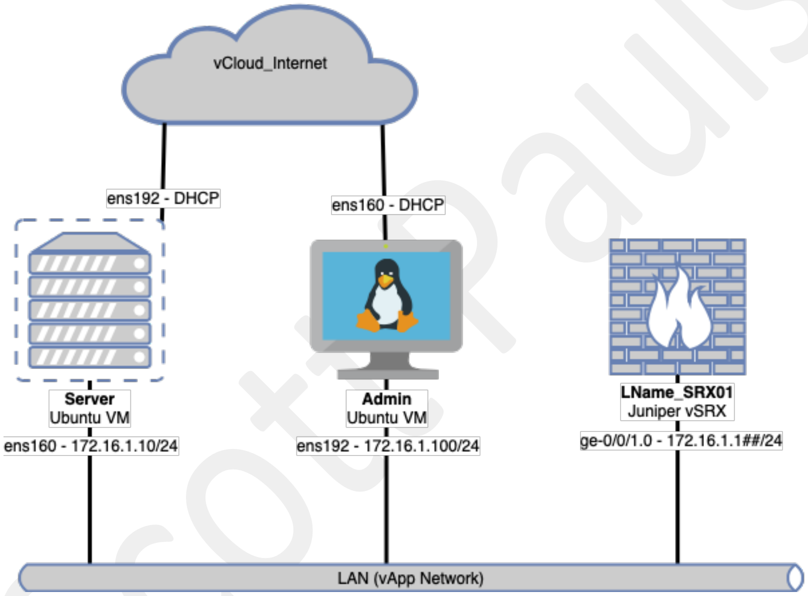
CSC387 Lab 10 – Juniper IP Services

Instructions

It's a bit of déjà vu in this lab – the big difference here is that we're working with Juniper. In this lab you'll set up LLDP, NTP, Syslog, and a few other Juniper services.

The following should be completed in the IA Lab Learn environment (http://ialab.dsu.edu). The vApp should already be deployed for you which includes the VMs and appropriate network cabling.

Network Diagram



Configuration Tasks/Notes

1. The VMs use the default credentials of **Password1!**

2. The IP addresses and interfaces on both Server and Admin are already configured for you. You only will need to set the IP address on the SRX.

3. Both the Server and Admin VMs are directly connected to the vCloud_Internet network. Log into both of them and authenticate to the captive portal. This will be imperative for NTP to work, it needs a real internet connection.

SRX01

1. Set the appropriate hostname on the SRX.

2. Configure the root account to have a password of **Password1!**

3. Create yourself a user account with the following guidelines:
    a. Name: **<first name>**
    b. Class: **super-user**
    c. Password: **Password1!**

4. Commit your config, then log out of the SRX and log back in with your own account. Your name needs to be visible in all screenshots so this will make that part easy.

4. Set the IP address to **172.16.1.101/24**.

5. Add the **ge-0/0/1.0** interface to the **trust** zone and make sure that all protocols and system-services are allowed in under host-inbound-traffic. The protocols and system-services statements are not there by default in the vSRX. Commit your config.

6. Ping from your admin VM to the SRX, it should be successful at this point.

7. Configure the device to allow SSH version 2 logins.

8. Commit your config.

Verification Step 1

LLDP

We're looking at having a multi-vendor setup in our environment. Let's start switching off of proprietary protocols.

1. Configure SRX01 to use LLDP.

2. Commit your config.

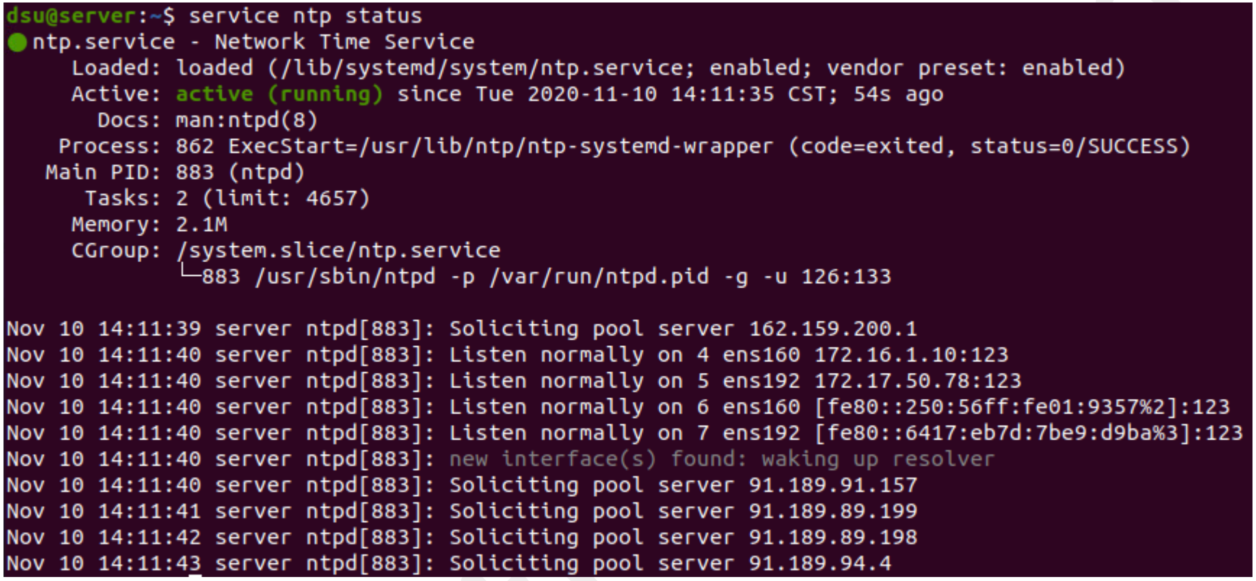
Verification Step 2

NTP

Before starting with centralized logging, you need to have accurate and precise time throughout your network.

1. Log into your server VM and ensure it is authenticated to the captive portal. You should be able to browse the web, ping Google, etc.

2. Make sure the NTP service is started and soliciting pools to your network. From the server, run **show ntp status** and your output should look something like this:



```
dsu@server:~$ service ntp status
● ntp.service - Network Time Service
     Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2020-11-10 14:11:35 CST; 54s ago
       Docs: man:ntpd(8)
    Process: 862 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
   Main PID: 883 (ntpd)
      Tasks: 2 (limit: 4657)
     Memory: 2.1M
     CGroup: /system.slice/ntp.service
             └─883 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 126:133

Nov 10 14:11:39 server ntpd[883]: Soliciting pool server 162.159.200.1
Nov 10 14:11:40 server ntpd[883]: Listen normally on 4 ens160 172.16.1.10:123
Nov 10 14:11:40 server ntpd[883]: Listen normally on 5 ens192 172.17.50.78:123
Nov 10 14:11:40 server ntpd[883]: Listen normally on 6 ens160 [fe80::250:56ff:fe01:9357%2]:123
Nov 10 14:11:40 server ntpd[883]: Listen normally on 7 ens192 [fe80::6417:eb7d:7be9:d9ba%3]:123
Nov 10 14:11:40 server ntpd[883]: new interface(s) found: waking up resolver
Nov 10 14:11:40 server ntpd[883]: Soliciting pool server 91.189.91.157
Nov 10 14:11:41 server ntpd[883]: Soliciting pool server 91.189.89.199
Nov 10 14:11:42 server ntpd[883]: Soliciting pool server 91.189.89.198
Nov 10 14:11:43 server ntpd[883]: Soliciting pool server 91.189.94.4
```

3. From the admin VM, browse to the server at http://172.16.1.10. You should be able to see the server's current time.

4. Set your SRX's time zone to be **America/Chicago**.

5. Commit your config.

6. In order for your time to sync to NTP, it must be reasonably close to the NTP clock. Update your firewall's time to be close to the server using the **set date** command from operational mode. Within a couple of minutes should be fine.

   Note: the vSRX uses a slightly different datetime format than the physical SRXs. Enter your time as **YYMMDDhhmm.ss**

7. Verify your SRX's time is close by running **show system uptime**. If your firewall's clock is not close to the NTP server's time, do not proceed until you set it correctly.

8. The NTP server is unauthenticated. Configure your SRX to connect to the NTP server via **172.16.1.10** using **version 4**.

9. Commit your config. It can take ~5 minutes or so for an NTP association to be made and sync the clocks.

Verification Step 3

Syslog

After you have successfully synced your firewall's clock to the NTP server, you can start pushing log files to syslog.

1. Configure your firewall's logging to go to the host **172.16.1.10**
    a. Log from **any** source and use the **notice** level

2. Prefix all of your log messages with your firewall's IP address.

3. Commit your config.

Verification Step 4

SNMP

After you've successfully confirmed that your firewall is pushing its log files to the syslog server, you need to read SNMP information from it.

1. Perform all SNMP configuration from the **[edit snmp]** level of the config.

2. Configure the SNMP server contact information with your name.

3. Configure your SRX with the SNMP community string of **dsu** and set the permissions with:
    a. Authorization: **read-only**
    b. Clients: **172.16.1.0/24**
    c. Clients Restrict: **0.0.0.0/0**

4. Commit your config.

Verification Step 5

J-Web

As you get into more advanced firewall configuration tasks, you'll need to have access to the web interface, J-Web.

1. Make sure HTTPS web-management is enabled as a system service on the SRX.

2. Log into J-Web from your admin VM. If you are brought to the configuration wizard, delete the **system autoinstallation** line from your config. Commit, then refresh the page and see if you can get into J-Web.

3. Once you are in J-Web, browse to **Configure → CLI Tools → CLI Viewer**.

Verification Step 6

Verification Steps

1. SSH into the SRX from your admin VM and authenticate. You should be able to remotely configure this device now through SSH.
2. On the SRX, run **show lldp detail** from operational mode. You should see that the protocol is enabled.
3. At the SRX's operational mode, run **show ntp associations**. You should see an ***** next to the NTP server's IP. If the * is there, run a **show system uptime** and the Time Source field will show **NTP CLOCK**.
4. Browse to http://172.16.1.10 from your admin VM. You should be able to see syslog entries displayed on the webpage. The syslog entry will have the log time as well as your firewall's IP as the source of the message.
5. After you've enabled the SNMP community string on your firewall, refresh the http://172.16.1.10 page and you should see that the server pulled your contact name and hostname of the SRX back.
6. You should be able to see your entire SRX config and copy/paste it to a text file if you'd like a backup.

What to Turn In

Go through each of the verification steps and take a screenshot. Please try to show each step in a single, clear screenshot to cut down the number of images. Also, paste all screenshots into a single Word/PDF document. Do not upload them to D2L as individual images – I won't grade them.