CompTIA Linux+: Troubleshooting

Troubleshooting Networks

Andrew Mallett
Author and Trainer

@theurbanpenguin www.theubanpenguin.com

Overview

Welcome to the troubleshooting course

Course Overview

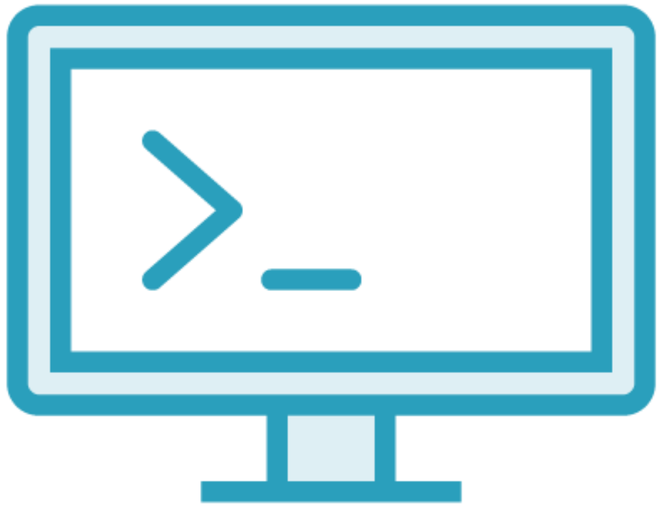
- Networks
- Memory / CPU
- Storage
- User Access
- Systemd

In Networking

- Name resolution
- Interface
- Firewalls

Lab Systems

Distribution Agnostic Lab Systems



CompTIA recommend using a mix of distributions, we include

- Alma Linux 8.5 (RHEL Rebuild)
- Ubuntu 20.04 LTS
- openSUSE Leap 15.2

We use Vagrant and VirtualBox for these machines, the Vagrantfile is available from Git.

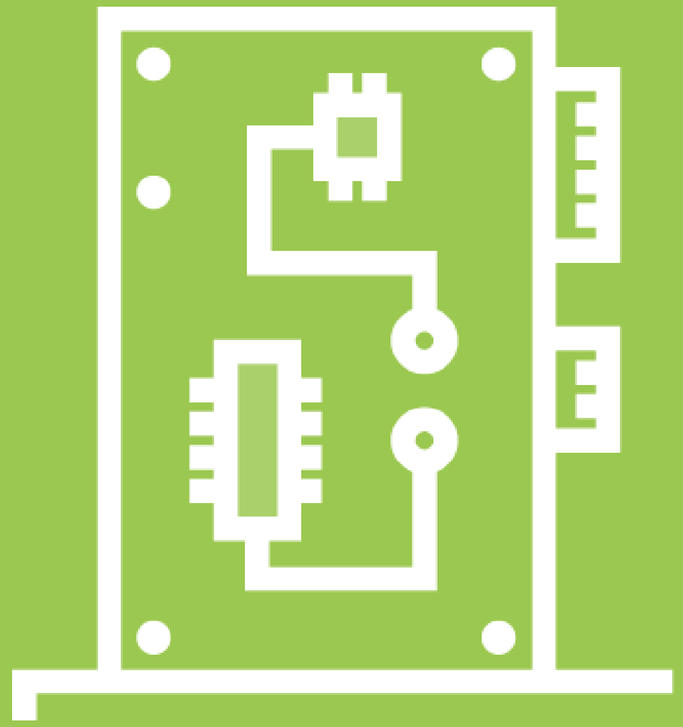
git clone https://github.com/theurbanpenguin/comptia-automation

Demo

For the first demonstration:

- Start the virtual machines
- Verify connectivity

NIC Issues



Dropped Packets

If your NIC (Network Interface Card) or port is playing up, you may be dropping packets cause packets to be re-sent and affect network performance.

```
$ ip -s link show enp0s8
$ cat /proc/net/dev
$ column -t /proc/net/dev
```

Viewing Dropped Packets

The main command is ip -s link, however we can interrogate the base file and introduce the column command.

Demo

Let's look for the command line:

- Check statistics from the NIC
- View raw data

Analyze Network Bandwidth

Network Bandwidth

We can monitor the packet and bandwidth available from the Linux CLI. We also need to check the speed of network devices that we are connected to and the type of device it is - switch vs hub.

```
$ sudo apt install -y nload
$ nload enp0s3
$ ethtool enp0s3
```

Install Nload and View Current Bandwidth and NIC Speed

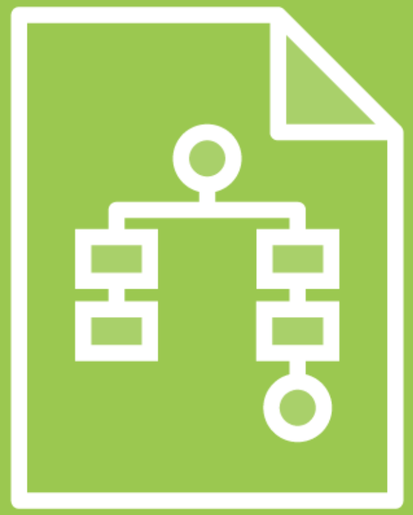
The CLI command nload is used to monitor the current bandwidth. The view the speed and configuration of a NIC we can use ethtool.

Demo

Checking Bandwidth:

- Check speed of NIC
- View current bandwidth

Resolve Host Names



Hostname Resolution

Hostname resolution may cause us issues too. Using the systemd tool, resolvectl, there is a lot we can diagnose as well as using tools such as dig and getent.

```
$ grep hosts /etc/nsswitch.conf
```

Ideally, DNS is Used Before Files

The default configuration allows the host files to be read before DNS. One would expect exploits to happen for easily on a server file than in DNS, misconfigured host records can expose your systems.

```
$ reslovectl
$ resolvectl query www.pluralsight.com
$ resolvectl dns enp0s3
$ sudo resolvectl dns enp0s8 1.0.0.1
```

Using Resolvectl

The CLI command resolvectl is part of the systemd eco-system and allows us the view annd configure DNS settings.

Demo

Checking Name Resolution:

- /etc/nsswitch.conf
- getent hosts
- dig
- resolvectl

Test Network Access and Network Configuration Issues

Network Access

A simple network test can be maintained with ping. If access via ICMP is not allowed pings will fail. Misconfigured network configuration may have us on the incorrect subnet.

```
$ ping $(/sbin/ip route show | awk '/default/ { print $3 }')
```

Automate Ping of Default Gateway

Automation is always great, often the first step in debugging network access is to ping the default gateway. This clever hack automates the resolution of the default gateway for ping.

```
$ ping 127.1
$ ping 1.1
```

You Don't Need All Octets

If the middle octets are all zeros in an IPv4 address, they can be omitted. This can be shown with the loopback address but is more useful on the Cloudflare DNS server 1.0.0.1. This is configured to accept ICMP pings.

```
$ ip -4 addr show
$ ip -4 route
```

Check Subnet Mask

The subnet mask can be seen in your route table or your address listing. If you have a misconfigured subnet mask you may not be able to connect to all hosts on your network.

```
$ echo net.ipv4.icmp_echo_ignore_all=1 | sudo tee /etc/sysctl.d/ping.conf
$ sudo sysctl --system
$ ping localhost
$ sudo apt install -y nmap
$ nmap -p 22 localhost
$ nmap -p 22 192.168.56.11-13
```

Port Scanning

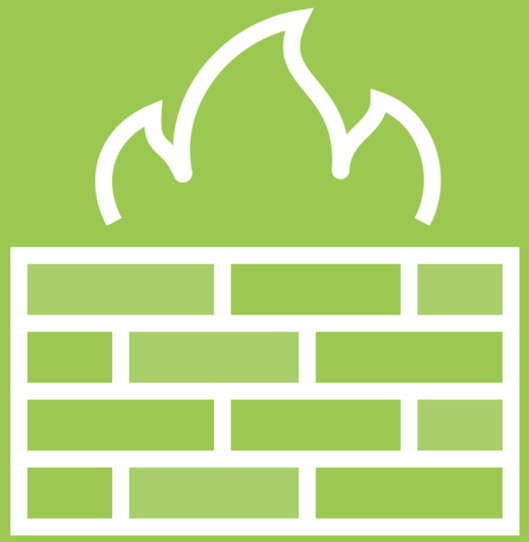
If ICMP is disabled on the hosts using the nmap port scanner may be an option but check it is allowed on your network.

Demo

Checking Network Access:

- Ping default gateway
- Shortened IPv4 addresses
- Disable ICMP
- Use nmap port scanner

Working With Firewalls



Firewall Issues

Firewalls can be useful, but they can also expose information about your system. The default firewall on RedHat based systems allows cockpit traffic through even if cockpit is not installed.

```
$ sudo systemctl start firewalld
$ sudo firewall-cmd --list-all
```

Enable Firewall AlmaLinux 8

The default firewall allows port 9090/tcp even though cockpit is not installed.

Working on OpenSUSE 15.2

```
$ sudo zypper in -y nmap
$ sudo nmap 192.168.56.11
```

On OpenSUSE

Installing nmap and scanning the default top 1000 ports will list 998 filtered ports, not allowed through firewall and 22/tcp open and 9090/tcp closed. This is a clue that it is RedHat based system without cockpit loaded.

Demo

Enable Firewall on AlmaLinux:

- Show what is allowed
- Scan from OpenSUSE
- Disable ICMP in Firewall

Summary

We have introduced network analysis as well as the troubleshooting course

- ip -s link
- nload
- ethtool
- resolvectl
- dig
- getent hosts
- ping 1.1
- ping $(/sbin/ip route show | awk '/default/ { print $3 }')
- nmap

Up Next:
Troubleshooting Memory and CPU Issues