 ::::22                  ::::*              LISTEN
udp      0      0 127.0.0.54:53           0.0.0.0:*          LISTEN
udp      0      0 127.0.0.53:53           0.0.0.0:*          LISTEN
udp      0      0 172.31.24.202:68         0.0.0.0:*          LISTEN
udp      0      0 127.0.0.1:323            0.0.0.0:*          LISTEN
udp6     0      0 ::1:323                 ::::*              LISTEN
ubuntu@ip-172-31-24-202:~$ |
```

Lists all listening TCP/UDP ports (numeric format).

```
ubuntu@ip-172-31-24-202:~$ sudo ss -tulwn
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
icmp6 UNCONN 0 0 *%ens5:58 *:*
udp UNCONN 0 0 127.0.0.54:53 0.0.0.0:*
udp UNCONN 0 0 127.0.0.53%lo:53 0.0.0.0:*
udp UNCONN 0 0 172.31.24.202%ens5:68 0.0.0.0:*
udp UNCONN 0 0 127.0.0.1:323 0.0.0.0:*
udp UNCONN 0 0 [:1]:323 [::]:*
tcp LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.54:53 0.0.0.0:*
tcp LISTEN 0 4096 *:22 *:*
ubuntu@ip-172-31-24-202:~$ |
```

Task 2.3 — Test remote port connectivity

```
ubuntu@ip-172-31-24-202:~$ nc -zv google.com 443
Connection to google.com (216.58.207.238) 443 port
[tcp/https] succeeded!
ubuntu@ip-172-31-24-202:~$
```

Uses netcat to check if Google's HTTPS port (443) is reachable.

Task 2.4 — Check network interfaces

Displays active network interfaces and their settings.

```
ubuntu@ip-172-31-24-202:~$ ifconfig
ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
        inet 172.31.24.202 netmask 255.255.240.0 broadcast 172.31.31.255
                inet6 fe80::4e1:37ff:fe:26d prefixlen 64 scopeid 0x20<link>
                    ether 06:e1:37:fc:02:6d txqueuelen 1000 (Ethernet)
                    RX packets 23361 bytes 7287924 (7.2 MB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 15828 bytes 1564751 (1.5 MB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
                    loop txqueuelen 1000 (Local Loopback)
                    RX packets 240 bytes 26503 (26.5 KB)
                    RX errors 0 dropped 0 overruns 0 frame 0
                    TX packets 240 bytes 26503 (26.5 KB)
                    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ip-172-31-24-202:~$
```

Task 2.5 — DNS lookup

- Query DNS records for google.com.
- dig give more details.

```
ubuntu@ip-172-31-24-202:~$ nslookup google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.207.238
Name:   google.com
Address: 2a00:1450:400f:80a::200e

ubuntu@ip-172-31-24-202:~$ dig google.com

; <>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16490
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.        177    IN      A      216.58.207.238

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue May 13 18:10:43 UTC 2025
;; MSG SIZE  rcvd: 55

ubuntu@ip-172-31-24-202:~$
```

Task 2.6 — Download test file

```
ubuntu@ip-172-31-24-202:~$ wget https://example.com/testfile.txt
--2025-05-13 18:11:42-- https://example.com/testfile.txt
Resolving example.com (example.com)... 23.192.228.80, 23.192.228.84, 23.215.0.136, ...
Connecting to example.com (example.com)|23.192.228.80|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2025-05-13 18:11:43 ERROR 404: Not Found.

ubuntu@ip-172-31-24-202:~$ curl -O https://example.com/testfile.txt
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total   Spent    Left  Speed
0          0       0       0      0  0 --:--:-- 0       0       0       0       0
0 1870      0  --:--:-- 1869
ubuntu@ip-172-31-24-202:~$ |
```

- `wget`: used for downloading.
 - `curl`: can be used for both downloading/uploading

Task 2.7 — Monitor bandwidth in real time

	12.5kb	25.0kb	37.5kb	50.0kb	62.5kb
ip-172-31-24-202.eu-north-1.compute.internal	=> 8.46.zcomnetworks.com.pk <= ip-172-31-0-2.eu-north-1.compute.internal			1.72kb 160b 2.35kb 310b 4.89kb 109b 0b 0b 176b	4.89kb 109b 2.35kb 310b 1.72kb 160b 176b
ip-172-31-24-202.eu-north-1.compute.internal	=> 169.254.169.123 <=			0b 0b 0b 0b 0b 0b	34b 34b 34b 34b

lftop -i eth0: displays real time information about network traffic

- -i: specifies network interface to monitor

Part 3: Compression & Decompression

Task 3.1 — Archive directory

```
ubuntu@ip-172-31-24-202:~$ sudo tar cvf network_data.tar /opt/network_data
tar: Removing leading '/' from member names
/opt/network_data/
ubuntu@ip-172-31-24-202:~$ |
```

tar: create and manage archive files.

- c: create new archive file.
- v: verbose mode
- f: specifies the filename

Task 3.2 — Compress archive

```
ubuntu@ip-172-31-24-202:~$ gzip network_data.tar
ubuntu@ip-172-31-24-202:~$ |
```

Task 3.3 — Decompress

```
ubuntu@ip-172-31-24-202:~$ gunzip network_data.tar.gz
ubuntu@ip-172-31-24-202:~$ |
```

Task 3.4 — Use bzip2 compression

```
ubuntu@ip-172-31-24-202:~$ bzip2 network_data.tar
ubuntu@ip-172-31-24-202:~$ bunzip2 network_data.tar.bz2
ubuntu@ip-172-31-24-202:~$ |
```

Expected Output Example:

```
ubuntu@ip-172-31-24-202:~$ ls -lh
total 16K
-rw-rw-r-- 1 ubuntu ubuntu 10K May 13 18:20 network_data.tar
-rw-rw-r-- 1 ubuntu ubuntu 1.3K May 13 18:12 testfile.txt
ubuntu@ip-172-31-24-202:~$ |
```

Part 4: Text Processing with `grep` & `awk`

Task 4.1 — Search for “error” in log files

```
ubuntu@ip-172-31-24-202:~$ grep "error" /var/log/syslog
2025-05-13T10:45:33.412963+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 2025-05-13 10:45:31.7793 ERROR EC2RoleProvider Failed to connect to Systems Manager with SSM role credentials. error calling RequestManagedInstanceRoleToken: AccessDeniedException: Systems Manager's instance management role is not configured for account: 205842488109
2025-05-13T10:45:33.513967+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 2025-05-13 10:45:31.7793 ERROR [CredentialRefresher] Retrieve credentials produced error: no valid credentials could be retrieved for ec2 identity. Default Host Management Err: error calling RequestManagedInstanceRoleToken: AccessDeniedException: Systems Manager's instance management role is not configured for account: 205842488109
2025-05-13T11:12:40.193084+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 2025-05-13 11:12:40.1368 ERROR EC2RoleProvider Failed to connect to Systems Manager with SSM role credentials. error calling RequestManagedInstanceRoleToken: AccessDeniedException: Systems Manager's instance management role is not configured for account: 205842488109
2025-05-13T11:12:40.293397+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 2025-05-13 11:12:40.1368 ERROR [CredentialRefresher] Retrieve credentials produced error: no valid credentials could be retrieved for ec2 identity. Default Host Management Err: error calling RequestManagedInstanceRoleToken: AccessDeniedException: Systems Manager's instance management role is not configured for account: 205842488109
2025-05-13T12:50:14.086719+00:00 ip-172-31-24-202 systemd[1]: apport-autoreport.path - Process error reports when automatic reporting is enabled (file watch) was skipped because of an unmet condition check (ConditionPathExists=/var/lib/apport/autoreport).
```

Task 4.2 — Count how many errors found

```
ubuntu@ip-172-31-24-202:~$ grep -c "error" /var/log/syslog
19
ubuntu@ip-172-31-24-202:~$ |
```

Task 4.3 — Extract specific fields (timestamps, messages)

```
ubuntu@ip-172-31-24-202:~$ grep "error" /var/log/syslog | awk '{print $1, $2, $3, $5}'
2025-05-13T10:45:33.412963+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 10:45:31.7793
2025-05-13T10:45:33.513967+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 10:45:31.7793
2025-05-13T11:12:40.193084+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 11:12:40.1368
2025-05-13T11:12:40.293397+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[545]: 11:12:40.1368
2025-05-13T12:50:14.086719+00:00 ip-172-31-24-202 systemd[1]: apport-autoreport.path - Process error reports when automatic reporting is enabled (file watch) was skipped because of an unmet condition check (ConditionPathExists=/var/lib/apport/autoreport).
2025-05-13T12:50:14.086725+00:00 ip-172-31-24-202 systemd[1]: -
2025-05-13T12:50:18.086725+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 12:50:16.4384
2025-05-13T12:50:18.158069+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 12:50:16.4384
2025-05-13T13:16:13.716367+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 13:16:13.6600
2025-05-13T13:16:13.816711+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 13:16:13.6601
2025-05-13T13:41:47.762538+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 13:41:47.7083
2025-05-13T13:41:47.862923+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 13:41:47.7083
2025-05-13T14:09:22.810970+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 14:09:22.7587
2025-05-13T17:39:17.151094+00:00 ip-172-31-24-202 systemd[1]: -
2025-05-13T17:39:17.151104+00:00 ip-172-31-24-202 systemd[1]: -
2025-05-13T17:39:28.878989+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 17:38:19.2868
2025-05-13T17:39:28.988206+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 17:38:19.2868
2025-05-13T18:03:44.144706+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 18:03:44.0854
2025-05-13T18:03:44.245216+00:00 ip-172-31-24-202 amazon-ssm-agent.amazon-ssm-agent[542]: 18:03:44.0854
ubuntu@ip-172-31-24-202:~$ |
```

Displays 1, 2, 3 and field from syslog lines containing the word “error”.

Task 4.4 — Combine commands to filter and summarize

```
ubuntu@ip-172-31-24-202:~$ grep "error" /var/log/syslog | awk '{print $5}' | sort | uniq -c | sort -nr
4 -
2 18:03:44.0854
2 17:38:19.2868
2 13:41:47.7083
2 12:50:16.4384
2 11:12:40.1368
2 10:45:31.7793
1 14:09:22.7587
1 13:16:13.6601
1 13:16:13.6600
ubuntu@ip-172-31-24-202:~$ |
```

The command extracts error messages, focuses on 5th field, count the occurrences of each unique error and displays in descending order.

What to Submit

A **single document** (Markdown or Word) with:

- Commands you ran (copied)
- Screenshots or copied **real-time outputs**
- A **brief explanation** (1-2 sentences) for each step

Upload on GitHub and Submit via: Google Form

Deadline

Submission due date: 5 days from assignment date.