IBM Security QRadar Incident Forensics
Version 7.3.0

QRadar Packet Capture Users Guide

IBM

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 25.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.

Contents

About this Packet Capture User Guide

This documentation provides you with information that you need to install and configure IBM® QRadar® Packet Capture.

Intended audience

System administrators who are responsible for installing QRadar Packet Capture must be familiar with network security concepts and device configurations.

Technical documentation

To find IBM Security QRadar product documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. Introduction to QRadar Packet Capture

IBM Security QRadar Packet Capture is a network traffic capture and search application. The QRadar Packet Capture appliance has only one capture port (DNA0) and you can install either a 10G or 1G SFP transceiver.

With QRadar Packet Capture, you can capture network packets at rates up to 10 Gbps from a live network interface, and write them to files without packet loss.

You can use QRadar Packet Capture to search captured network traffic by time and packet envelope data. With sufficient appliance resources and tailored searches, you can use search and recorder data simultaneously without data loss.

QRadar Packet Capture appliances that have a 10G transceiver supports clusters, which expands the overall data storage and computational ability, when compared to a single standalone server. QRadar Packet Capture appliances that have a 1G transceiver do not support clusters.

QRadar Packet Capture capabilities

Some features included with QRadar Packet Capture:

Standard PCAP file format

A file format that is used to store network traffic. The file format integrates with existing third-party analysis tools.

High-performance packet-to-disk recording

Capture network packets from a live network.

Multi-core support

QRadar Packet Capture is designed for use with multi-core architectures.

Direct-IO disk access

QRadar Packet Capture uses direct IO access to disks to obtain maximum disk write throughput.

Real-time indexing

QRadar Packet Capture can produce an index automatically during packet capture. The index can be queried with Berkeley Packet Filter (BPF) like syntax and/or HTTP domain or base URL strings to quickly retrieve interesting packets in a specified time interval.

Cluster-capable to increase capture data capacity (10G edition only).

You can enable data nodes to create a cluster for added storage capacity.

Dump format

Capture files are saved in the standard PCAP format with time stamps in microsecond resolution. Capture files are stored in sequential order based on the file size. The capture files are stored in directories. When the space in the directory becomes full, the capture files are overwritten, based on preconfigured recording parameters.

Capture Speed

For packet capture appliances, the speed of capturing network traffic depends on whether you have data nodes attached to the master node:

- For packet capture appliances that don't have data nodes attached, the maximum capture speed is up to 7 Gbps.
- For packet capture appliances that have data nodes attached to the master node, the capture speed increases up to 10 Gbps.

For more information about forwarding packets to QRadar Packet Capture, see the *IBM Security QRadar Administration Guide*.

Related concepts:

Chapter 3, “Capture usage overview,” on page 7
To capture traffic to disk, start the capture application. The Recorder component saves the network traffic data into a pre-configured directory. When the space in the directory becomes full, existing files are overwritten.

Chapter 2. QRadar Packet Capture setup

Some basic configuration is required before you use IBM Security QRadar Packet Capture.

Supported web browsers

The following web browsers are supported:

- Google Chrome Version 44.0.2403.157 or later.
- Mozilla Firefox Version 40.0.3 or later.

Setting up your network

To make QRadar Packet Capture available remotely, an IP address must be assigned to one of the Ethernet ports, typically eth2, eth3, or eth4. By default, the system is configured to use DHCP. For initial configuration you might need to connect a VGA-compatible monitor.

For the initial configuration, carry out the following steps:

1. Turn on the QRadar Packet Capture appliance.
2. Use SSH and port 4477 to log in as the root user.

   The default user name is: `root`. The default password is: `P@ck3t08.`.

   To change the default password, see "Changing the operating system account password" on page 5.
3. To ensure that your system is up-to-date, apply available software fixes on IBM Fix Central (www.ibm.com/support/fixcentral/).
4. Configure a static IP address for your own network:
   a. To get the MAC address or the eth2 interface, type the following command:

      ```
      ifconfig | grep eth2
      ```

      The eth0 and eth1 interfaces are not available. Use eth2 for M4 xSeries hardware.

   b. Note the MAC address.

   c. Edit the settings in the `/etc/sysconfig/network-scripts/ifcfg-eth2` file:

      - Add the following text as the first line: `DEVICE=eth2`
      - Uncomment the MAC address of the eth2 port: `HWADDR=xx:xx:xx:xx:xx`
      - Ensure that the following setting is configured: `BOOTPROTO=static`
      - Ensure that you use information that is relevant to your network and that the output looks similar to the following static example:

        ```
        DEVICE=eth2
        #HWADDR=xx:xx:xx:xx:xx
        BOOTPROTO="static"
        BROADCAST="192.168.1.255"
        DNS1="0.0.0.0"
        DNS2="0.0.0.0"
        GATEWAY="192.168.1.2"
        IPADDR="192.168.1.1"
        NETMASK="255.255.255.0"
        NM_CONTROLLED="no"
        ONBOOT="yes"
        ```
5. Save the file.

6. To apply the settings, run the following command:

   ```
   service network restart
   ```

7. Verify your interface setting by running the following command:

   ```
   ifconfig | more
   ```

DHCP example: In CentOS6.2, edit the following settings in the /etc/sysconfig/network-scripts/ifcfg-eth0 file or the /etc/sysconfig/network-scripts/ifcfg-eth1 file.

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

Remote login

After you set up an IP address locally, you can administer the appliance by remotely logging on by using SSH on port 4477.

Configuring your license

Before you use QRadar Packet Capture, you must configure a license for the QRadar Packet Capture appliance and the QRadar Packet Capture software.

Procedure

1. To configure licensing for a QRadar Packet Capture appliance that has an SFP 1G transceiver installed, complete the following steps:
   a. Contact your IBM representative to obtain the license key for the master node.
   b. In QRadar Packet Capture, click **Help** > **Update Master License**.
   c. To apply a license to a QRadar Packet Capture appliance, paste the value into the **License Key** field.
   d. Paste the values for the **System ID** and **License Key** into their respective fields.
   e. Click **Update Master License** to apply the changes.
2. To configure licensing for a QRadar Packet Capture appliance that has an SFP+ 10G transceiver installed, complete the following steps:
   a. Contact your IBM representative to obtain a license key for your data nodes.
   b. In QRadar Packet Capture to apply the master license, click **Help** > **Update Master License**.
   c. Paste the values for **License Key** and **System ID** into their respective fields.
   d. Click **Update Master License** to apply the changes.
   e. Depending on the number of data nodes that you have in a cluster, you need to update by clicking **Help** > **Node1**.
   f. To update the data node licenses, paste the values for **License Key** and **System ID** into their respective fields.
   g. To update the data node, click **Update Node1 License** to apply the changes.

Administering users

To enable users to access and use IBM Security QRadar Packet Capture, you must add a user, assign them an appropriate role, and configure their login credentials.

Before you begin

Make sure that you are logged into QRadar Packet Capture as the `root` user. Or alternatively, ensure that you can use a `sudo` command to create a user.

Procedure

1. To create a user, run the following command:

   ```
   ./usr/local/nc/bin/nc_user_manager add <username> <password>
   <Admin|Guest>
   ```

   If there is already an existing user name <*username*> this command fails.

   If the role specified is neither admin nor guest this command fails.

   When a user is added, you can use the same username and password for both product login and REST API login.
2. To delete a user, run the following command:

   ```
   ./usr/local/nc/bin/nc_user_manager delete <username> <password>
   ```

   If there is already an existing user name <*username*> this command fails.

   This command fails if the <*username*> and <*password*> do not match what is recorded in QRadar Packet Capture.

   When a user is deleted, you can use the same username and password for both product login and REST API login.

Changing the operating system account password

After you set up the appliance, change the default operating system password for IBM Security QRadar Packet Capture.

You must be `root` user to change the operating system account.

The QRadar Packet Capture passwords are independent of the operating system passwords.

Procedure

1. Use SSH and port `4477` to log in as the `root` user.

   The default password for the `root` user is `P@ck3t08.`.
2. To change the passwords for the `root` user account, use the **`passwd`** command.

Synchronizing the QRadar Packet Capture server time with the QRadar Console system time

To ensure that IBM Security QRadar deployments have consistent time settings so that searches and data-related functions work properly, all appliances must synchronize with the QRadar Console appliance. An administrator must update iptables on the QRadar Console appliance and then configure it to accept rdate communication on port 37.

Before you begin

You must know the IP address or host name of the QRadar Console. The host name must resolve correctly by using nslookup.

By default, the time zone for QRadar Packet Capture device is set to UTC (Coordinated Universal Time).

Important: If you change the default time zone on the QRadar Packet Capture device, the rest of the QRadar environment might not function properly.

Procedure

1. Use SSH to log in to the QRadar Packet Capture appliance as the `root` user.
2. To turn off the Network Time Protocol (NTP) service, type the following command: `service ntpd stop`.
3. To turn off check configuration for NTP, type the following command: `chkconfig ntpd off`.
4. Schedule synchronization as a cron job by editing the `crontab` (crontable) file.
   a. Type the following command: `crontab -e`.
   b. To configure the appliance to synchronize with the QRadar Console every 10 minutes, type the following command: `*/10 * * * * rdate -s` *`Console_IP_Address`*.

      Use an IP address or host name for the *Console_IP_Address* variable.
   c. Save your configuration changes.
   d. Turn on crond by typing the following commands:
      ```
      service crond start
      chkconfig crond on
      ```
5. Update the iptables on the QRadar Console to accept rdate traffic from QRadar Packet Capture devices.
   a. Use SSH to log in to the QRadar Console appliance as the `root` user.
   b. Edit the `/opt/qradar/conf/iptables.pre` file.
   c. Type the following command:
      ```
      -A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP address>
      ```
      If you have multiple QRadar Packet Capture appliances, add each IP address as a single line.

      Example:
      ```
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
      ```
   d. Save the `iptables.pre` file.
   e. Update the iptables on the QRadar Console by typing the following command:
      ```
      ./opt/qradar/bin/iptables_update.pl
      ```

Related concepts:

Chapter 3, "Capture usage overview," on page 7
To capture traffic to disk, start the capture application. The Recorder component saves the network traffic data into a pre-configured directory. When the space in the directory becomes full, existing files are overwritten.

Chapter 3. Capture usage overview

To capture traffic to disk, start the capture application. The Recorder component saves the network traffic data into a pre-configured directory. When the space in the directory becomes full, existing files are overwritten.

Troubleshooting: If you see that no data is being collected, ensure that there is traffic over the connections. To capture traffic, you must use a Tap or SPAN (mirror) port. When you use a SPAN port on a switch, if the switch assigns a lower priority to the SPAN port, some packets might be dropped.

Getting started

After you set up the system, log in to IBM Security QRadar Packet Capture by following these steps:

1. Open a web browser and type the following URL:
   `https://PCAP_IP_Address:41390`
2. Log in by using the following user account information:
   User: `continuum`
   Password: `P@ck3t08..`

Troubleshooting: If a user fails to give the correct password five times in a row within a 10 minute period, the user is locked out for 30 minutes. The user account can be unlocked manually by a system administrator.

By default, the Capture State page is displayed. You can control recordings by clicking the **Start Capture** or **Stop Capture**.

Capture state

The following information is provided on the Capture State page:

- **Interface capturing on**
- **Capture status**
- **Start/Stop time**
- **Duration of time the system has been capturing**
- **Throughput rate**
- **Packets Captured**
- **Bytes Captured**
- **Packets Dropped**
- **Storage Space Available**

In a cluster configuration, the storage usage is displayed for each enabled data node. If the QRadar Packet Capture Data Node is unreachable because of a network configuration issue or an improper connection, instead of the storage statistics, the following message is displayed: `Slave node is enabled but is currently unreachable.`

Troubleshooting

To view the system information about the configured capture interfaces, click **Troubleshooting**.

Server information

To view the server storage information, click **Server information**.

Network characterization

View the throughput of the network in graphical format.

The default maximum capture-to-disk throughput is 10 Gbps.

Capture history

View the history of the packet captures that took place or are in progress.

Inline compression

To support forensics investigations, you can retain raw packet content for a longer duration of time by increasing the available virtual storage capacity without adding physical disks. You can now use the new inline compression option to store larger amounts of data on the QRadar Packet Capture appliance.

The amount of compression is related to the amount of compressed video content in the payload. For example, if you have 5% compressed video in the payload, you get 13:1 compression. The compression:storage ratio is the ratio between the uncompressed size and compressed size.

Table 1. Inline compression ratios

Percentage (%) of compressed video payload	Compression:storage amplification ratio
0	17:1
5	13:1
10	6:1
20	4:1
40	2.4:1

Related concepts:

Chapter 1, “Introduction to QRadar Packet Capture,” on page 1
IBM Security QRadar Packet Capture is a network traffic capture and search application. The QRadar Packet Capture appliance has only one capture port (DNA0) and you can install either a 10G or 1G SFP transceiver.

Related tasks:

“Synchronizing the QRadar Packet Capture server time with the QRadar Console system time” on page 5
To ensure that IBM Security QRadar deployments have consistent time settings so that searches and data-related functions work properly, all appliances must synchronize with the QRadar Console appliance. An administrator must update iptables on the QRadar Console appliance and then configure it to accept rdate communication on port 37.

Chapter 4. Cluster

Use the QRadar Packet Capture appliance as a standalone single server, or as a cluster of servers.

10G editions support clusters which expands the overall data storage capacity and computational ability when compared to a single standalone server. Clusters contain a master. You can connect up to two QRadar Packet Capture data node appliances to each QRadar Packet Capture master system.

The **Cluster** tab displays two data nodes, along with their current status.

Data Nodes are not part of the cluster by default, and have a status of disabled.

Enabling Data Nodes

After you physically connect IBM Security QRadar Packet Capture Data Nodes to the QRadar Packet Capture master mode, you must enable the QRadar Packet Capture Data Nodes. Enabled and connected QRadar Packet Capture Data Nodes creates a cluster for the added storage capacity and enhanced capture performance.

For information about connecting the appliances, see the *QRadar Packet Capture Quick Reference Guide.*

Before you begin

Make sure that the capture server is running.

Procedure

1. To enable data nodes, follow these steps:
   a. In **Cluster** tab, for each data node, select **Enable**. The status shows **Connected**.
   b. Restart the capture server. The QRadar Packet Capture Data Nodes are now enabled.

   When the QRadar Packet Capture Data Nodes are connected and running, the status of them in the cluster changes to “connected”.

   After the master node connects to a data node the compressed (virtual) storage size that is displayed on the dashboard includes the storage size of the connected data nodes.
2. To disable data nodes, follow these steps:
   a. In Cluster tab, for each data node select **Disable**. The status shows **Disconnected**.
   b. Restart the capture server. The QRadar Packet Capture Data Nodes are now disabled, and are no longer associated with the master.

   A disconnected data node no longer stores data.

   After the master node is disabled the compressed (virtual) storage size on the dashboard decreases.

   If Data Node1 or Data Node2 are licensed, the license column displays either **Permanent** or **Evaluation**, depending on the license that you used.

Chapter 5. QRadar Packet Capture graphs

In IBM Security QRadar Packet Capture, use either a live or historical graph to visualize packet capture statistics.

Live graph

The Live graph tracks the following packet capture statistics about the current packet capture:

- Throughput in Gbps (gigabits per second)
- Total packets per second
- TCP_packets per second
- UDP_packets per second
- Packets per second for non-UDP traffic
- Number of system events
- Packet compression ratio

Hover your mouse over the graph and get the statistics for that point on the graph.

You can click the graph at a point in time, and automatically generate a search request. You can also click on the display style icons, to change the view of the graph.

Historical graph

The Historical graph provides a long-term overview of the packet capture history. The history timeline options include 1 hour, 1 day, and 1 week.

Hover your mouse over the graph and get the statistics for that point on the graph.

Click the graph at a point in time to automatically generate a search request is automatically generated.

Chapter 6. Searching packets within a time range for diagnostic testing

Index data that is created at the time of capture is used to produce a packet capture (pcap) file that contains the packets that match the specified time range and packet metadata information.

Restriction: These searches are for diagnostics purposes only. Manual cleanup is required to avoid filling the extraction partition.

Procedure

1. Click the **Search** page.

   Default values are already entered.
2. Select the interface for the captured traffic that you want to search.

   If you have a single interface configuration, it is automatically selected.
3. Specify a value or change the defaults for the beginning and ending of the time range that you want to search in.
4. Specify a Berkeley Packet Filter (BPF).

   Use BPF syntax to specify BPF filters. An expression consists of one or more primitives. Complex filter expressions are built by using AND, OR, and NOT operators.

   These examples are primitive filters

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   These examples are complex filters

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```
5. Specify the number of packets to extract.

   The default maximum number of packets to extract is 10,000. If you change the number to 0, all packets that match the timeline and filter are extracted.
6. Click **Start Search**.
7. In the **Action** column of the search page, use the **Chunking** option to split search requests into smaller data segments so that you can access data while the entire search request is still running. You request a search by first specifying the PCAP file number, and then clicking **Download PCAP File**.

Data segments are 128MB, and the last data segment can be any size smaller than 128MB.

8. To see the state of the search queue, view the **Search request queue**.
9. To see a history of all completed searches, view the **Request log**.
10. Clean up manual searches to ensure sufficient space for forensics recovery processes:
    a. Log in as root.

       username: root

       password: P@ck3t08..

    b. Run the following command:

       ```
       rm -r /extraction/<name_of_search>
       ```

       The <*name_of_search*> variable is the name column on the Completed Searches page.

Chapter 7. Configuring pre-capture filters

Pre-capture filters filter network traffic before writing the captured data to disk.

Procedure

1. Create a pre-capture filter.
   a. Click the **Pre capture filter** menu.
   b. Enter the settings for the Filter Name and Search Filter options.

      A capture filter takes the form of primitive expressions that are connected by conjunctions (and/or) and optionally preceded by not.

      In the following example, all traffic that is destined for port 80 is dropped:

      ```
      not dst port 80
      ```

      In the following example, only the traffic for these two hosts are captured and all other traffic is dropped:

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```

   c. Complete the pre-capture filter by clicking **Add**. The last pre-capture filter added to the list is the active filter. The history of previous filters is also displayed.
2. Restart the capture server to activate the newly added filter.
3. Permanently delete the filter by selecting **Delete**. You must restart the capture server.

Chapter 8. Configuring active triggers

Active triggers alert you when an event that you specified occurs on your network. For example, you specify an IP address as the search filter to be alerted when traffic that contains the IP address is captured.

Procedure

1. Create an active trigger.
   a. Click the **Active Trigger** menu.
   b. Enter the settings for the Trigger name and Time frame options.
   c. Complete the active trigger by clicking **Add**.

      Restriction: You can specify up to five active triggers.
2. Review trigger events in the **Event Log** as they occur. Clicking an active trigger event automatically generates a search request, within the specified time parameters around the triggered event. The search time includes seconds before and seconds after the event.
3. Delete the configured trigger by selecting **Delete**.

Chapter 9. Troubleshooting QRadar Packet Capture issues

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and to explain how to resolve the problem.

Is the latest version of the QRadar Packet Capture software installed?

Always upgrade to the latest release version of the software. Immediately after you apply a software update, or after any new installation, ensure that you restart the system so that the changes are applied. In cluster configurations, always make sure that both the master and all data node systems are upgraded to the same version.

Do you have the suggested firmware for the RAID controller and hard drives?

If you encounter reliability or performance issues related to the firmware revision installed on the 3650 M4 RAID controller and hard drives, ensure that you have the minimum firmware revisions:

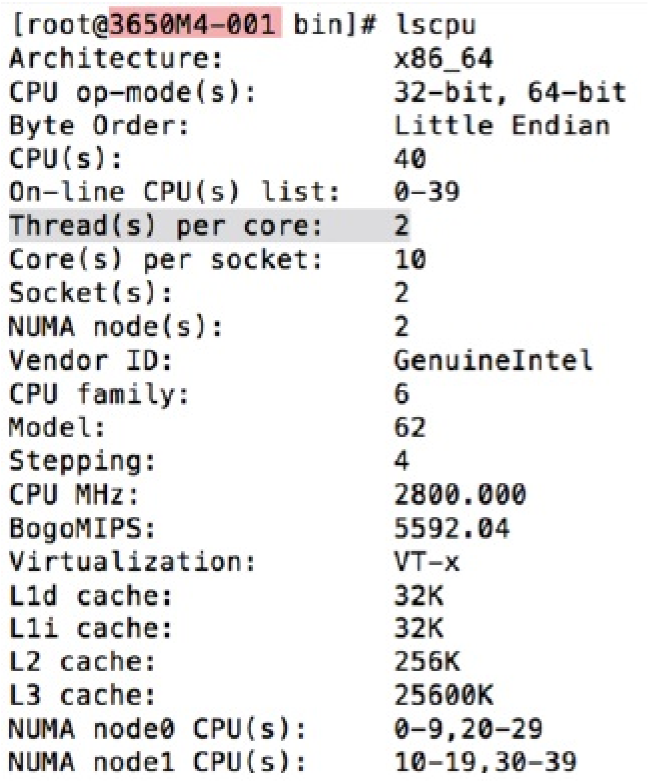
- For the 3650 M4, the M5200 RAID controller firmware revision: version 24.7.0-0052 on May 27, 2015 or later.

  Run the `.bin` files from the Red Hat Linux command line.
- For IBM Lenovo, revision from May 15, 2015 or later.

  Run the `.bin` files from the Red Hat Linux command line.

Is the HyperThreading enabled in the BIOS?

HyperThreading is enabled in the BIOS by default. Run the `lscpu` command, and review the output to ensure "Thread(s) per core is equal to 2". Here is the sample output of the command for IBM 3650-M4:



```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

Is the capture port correctly connected?

The IBM Security QRadar Packet Capture device can capture only on Interface 0.

Is the Ethernet network connection correctly configured?

To ensure that an Ethernet interface is assigned to an IP address, run the `ifconfig` command for the interface that is connected.

If no address is configured, edit the corresponding `ifcfg-eth*` file to configure an address.

- In this DHCP example, edit the following settings in `/etc/sysconfig/network-scripts/ifcfg-`*eth2* and replace the *eth2* with the appropriate setting.

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```

- In this static IP address example, edit the following settings in `/etc/sysconfig/network-scripts/ifcfg-`*eth2* and replace the *eth2* with the appropriate setting.

  ```
  BOOTPROTO="static"
  BROADCAST="192.168.1.255"
  DNS1="0.0.0.0"
  DNS2="0.0.0.0"
  GATEWAY="192.168.1.2"
  IPADDR="192.168.1.1"
  NETMASK="255.255.255.0"
  NM_CONTROLLED="no"
  ONBOOT="yes
  ```

After you change the settings, run the ifconfig command to configure the network interface.

Is the system time correctly configured?

By default, the system time is set to Coordinated Universal Time (UTC), and is configured to use Network Time Protocol (NTP) and public servers to maintain the correct system time.

Are there system hardware problems?

1. Ensure that the traffic is being generated properly and is being received by the Network Interface Card (NIC).

   Look at the lights that are immediately to the right of the Interface 0 connection. The bottom one must be solidly on, which signifies a link. The top one must be flashing, which signifies traffic activity.
2. Run the /usr/local/nc/bin/dpdk_nic_bind.py –status command.

   The result of the command must resemble the following output:

```
Network devices using DPDK-compatible driver
============================================
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
===================================
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====================
<none>
```

Is the system capturing traffic?

To confirm whether the system is capturing traffic after a capture session is started, use one of the following methods:

- Look at the lights that are immediately to the right of the Interface 0 connection. The top one must be flashing, which signifies traffic activity.
- From the Network Characterization page, you see graphical output.
- From the command line, run the du –h /storage0/int0 command.

  The result resembles the following output:

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

  If you run this command repeatedly, the number of subdirectories and allocation amounts that are returned increase.

Is the QRadar Packet Capture Data Node enabled?

When the QRadar Packet Capture Data Node is physically connected to the master node, you must also ensure that it is enabled in the UI to work with the master server. The system currently supports up to two QRadar Packet Capture Data Nodes.

If the **Cluster** tab shows that the QRadar Packet Capture Data Nodes are connected and enabled, and the **System ID** setting is missing from the **Update Node(n) License** screen under the **Admin** tab, you must ensure that the specific QRadar Packet Capture Data Node has the same QRadar Packet Capture Data Node software version installed as the master node. Ensure that this requirement is met after you update to the latest software version.

As `root` user, run the following command to check software version that is installed on the QRadar Packet Capture Data Node and master node:

```
cat /root/version.txt
```

The QRadar Packet Capture Data Node software version must be the same version as what is installed on the master node.

How is a license for the QRadar Packet Capture Data Node applied from the command line?

To ensure that you are in the QRadar Packet Capture Data Node, as `root` user, run the following command :

```
cat /root/version.txt
```

To verify that you are connected to the QRadar Packet Capture Data Node, look for a D that is appended to the end of the version number, for example, 7.2.7.256D.

To apply the license to the QRadar Packet Capture Data Node, as a `root` user, run the script: `nc_set_license.sh` as `root`.

Notes:

- To make the new license effective, you must restart the QRadar Packet Capture Data Node.
- If the QRadar Packet Capture Data Node is already licensed at the time of manufacturing, you don't have to run the script. The license is effective as soon as the system is started.

If the license you applied is not valid, an error message displays:

```
Warning: LicenseKey is *NOT* valid.
```

What is LEEF 2.0 logging format?

The LEEF (Log Event Extended Format) messages are added to the `/var/log/messages` file in the following format:

```
<DateTime> <ServerIP> LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|<ID>|cat=<category> msg=<message>
```

For example, when packet capture server starts on a system that has an IP address 10.91.170.20, the following LEEF message is added to the /var/log/messages file:

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|Started|cat=PacketCapture
```

Why does the Create Search request return a NoSpace error?

If the /extraction directory is full when you create a search, the server returns NoSpace error.

What happens when a search pauses?

A search is paused when the used space in the /extraction directory exceeds 6.7 GB. A LEEF message is sent to Syslog indicating that the search is paused. The event log displays a warning similar to:

```
!WARNING: Extraction Storage Full! Search cannot proceed!!
```

To ensure that a paused search is resumed, you must create space by deleting older, previously completed searches. To delete an old search, follow these steps:

1. Click the **Search** main menu option.
2. In the **Search Request Log** frame delete older searches by clicking on **Delete Search**.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA