QRadar Community Edition V7.3.3 Launch

Shane Lundy
QRadar Offering Manager
IBM Security
Shane.Lundy1@ibm.com

Sree Ananthasayanam
Advisory Software Developer
IBM Security
Sree.Ananthasayanam@ca.ibm.com

Jose Bravo
NA Security Architect
IBM Security
jbravo@us.ibm.com

Jonathan Pechta
QRadar Support Content Lead
IBM Security
jonathan.pechta1@ibm.com

IBM **Security**

21 February 2020

IBM

Agenda

Announcements

- QRadar V7.3.3 Patch 2 is available on IBM Fix Central.
- 27 February 2020: Let's talk about the Log Source Management app

  Invitation: https://ibm.biz/logsourceinvite
- Official Support Forums are moving at the end March, more details coming soon. Bookmark the following IBM short URLs:

  https://ibm.biz/qradarceforums (QRadar Community Edition Q&A) or
  https://ibm.biz/qradarforums (QRadar Support Forum)
- New support pages coming soon for Parsing 101

About QRadar Community Edition

The QRadar Community Edition in 7.3.3 is now being delivered as an OVA file.

- Based off of QRadar 7.3.3 general availability (GA) build.
- The OVA download contains the CentOS Operating System preinstalled and bundled with the 7.3.3 QRadar Community Edition ISO.
- The QRadar Community Edition is based on a smaller footprint for non-enterprise use.
- The perpetual license is a low memory and includes a 50 events per second (EPS) and 5,000 Flows per minute.
- Apps are supported and can allocate 10% of the Console's memory.

0: Community Edition Support

- QRadar Community Edition is a forum support only product.
- An IBM id is required to use the forums.
- If you are an existing Full QRadar SIEM user, QRadar Support does not take cases for QRadar Community Edition installations.
- QRadar Community Edition is an export restricted product. If you have download issues or receive error 53e, additional checks are required before you can download the OVA file.

- Software updates (fix packs, interim fixes) are not available for QRadar Community Edition.
- Where to I find logs to troubleshoot my QRadar Community Edition instance?

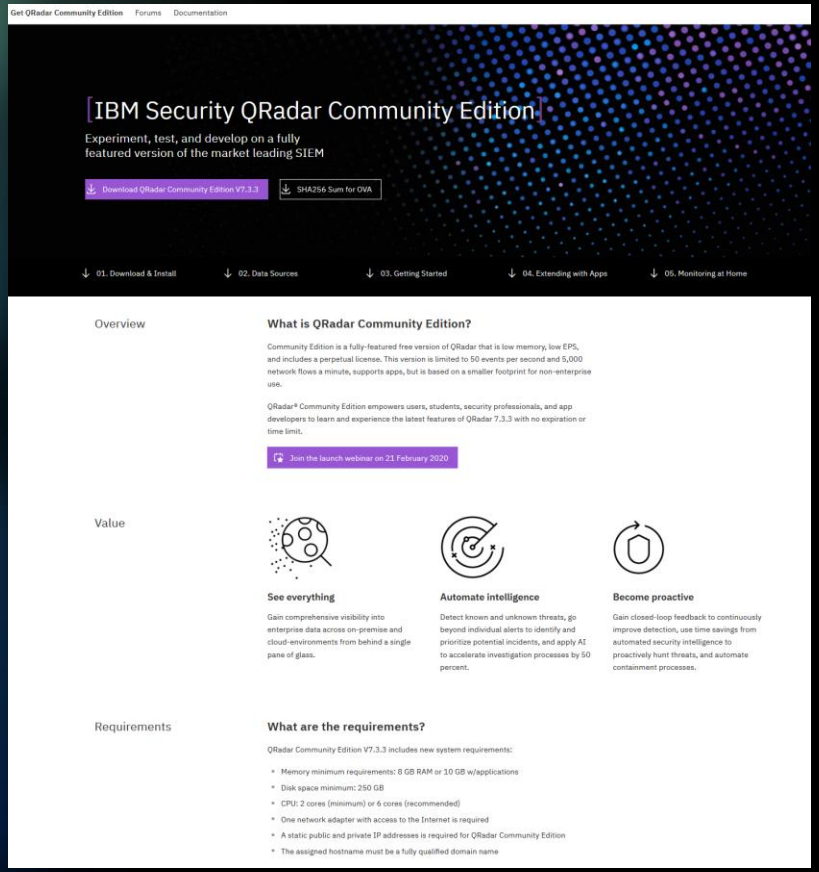
General

`/var/log/qradar.log`
OR
`/var/log/qradar.error`

Installation

`/var/log/setup-{version}/qradar_setup.log`

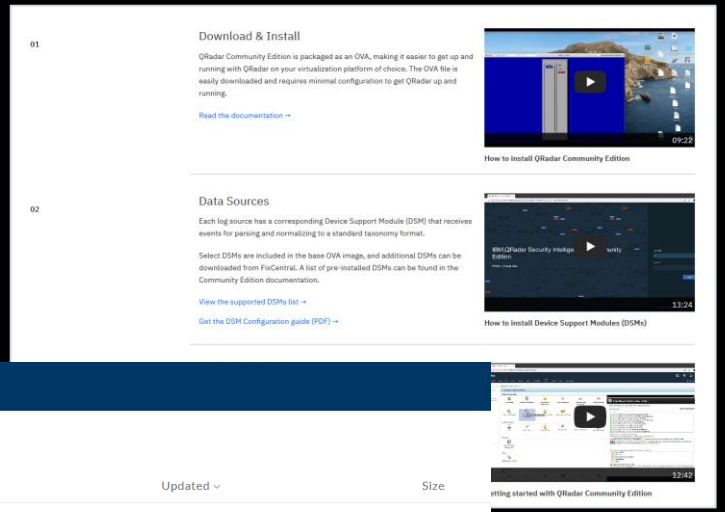
1: Read the documentation

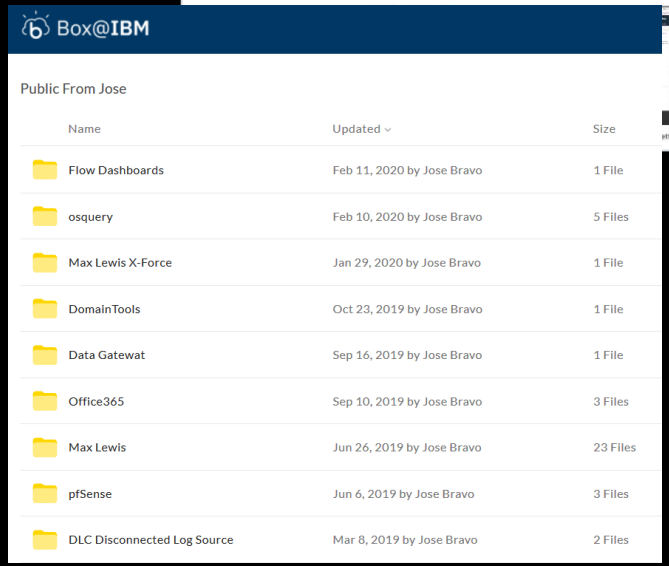


- New look for the download page.
- The Documentation and forums available in the menu at the top of the page.
- Start by reviewing **system requirements** and **network requirements** is crucial to your success.
- Network configuration is done during the OVA import or shortly after the import completes.

NOTE: The previous implementation required installation of CentOS iso followed by the QRadar installation. Networking was part of this process.

2: OVA & install video tips





- The Open Virtual Appliance (OVA) format is a tar file containing the CentOS operating system and the QRadar software ISO.
- Research virtualization products before you download and install:
  - Ease of setting networking configuration
  - Direct import for the OVA format
  - Cost
- Ensure the OVA file is downloaded in the correct format.
- Check the SHASUM 256 of your downloaded OVA file.
- Get more Jose videos: http://ibm.biz/jbravovideos

3: System requirement

Ensure to size your CPU, RAM, and disk storage specifications for future usage and additional applications.

- Minimum RAM: 8 GB
- Better: 10 GB (Ariel queries and X-Force tests)

8 / 10

Apps will use additional RAM. Each app has a ‘Memory required’ specification on the X-Force App Exchange.

10 %

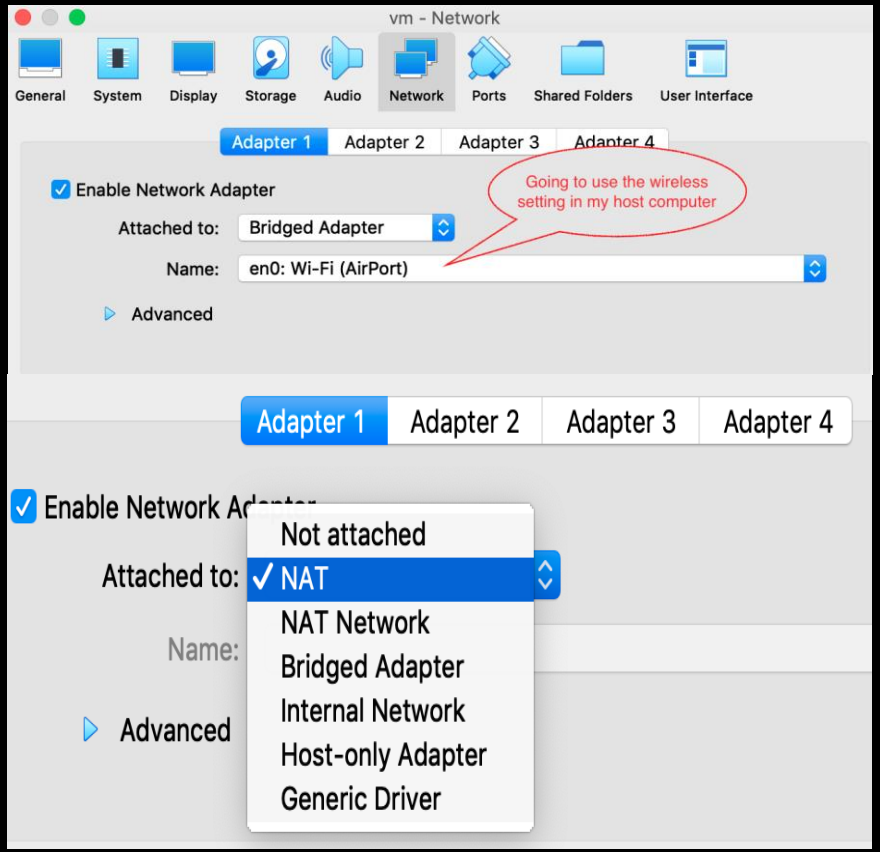
Minimum storage size requirements are enforced – minimum 250 GB during import

250 GB

- 2 CPU Core (minimum)
- 6 CPU cores (recommended)
- 8 CPU cores (Ariel / X-Force Rules)

2/6/8

4: Network configuration



Your network adapter must have Internet access.

1. Bridged Adapter
   - Use when you plan to limit usage to a single network. Can use the Wi-Fi or a wired connection of the host.
   - IP assigned based on the host network, hence direct access is possible
2. NAT
   - Use when multiple networks access is required
   - VM assigned IP is in a separate network
   - VM has external access, but direct external access is not possible
   - You must ensure port forwarding

5: Network requirements

1. Ensure Static Private and Public IP addresses are assigned to the VM
2. The hostname must be the Fully Qualified Domain Name
3. Network adapter with Internet access can ping an external IP address
4. Manually edit configuration to assign
   - Static IP
   - CIDR Netmask
   - Gateway
   - DNS values

& Network confirmation

1. To check for IP on the network adapter, type: **`ip a`**
2. To confirm the configured hostname, type: **`hostname`**
3. To check for Internet access, type: **`ping 9.9.9.9`**
4. To manually edit network configuration, type: **`nmtui`**

   NOTE: Network configuration values should be the same as the Host computer's Networking Details.

6: Troubleshooting errors

`Generating AUTO_INSTALL_INSTRUCTIONS file failed`

```
Complete!
/media/cdrom/inc/setup.funcs: line 3313: [: ==:
unary operator expected panic: runtime error: index
out of range

Goroutine 1 [running]:
q1git.canlab.ibm.com/pi/sisetup/mi.GetDefaultManage
mentInterface(0xc420085780, 0x0, 0x0,0x0)
  /builds/pi/sisetip/.gogradle/project_gopath
/src/q1git.canlab.ibm.com
  /builds/pi/sisetip/.gogradle/project_gopath
/src/q1git.canlab.ibm.com/pi/sisetup/main/go:22
+0x22
ERROR: Generating AUTO_INSTALL_INSTRUCTIONS file
failed.
The installation failed. Review your virtual
machine (VM) configuration, and then restart the
process on a new VM. For more information, see the
installation instructions.

[root@localhost ~]#
```

What does this mean?

- Generic message when the setup is aborted
- QRadar Community Edition generates a file that extracts and saves your configuration file as part of the installation process.
- If configuration is not set up correctly, the AUTO_INSTALL_INSTRUCTIONS file is not generated correctly.
- Fix the network configuration parameters before you start your QRadar Community Edition setup.

6: Troubleshooting errors (cont)

Generating AUTO_INSTALL_INSTRUCTIONS file failed

```
Complete!
/media/cdrom/inc/setup.funcs: line 3313: [: ==:
unary operator expected panic: runtime error: index
out of range

Goroutine 1 [running]:
q1git.canlab.ibm.com/pi/sisetup/mi.GetDefaultManage
mentInterface(0xc420085780, 0x0, 0x0,0x0)
  /builds/pi/sisetip/.gogradle/project_gopath
/src/q1git.canlab.ibm.com
  /builds/pi/sisetip/.gogradle/project_gopath
/src/q1git.canlab.ibm.com/pi/sisetup/main/go:22
+0x22
ERROR: Generating AUTO_INSTALL_INSTRUCTIONS file
failed.
The installation failed. Review your virtual
machine (VM) configuration, and then restart the
process on a new VM. For more information, see the
installation instructions.

[root@localhost ~]# hostname
localhost

[root@localhost ~]#
```

Issue

- Hostname is not a Fully Qualified Hostname (FQDN)
- To confirm hostname, type: **`hostname`**

To resolve

1. Import the ova
2. Assign the FQDN to the hostname and then run setup.

   $ hostname –f

   $ hostname $(hostname -f)

6: Troubleshooting errors (cont)

```
Generating AUTO_INSTALL_INSTRUCTIONS
file failed
```

```
[root@localhost ~]# ip a

1: lo: <LOOPBACK,UP, LOWER_UP> mtu 65536 qdisc
noqueue state UNKNOWN group default qlen 1000
  link/lookback 00:00:00:00:00:00
  brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu
1500 qdisc pfifo_fast state UP group default qlen
1000
  link/ether 00:00:27:24:46:b6
  brd ff:ff:ff:ff:ff:ff

[root@localhost ~]#
```

Issue

- Primary network adapter (enp0s17) has no IP assigned to it
- Run the command: **`ip a`**

To resolve

1. Recreate new vm with the correct configuration.
2. Manual edit network configuration with the **`nmtui`** command before you begin your QRadar Community Edition setup.
3. See product manual to configure a Static IP and networking correctly.

6: Troubleshooting errors (cont)

```
Generating AUTO_INSTALL_INSTRUCTIONS
file failed
```

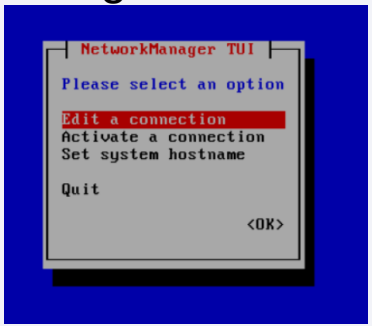
```
[root@localhost ~]# ping 9.9.9.9
connect: Network is unreachable

[root@localhost ~]#
```

Issue

- No Internet Access
- To check, type: **`ping 9.9.9.9`**

To resolve

1. Import the OVA file.
2. Confirm your network configuration with **`nmtui.`**



3. Follow on-screen to ensure correct network connections

7: Troubleshooting errors

Failed to run qradar_netsetup

```
Installing QRadar changes..
Activating system with key 3Q7xxx-5xxxxx-3xxxxx-
3xxxxx
Appliance ID is 300
Installing 'QRadar Community Edition' with id 300
Configuring network…
ERROR: Failed. Exit code: 1. Case 1.
ERROR:

ERROR: Failed to run qradar_netsetup.!
  (see log /var/log/setup-2019.14.0.2019031163225/
  qradar_setup.log for further details or use -h
  for help.
The installation failed. Review your virtual machine
(VM) configuration, and then restart the process on
a new VM. For more information, see the installation
instructions.


[root@localhost ~]#
```

Issue

- Reason for failure – internet connection to the vm is set incorrectly
- Network connection is incorrect
- External access is unavailable

To resolve

1. Import OVA and before running setup check network settings.
2. Confirm your network configuration with **`nmtui`**.
3. Manually edit configuration to assign Static IP, CIDR Netmask, Gateway and DNS values. These values should be the same as the Host computer's Networking Details.

8: Log in to QRadar Community Edition

- You can access QRadar Community Edition from a supported web browser:

  https://<ip_address>/console
  OR
  https://<dns>/console

- If you are using a locally hosted virtual machine with a local IP address, you can access QRadar Community Edition at:

  https://<ip_address>:8444/console
  OR
  https://<dns>:8444/console

- Login as administrator using username “admin” and the password you set

64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later
Microsoft Internet Explorer	11.0
64-bit Google Chrome	Latest

9: Event sources and DSMs

- Only select DSMs, protocols, and scanners are installed by default in QRadar Community Edition.
- QRadar Weekly Auto Updates is enabled for QRadar Community Edition.
- Users can run an update, then install DSMs and protocols from the user interface.

  Admin > Auto Update > Get New Updates

- Use the DSM Configuration Guide (linked on the QRadar Community Edition page) to ensure related protocols are installed and to configure your log sources.

Optionally, administrators can get default DSMs from the ISO file, but these might not be the latest RPMs.

1. Mount the ISO file.
2. Navigate to */media/cdrom/post/dsmrpms*
3. Specify rpm name you want to install.

```
[root@localhost ~]# sudo mount -o loop
/opt/ibm/cloud/iso/QRadarCE2019.14.0.20191031163225
.GA.iso /media/cdrom

[root@localhost ~]# cd /media/cdrom/post/dsmrpms

[root@localhost ~]# yum -y install DSM-Cisco
Umbrella-7.3-20200110194225.noarch.rpm

[root@localhost ~]# reboot
```

4. Ensure you reboot the VM after setup.

Demo and questions

Ask questions in the Q&A panel

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions