IBM QRadar Network Packet Capture

Installation Guide

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 19.

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.3.1 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to installing QRadar Network Packet Capture

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

Intended audience

System administrators who are responsible for installing QRadar Network 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. Installation overview

IBM QRadar Network Packet Capture appliances that are supplied by IBM come with the software preinstalled. You might need to install the software on your IBM supplied appliance if, for example, you are recovering from a hardware failure.

Custom installations are supported as long as the appliance meets the minimum requirements. For more information, see "Minimum requirements for custom installations" on page 9.

You can upgrade directly to QRadar Network Packet Capture V7.3.1 from earlier versions.

Chapter 2. Installations on IBM supplied appliances

The IBM QRadar Network Packet Capture installation options impact the configuration and capture data differently, depending on whether you choose to install, reinstall, or upgrade the software.

Table 1: Installation actions on IBM supplied appliances

Action	Description
Upgrade	Both the QRadar Network Packet Capture software and Red Hat Enterprise Linux operating system are upgraded. The configuration files and packet capture files remain unchanged.
Reinstall	Both the QRadar Network Packet Capture software and Red Hat Enterprise Linux operating system are upgraded. The configuration files are reset, and the packet capture files are unchanged.
Install	Both the QRadar Network Packet Capture software and Red Hat Enterprise Linux operating system are upgraded. The configuration files are reset, and the packet capture files are deleted.

QRadar Network Packet Capture hardware

You can use a QRadar Network Packet Capture appliance to store and manage data that is used by IBM Security QRadar Incident Forensics when no other network packet capture (PCAP) device is deployed. You can install any number of these appliances as a tap on a network or subnetwork to collect the raw packet data.

QRadar Network Packet Capture appliance

Before you can capture packets, you must configure QRadar Network Packet Capture network and connection settings.

The QRadar Network Packet Capture appliance can be identified by the wording “IBM QRadar PCAP G3” on the front panel of the hardware, as shown in the following diagram.

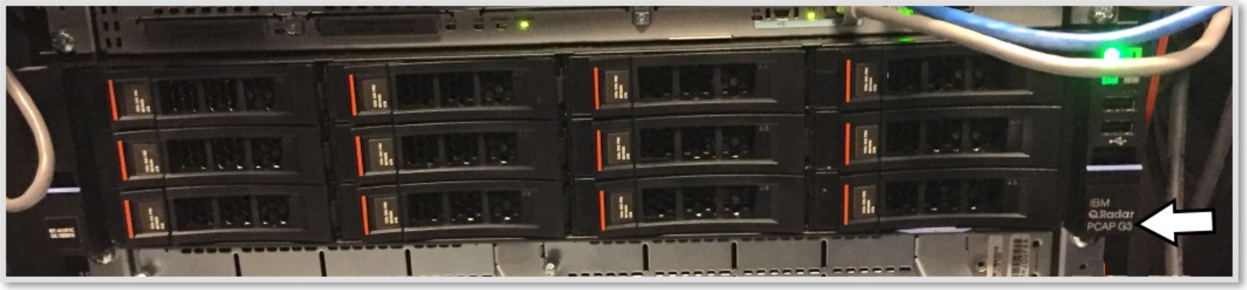


Figure 1: Front panel of the QRadar Network Packet Capture appliance

The QRadar Network Packet Capture appliance is installed with an Intel X520 Ethernet adapter and a Napatech NT40E3-4-PTP accelerator.

Use only the Napatech card for packet capture. The Intel X520 is for management purposes only and cannot be used for packet capture on this server.

The placement for the Intel X520 and Napatech NT40E3-4-PTP hardware can be seen in the following diagram of the rear panel of the server.

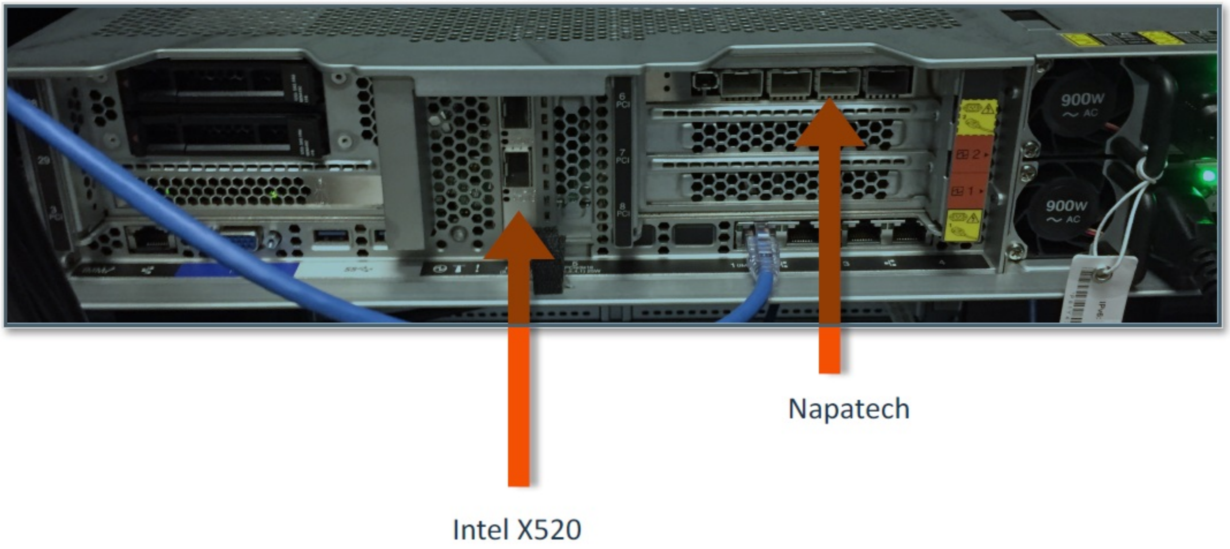


Figure 2: Rear panel of the QRadar Network Packet Capture appliance

Napatech NT40E3-4-PTP accelerator

The Napatech NT40E3-4-PTP accelerator provides full packet capture and analysis with zero packet loss, allowing a single appliance to capture data from up to four capture port sources. You can configure port forwarding to capture on one port and mirror out another port.

Dual-rate ports 10G/1G support the following SFP modules:

- SFP+ 10GBASE-SR
- SFP+ 10GBASE-RR
- SFP 1000BASE-SX
- SFP 1000BASE-LX
- SFP 1000BASE-T

The following diagram shows the Napatech SR SFP+ modules installed (Avago) on an appliance:

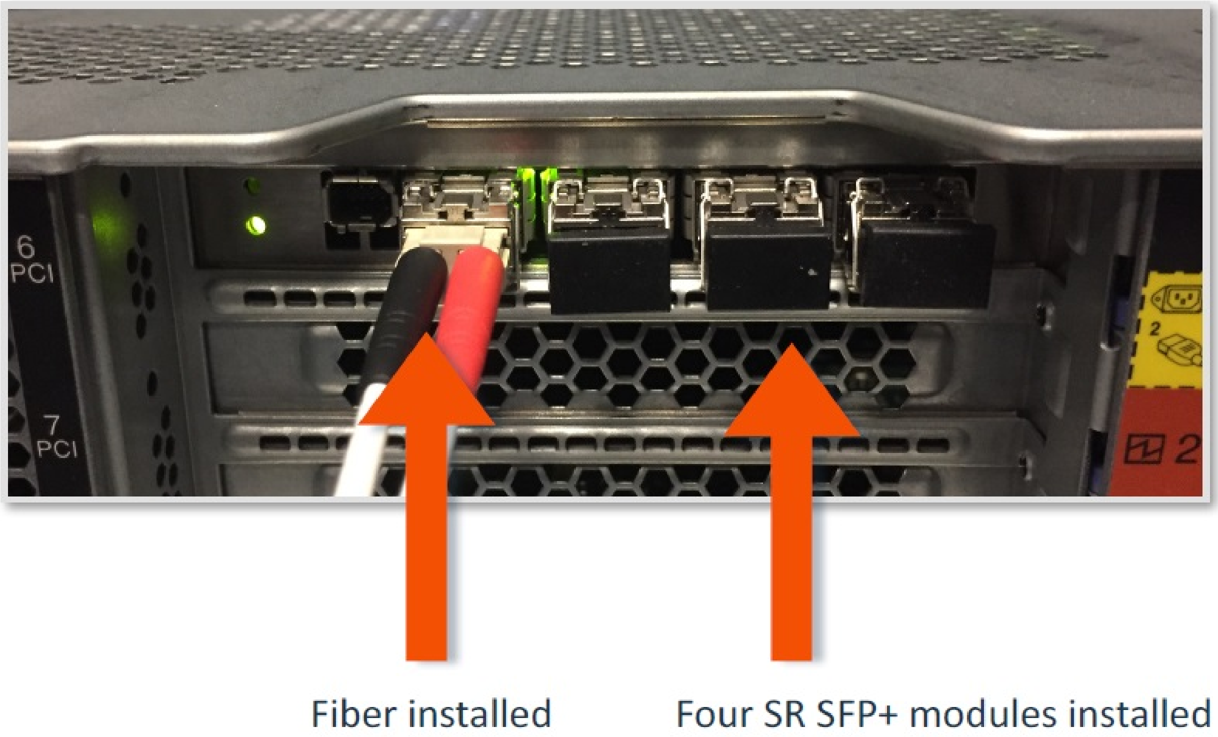


Figure 3: Napatech SR SFP+ modules installed on an appliance

The Napatech card has two sets of four SFP+ modules. One set is Transceiver Dual SFP+ short range and one set is Transceiver Dual SFP+ long range.

The approved SFP+ modules for the Napatech card are listed here:

- IBM D10E7LL 10G LR (QTY 2) Avago (included with appliance)
- IBM D10E8LL 10G SR (QTY 2) Avago (included with appliance)
- Napatech 802-0039-01-01 10G SR Finisar
- Napatech 10G LR 802-0039-01-01 Finisar

The approved SFP+ modules for the Intel X520 card are listed here:

- IBM D10E8LL 10G SR (QTY 2) Avago (included)
- Lenovo 46C3447 10G SR Avago
- Lenovo 46C3447 10G SR Finisar
- Intel E10GSFPSR 1/10G SX/R Finisar
- Intel E10GSFPSR 1/10G SX/R Avago
- Intel E10GSFPLR 1/10G LX/R Finisar

Upgrading QRadar Network Packet Capture on IBM hardware

Use these instructions to keep your existing configuration and captured data when you upgrade your IBM-supplied appliance to use QRadar Network Packet Capture V7.3.0 or V7.3.1.

Before you begin
Ensure that the following requirements are met:

- You are logged in to the QRadar Network Packet Capture appliance as an administrator.
- You are using an IBM-supplied QRadar Network Packet Capture appliance. For more information about installing or upgrading your own hardware, see Installations on custom appliances.

- If you are using a USB flash drive to upgrade, connect a keyboard and monitor by using the VGA connection.

Procedure

1. Download the `.iso` image from IBM Fix Central (www.ibm.com/support/fixcentral).

   The `.iso` file is named *`x.x.x-QRadar-NETPCAP-Upgrade-nnnn.iso`*, where:

   - `x.x.x` is the release version.
   - nnnn is a four-digit number that is allocated to the build.

   For example, if you are upgrading to QRadar Network Packet Capture V7.3.1, select *7.3.1-QRadar-NETPCAP-Upgrade-1404.iso*.
2. To use IMM2 to mount the `.iso` image, follow these steps:
   a) Log in to the IMM2 management module.

      You must access the IMM2 management module by using Active X with Internet Explorer, or a browser that supports Java™.

   b) Click **Remote Control**.
   c) To start the remote control session, click **Active X** if you are using Internet Explorer, or click **Java** for all other browsers.
   d) Click **Start Remote Control in Single User Mode** to start the session.
   e) On the **Virtual Media** menu, click **Activate**.
   f) On the **Virtual Media** menu, click **Select Devices to Mount**.
   g) In the **Select Devices to Mount** window, click **Add Image**.
   h) Locate the `.iso` image that you want to use, and click **Open**.
   i) Select the **Mapped** check box next to the drive to mount, and click **Mount Selected**.

   To watch a video tutorial about using the IMM2 management module to mount an `.iso`, see QRadar: Mounting ISOs Using IMM (https://www-01.ibm.com/support/docview.wss?uid=swg21974632).
3. Alternatively, you can copy the `.iso` to a bootable USB flash drive.

   For more information, see Creating a bootable USB flash drive with Red Hat Linux.
4. Restart the appliance.
5. On the **Boot Devices Manager** window, select the **Upgrade** option to start the upgrade process.

   ⚠ **Warning:** The upgrade process ensures that your configuration files and captured data remain intact. Choosing any other option might reset your configuration and delete your capture data.
6. After the upgrade is completed, restart the appliance.

Results

QRadar Network Packet Capture is upgraded.

Installing QRadar Network Packet Capture on IBM hardware

IBM QRadar Network Packet Capture appliances already have the QRadar Network Packet Capture software preinstalled. You might need to reinstall the software if, for example, you are recovering from a hardware failure.

Before you begin

Before you install the software, make sure that the following requirements are met:

- You are using an IBM-supplied QRadar Network Packet Capture appliance.

- You are logged in to the appliance as an administrator.
- If you are using a USB flash drive to install, connect a keyboard and monitor by using the VGA connection.

About this task

⚠ **Warning:** QRadar Network Packet Capture configurations are lost when you reinstall the appliance. For more information about the impact on your configuration and capture data, see Chapter 1, “Installation overview,” on page 1.

Procedure

1. Download the `.iso` image from IBM Fix Central (www.ibm.com/support/fixcentral).

   The `.iso` file is named either *x.x.x-QRadar-NETPCAP-Upgrade-nnnn.iso* or *x.x.x-QRadar-NETPCAPFULL-nnnn.iso*, where:

   - `x.x.x` is the release version.
   - nnnn is a four-digit number that is allocated to the build.

   For example, if you want to do a clean installation of QRadar Network Packet Capture V7.3.1 and remove capture data that was previously collected, download *7.3.1-QRADAR-NETPCAPFULL-1404.iso*.

   If you want to reinstall or upgrade to QRadar Network Packet Capture V7.3.1 and keep captured data, select *7.3.1-QRADAR-NETPCAP-Upgrade-1404.iso*.
2. To use IMM2 to mount the `.iso` image, follow these steps:
   a) Log in to the IMM2 management module.

      You must access the IMM2 management module by using Active X with Internet Explorer, or a browser that supports Java.

   b) Click **Remote Control**.

   c) To start the remote control session, click **Active X** if you are using Internet Explorer, or click **Java** for all other browsers.

   d) Click **Start Remote Control in Single User Mode** to start the session.

   e) On the **Virtual Media** menu, click **Activate**.

   f) On the **Virtual Media** menu, click **Select Devices to Mount**.

   g) In the **Select Devices to Mount** window, click **Add Image**.

   h) Locate the `.iso` image that you want to use, and click **Open**.

   i) Select the **Mapped** check box next to the drive to mount, and click **Mount Selected**.

   To watch a video tutorial about using the IMM2 management module to mount an `.iso`, see QRadar: Mounting ISOs Using IMM (https://www-01.ibm.com/support/docview.wss?uid=swg21974632).
3. Alternatively, you can copy the `.iso` to a bootable USB flash drive.

   For more information, see Creating a bootable USB flash drive with Red Hat Linux.
4. Restart the appliance.
5. When the splash menu is displayed, select the boot device.
   - If you are installing on a Lenovo appliance, follow these steps:
     a. Select **<F12> Select Boot Device** to open the **Boot Devices Manager** window.
     b. Select **CD/DVD**.
   - If you are installing on a Dell appliance, follow these steps:
     a. Select **<F11>** to open the **Boot Devices Manager** window.
     b. Select **One-shot UEFI Boot Menu** and then select **Virtual Optical Drive**.

Note: If you are using a USB flash drive and the USB is not listed as a bootable device, restart the QRadar Network Packet Capture appliance.

6. Select either **Install** or **Reinstall** to start the installation process.

   The installation options are different depending on which `.iso` you downloaded.

   ⚠ **Warning:** When you choose **Install**, existing capture data is deleted. If you want to keep existing capture data, you must use the upgrade `.iso`, and select **Reinstall**.
7. After the installation is completed, restart the appliance.

Results

QRadar Network Packet Capture is installed. You can configure the IP and network settings.

Configuring IP address and network settings

By default, IBM QRadar Network Packet Capture uses the IP address of 192.168.100.100. You can use either DHCP or manually configure network settings.

Before you begin

If your QRadar Network Packet Capture appliance is member of a group, do not change the network configuration settings as indicated below. In this case, unregister from the group, change the network configuration, and reregister with the group. Use a full DHCP infrastructure that assigns QRadar Network Packet Capture devices IP address and host name from DHCP.

Procedure

1. Configure your network settings on the QRadar Network Packet Capture console by completing these steps:
   a) Click **Configure network** and press Enter.
   b) At the **QRadar Network Packet Capture IP Settings** prompt, configure the network settings, and then press Enter to apply the settings.
   c) If you are using DHCP, press the Tab key until **Use DHCP** is highlighted, then press Enter.
2. Configure your network settings in QRadar web UI by using the following steps:
   a) On the **Admin** tab, go to the **Configure network** section and configure your IP address or DHCP options.

      Leave the **DNS** field blank; a DNS infrastructure is not required for QRadar Network Packet Capture.
   b) Select **Apply** to save your changes.

Chapter 3. Installations on custom appliances

You can install IBM QRadar Network Packet Capture on your own custom appliance if it meets the minimum hardware and software requirements. The requirements might be different, depending on which version of the software that you want to install.

The installation options impact the configuration and capture data differently, depending on whether you choose to install, reinstall, or upgrade the software.

Table 2: Installation actions on custom appliances

Action	Description
Upgrade	The QRadar Network Packet Capture software is upgraded. The configuration files and packet capture files remain unchanged.
Re-install	The QRadar Network Packet Capture software is upgraded. The configuration files are reset, and the packet capture files are unchanged.
Install	The QRadar Network Packet Capture software is upgraded. The configuration files are reset, and the packet capture files are deleted.

Minimum requirements for custom installations

Before you install IBM QRadar Network Packet Capture that uses custom hardware, ensure that your system meets the minimum requirements.

- Requirements for QRadar Network Packet Capture V7.3.1
- Requirements for QRadar Network Packet Capture V7.2.8 and V7.3.0
- Performance sizing guidelines

Minimum requirements for QRadar Network Packet Capture V7.3.1

You can install QRadar Network Packet Capture V7.3.1 on any system that meets the following minimum requirements:

Table 3: Minimum system requirements for QRadar Network Packet Capture V7.3.1

Description	Minimum requirement
CPU	Intel Broadwell or newer, six cores
Memory	32 GB
RAID Controller	Must be controlled by Red Hat Enterprise Linux 7.3.
Hard disks	1 TB 3.5" 7200 RPM, 3 disks minimum, RAID 5 50 GB is required for the operating system, and the remainder is required for the storage and staging.
Operating system	Red Hat Enterprise Linux 7.3

Table 3: Minimum system requirements for QRadar Network Packet Capture V7.3.1 (continued)

Description	Minimum requirement
Network Accelerator	Napatech NT40e3

Minimum requirements for QRadar Network Packet Capture V7.2.8 and V7.3.0

QRadar Network Packet Capture V7.2.8 and V7.3.0 must be installed on either a Dell or Lenovo system that meets the following system requirements.

Table 4: Minimum system requirements for QRadar Network Packet Capture V7.2.8 and V7.3.0

Description	Lenovo	Dell
CPU	E5-2680 v4 12C 2.5 GHz 30 MB 2133 MHz	E5-2660 v3 2.6 GHz 25 MB 2133 MHz
Memory	128 GB	128 GB
RAID Controller	M1215 SAS/SATA	PERC H730P, 2 GB Cache
Operating system	Red Hat Enterprise Linux 7.3	Red Hat Enterprise Linux 7.3
OS HDD	2 x 1 TB, 7.2 K, 12 Gbps, NL SAS 2.5”, G3HS RAID 1	2 x 1 TB, 7.2 K, 12 Gbps, NL SAS 2.5” RAID 1
CAP HDD	12 x 6 TB, 7.2 K, 12 Gbps, NL SAS 3.5”, G2HS 512e RAID 5	12 x 6 TB, 7.2 K, 12 Gbps, NL SAS 3.5” 512e RAID 5
Network Accelerator	Napatech NT40E3-4	Napatech NT40E3-4

Sizing guidelines

While performance varies based on the exact configuration and tuning of the system components, the following guidelines can help you configure the system to achieve the best possible performance in your environment.

The guidelines are based on the following assumptions:

- The disks for capturing network packet data meet the following specifications:
  - 3.5 inches, 7200 RPM or better.
  - Sustained IO of 200 MiB/s or better.
  - Controlled by a hardware RAID 5 controller.
- The operating system is Red Hat Enterprise Linux 7.3 or later, and is installed on a separate disk.
- The system uses an Intel processor, and is not running other processes.

Table 5: Sizing guidelines for custom hardware

Capture rate	Number of disks	Memory	Minimum number of cores
0 - 2 Gbps	3	32 GB	6
5 Gbps	7	32 GB	6

Table 5: Sizing guidelines for custom hardware (continued)

Capture rate	**Number of disks**	**Memory**	**Minimum number of cores**
8 Gbps	10	64 GB	8
10 Gbps	12	128 GB	10

Installing on custom appliances without internet access

The IBM QRadar Network Packet Capture installation process requires access to the Red Hat Enterprise Linux kernel. If the appliance does not have access to the internet, you must make the original Red Hat Enterprise Linux `.iso` available so that the package can be installed locally.

Procedure

1. To enable the Red Hat Enterprise Linux `.iso` for local package installation, type these commands on the console:
   a) Type `mkdir /mnt/rhel`.

      If the `.iso` is available directly on the appliance, skip to step 1c.

   b) Type the following command, where `/dev/sr0` is the device where the ISO or DVD is available.

      ```
      dd if=/dev/sr0 of=/tmp/rhel.iso bs=8192
      ```

   c) To mount the `.iso` and copy the `.repo` file, type these commands:

      ```
      mount -o loop /tmp/rhel.iso /mnt/rhel
      ```

      ```
      cp /mnt/rhel/media.repo /etc/yum.repos.d/rhel7dvd.repo
      ```

   d) To set the file permissions, type the following command:

      ```
      chmod 644 /etc/yum.repos.d/rhel7dvd.repo
      ```

2. Edit the new `/etc/yum.repos.d/rhel7dvd.repo` repository file.
   a) Change `gpgcheck=0` to 1.

   b) Add these lines to the file:

      ```
      enabled=1
      baseurl=file:///mnt/rhel
      gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
      ```

3. Type these commands to clear the caches:

   ```
   yum clean all
   subscription-manager clean
   ```

4. To confirm that the packages list is available from the repository, type `yum --noplugins list`.

Results

The appliance is set up for local package installation and you can proceed to install the QRadar Network Packet Capture software. For more information, see “Installing QRadar Network Packet Capture V7.3.1 on non-IBM hardware” on page 13.

Upgrading QRadar Network Packet Capture on customer supplied hardware

Use these instructions to upgrade QRadar Network Packet Capture that is installed on hardware that was not supplied by IBM. When you upgrade, your existing configuration and captured data remain intact.

Before you begin

Ensure that the following requirements are met:

- Your system meets the minimum hardware requirements.

  Important: The minimum requirements might be different depending on which version of QRadar Network Packet Capture that you are upgrading to. For more information, see "Minimum requirements for custom installations" on page 9.
- You are logged in to the appliance as an administrator.
- If you are using a USB flash drive to upgrade, connect a keyboard and monitor by using the VGA connection.

Procedure

1. Download the `.iso` image from IBM Fix Central (www.ibm.com/support/fixcentral).

   The `.iso` file is named *x.x.x-QRadar-NETPCAP-Upgrade-nnnn.iso*, where:

   - `x.x.x` is the release version.
   - nnnn is a four-digit number that is allocated to the build.

   For example, if you are upgrading to QRadar Network Packet Capture V7.3.1, select *7.3.1-QRadar-NETPCAP-Upgrade-1404.iso*.
2. To use IMM2 to mount the `.iso` image, follow these steps:
   a) Log in to the IMM2 management module.

      You must access the IMM2 management module by using Active X with Internet Explorer, or a browser that supports Java.

   b) Click **Remote Control**.

   c) To start the remote control session, click **Active X** if you are using Internet Explorer, or click **Java** for all other browsers.

   d) Click **Start Remote Control in Single User Mode** to start the session.

   e) On the **Virtual Media** menu, click **Activate**.

   f) On the **Virtual Media** menu, click **Select Devices to Mount**.

   g) In the **Select Devices to Mount** window, click **Add Image**.

   h) Locate the `.iso` image that you want to use, and click **Open**.

   i) Select the **Mapped** check box next to the drive to mount, and click **Mount Selected**.

   To watch a video tutorial about using the IMM2 management module to mount an `.iso`, see QRadar: Mounting ISOs Using IMM (https://www-01.ibm.com/support/docview.wss?uid=swg21974632).
3. Alternatively, you can copy the `.iso` to a bootable USB flash drive.

   For more information, see Creating a bootable USB flash drive with Red Hat Linux.
4. Restart the appliance.
5. On the **Boot Devices Manager** window, select the **Upgrade** option to start the upgrade process.

   Important: Select the **Upgrade** option only. If you select any of the other options, you reset the hardware configuration and potentially lose your capture data.
6. After the upgrade is completed, restart the appliance when prompted.

Results

QRadar Network Packet Capture is upgraded.

Installing QRadar Network Packet Capture V7.3.1 on non-IBM hardware

Use these instructions to install QRadar Network Packet Capture on hardware that was not supplied by IBM.

Before you begin

Use this checklist to prepare the system for installation:

- Ensure that your system meets the minimum hardware requirements. For more information, see "Minimum requirements for custom installations" on page 9.
- Install Red Hat Enterprise Linux 7.3 or later on your appliance.
- Configure your IP address settings.
- Create a folder called `/mnt/capture` that points to the capture data storage location. Use a separate volume for this folder.
- Create a folder called `/mnt/staging`.

  This folder is used for storing search results before they are downloaded. Ensure that this folder has a minimum of 500 GB available storage and is not located in the system volume.
- If your appliance does not have access to the internet, the Red Hat Enterprise Linux `.iso` must be accessible to the appliance to ensure that the QRadar installation script can access the kernel package. For more information, see "Installing on custom appliances without internet access" on page 11.

About this task

⚠ **Warning:** QRadar Network Packet Capture configurations are lost when you reinstall the appliance.

For more information about the way that different installation actions impact the configuration and capture data, see Chapter 3, "Installations on custom appliances," on page 9.

Procedure

1. Download the `.iso` image from IBM Fix Central (www.ibm.com/support/fixcentral).

   The `.iso` file is named *x.x.x-QRadar-NETPCAP-Upgrade-nnnn.iso*, where:

   - `x.x.x` is the release version.
   - nnnn is a four-digit number that is allocated to the build.
2. Mount the ISO image.

   For example, type `mount -o loop <QRadar_ISO> /install`.
3. Run the setup script and follow the installation instructions.

   For example, type `/install/setup`.

   Note: Your system must be configured for package installation either by being connected to the internet, or the Red Hat Enterprise Linux `.iso` must be available for local package installation.
4. When the installation is complete, restart the appliance.

Results

QRadar Network Packet Capture is now available at `https://hostname`.

Installing QRadar Network Packet Capture V7.2.8 and V7.3.0 on non-IBM hardware

Install QRadar Network Packet Capture V7.2.8 or V7.3.0 software by using the ISO image, loaded on USB media.

Before you begin

Ensure that the following requirements are met:

- Your system meets the minimum hardware requirements.

  Important: The minimum requirements are different depending on which version of QRadar Network Packet Capture that you are installing. For more information, see "Minimum requirements for custom installations" on page 9.
- A keyboard and monitor are connected by using the VGA connection.

About this task

⚠ **Warning:** QRadar Network Packet Capture configurations are lost when you reinstall the appliance. For more information about the way that different installation actions impact the configuration and capture data, see Chapter 3, "Installations on custom appliances," on page 9.

Procedure

1. Download the `.iso` image from IBM Fix Central (www.ibm.com/support/fixcentral).

   The `.iso` file is named *`x.x.x-QRadar-NETPCAP-Upgrade-nnnn.iso`*, where:

   - `x.x.x` is the release version.
   - nnnn is a four-digit number that is allocated to the build.
2. Burn the ISO image to a USB device.

   For more information, see Creating a bootable USB flash drive with Red Hat Linux.
3. Press **F12** to enter Boot Manager.
4. Select the USB storage device that contains the image.
   For example, select **One Shot BIOS Boot**.
5. Select the **Disk connected to front USB2: xxxx**.

   Note: If **USB2** is not available in **One Shot BIOS Boot**, the USB key was not recognized as a bootable device. Restart the QRadar Network Packet Capture appliance to resolve this issue.

   The appliance restarts and installs QRadar Network Packet Capture.
6. After the installation is complete, restart the appliance when prompted.

Results

QRadar Network Packet Capture is installed. You can now configure your IP and network settings.

Chapter 4. Verify the QRadar Network Packet Capture installation

After you configure QRadar Network Packet Capture on your IBM-supplied appliance, ensure that it is working correctly by checking the capture port, time synchronization, and the accelerator LEDs on the back of the appliance.

To verify the installation on your custom appliance, use the external LED lights.

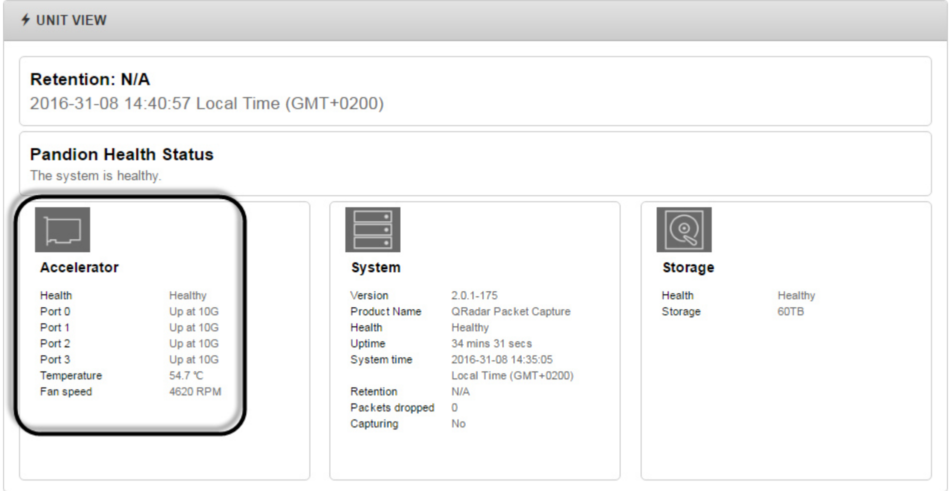
Verifying the capture port

Follow these steps to verify the status and link speed of the capture port on your IBM-supplied appliance.

Procedure

On the **Dashboard** tab, check that the **Accelerator** window shows the status of each capture port.

Link status and health of the system is visible even when data capture is not started. If the port is active, the link speed of the port is displayed.



UNIT VIEW

Retention: N/A
2016-31-08 14:40:57 Local Time (GMT+0200)

Pandion Health Status
The system is healthy.

Accelerator

Health	Healthy
Port 0	Up at 10G
Port 1	Up at 10G
Port 2	Up at 10G
Port 3	Up at 10G
Temperature	54.7 ℃
Fan speed	4620 RPM

System

Version	2.0.1-175
Product Name	QRadar Packet Capture
Health	Healthy
Uptime	34 mins 31 secs
System time	2016-31-08 14:35:05 Local Time (GMT+0200)
Retention	N/A
Packets dropped	0
Capturing	No

Storage

Health	Healthy
Storage	60TB

*Figure 4: **UNIT VIEW** widget.*

Verifying the time synchronization

Review the SYSLOGS messages on the **Admin** tab to verify the time synchronization and the status for the capture network interface card on your IBM-supplied appliance.

Use the external LED lights to verify external time synchronization on your custom appliance.

About this task

Procedure

1. Review the logs for a general message that indicates that the time synchronization source was changed, or that the accelerator obtained or released the lock against the time source.

The following syntax is representative of a general entry:

```
Adapter < number > time-sync status:
In-Sync: < Yes | No >
Current time-sync reference: < OsTime | PTP >
Skew (ns): < number >
Clock rate adjustment (ns): < number >
Clock Hard Reset: < Yes | No >
```

For example, a general time synchronization might look like this entry:

```
Adapter 0 time-sync status:
In-Sync: Yes
Current time-sync reference: OsTime
Skew (ns): -1
Clock rate adjustment (ns): 503
Clock Hard Reset: No
```

2. If you are synchronizing against a Precision Time Protocol (PTP) master, review the logs to look for an extra entry that contains detailed information about the status of the adapter in PTP mode.

   The following syntax is representative of a PTP entry:

   ```
   Adapter < number > PTP time-sync status:
   PTP Time: "--" | < PTP clock time > [ "(TAI)" ]
   Port: < IPv4_address > | < IPv6_address > | "IEEE 802.3"
   Link Status: < Down | 10M | 100M >
   IPv4 Subnet Mask: < IPv4_address >
   IPv4 Gateway: < IPv4_address >
   DHCP Enabled: "Yes" | "No"
   Profile Id: < six_times_2_hex digits >
   Profile: < Default | Telecom | Power >
   Clock Id: < six_times_2_hex digits >
   Domain: < number > | "--"
   VLAN: < number >
   Delay Mechanism: "E2E", "P2P", "N/A"
   PTP Filter: "Min", "PDV", "None", "N/A"
   DelayAssemetry: < number >
   Clock State: "Faulty" | "INACTIVE" | "SLAVE" | "--"
   Mean Path Delay: <number>
   GM Clock Identity: < 16_hex_digits >
   ```

   For example, a PTP time synchronization might look like this log entry:

   ```
   Adapter 0 time-sync status:
   Adapter 0 PTP time-sync status:
   PTP Time: Thu 26-May-2016 12:44:03.123456789 (TAI)
   Port: 192.168.3.77
   Link Status: 100M
   IPv4 Subnet Mask: 192.168.3.0
   IPv4 Gateway: 192.168.3.1
   DHCP Enabled: Yes
   Profile Id: 00:1b:1a:2b:3c:4d
   Profile: Default
   Clock Id: 00:0d:1a:2b:3c:4d
   Domain: 0
   VLAN: 0
   Delay Mechanism: E2E
   PTP Filter: None
   Delay Assemetry: 0
   Clock State: SLAVE
   Mean Path Delay: 0
   GM Clock Identity: 000de9fffe03a2aa
   ```

Verify by using the external LEDs

Use the state and color of the external LEDs to help you verify and troubleshoot your IBM QRadar Network Packet Capture installation.

The following image shows the location and function of each light on the accelerator card.

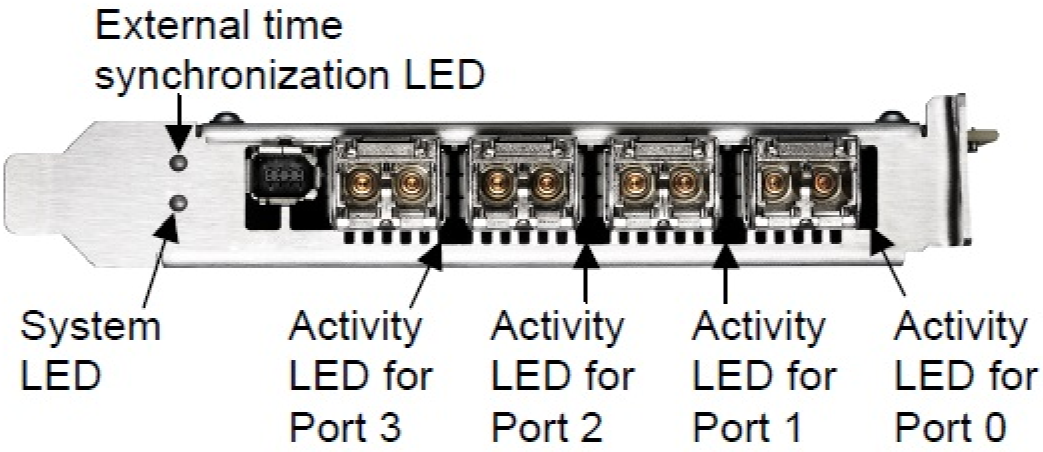


Figure 5: Location of the external LEDs

Activity LEDs

The following table describes the typical states that are indicated by the color of the Activity LEDs.

Table 6: Activity LEDs and operating status of the appliance.

State and Color	Condition
Off	The driver is not loaded, the Ethernet link is down, or the port is disconnected.
Constant green	The driver is loaded and the Ethernet link is up, but there is no traffic.
Flashing green	The driver is loaded but there is traffic on the Ethernet link.

System LED

The following table describes the typical states that are indicated by the color of the System LED.

Table 7: System LED and operating status of the appliance.

State and Color	Condition
Off	The power is off.
Constant red	During start-up and the power is on. The accelerator is checking the power supplies.
Flashing red	After start-up and the power is on, there is an unrecoverable hardware error.
Constant yellow	During start-up the power is on, and the power supplies are working.
Flashing yellow	A new entry in the hardware log.

Table 7: System LED and operating status of the appliance. (continued)

State and Color	Condition
Constant green	The FPGA is loaded, and the system is running.

External time synchronization LED

The following table describes the typical states that are indicated by the color of the external time synchronization LED.

Table 8: External time synchronization LED and the operating status of the appliance.

State and Color	Condition
Off	No driver is loaded or the Ethernet link on the Precision Time Protocol (PTP) port is down.
Constant yellow	The Ethernet link on the PTP port is up.

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.

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.