Albert Morris
October 29, 2019

Installing Qradar videos used:
https://www.youtube.com/watch?v=i-qA3-b6_ME
https://www.youtube.com/watch?v=2ButNPY4nLQ
Qradar's documentation on how to install Qradar Community Edition:
https://developer.ibm.com/qradar/wp-content/uploads/sites/89/2018/08/b_qradar_community_edition.pdf

Download and Installing Qradar CE

1. Download CentOS 7.5 and Qradar.iso
    a. https://developer.ibm.com/qradar/ce/
2. When installing it, make sure the domain name is **qradar.local**,internet is wired(ethernet) ,DHCP is disabled and the internet is set to grab the existing static setting by default.
3. Make sure it has 8GB of swap
    a. To do this, when formatting the drive for the new partitions, take one Gigabyte off the hard drive to have enough space to add that extra Gigabyte to the Swap.
4. Transfer the QradarCE, 3.7 GB .iso file to the centos with a program like filezilla through SFTP.
5. Follow this command once file is transfered
    a. Cd /tmp (where you should store the file)
    b. Chmod 777 Qradar….
    c. Mount Q(tabcomplete) /media/
    d. /media/setup
    e. Reboot
    f. Mount Q(tabcomplete) /media/
    g. /media/setup
    h. Service tomcat restart

Visit the website: https://QradarsIPaddress/console
To get to the console, (step 10 in installation guide)

Port Mirroring - Configuring it on CentOS

1. Run ip add and look at the last interface
2. Plug in the ethernet adapter through the USB
3. Run IP add and see search for a new interface that is in status down. The name in our case was enp0s20u3
4. Run this command to see if any data is going through the device:
    a. ip -s link show enp0s20u3
5. If there are numbers other than 0 and 0 coming across the
6. Navigate to /etc/sysconfig/netwrok-scripts/
7. Generate a new unique identifier (UUID) for the interface and take note of the number
    a. uuidgen enp0s20u3
8. Copy the config of the existing interface
    a. cp ifcfg-em1 ifcfg-enp0s20u3
9. Delete everything and fill in the following information which is found in the interface
    a. # WARNING: Please use qchange_netsetup to make changes to this file
    b. TYPE=Ethernet
    c. NAME=enp0s20u3
    d. UUID=39d8e013-20fe-40b5-84ce-4274f492e90c
    e. DEVICE=enp0s20u3
    f. ONBOOT=yes
    g. HWADDR=00:50:b6:e5:7b:42
10. Run this command to get the interface up
    a. Ifup NameOfTheInterface
11. Run this command again on the same interface to test if there is any data flowing through it
    a. ip -s link show enp0s20u3
12. Restart the whole computer

In Qradar- Add a flow Source

1. Admin>Data Sources>expand the Data Sources tab> Flows
2. Click on Flow sources
3. Add
4. On the type: pick Network Interface Card
    a. Pick the second card (which will be the same interface we just set up)
5. https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/t_qradar_adm_add_flow_source.html

Shipping Linux logs

1. In the linux server navigate to /etc/rsyslog.cnf
    a. At the bottom insert
        i. *.* @ipAddress:port#
2. Good resource: https://help.papertrailapp.com/kb/configuration/configuring-remote-syslog-from-unixlinux-and-bsdos-x
3. Possible tool to use:
    a. https://www.syslog-ng.com/

Installing Pulse

1. Download online from the IBM helper once IBM account is bound which takes a process of creating a security token and a few more steps followed on IBM's documentation
    a. https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.Pulseapp.doc/t_Qapps_PulseDashboard_install.html
2. Download from IBM store online and import it through the web interface through the portal.
    a. On the QRadar Console, click **Admin** > **Extensions Management.**
    b. On the Extensions Management page, click **Browse** and select the app archive that you want to upload.
    c. Select Install immediately, and click **Add.**

Sources:

To create the new ifcfg
https://www.youtube.com/watch?v=hnACmk9n8SM
Add Flow Source (Qradar Docs)
https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/t_qradar_adm_add_flow_source.html