📚 **Troubleshooting in Linux**📚

Article by – Krishan Bhatt

1. Identify the Issue: Suppose you're unable to connect to the internet.

2. Check Network Configuration:

- Use the command ifconfig or ip addr to check the network interface status.

- Ensure that the interface is up and has an IP address assigned.

3. Ping Test:

- Use the ping command to test connectivity to a known website or IP address:

```
ping www.example.com
```

3.

- If ping fails, it indicates a problem with the network connection.

4. Check DNS Configuration:

- Verify DNS resolution by pinging an IP address directly:

```
ping 8.8.8.8
```

4.

- If successful, the issue might be with DNS configuration. Check /etc/resolv.conf for correct DNS server settings.

5. Firewall Settings:

- Check firewall rules using iptables or firewall-cmd (depending on your Linux distribution).
- Ensure that outgoing traffic is not blocked.

6. Network Service Status:

- Check the status of network-related services such as NetworkManager or systemd-networkd.
- Restart the service if necessary:

sudo systemctl restart NetworkManager

7. Hardware Check:

- Ensure that the network cable is properly connected (for wired connections).
- For wireless connections, ensure that the wireless adapter is enabled and connected to the correct network.

8. Driver Issues:

- Check if the appropriate drivers are loaded for your network interface:

lspci -nnk | grep -i net -A2

8.

- Look for any errors indicating missing or malfunctioning drivers.

9. Logs:

- Check system logs for any relevant error messages:

dmesg | grep -i error

9.

- Look for errors related to network interfaces or connectivity.

10. Additional Tools:

- Use tools like traceroute or mtr to diagnose network routing issues.
- netstat can help in examining network connections and listening ports.

11. Check Network Interface Status:

- Use the command ifconfig or ip addr to check if the network interface is in the UP state and has the correct IP configuration.

12. Restart Networking Service:

- Sometimes restarting the networking service can resolve issues:

```
sudo systemctl restart networking
```

13. Check Network Configuration Files:

- Verify configuration files like /etc/network/interfaces for correct network settings, especially if you're using a static IP configuration.

14. Check Routing Table:

- Use the route command to examine the routing table:

```
route -n
```

14.

- Ensure that the default gateway is set correctly.

15. DNS Troubleshooting:

- Use the nslookup or dig command to troubleshoot DNS resolution:

```
nslookup example.com
dig example.com
```

15.

- Verify that DNS servers are reachable and returning the correct information.

16. Check Network Connectivity with Specific Ports:

- Use the telnet or nc command to test connectivity to specific ports on remote servers:

```
telnet example.com 80
nc -vz example.com 443
```

17. Check Network Traffic:

- Use packet sniffing tools like tcpdump or Wireshark to inspect network traffic for abnormalities or errors:

```
sudo tcpdump -i <interface> -n icmp
```

18. Check Disk Space:

- Insufficient disk space can lead to various system issues. Use the df command to check disk space:

```
df -h
```

19. Check System Load:

- High system load can indicate resource exhaustion. Use the top or htop command to monitor system resource usage:

```
top
```

20. Check Log Files:

- Examine log files in /var/log for any error messages related to networking, system services, or hardware:

```
tail -f /var/log/syslog
```

21. Check Permissions:

- Ensure that necessary files and directories have correct permissions, especially if services are failing to start:

```
ls -l /path/to/file
```

22. Check SELinux/AppArmor:

- If SELinux or AppArmor is enabled, check their logs and policies to ensure they're not blocking network operations unintentionally.

23. Check System Health:

- Use monitoring tools like sar or vmstat to monitor system health metrics like CPU, memory, and disk usage:

```
sar -u
```

24. Check System Updates:

- Ensure that the system is up-to-date with the latest patches and updates:

```
sudo apt update && sudo apt upgrade
```

25. Check Hardware Health:

- Use tools like smartctl to check the health of storage devices:

```
sudo smartctl -a /dev/sda
```

26. Check for Malware:

- Scan the system for malware using antivirus tools like clamscan.

27. Check System Clock:

- Ensure that the system clock is synchronized with a reliable time source:

```
timedatectl status
```

28. Check Filesystem Integrity:

- Use the fsck command to check and repair filesystem integrity issues:

```
sudo fsck /dev/sda1
```

29. Check Kernel Parameters:

- Examine and adjust kernel parameters if necessary, especially related to networking:

```
sysctl -a | grep net
```

30. Consult Documentation and Online Resources:

- Refer to official documentation, forums, and community resources for specific issues or error messages encountered.

31. Check Network Interface Status:

- Use commands like ifconfig, ip addr, or ip link to check the status of network interfaces. Ensure that the interfaces are up and running.

32. Restart Network Interface:

- Sometimes restarting a network interface can resolve connectivity issues:

sudo ifdown <interface>

sudo ifup <interface>

33. Check Network Configuration Files:

- Verify configuration files like /etc/network/interfaces or /etc/sysconfig/network-scripts/ifcfg-<interface> for correct network

settings, including IP address, subnet mask, gateway, and DNS servers.

34. Check Routing Table:

- Use the route command to examine the routing table:

route -n

- Ensure that the correct routes are configured, especially the default gateway.

35. Check ARP Table:

- Use the arp command to view the Address Resolution Protocol (ARP) cache:

arp -a

- Verify that the MAC addresses are correctly mapped to IP addresses.

36. Check Firewall Settings:

- Verify firewall rules using tools like iptables or firewall-cmd to ensure that they're not blocking necessary network traffic:

sudo iptables -L

sudo firewall-cmd --list-all

37. Check Network Services:

- Verify that essential network services like DHCP, DNS, and NTP are running:

sudo systemctl status dhcpd

sudo systemctl status named

sudo systemctl status ntpd

38. Check DNS Configuration:

- Verify DNS resolution by using tools like nslookup or dig to query DNS servers:

nslookup example.com

dig example.com

- Ensure that DNS servers are reachable and returning the correct information.

39. Check Network Connectivity with Other Devices:

- Test network connectivity by pinging other devices on the same network to isolate the issue:

ping <IP_address>

40. Check Cable Connections:

- For wired connections, ensure that cables are securely connected to both the computer and the network switch or router.

41. Check Wireless Connection:

- For wireless connections, ensure that the correct SSID and passphrase are configured, and the wireless adapter is enabled:

sudo iwconfig

42. Check Network Logs:

- Examine log files in /var/log for any error messages related to networking, such as syslog or messages:

tail -f /var/log/syslog

43. Check Network Performance:

- Use tools like ping, traceroute, or mtr to diagnose network performance issues, such as packet loss or latency.

44. Check Bandwidth Usage:

- Monitor bandwidth usage using tools like iftop or nload to identify any abnormal traffic patterns or congestion.

45. Check for Network Hardware Failures:

- Verify that network hardware, such as network cards, cables, switches, and routers, are functioning correctly. Replace any faulty hardware if necessary.

46. Check Physical Volumes (PVs):

- Use the pvdisplay command to check the status of physical volumes:

pvdisplay

- Verify that all physical volumes are in the correct state and not experiencing any errors.

47. Check Volume Groups (VGs):

- Use the vgdisplay command to examine the status of volume groups:

vgdisplay

- Ensure that volume groups are active and have sufficient free space.

48. Check Logical Volumes (LVs):

- Use the lvdisplay command to view the attributes of logical volumes:

lvdisplay

- Verify the status and size of logical volumes.

49. Check LVM Metadata:

- Use the pvck, vgck, and lvck commands to check the consistency of LVM metadata:

pvck /dev/sdX

vgck <volume_group_name>

lvck <logical_volume_path>

50. Check LVM Configuration Files:

- Verify the contents of configuration files like /etc/lvm/lvm.conf for any misconfigurations or inconsistencies.

51. Check Disk Health:

- Use tools like smartctl to check the health of physical disks:

smartctl -a /dev/sdX

- Replace any failing disks to prevent data loss.

52. Check for Failed Disk Devices:

- Identify and replace any failed or missing disk devices in the volume group:

vgdisplay --partial

53. Check File System Integrity:

- Use tools like e2fsck or xfs_repair to check and repair the integrity of ext2, ext3, or XFS file systems residing on logical volumes:

sudo e2fsck -f /dev/mapper/<volume_group>-<logical_volume>

sudo xfs_repair /dev/mapper/<volume_group>-<logical_volume>

54. Check LVM Snapshots:

- Ensure that LVM snapshots are properly managed and not consuming excessive disk space:

lvdisplay --maps

55. Check Disk Space Usage:

- Use the df command to check disk space usage on logical volumes:

df -h

- Identify any volume group or logical volume that is running out of space.

56. Check LVM Events and Logs:

- Examine LVM-related logs in /var/log/messages or /var/log/syslog for any error messages or warnings.

57. Check for Disk Read/Write Errors:

- Monitor disk I/O errors using tools like dmesg or smartctl to identify potential disk failures or connectivity issues.

58. Check LVM Performance:

- Evaluate LVM performance using tools like iostat, vmstat, or sar to identify any bottlenecks or performance issues.

59. Check for External Factors:

- Consider external factors such as power outages, hardware failures, or software updates that may have affected LVM functionality.

60. Consult LVM Documentation and Community Resources:

- Refer to official LVM documentation and online forums for additional guidance and troubleshooting tips specific to your issue.

- Examine system logs located in /var/log (e.g., syslog, messages, auth.log) for any error messages or warnings that may indicate the cause of the issue:

tail -n 100 /var/log/syslog

62. Check Process Status:

- Use the ps command to check the status of running processes. Look for any processes that are consuming excessive CPU or memory resources:

ps aux | grep <process_name>

63. Check Disk Space:

- Use the df command to check disk space usage on the filesystems:

df -h

- Identify any filesystems that are running out of space and may be causing issues.

64. Check Memory Usage:

- Use the free command to check memory usage and available memory:

```
free -h
```

- Identify any memory-intensive processes or memory leaks.

65. Check CPU Usage:

- Use the top command to monitor CPU usage in real-time:

```
top
```

- Identify any processes consuming high CPU resources.

66. Check for Hanging Processes:

- Use the ps command with the H option to display hierarchical process trees and identify any hanging processes:

```
ps auxf
```

67. Check for Stuck I/O Operations:

- Use tools like iotop or atop to monitor disk I/O operations and identify any processes causing high disk activity:

iotop

68. Check Network Connectivity:

- Use the ping command to test network connectivity to external hosts or IP addresses:

ping <host_or_ip>

69. Check DNS Resolution:

- Test DNS resolution using tools like nslookup or dig to ensure that DNS servers are resolving domain names correctly:

nslookup example.com

70. Check Firewall Rules:

- Verify firewall rules using tools like iptables or firewall-cmd to ensure that they're not blocking necessary network traffic:

sudo iptables -L

sudo firewall-cmd --list-all

71. Check for Pending Software Updates:

- Use package management tools like apt, yum, or dnf to check for available updates and ensure that the system is up-to-date:

sudo apt update

sudo apt list --upgradable

72. Check User Permissions:

- Verify that users have the necessary permissions to access files and directories:

ls -l /path/to/file

73. Check System Time and Date:

- Ensure that the system time and date are accurate. Use the date command to check and adjust the system time if necessary:

date

74. Check Hardware Health:

- Monitor hardware health using tools like smartctl for disk drives or hardware monitoring utilities provided by the server manufacturer.

75. Check for Malware:

- Scan the system for malware using antivirus tools like clamscan to detect and remove any malicious software.

76. Check Configuration Files:

- Review system configuration files (e.g., /etc/hosts, /etc/resolv.conf, /etc/network/interfaces) for any misconfigurations that may be causing issues.

77. Check for Pending Reboots:

- Verify if a system reboot is pending after recent updates or configuration changes:

sudo needs-restarting

78. Check for Recently Installed Software:

- Identify and uninstall any recently installed software packages that may be causing conflicts or issues.

79. Check for Recent System Changes:

- Consider any recent changes to the system configuration, software installations, or updates that may have triggered the issue.

80. Consult Online Resources and Documentation:

- Search online forums, communities, and official documentation for solutions to common Linux issues and troubleshooting tips specific to your problem.