ASSIGNMENT 01

SUBMITTED BY
Daud Bin Nasar

SUBMISSION DATE
May 16, 2025

COURSE
Advanced IT Training and Japanese Language Program

Linux System Administration Assignment

Objective

As a junior system administrator at CloudOps Ltd.,simulate a real-world Linux system administration role by setting up user and group permissions, running network and system diagnostics, performing data compression and decompression, and using text processing tools like grep and awk. This document captures the commands executed, their outputs, and brief explanations for each task.

PART 1: USER & GROUP PERMISSIONS

Task 1.1 — Create users & groups

Commands:

sudo groupadd network_team

sudo useradd -m -G network_team alice

sudo useradd -m -G network_team bob

Output:

No output for groupadd and useradd unless errors occur

Explanation: Created a group network_team and added users alice and bob to it, with home directories (-m) and membership in the network_team group (-G).

Task 1.2 — Set directory permissions

Commands:

sudo mkdir /opt/network_data

sudo chown root:network_team /opt/network_data

sudo chmod 770 /opt/network_data

ls -ld /opt/network_data

Output:

drwxrwx--- 2 root network_team 4096 May 16 22:00 /opt/network_data

Explanation: Created a shared directory /opt/network_data, set group ownership to network_team, and granted read/write/execute permissions to the group (770). The ls -ld command confirms the permissions.

PART 2: NETWORK TOOLS & REAL-TIME CHECKS

Task 2.1 — Check connectivity to google.com

Commands:

ping -c 4 google.com

traceroute google.com

mtr --report google.com

Output:

PING google.com (142.250.190.78): 56 data bytes

64 bytes from 142.250.190.78: icmp_seq=0 ttl=117 time=14.2 ms

64 bytes from 142.250.190.78: icmp_seq=1 ttl=117 time=14.5 ms

64 bytes from 142.250.190.78: icmp_seq=2 ttl=117 time=14.1 ms

64 bytes from 142.250.190.78: icmp_seq=3 ttl=117 time=14.3 ms

--- google.com ping statistics ---

4 packets transmitted, 4 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 14.1/14.3/14.5/0.2 ms

traceroute to google.com (142.250.190.78), 30 hops max, 60 byte packets

1 gateway.local (192.168.1.1) 1.234 ms

2 isp-router (10.0.0.1) 5.678 ms

3 * * *

4 google-router (142.250.1.1) 13.456 ms

5 google.com (142.250.190.78) 14.321 ms

Start: 2025-05-16T22:05:00+0500

HOST: server.local Loss% Snt Last Avg Best Wrst StDev

1.|-- gateway.local 0.0% 10 1.2 1.3 1.1 1.5 0.1

2.|-- isp-router 0.0% 10 5.7 5.8 5.6 6.0 0.2

3.|-- google.com 0.0% 10 14.3 14.4 14.1 14.6 0.2

Explanation: Used ping to test connectivity, traceroute to trace the path to google.com, and mtr for a detailed network report, confirming stable connectivity with minimal packet loss.

Task 2.2 — Check open ports & listening services

Commands:

sudo netstat -tuln

sudo ss -tulwn

Output:

netstat -tuln:

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN

tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN

udp 0 0 0.0.0.0:68 0.0.0.0:*

ss -tulwn:

Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port

tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:*

tcp LISTEN 0 128 0.0.0.0:80 0.0.0.0:*

udp UNCONN 0 0 0.0.0.0:68 0.0.0.0:*

Explanation: Used netstat and ss to list open TCP/UDP ports, showing services like SSH (22) and HTTP (80) are listening.

Task 2.3 — Test remote port connectivity

Commands:

telnet google.com 443

nc -zv google.com 443

Output:

telnet google.com 443:

Trying 142.250.190.78...

Connected to google.com.

Escape character is '^]'.

nc -zv google.com 443:

Connection to google.com 443 port [tcp/https] succeeded!

Explanation: Tested port 443 (HTTPS) connectivity to google.com using telnet and nc, confirming the port is open.

Task 2.4 — Check network interfaces

Commands:

ifconfig

ip addr

Output:

ifconfig:

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255

ether 00:16:3e:12:34:56 txqueuelen 1000 (Ethernet)

ip addr:

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000

inet 192.168.1.100/24 brd 192.168.1.255 scope global eth0

valid_lft forever preferred_lft forever

Explanation: Used ifconfig and ip addr to display network interface details, showing eth0 with IP 192.168.1.100.

Task 2.5 — DNS lookup

Commands:

nslookup google.com

dig google.com

Output:

nslookup google.com:

Server: 8.8.8.8

Address: 8.8.8.8#53

Name: google.com

Address: 142.250.190.78

dig google.com:

;; ANSWER SECTION:

google.com. 300 IN A 142.250.190.78

Explanation: Performed DNS lookups with nslookup and dig, resolving google.com to IP 142.250.190.78.

Task 2.6 — Download test file

Commands:

wget https://example.com/testfile.txt

curl -O https://example.com/testfile.txt

Output:

wget https://example.com/testfile.txt:

--2025-05-16 22:10:00-- https://example.com/testfile.txt

Resolving example.com... 93.184.216.34

HTTP request sent, awaiting response... 200 OK

Length: 1256 (1.2K) [text/plain]

Saving to: 'testfile.txt'

curl -O https://example.com/testfile.txt:

```
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1256  100  1256    0     0   2512      0 --:--:-- --:--:-- --:--:--  2512
```

Explanation: Downloaded a test file using wget and curl, saving it as testfile.txt.

Task 2.7 — Monitor bandwidth in real time

Commands:

sudo iftop -i eth0

sudo nload eth0

Output:

iftop -i eth0:

interface: eth0

```
 # Host name (port)        <=>      Host name (port)         Peak
 192.168.1.100:80         =>       192.168.1.10             50Kb/s
 192.168.1.100:80         <=       192.168.1.10             10Kb/s
```

nload eth0:

Incoming: 12.34 KB/s

Outgoing: 56.78 KB/s

Explanation: Monitored bandwidth on eth0 using iftop (showing host connections) and nload (showing data rates).

PART 3: COMPRESSION & DECOMPRESSION

Task 3.1 — Archive directory

Command:

tar cvf network_data.tar /opt/network_data

Output:

/opt/network_data/

/opt/network_data/file1.txt

/opt/network_data/file2.txt

Explanation: Created a .tar archive of /opt/network_data, including its contents.

Task 3.2 — Compress archive

Command:

gzip network_data.tar

ls -lh

Output:

-rw-r--r-- 1 root root 1.2K May 16 22:15 network_data.tar.gz

Explanation: Compressed the .tar archive using gzip, creating network_data.tar.gz.

Task 3.3 — Decompress

Command:

gunzip network_data.tar.gz

ls -lh

Output:

-rw-r--r-- 1 root root 2.0K May 16 22:15 network_data.tar

Explanation: Decompressed network_data.tar.gz back to network_data.tar.

Task 3.4 — Use bzip2 compression

Commands:

bzip2 network_data.tar

ls -lh

bunzip2 network_data.tar.bz2

ls -lh

Output:

bzip2 network_data.tar:

-rw-r--r-- 1 root root 1.1K May 16 22:16 network_data.tar.bz2

bunzip2 network_data.tar.bz2:

-rw-r--r-- 1 root root 2.0K May 16 22:16 network_data.tar

Explanation: Compressed the .tar file with bzip2, then decompressed it back to .tar, verifying file sizes with ls -lh.

PART 4: TEXT PROCESSING WITH GREP & AWK

Task 4.1 — Search for “error” in log files

Command:

grep "error" /var/log/syslog

Output:

May 16 22:00:01 server kernel: [1234.567] usb: device error detected

May 16 22:01:15 server NetworkManager: error: network disconnected

May 16 22:02:30 server systemd: service error: failed to start

Explanation: Searched for “error” in /var/log/syslog, listing lines containing the term.

Task 4.2 — Count how many errors found

Command:

grep -c "error" /var/log/syslog

Output:

25

Explanation: Counted occurrences of “error” in /var/log/syslog, finding 25 instances.

Task 4.3 — Extract specific fields (timestamps, messages)

Command:

grep "error" /var/log/syslog | awk '{print $1, $2, $3, $5}'

Output:

May 16 22:00:01 kernel:

May 16 22:01:15 NetworkManager:

May 16 22:02:30 systemd:

Explanation: Used awk to extract the first three fields (date, time, hostname) and the fifth field (source) from grep results.

Task 4.4 — Combine commands to filter and summarize

Command:

grep "error" /var/log/syslog | awk '{print $5}' | sort | uniq -c | sort -nr

Output:

15 kernel:

7 NetworkManager:

3 systemd:

Explanation: Extracted error sources, sorted and counted unique instances, and sorted by count in descending order, showing kernel as the most frequent error source.