IBM QRadar Network Insights
7.4.3

Installation and Configuration Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 59.

Contents

Introduction to installing QRadar Network Insights

This guide contains information about analyzing network data in real-time by using IBM® QRadar® Network Insights.

Intended audience

Investigators extract information from the network traffic and focus on security incidents, and threat indicators.

Technical documentation

To find IBM QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical 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 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 QRadar.

Chapter 1. What's new in QRadar Network Insights

Stay up to date with the new features that are available in IBM QRadar Network Insights.

What's new in QRadar Network Insights 7.4.3

IBM QRadar Network Insights 7.4.3 is now easier to install.

Simplified installation process

Now you can install QRadar Network Insights directly from the QRadar installation media. With this simplified installation process, you do not have to download a separate installation file for QRadar Network Insights.

This change affects new installations only. The process to upgrade your deployment does not change.

Learn more about installing QRadar Network Insights...

What's new in QRadar Network Insights 7.4.2

IBM QRadar Network Insights 7.4.2 introduces stacking support for the QRadar Network Insights 1940 appliances.

QRadar Network Insights 1940 appliance stacking

You can stack the new QRadar Network Insights 1940 appliances (appliance type 6600) to scale performance by balancing the network packet data load across multiple appliances. By distributing the data processing and analysis, stacked appliances can help you handle higher data volumes and improve flow throughput performance at the highest inspection levels.

In a stacked configuration, the QRadar Network Insights 1940 appliances provide one port for incoming traffic and one port for outgoing traffic. Each appliance stack must include the same type of appliance. For example, you can't have one appliance stack that includes both QRadar Network Insights 1920 and 1940 appliances.

Learn more about stacking appliances...

What's new in QRadar Network Insights 7.4.1

IBM QRadar Network Insights 7.4.1 introduces support for 40 Gbps network connectivity.

Support for 40 Gbps connectivity

The IBM QRadar portfolio expands its threat detection capabilities with the addition of the IBM QRadar Network Insights 1940 appliance, providing the ability to deploy a dedicated appliance on a 40 Gbps network.

The IBM QRadar Network Insights 1940 appliance is available on both Lenovo (1940) and Dell (1940-C) hardware platforms with appliance ID 6600.

Network connectivity is not indicative of the data throughput levels that each appliance is capable of.

Learn more about QRadar Network Insights appliances.....

Learn more about the performance of QRadar Network Insights appliances at various flow inspection levels.....

What's new in QRadar Network Insights 7.4.0

IBM QRadar Network Insights 7.4.0 includes the following new features and enhancements to help you administer your IBM QRadar Network Insights appliances.

QRadar Network Insights software installation is now available

Now you can install QRadar Network Insights on your own hardware or as a virtual machine. This new capability provides the same type of flow analysis that was previously available only with a physical appliance that used a Napatech network interface card.

Learn more about QRadar Network Insights software installations...

Learn more about QRadar Network Insights virtual appliance installations...

Separate installation file for QRadar Network Insights

In previous releases, the QRadar Network Insights installation files were combined with the QRadar Incident Forensics installation files in a single `.iso` file. In 7.4.0, each product is installed by using a separate `.iso` file.

The process to upgrade your deployment does not change, and only a single file is required. You must ensure that you download the correct `.sfs` file for your deployment.

Note:

If your deployment does not include QRadar Incident Forensics, you can upgrade to QRadar Network Insights 7.4.0 by using the QRadar patch update file.

If your deployment includes both QRadar Network Insights and QRadar Incident Forensics, you can upgrade to QRadar Network Insights 7.4.0 by using the QRadar Incident Forensics patch update file.

Both patch update files are available on IBM Fix Central.

The following examples show what the file names might look like on IBM Fix Central:

- To install QRadar Network Insights in a new deployment, the `.iso` file name looks similar to this example:

  Rhe764qni*<build_version>*.stable-*<identifier>*.iso
- To upgrade QRadar Network Insights in a deployment that does not include QRadar Incident Forensics, the `.sfs` file name looks similar to this example:

  *<identifier>*_QRadar_patchupdate-*<build_number>*.sfs

  This `.sfs` file upgrades the entire QRadar deployment.
- To upgrade QRadar Network Insights in a deployment that does include QRadar Incident Forensics, the `.sfs` file name looks similar to this example:

  *<identifier>*_Forensics_patchupdate-*<build_number>*.sfs

  This `.sfs` file upgrades the entire QRadar deployment, including QRadar Incident Forensics and QRadar Network Insights.

Learn more about upgrading QRadar Network Insights...

Domain management for QRadar Network Insights flow sources

Now you can assign domains or tenants based on a QRadar Network Insights flow source or interface that the traffic originated from. By segmenting your network into different domains, you can ensure that information is available only to those users who need it.

Learn more about segmenting data based on flow sources...

Chapter 2. Real-time threat investigations with QRadar Network Insights

IBM QRadar Network Insights is a network threat analytics solution that provides visibility into deep application-level content to better detect insider threats, data exfiltration, and malware activity, and provides real-time analysis of network data and an advanced level of threat detection and analysis.

You can install IBM QRadar Network Insights on a QRadar appliance, or you can install it on your own hardware or a virtual appliance.

Integration with IBM QRadar Incident Forensics

QRadar Network Insights provides QRadar with deep visibility into application activities, extracts artifacts, and identifies assets, applications, and users that participate in network communications. It is tightly integrated with IBM QRadar Incident Forensics for post incident investigations and threat hunting activities.

QRadar Incident Forensics and IBM QRadar Network Packet Capture captures, reconstructs, and replays the entire conversation, but QRadar Network Insights provides the incident detection, and informs you whether suspect items or topics of interest were discussed at any time during the conversation.

Suspect content can originate from a wide variety of sources, such as malware, non-standard ports, regex, or Yara rules. For more information about suspect content, see Advanced inspection level attributes in the *QRadar Network Insights User Guide*.

Chapter 3. QRadar Network Insights appliances

QRadar Network Insights appliances connect to network TAPs, SPAN, or mirror ports to access full packet data for real-time analysis. All QRadar Network Insights appliances provide detailed analysis of network flows to extend the threat detection capabilities of QRadar.

M7 appliances

- IBM QRadar Network Insights 1901 (MTM 4723-N9C)
- IBM QRadar Network Insights 1920 (MTM 4723-N2A)
- IBM QRadar Network Insights 1940 (MTM 4723-N4B)

QRadar M6 appliances

- IBM QRadar Network Insights 1901 (MTM 4563-F8Y)
- IBM QRadar Network Insights 1910 (MTM 4563-F7Y)
- IBM QRadar Network Insights 1920 (MTM 4563-F5F)
- IBM QRadar Network Insights 1940 (MTM 4563-F6G)
- IBM QRadar Network Insights 1940-C (MTM 4654-F7G)

QRadar M5 appliances

- IBM QRadar Network Insights 1901 (MTM 4412-F4Y)
- IBM QRadar Network Insights 1901-C (MTM 4654-F6Y)
- IBM QRadar Network Insights 1910 (MTM 4412-F5Y)
- IBM QRadar Network Insights 1910-C (MTM 4654-Q9C)
- IBM QRadar Network Insights 1920 (MTM 4412-F3F)
- IBM QRadar Network Insights 1920-C (MTM 4654-F4F)

QRadar M4 appliances

- IBM QRadar Network Insights 1920-C (MTM 4531-F3F)

Appliance IDs

When you install QRadar Network Insights, you must specify the ID that matches the type of appliance that you want to install. The following table shows the appliance IDs.

Table 1. QRadar Network Insights appliances

QRadar Network Insights appliances	Appliance ID
QRadar Network Insights 1901	6300
QRadar Network Insights 1910	6400
QRadar Network Insights 1920	6200
QRadar Network Insights 1940	6600
Software or virtual appliance installations	6500

You can stack the QRadar Network Insights 1920 appliances (type 6200) to distribute network packet data across multiple Napatech cards. You cannot stack appliances in a QRadar Network Insights software installation.

For more information, see Chapter 13, “QRadar Network Insights appliance stacking,” on page 47.

Related concepts

QRadar Network Insights appliance stacking

You can stack QRadar Network Insights appliances to scale performance by load balancing the network packet data across multiple appliances. By distributing the data processing and analysis, stacked appliances can help you handle higher data volumes and improve flow throughput performance at the highest inspection levels.

Performance levels based on flow inspection levels

Chapter 4. Upgrading QRadar Network Insights

You must upgrade all of your IBM QRadar products in your deployment to the same version.

Restriction: Resizing logical volumes is not supported.

Before you begin

Custom changes that you make to QRadar configuration files do not persist when you upgrade your deployment. Before you upgrade, back up any customized configuration files so that you can refer to them after the upgrade. After the upgrade is complete, do not overwrite the new configuration files with the old files. You must manually re-apply the customized settings.

The file that you use to upgrade QRadar Network Insights depends on which products are installed in your deployment. You must download the correct upgrade file from Fix Central (www.ibm.com/support/fixcentral/).

Table 2. Patch files for upgrading QRadar Network Insights

Deployment scenario	Fix Central download
Deployment does not include QRadar Incident Forensics	Use the QRadar patch file, which looks similar to this one: `<identifier>_QRadar_patchupdate-<build_number>.sfs` This file upgrades QRadar and QRadar Network Insights appliances.
Deployment includes QRadar Incident Forensics	Use the QRadar Incident Forensics patch file, which looks similar to this one: `<identifier>_Forensics_patchupdate-<build_number>.sfs` This `.sfs` file upgrades the entire QRadar deployment, including QRadar Incident Forensics and QRadar Network Insights.

Procedure

1. Download the patch update file from IBM Fix Central (www.ibm.com/support/fixcentral).
2. Use SSH to log in to your system as the root user.
3. Copy the patch file to the `/tmp` directory or to another location that has sufficient disk space.
4. To create the `/media/updates` directory, type the following command:

   ```
   mkdir -p /media/updates
   ```
5. Change to the directory where you copied the patch file.
6. To mount the patch file to the `/media/updates` directory, type the following command:

   ```
   mount -o loop -t squashfs <patchupdate_filename>.sfs /media/updates/
   ```
7. To run the upgrade installer, type the following command:

   ```
   /media/updates/installer
   ```

   The first time that you run the patch installer script, there might be a delay before the first patch installer menu is displayed.
8. Provide answers to the pre-patch questions based on your deployment.

9. Use the upgrade installer to upgrade all hosts in your deployment.

   If your SSH session is disconnected while the upgrade is in progress, the upgrade continues. When you reopen your SSH session and rerun the installer, the installation resumes.
10. After the upgrade is complete, type the following command to unmount the software update:

    ```
    umount /media/updates
    ```

Related concepts

Troubleshooting

To isolate and resolve problems with your IBM product, use the following troubleshooting and support information.

Related tasks

Installing QRadar Network Insights software on a QRadar appliance

Creating a stack

Create a stack to help you handle higher data volumes and improve flow throughput performance at the highest inspection levels. You can stack only the QRadar Network Insights 1920 (type 6200) and QRadar Network Insights 1940 (type 6600) appliances.

Chapter 5. Installing QRadar Network Insights software on a QRadar appliance

When you purchase an IBM QRadar Network Insights appliance, QRadar Network Insights is already installed. However, you might need to reinstall the software if, for example, you have a hardware failure.

Before you begin

Before you install QRadar Network Insights, ensure that the following requirements are met:

- The appliance hardware is installed.
- A keyboard and monitor are connected by using the VGA connection.

You must download the QRadar Network Insights installation file from IBM Fix Central (www.ibm.com/support/fixcentral/).

New in 7.4.3 You can install QRadar Network Insights 7.4.3 directly from the QRadar installation media.

The following table shows which installation file is required based on the version of QRadar Network Insights that you want to install.

Table 3. QRadar Network Insights installation files

Installation version	Installation file
QRadar Network Insights 7.4.3	Use the QRadar installation file, which looks similar to this one: `<rhel_identifier>QRadar<build_number>.iso` This file installs the QRadar Console and the managed hosts, including QRadar Network Insights.
QRadar Network Insights 7.4.2, 7.4.1, or 7.4.0	Use the QRadar Network Insights installation file, which looks similar to this one: `<rhel_identifier>QNI<build_number>.iso` This file installs only the QRadar Network Insights appliance. You must use the QRadar installation file to install the QRadar Console and other managed hosts.

About this task

Install the QRadar Console on one appliance, and the QRadar Network Insights managed host on another appliance.

Restriction: Software versions for all appliances in a deployment must be the same version and fix level. Deployments that use different versions of software are not supported.

Resizing logical volumes is not supported.

QRadar Network Insights requires only a connection to the QRadar console. You can deploy QRadar Network Insights separately from the IBM QRadar Incident Forensics deployment.

Procedure

1. Download the ISO installer from Fix Central (www.ibm.com/support/fixcentral/).
2. Mount the ISO installation file.

a) Map the ISO to a device for your appliance by using the Integrated Management Module (IMM) or the Integrated Dell Remote Access Controller (iDRAC), or insert a bootable USB drive that you've created with the ISO.

   For information about creating a bootable USB flash drive, see "USB flash drive installations" in *IBM QRadar Installation Guide*.

b) Restart your appliance.

3. When prompted, type `flatten` and press Enter.
4. Follow the instructions in the installation wizard.

   On the **Select the Appliance ID** page, choose from the following appliance ID options:

Table 4. QRadar Network Insights appliances

QRadar Network Insights appliances	Appliance ID
QRadar Network Insights 1901	6300
QRadar Network Insights 1910	6400
QRadar Network Insights 1920	6200
QRadar Network Insights 1940	6600
Software or virtual appliance installations	6500

   The QRadar Network Insights appliance reboots during the installation.
5. Add the QRadar Network Insights managed host to QRadar:
   a) Log in to QRadar:

      `https://`*`IP_Address_QRadar`*

      The default user name is `admin`. The password is the password of the root user account.

   b) On the **Admin** tab, in the **System Configuration** section, click **System and License Management**.
   c) In the **Display** list, select **Systems**.
   d) On the **Deployment Actions** menu, click **Add Host**.
   e) Configure the settings for the managed host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.
   f) Click **Add**.
   g) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.
6. Apply your license key.
   a) On the **Admin** tab, click **System Configuration**.
   b) Click the **System and License Management** icon.
   c) From the **Display** list, select **Licenses**, and upload your license key.
   d) Select the unallocated license and click **Allocate System to License**.
   e) From the list of licenses, select the license, and click **Allocate License to System**.

   Apply your QRadar Network Insights license key to the managed host.

What to do next

After you install the QRadar Network Insights software, you must add the appliance to the QRadar Console as a managed host and then configure it.

Related concepts

Appliance configuration

QRadar Network Insights software installations on your own hardware

QRadar Network Insights software installations on VMWare ESXi

Troubleshooting

To isolate and resolve problems with your IBM product, use the following troubleshooting and support information.

Related tasks

Upgrading QRadar Network Insights

Adding the QRadar Network Insights appliance as a managed host

Chapter 6. Adding the QRadar Network Insights appliance as a managed host

After you install the QRadar Network Insights appliance, you must add the appliance to the QRadar Console as a managed host.

Before you begin

Ensure that the QRadar Network Insights appliance uses the same software version and fix pack level as the QRadar Console that you are using to manage it.

Procedure

1. Log in to the QRadar Console as an administrator.
2. On the navigation menu ( ), click **Admin**.
3. In the **System Configuration** section, click **System and License Management**.
4. In the **Display** list, select **Systems**.
5. On the **Deployment Actions** menu, click **Add Host**.
6. Configure the settings for the QRadar Network Insights managed host and then click **Add**.
7. On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

   Important: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

What to do next

Configure the QRadar Network Insights appliance.

Optionally, you can install the QRadar Network Insights content extension. The content extension includes custom rule engine content, including rules, searches, reports, and custom property extractions, that provide analysis, alerts, and reports for QRadar Network Insights.

Related tasks

Installing QRadar Network Insights software on a QRadar appliance

Chapter 7. QRadar Network Insights software installations on your own hardware

New in 7.4.0

You can install QRadar Network Insights on your own hardware. The software installation uses a Red Hat Enterprise Linux operating system that you provide.

Complete the following tasks in order:

__ 1. Ensure that your system meets the minimum system requirements for QRadar Network Insights installations.

__ 2. Ensure that you have entitlement for a QRadar Software Node. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

__ 3. Install Red Hat Enterprise Linux (RHEL).

__ 4. Install QRadar Network Insights

You cannot stack appliances in a QRadar Network Insights software installation.

Related concepts

QRadar Network Insights software installations on VMWare ESXi

Related tasks

Installing QRadar Network Insights software on a QRadar appliance

Prerequisites for installing QRadar Network Insights on your own appliance

Before you install IBM QRadar Network Insights on your own appliance, ensure that you follow these installation guidelines and that your hardware meets the system requirements.

Installation requirements

Follow these guidelines when installing QRadar Network Insights software on your own appliance:

- You must acquire entitlement to a QRadar Software Node for a QRadar Network Insights software installation.

  To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.
- Do not install software other than QRadar Network Insights on your hardware.

  Unapproved RPM installations can cause dependency errors when you upgrade QRadar Network Insights software and can also cause performance issues in your deployment.
- Do not update your operating system or packages before or after QRadar Network Insights installation.

Minimum system requirements

The following table describes the system requirements for QRadar Network Insights software installations:

Restriction: Resizing logical volumes is not supported.

Table 5. Minimum system requirements for QRadar Network Insights software installations

Requirement	Details
CPU	The system must use a processor that is supported by the Red Hat Enterprise Linux (RHEL) version that is required for the QRadar Network Insights installation. To determine which version of RHEL is required, see "Installing RHEL on your hardware" on page 16. To determine which processors are supported by the version of RHEL, refer to the vendor documentation. Virtualization hardware extensions such as Intel VT or AMD-V must be enabled in the BIOS. This requirement does not apply to the following systems: • Appliances that have a Napatech card. • Virtual hosts such as EC2 instances and VMware guests.
Storage	Capacity: 480 GB IOPS: 300 Data transfer rate (MB/s): 300
Memory (RAM)	64 GB If a memory upgrade is required, you must upgrade it before you install QRadar Network Insights.
Network capture cards	One of the following network interface cards for traffic capture: • Napatech NT40E3 • Intel x520 • Intel x710 Maximum of one capture card per host.
Network management interface	One of the following network interface cards for management: • RJ-45 10/100/1000 Mb Ethernet systems management port • 10 GbE SFP+ port

Installing RHEL on your hardware

Your appliance must have the Red Hat Enterprise Linux (RHEL) operating system installed on it before you install IBM QRadar Network Insights.

Before you begin

Download the Red Hat Enterprise Linux Server ISO x86_64 Boot ISO from https://access.redhat.com
Refer to the Red Hat version table to choose the correct version.

Table 6. Red Hat version	
IBM QRadar version	**Red Hat Enterprise Linux version**
IBM QRadar 7.4.0	Red Hat Enterprise Linux V7.6 64-bit
IBM QRadar 7.4.1	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.2	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.3	Red Hat Enterprise Linux V7.7 64-bit

You must acquire entitlement to a QRadar Software Node for a QRadar Network Insights software installation. To acquire entitlement to a QRadar Software Node, contact your QRadar Sales Representative.

Procedure

1. Map the ISO to a device for your appliance by using the Integrated Management Module (IMM) or the Integrated Dell Remote Access Controller (iDRAC), or insert a bootable USB drive with the ISO.

   For information about creating a bootable USB flash drive, see "USB flash drive installations" in *IBM QRadar Installation Guide*.
2. Insert the portable storage device into your appliance and restart your appliance.
3. From the starting menu, do one of the following options:
   - Select the device that you mapped the ISO to, or the USB drive, as the boot option.
   - To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in `legacy` mode.
4. When prompted, log in to the system as the root user.
5. Follow the instructions in the installation wizard to complete the installation:
   a) Set the language to English (US).
   b) Click **Date & Time** and set the time for your deployment.
   c) Click **Software selection** and select **Minimal Install**.
   d) Click **Installation Destination** and select the **I will configure partitioning** option.
   e) Select **LVM** from the list.
   f) Click the **Add** button to add the mount points and capacities for your partitions, and then click **Done**.
   g) Click **Network & Host Name**.
   h) Enter a fully qualified domain name for your appliance host name.
   i) Select the interface in the list, move the switch to the **ON** position, and click **Configure**.
   j) On the **General** tab, select the **Automatically connect to this network when it is available** option.
   k) On the **IPv4 Settings** or **IPv6 Settings** tab, select **Manual** in the **Method** list.
   l) Click **Add**.
      - For an IPv4 deployment, enter the IP address, Netmask, and Gateway for the appliance in the **Addresses** field.
      - For an IPv6 deployment, enter the IP address, Prefix, and Gateway in the **Addresses** field.

   m) Add two DNS servers.
   n) Click **Save** > **Done** > **Begin Installation**.
6. Set the root password, and then click **Finish configuration**.
7. After the installation finishes, disable SELinux by modifying the `/etc/selinux/config` file, and restart the appliance.

What to do next

"Installing QRadar Network Insights on your own hardware" on page 18

Installing QRadar Network Insights on your own hardware

New in 7.4.0

You can install IBM QRadar Network Insights 7.4.0 or later on your own hardware.

Software installations for earlier versions of QRadar Network Insights are not supported.

Before you begin

Download the installation file from Fix Central (www.ibm.com/support/fixcentral/). The following table shows which installation file is required based on the version of QRadar Network Insights that you want to install.

Table 7. QRadar Network Insights installation files

Installation version	Installation file
QRadar Network Insights 7.4.3	Use the QRadar installation file, which looks similar to this one: *<rhel_identifier>*QRadar*<build_number>*.iso This file installs the QRadar Console and the managed hosts, including QRadar Network Insights.
QRadar Network Insights 7.4.2, 7.4.1, or 7.4.0	Use the QRadar Network Insights installation file, which looks similar to this one: *<rhel_identifier>*QNI*<build_number>*.iso This file installs only the QRadar Network Insights appliance. You must use the QRadar installation file to install the QRadar Console and other managed hosts.

Procedure

1. Copy the installation `.iso` file to the device.
2. Create the `/media/cdrom` directory by typing the following command:

   ```
   mkdir /media/cdrom
   ```

3. Mount the `.iso` file by using the following command:

   ```
   mount -o loop <software_installation_file.iso> /media/cdrom
   ```

4. Run the installation setup wizard by using the following command:

   ```
   /media/cdrom/setup
   ```

   Note: A new kernel might be installed as part of the installation, which requires a system restart. Repeat the commands in steps 3 and 4 after the system restart to continue the installation.
5. On the **Software Installed System** window, select **Software Install**.
6. On the **Software Appliance Assignment** window, choose **Network Insights**.
7. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**
8. Select the continent and time zone.

   The default selection is the time zone that is specified in the Red Hat Enterprise Linux install.
9. On the **Management Interface Setup** window, select the management interface.

10. On the **Network Information Setup** window, the host name and IP address is automatically loaded.

    You can enter a static IP address, or use the assigned IP address.
11. On the **Root Password Setup** window, set a password.

    This is the password that you use to add the managed host to the QRadar Console.
12. Click **Finish**.
13. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.
14. Add the QRadar Network Insights managed host to QRadar:
    a) Log in to QRadar:
    `https://`*`IP_Address_QRadar`*

    The default user name is `admin`. The password is the password of the root user account.
    b) On the **Admin** tab, in the **System Configuration** section, click **System and License Management**.
    c) In the **Display** list, select **Systems**.
    d) On the **Deployment Actions** menu, click **Add Host**.
    e) Configure the settings for the managed host by providing the fixed IP address and the root password.
    f) Click **Add**.
    g) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.
15. Apply your license key.
    a) On the **Admin** tab, click **System Configuration**.
    b) Click the **System and License Management** icon.
    c) From the **Display** list, select **Licenses**, and upload your license key.
    d) Select the unallocated license and click **Allocate System to License**.
    e) From the list of licenses, select the license, and click **Allocate License to System**.

    Only the QRadar Network Insights managed host requires a license. The QRadar Console does not need a QRadar Network Insights license.

Chapter 8. QRadar Network Insights software installations on VMWare ESXi

New in 7.4.0

You can install QRadar Network Insights software on a VMWare ESXi virtual machine.

A virtual appliance provides the same visibility and function in your virtual network infrastructure that QRadar Network Insights appliances provide in your physical environment.

To install a virtual appliance, complete the following tasks in order:

__ • Ensure that your virtual appliance meets the minimum system requirements.

__ • Create a virtual machine.

__ • Install QRadar Network Insights software on the virtual machine.

__ • Add the virtual appliance to your QRadar deployment.

You cannot stack virtual QRadar Network Insights appliances.

Your ESXi server network adapter must be in promiscuous mode for your QRadar Network Insights virtual appliances to receive network traffic.

Important: Do not install software other than QRadar Network Insights on the virtual machine.

Related concepts

QRadar Network Insights software installations on your own hardware

Related tasks

Installing QRadar Network Insights software on a QRadar appliance

Minimum system requirements for virtual appliance installations for QRadar Network Insights

Before you install IBM QRadar Network Insights, ensure that your virtual appliance meets these minimum system requirements.

Table 8. Requirements for virtual appliances

Requirement	Description
VMware Server	VMware ESXi Version 6.7+ For more information about VMWare clients, see the VMware website (www.vmware.com)
VMware compatibility level	Hardware version 14+ (ESXi 6.7+)
VMware CPU settings	Enable hardware virtualization passthrough. Enable I/O MMU.
Virtual disk size	480 GB
Network adapters	At least two network adapters are required. One adapter is dedicated to network management, and at least one more adapter is required for network capture.

Table 8. Requirements for virtual appliances (continued)	
Requirement	**Description**
CPU cores	28 cores
Cores per socket	28 (Sockets: 1) If you are using a higher number of cores and monitoring a single network interface, place as many cores on a single socket as possible.
Memory	64 GB

Installing QRadar Network Insights software on a virtual machine

New in 7.4.0 You can install QRadar Network Insights 7.4.0 or later on a virtual machine. Installing earlier versions of QRadar Network Insights is not supported.

After you create your virtual machine, install the QRadar Network Insights software.

Restriction: Resizing logical volumes is not supported.

Before you begin

Download the installation file from Fix Central (www.ibm.com/support/fixcentral/). The following table shows which installation file is required based on the version of QRadar Network Insights that you want to install.

Table 9. QRadar Network Insights installation files	
Installation version	**Installation file**
QRadar Network Insights 7.4.3	Use the QRadar installation file, which looks similar to this one: *<rhel_identifier>*QRadar*<build_number>*.iso This file installs the QRadar Console and the managed hosts, including QRadar Network Insights.
QRadar Network Insights 7.4.2, 7.4.1, or 7.4.0	Use the QRadar Network Insights installation file, which looks similar to this one: *<rhel_identifier>*QNI*<build_number>*.iso This file installs only the QRadar Network Insights appliance. You must use the QRadar installation file to install the QRadar Console and other managed hosts.

Procedure

1. In the left navigation pane of your VMware vSphere Client, select your virtual machine.
2. In the right pane, click the **Summary** tab.
3. In the **Commands** pane, click **Edit Settings**.
4. In the left pane of the **Virtual Machine Properties** window, click **CD/DVD Drive 1**.
5. In the **Device Status** pane, select the **Connect at power on** check box.
6. In the **Device Type** pane, select **Datastore ISO File** and click **Browse**.
7. In the **Browse Datastores** window, locate and select the ISO file, click **Open** and then click **OK**.
8. After the ISO image is installed, right-click your virtual machine and click **Power** > **Power On.**

Note: The installation process takes approximately one hour to complete.

9. Log in to the virtual machine by typing `root` for the user name.

   The user name is case-sensitive.

10. Review the **End User License Agreement** (EULA) and accept the license.

    Tip: Press the Space bar to advance through the document.

11. Select **Software Install**.
12. On the **Select the Appliance ID** page, choose **QRadar Network Insights Software (6500)**.
13. For the type of setup, select **normal**.
14. Follow the instructions in the installation wizard to complete the installation.

    The **Network Information Setup** window prompts for the following network settings:

    - Host name (fully qualified domain name)
    - IP Address
    - Network Mask
    - Gateway
    - Primary DNS
    - Secondary DNS (Optional)
    - Public IP address (Not supported)

    After you configure the installation parameters, a series of messages are displayed. The installation process might take several minutes.

15. Add the QRadar Network Insights managed host to QRadar:
    a) Log in to QRadar:
    `https://`*`IP_Address_QRadar`*

    The default user name is `admin`. The password is the password of the root user account.

    b) On the **Admin** tab, in the **System Configuration** section, click **System and License Management**.
    c) In the **Display** list, select **Systems**.
    d) On the **Deployment Actions** menu, click **Add Host**.
    e) Configure the settings for the managed host by providing the fixed IP address, and the root password to access the operating system shell on the appliance.
    f) Click **Add**.
    g) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.
16. Apply your license key.
    a) On the **Admin** tab, click **System Configuration**.
    b) Click the **System and License Management** icon.
    c) From the **Display** list, select **Licenses**, and upload your license key.
    d) Select the unallocated license and click **Allocate System to License**.
    e) From the list of licenses, select the license, and click **Allocate License to System**.

    Only the QRadar Network Insights managed host requires a license. The QRadar Console does not need a QRadar Network Insights license.

Chapter 9. QRadar Network Insights installations on Amazon Web Services

You can send your Amazon Web Services (AWS) network traffic to IBM QRadar Network Insights for content inspection and monitoring.

To deploy QRadar Network Insights on Amazon Web Services (AWS), follow this procedure:

__ 1. Review the minimum system requirements.

Ensure that the instance that you plan to install meets the minimum system requirements.

__ 2. Use the IBM QRadar SIEM `.ami` image on AWS Marketplace to install the QRadar components.

You must install a QRadar Console and a QRadar Network Insights managed host. Other managed hosts, such as flow processors, are optional.

For information about how to install QRadar components on AWS, see Configuring a QRadar 7.4.3 virtual appliance on Amazon Web Services.

__ 3. Add the QRadar Network Insights managed host to the QRadar Console.

__ 4. Configure the flow sources.

__ 5. Configure a traffic mirroring session.

__ 6. Verify that the deployment is receiving flow data.

Deployment architecture

The following image shows the traffic flow in a deployment that includes two QRadar Network Insights mirror targets. One QRadar Network Insights instance is used as a flow source for a Flow Processor, while the other instance sends network traffic directly to the QRadar Console.

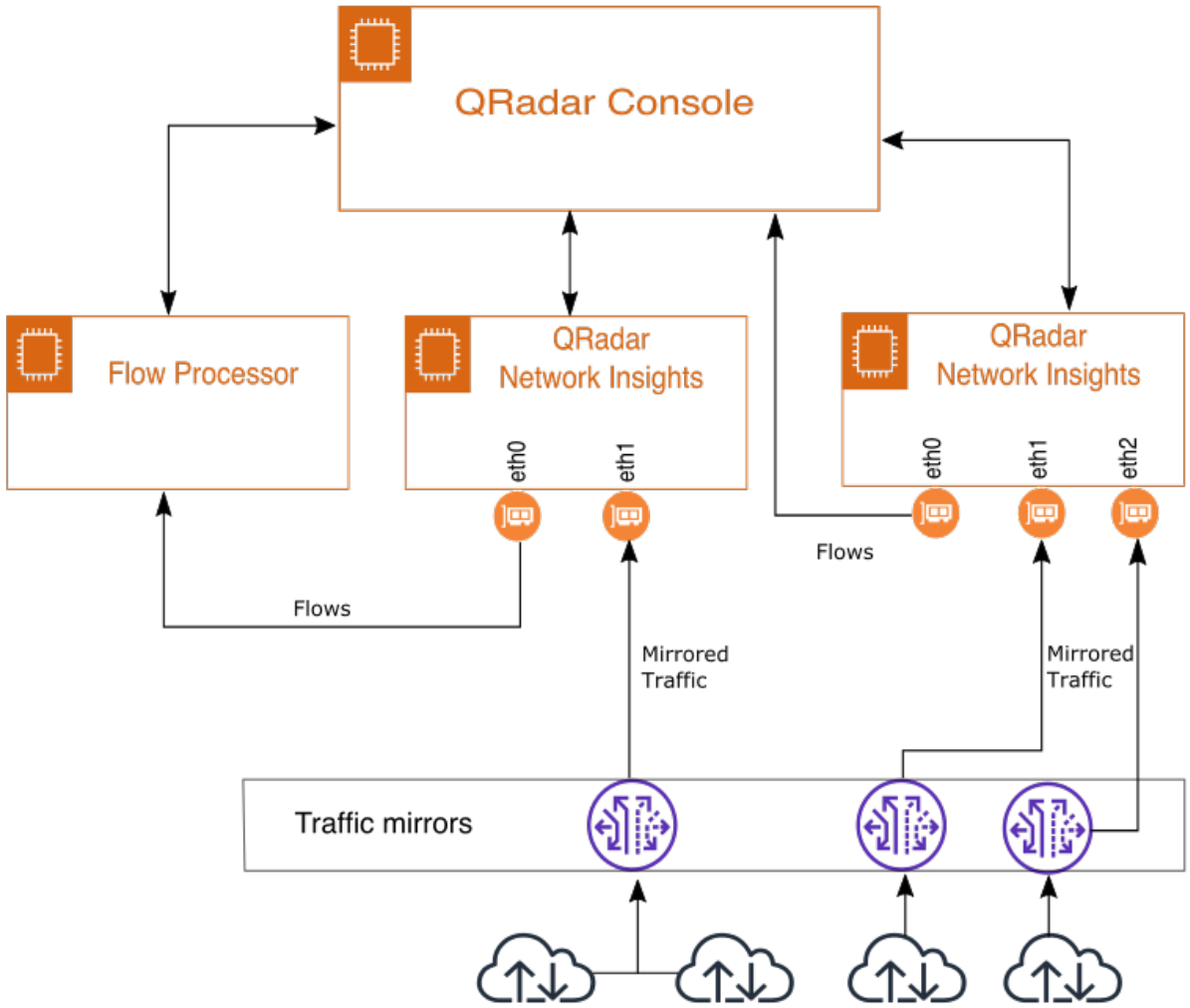


Figure 1. Example of a QRadar Network Insights deployment on Amazon Web Services

Related information

Deploying a QRadar Console in AWS (YouTube video)

Deploying a QRadar Managed Host in AWS (YouTube video)

System requirements for QRadar Network Insights on Amazon Web Services installations

To prepare for the IBM QRadar Network Insights installation, ensure that your virtual appliance meets the minimum system requirements.

The QRadar Network Insights instance must meet the following requirements:

Requirement	Value
Processor	8 cores (minimum) **Tip:** To see the number of cores that are included in each instance type, in the AWS **Launch an instance** window, click **Compare instance types**. Click the gear ( ) icon to include the **Cores** column in the table.
Memory	64 GB (minimum)

Requirement	Value
Storage	QRadar Network Insights requires two EBS General Purpose SSD volumes: • 1 x 122 GiB (OS and Software) • 1 x 250 GiB (Data) The 122 GiB volume for the OS and software is configured automatically by the QRadar `.ami`. You must configure the additional 250 GiB volume for data manually. **Warning:** It is not possible to increase storage after installation.
Networking	QRadar Network Insights requires a minimum of two NIC interfaces: • One management interface • One monitoring interface For larger compute-optimized instance types, you can add more monitoring interfaces. The Maximum Transmission Unit (MTU) for the monitoring interface must be set to 9001.
Security Groups	The management interface must have an assigned security group that includes rules to allow SSH, NetFlow, and messaging connections between the QRadar Network Insights host and the QRadar Console and any flow collectors or processors that might be installed. The monitoring interface must have an assigned security group that allows VXLAN traffic (UDP port 4789) from the mirror source. The Network ACL (VPC) level also must allow VXLAN traffic.

To view the system requirements for other IBM QRadar virtual appliances, see System requirements for virtual appliances in the *IBM QRadar Installation Guide*.

Examples of QRadar Network Insights appliance specifications

You must ensure that the instance type and configuration of the QRadar Network Insights instance can support the flow inspection level that you want to achieve.

The following table shows examples of hardware configurations and the performance impact that it can have at various inspection levels. You can use this information as a guideline when you size your virtual appliance.

Note: System performance and data throughput depend on many factors, including the volume and type of files that are observed in the network traffic. Individual performance improvements are not guaranteed.

Table 10. Examples of QRadar Network Insights virtual appliance configurations

CPUs	Memory (GiB)	Maximum monitoring interfaces	Flow inspection level performance
8 cores	64	1	Basic: 1 Gbps Enriched: 800 Mbps Advanced: 300 Mbps

Table 10. Examples of QRadar Network Insights virtual appliance configurations (continued)			
CPUs	**Memory (GiB)**	**Maximum monitoring interfaces**	**Flow inspection level performance**
20 cores	160	2	Basic: 2 Gbps Enriched: 1.8 Gbps Advanced: 750 Mbps * Performance is aggregate across all monitoring interfaces.

Related information

General purpose instances (AWS Documentation)

CPU cores and threads per CPU core per instance type (AWS Documentation)

Traffic mirroring

Traffic mirroring sends network traffic from an Amazon EC2 instance (source) to a IBM QRadar Network Insights instance (target) for content inspection and monitoring.

You use the Amazon Web Services (AWS) Management Console to attach an elastic IP address to your QRadar Network Insights instance. Then, you create a traffic mirroring session and define the filters that determine which traffic to forward to the QRadar Network Insights instance.

Before you can configure traffic mirroring, you must have a QRadar Network Insights instance with a monitoring interface that is attached to it.

To configure traffic mirroring, follow this general procedure.

1. Identify the Interface ID of the Amazon EC2 instance that forwards the mirrored traffic. You use this ID when you create the mirror session.
2. Assign an Elastic IP address to the Amazon EC2 instance that forwards the mirrored traffic.
3. Create a mirror target to specify which instance receives the mirrored traffic.
4. Create a mirror filter to specify what traffic gets sent to the target instance.

   When you configure the traffic mirroring rules, you can use the following parameters to mirror all inbound traffic. To reduce the overhead of traffic mirroring, you can change the parameters to mirror only certain types of traffic. For example, you can mirror only TCP protocols or traffic for a specific source or destination.

Parameter	Value
Rule action	Accept
Protocol	All protocols
Source CIDR block	0.0.0.0/0
Destination CIDR block	0.0.0.0/0

5. Create a mirror session to start mirroring traffic between the source and target instances.

For more information about AWS traffic mirroring and how to set it up, see What is traffic mirroring? in the Amazon Web Services documentation portal.

Related tasks

Verifying that the QRadar Network Insights host is receiving flow data

Related information

What is Traffic Mirroring? (AWS Documentation)

Adding another traffic monitoring interface to the QRadar Network Insights instance

Follow these steps if you want to add another traffic monitoring interface after you install IBM QRadar Network Insights.

Procedure

1. Create a network interface and add it to the QRadar Network Insights instance.
   a) Create a network interface in the same VPC and subnet as your QRadar Network Insights instance.

      Give it a name that you can easily recognize.
   b) Attach the interface to your QRadar Network Insights instance.
   c) In the AWS Console, view the QRadar Network Insights instance and note the new device name. For example, the device name might be `eth2`.
2. Use SSH to log in to the QRadar Console as root user.
3. From the QRadar Console, use SSH to connect to the QRadar Network Insights instance as root user.
4. Specify the configuration parameters for the QRadar Network Insights instance.
   a) Create the per-interface configuration file `/etc/sysconfig/network-scripts/ifcfg-<device name>` where *<device name>* is the name of the interface.
   b) Edit the configuration file and add or update the following parameters:

```
BOOTPROTO=none
DEVICE=<device name>
IPV6INIT=no
ONBOOT=yes
MTU=9001
```

5. Restart the `hostcontext` service.

```
systemctl restart hostcontext
```

6. Verify that the new interface is added to the device list file.

```
/opt/qradar/conf/capabilities/device.list
```

What to do next

Log in to QRadar and add a flow source for the new network interface. Ensure that the flow source is enabled.

Related information

Adding a flow source

Enabling flow sources

Verifying that the QRadar Network Insights host is receiving flow data

After the traffic mirror session is configured, you can verify that the IBM QRadar Network Insights managed host is receiving flow data.

Before you begin

You must configure a QRadar Console and a QRadar Network Insights managed host in your Amazon Web Services (AWS) environment.

You must configure a traffic mirroring session to forward traffic to the monitoring interface.

Procedure

1. Use SSH to log in to the target QRadar Network Insights instance.
2. To verify that the traffic is reaching the QRadar Network Insights instance, type this command:

   ```
   tcpdump -i <eth1>
   ```

   where <eth1> is the Interface Name of the mirror target.
3. Alternatively, you can configure Amazon CloudWatch Logs.

   Amazon CloudWatch Logs collect data about the flow logs that are sent to the QRadar Network Insights monitoring interface. The flow log data is useful when you want to verify that QRadar Network Insights is receiving mirrored traffic.

   For more information, see What is Amazon CloudWatch? in the AWS documentation portal.

Related concepts

Traffic mirroring

Troubleshooting QRadar Network Insights on Amazon Web Services

Troubleshooting QRadar Network Insights on Amazon Web Services

Use this information to help you troubleshoot your IBM QRadar Network Insights on Amazon Web Services (AWS) deployment.

Unable to connect to a managed host due to unprotected private key file

You receive the following warning when you try to connect to a managed host by using a private key file.

```
WARNING: UNPROTECTED PRIVATE KEY FILE!
```

You might receive this message when the `.pem` key file is publicly readable. To resolve this problem, change the permissions on your `.pem` key file to 600 by typing this command:

```
chmod 600 <key_file>
```

Connection refused when trying to connect to the QRadar Network Insights host

When you try to connect to your disconnected QRadar Network Insights host by using a private key, you receive this message:

```
Connection Refused
```

The security profile that is attached to the QRadar Network Insights managed host instance does not allow incoming SSH connections from the source IP address.

To resolve this problem, add an incoming rule to the security profile that is attached to the QRadar Network Insights instance. Configure the rule to allow SSH connections from the source IP address.

For more information, see Security profiles on the AWS Documentation portal.

A public IP address is not assigned to the QRadar Network Insights instance

This problem might occur under the following conditions:

- The instance was not configured to have a public IP address assigned automatically when it is launched.
- Multiple network interfaces are attached to the instance and it was restarted.

To resolve this issue, associate an Elastic IP to the management interface. Alternatively, you can use SSH from either the QRadar Console or another instance on the same subnet to connect to the private IP address of the QRadar Network Insights instance.

QRadar Network Insights does not see extra NIC card

You added an extra network interface card (NIC) to the QRadar Network Insights instance, but it is not recognized. More configuration is required for the operating system on the QRadar Network Insights instance to recognize the new network interface.

For more information, see "Adding another traffic monitoring interface to the QRadar Network Insights instance" on page 29.

Unable to connect to the QRadar Network Insights managed host by using SSH from the QRadar Console

When a QRadar Network Insights host is managed by a console, the iptables rules are updated to restrict direct SSH access. You must connect to the managed host by first connecting to the QRadar Console. Since AWS instances do not have a console connection option, there is no way to connect to the managed host if the QRadar Console is unable to use SSH to log in.

To resolve this problem, use SSH to connect to the QRadar Console. Then, use SSH from the QRadar Console to the managed hosts management interface (eth0) as root user.

If the QRadar Console can't connect to the managed host, you should re-create the QRadar Network Insights instance.

To avoid locking yourself out of QRadar, configure the firewall on the managed host to allow SSH connections from trusted sources. For more information, see the *Managing IPtables firewall ports* Technical Note on the IBM Support website.

Monitored traffic doesn't show up on the Network Activity tab

Monitored traffic does not show up on the Network Activity tab, but the `tcpdump` command indicates that the monitoring interface is receiving it.

When you add a QRadar Network Insights host, a flow source is created but it is disabled by default.

To resolve this problem, verify that the flow source for the network interface exists for both the QRadar Network Insights appliance and the monitoring instance. Ensure that there are no changes to be deployed. If the flow source does not exist, create it and enable it.

For more information, see Adding a flow source and Enabling a flow source.

Mirrored traffic is not received by multiple mirror targets

Traffic mirroring can send individual packets to only a single target interface. To split traffic between targets, you must set up multiple mirror sessions. The mirror filters for each session must be specific enough to ensure that the traffic is mirrored to only a single target interface.

To see an example of how to split traffic between targets, see Example: Mirror inbound TCP and UDP traffic to two different appliances on the AWS Documentation portal.

The QRadar Network Insights monitoring interface does not receive mirrored traffic

By default, AWS enables filtering based on source and destination checks on the network interfaces.

Disabling the source and destination checks allows an instance to handle network traffic that isn't destined for the instance. For example, instances that run services such as network address translation, routing, or a firewall should disable the source and destination check attributes.

To disable the source and destination check attributes, follow these steps:

1. In the left navigation pane of the AWS Dashboard, click Network interfaces.
2. Right-click on the instance and click **Change Source/Dest Check**.
3. Click **Disabled** and click **Change**.
4. Repeat the steps for each network interface.

For more information, review Elastic Network interface (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html) on the AWS Documentation portal.

Mirrored traffic is incomplete

The following traffic types cannot be mirrored:

- ARP
- DHCP
- Instance metadata service
- NTP
- Windows activation

For more information, see the following pages on the AWS Documentation Portal.

- What is Traffic Mirroring? (https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html)
- Traffic Mirroring quotas and considerations (https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-considerations.html)

QRadar Network Insights instance fails the AWS system status check

Jumbo frames can sometimes cause the QRadar Network Insights instance to restart, resulting in an AWS system status check failure.

To resolve this problem, set the Maximum Transmission Unit (MTU) for the monitoring interface to 9001.

- To change the MTU temporarily, type this command:

```
sudo ip link set dev eth<#> mtu 9001
```

- To set the MTU permanently, edit the `/etc/sysconfig/network-scripts/ifcfg-eth<#>` script for the interface, and edit the MTU line to `MTU=9001`.

For more information, see Network maximum transmission unit (MTU) for your EC2 instance (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html) on the AWS Documentation portal.

Related tasks

Verifying that the QRadar Network Insights host is receiving flow data

Chapter 10. Appliance configuration

After your IBM QRadar Network Insights appliance is installed, you must attach the appliance to the QRadar Console as a managed host.

On initial installation, QRadar Network Insights is configured to capture a maximum of 64 bytes of raw payload data. There are a number of configuration changes that you can make after the software is installed, such as changing the size of the payload capture, the flow collector format, and traffic decryption settings.

After the appliance is configured, it reads the raw packets from the network tap or span port and then generates IPFIX packets. The IPFIX packets are sent to flow processes in the deployment.

Related tasks

Installing QRadar Network Insights software on a QRadar appliance

Configuring the size of the raw payload data capture

You can use IBM QRadar Network Insights to extract raw payload data.

The **Maximum Raw Payload Size** for each appliance is inherited from the QRadar Network Insights global settings.

About this task

On initial installation, IBM QRadar Network Insights is configured to capture a maximum of 64 bytes of raw payload data. To stop capturing payload data, set the **Maximum Raw Payload Size** to 0.

When you change the global setting, the new value is inherited by all QRadar Network Insights appliances that are configured to use the global setting. This includes new appliances that you add after the setting is changed.

For QRadar Network Insights 6200, 6600, 6610 appliances, you can override the global settings by configuring custom **Maximum Raw Payload Size** settings. After an appliance is configured to use a custom setting, it is not affected by changes to the global setting. To revert an appliance back to using the global setting, you must edit the host connection and set the **Maximum Raw Payload Size** to **Global**.

Note:

You can increase the raw payload size up to 32 768 bytes, but larger payloads can impact performance. Adjust the byte size in small increments, and monitor the disk capacity to ensure that it does not fill up quickly.

If the size of the QRadar Network Insights maximum raw payload is larger than the QFlow content capture length, some payloads might be truncated. Ensure that the QFlow capture is the same size or greater than the QRadar Network Insights payload size. For more information about flows, see Flow Sources.

Procedure

1. Log in to QRadar as an administrator.
2. To configure the global settings, follow these steps:
   a) On the **Admin** tab, click **System Settings**.
   b) Click **QRadar Network Insights Settings**.
   c) In the **Maximum Raw Payload Size**, select the maximum amount of data that you want to capture.

      To turn payload data capture off, set the **Maximum Raw Payload Size** to 0.

      Appliances that use a custom **Maximum Raw Payload Size** setting are not affected by changes to the global setting. You must configure the customized appliances individually.

d) Click **Save**.

3. To configure the settings for individual QRadar Network Insights appliances, follow these steps:
   a) On the **Admin** tab, click **System and License Management**.
   b) Select the appliance that you want to modify, and click **Deployment actions** > **Edit Host Connection**.
   c) Set the flow collector and the flow source connection and click **Save**.
   d) Specify the **Maximum Raw Payload Size** for the appliance.

      Appliances that are configured to use a custom **Maximum Raw Payload Size** are not affected by future changes to the global setting.

   e) Click **Next** and then click **Save**.
4. From the menu bar on the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

   Warning: When you deploy the full configuration, QRadar services restart. During this time, events and flows are not collected, and offenses are not generated.

5. Refresh your web browser.

Configuring the Flow Collector format

Flow collectors can export data to flow processors in either TLV (type-length-value) or Payload format.

The TLV format stores the content metadata properties in the flow record, and can be searched without extra configuration in QRadar.

The payload format stores the content metadata properties in the **payload** field of the flow record. To run searches on the data, you must use custom properties to extract the data from the payload.

Before you begin

Before you configure the format that the Flow Collector uses, ensure that you complete the following tasks:

__ • Install a QRadar Console with a QRadar Network Insights appliance attached as a managed host.

__ • Perform a full deployment after you attach the IBM QRadar Network Insights appliance as a managed host.

Important: Content extension v1.3.0 introduced support for TLV fields, which supersedes earlier content extensions that were based on custom properties. If you are using content extension v1.3.0 or later, you must set the flow collector format to TLV; otherwise the rules in the content pack don't work.

Procedure

1. Log in to QRadar: `https://QRadar_IP_Address`

   The default user name is `admin`. The password is the password of the root user account.

2. On the navigation menu (☰), click **Admin**.
3. In the navigation pane, click **System Settings**.
4. Click the **QFlow Settings** menu, and in the **IPFIX Additional Field Encoding** field, choose the format.

Table 11. QFlow format options	
Flow Collector format	**Description**
TLV	Default setting for the flow collector format. Must be used when there is a QRadar Network Insights appliance in the environment. QRadar Network Insights V7.3.0 or later supports only TLV for content flows. Can be used when there is no QRadar Network Insights appliance in the environment.
`Payload`	Can be used when there is no QRadar Network Insights appliance in the environment.

5. Click **Save**.
6. From the menu bar on the **Admin** tab, click **Deploy Full Configuration** and confirm your changes.

Warning: When you deploy the full configuration, QRadar services are restarted. During this time, events and flows are not collected, and offenses are not generated.

7. Refresh your web browser.

Configuring the DTLS communications protocol

To prevent eavesdropping and tampering, you can set up Datagram Transport Layer Security (DTLS) on a QRadar Network Insights managed host. This encrypts the IPFIX connection between the QRadar Network Insights managed host and the Flow Processor or Flow Collector that receives the traffic.

Configuring DTLS is optional, and is not required for QRadar Network Insights to work.

Before you begin

Ensure that your QRadar Network Insights appliance is attached as a managed host. For more information, see Chapter 6, “Adding the QRadar Network Insights appliance as a managed host,” on page 13.

About this task

You can have more than one QRadar Network Insights appliance that points to a single DTLS port, but configuring multiple DTLS ports is not supported.

After you configure the DTLS communications protocol, if you change the QRadar Flow Collector or flow source of any QRadar Network Insights managed hosts in your deployment, you must deploy the changes.

Procedure

1. On the **Admin** tab, in the **System Configuration** section, click **System and License Management**.
2. Select the managed host, and on the **Deployment Actions** menu, click **Edit Host Connection**.
3. On the **Modify QRadar Network Insights Connection** page, select the QRadar Flow Collector and flow source.
4. Click **Save**.
5. Specify whether to configure the QRadar Network Insights appliance as a stand-alone or stacked appliance.
6. Click **Next**, and then click **Save**.
7. Close the **System and License Management** page.
8. On the **Admin** tab menu bar, click the **Deploy Changes** icon.

Installing the QRadar Network Insights content extension

QRadar Network Insights content extensions include extra content, such as rules, reports, searches, and custom properties, that can be used to provide in-depth analysis, alerts, and reports in QRadar Network Insights deployments.

Before you begin

Download the QRadar Network Insights content extension to your local computer from the IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub/extension/5faf57a09236654323cbc4db41bd74f4).

Procedure

1. Log in to the QRadar Console as an administrator.
2. On the navigation menu ( ), click **Admin**.
3. Click **Extension Management**.
4. To upload an extension and install it immediately, follow these steps:
   a) Click **Add** and select the extension to upload.
   b) To install the extension immediately, select the **Install immediately** check box, and then click **Add**.
5. To preview the contents of an extension before you install it, follow these steps:
   a) Select the extension from the list, and click **More Details**.

      The content items are compared to content items that are already in the deployment. If the content items exist, you can choose to overwrite them or to keep the existing data.
   b) Select **Replace existing items**. This setting ensures that existing custom properties are updated when the extension is installed.
   c) Click **Install**.
   d) Review the installation summary, and click **OK**.

Results

After the extension is added, a yellow caution icon in the **Status** column indicates potential issues with the digital signature. Hover the mouse over the triangle for more information. Extensions that are unsigned or are signed by the developer, but not validated by your vendor, might cause compatibility issues in your deployment.

Decrypting SSL and TLS traffic in QRadar Network Insights

To find hidden threats, it might be necessary to decrypt SSL and TLS traffic that is processed by IBM QRadar.

For IBM QRadar Network Insights deployments, it is recommended that you use a dedicated man-in-the-middle solution where the clear text output is fed into QRadar.

If you do not want to deploy a man-in-the-middle solution, limited decryption capabilities are available within QRadar if the required keys are available. You will experience performance degradation if you enable the decryption capability.

Decryption is supported for the following protocols:

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

Restriction:

The following restrictions apply:

- Traffic cannot be decrypted if SSL or TLS compression is in use.
- The `Diffie Hellman` key exchange mechanism is not supported when encrypted traffic is decrypted through a private key. When you use a private key, other key exchange methods, such as RSA, are supported. This restriction does not apply when traffic is decrypted with information that is found in a key log.

Decrypting SSL and TLS traffic by using a server's private key

By providing a server's IP address and its private key, you can decrypt traffic that is going to that host.

Procedure

1. Use SSH to log in to the QRadar Network Insights host as the root user.
2. Review the location of the keys in the `/opt/qradar/conf/forensics_config.xml` file.

   ```
   <keybag
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

   You will use the `keydir` and `keylogs` locations in the next steps.
3. Copy one or more private keys into the `keydir` directory.
4. In the `keydir` directory, modify the `key_config.xml` file to specify your key file and the IP addresses that it applies to.

   The key file can apply to a single IP address, a range of IP addresses, or both. For example, the `key_config.xml` file might look like this:

   Example:

   ```
   <keys>
   <key file=" /opt/ibm/forensics/decapper/keys/key_name">
   <address>10.2.3.4</address>
   <range>10.2.3.0-10.2.3.255</range>
   </key>
   </keys>
   ```
5. Restart the decapper service by typing the following command:

   ```
   systemctl restart decapper
   ```

Results

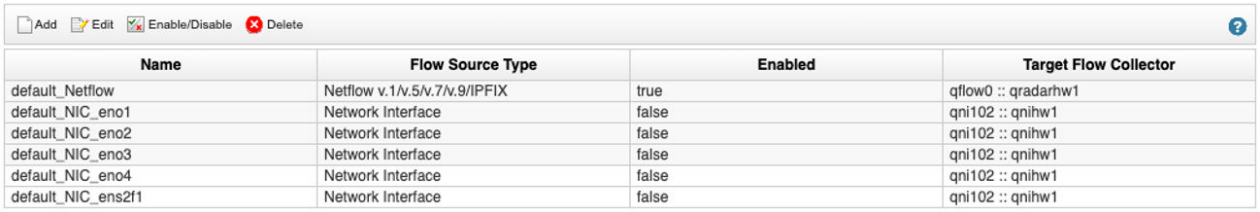
From this point on, all analysis of new recoveries or flows use the new keys to decrypt traffic.

Chapter 11. Flow sources

When you install an IBM QRadar Network Insights host, two types of flow sources are required. A QRadar Network Insights host processes raw traffic from a network interface flow source and then exports these flow records to an IPFIX flow source running elsewhere in your QRadar deployment.

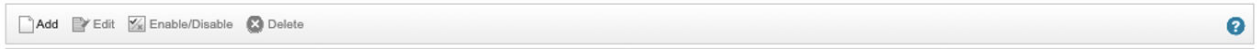
On QRadar Network Insights hosts, an input flow source is automatically created for all non-management interfaces that are available on the host. Except for Napatech interfaces, these flow sources are disabled by default, so you must enable the flow source if you want to use it for monitoring network flows.

In the following example, a QRadar Network Insights host *(qnihw1)* is connected to a QRadar Console *(qradarhw1)*. The system does not create a flow source for the management interface of the appliance *(ens2f0)*.



Name	Flow Source Type	Enabled	Target Flow Collector
default_Netflow	Netflow v.1/v.5/v.7/v.9/IPFIX	true	qflow0 :: qradarhw1
default_NIC_eno1	Network Interface	false	qni102 :: qnihw1
default_NIC_eno2	Network Interface	false	qni102 :: qnihw1
default_NIC_eno3	Network Interface	false	qni102 :: qnihw1
default_NIC_eno4	Network Interface	false	qni102 :: qnihw1
default_NIC_ens2f1	Network Interface	false	qni102 :: qnihw1

For appliances that use a Napatech network interface, the auto-detected flow source is enabled by default, and cannot be edited, disabled, or deleted. The flow source appears as **napatech0**.



Name	Flow Source Type	Enabled	Target Flow Collector
default_Netflow	Netflow v.1/v.5/v.7/v.9/IPFIX	true	qflow0 :: qradarhw1
default_NAPATECH_napatech0	Napatech Interface	true	qni102 :: qnihw1
default_NIC_eno2	Network Interface	false	qni102 :: qnihw1
default_NIC_eno3	Network Interface	false	qni102 :: qnihw1
default_NIC_eno4	Network Interface	false	qni102 :: qnihw1

Configure an IPFIX flow source for QRadar Network Insights to export its flows to. By default, default_NetFlow sources are automatically created for QRadar Console, Flow Processor, and Flow Collector hosts. For more information on these flow sources, see Flow Sources.

Enabling flow sources

Flow sources that are used to monitor network flows must be enabled. After you enable the flows, you must deploy the changes.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **Data Sources** section, under **Flows**, click **Flow Sources**.
3. Select the flow source that you want to enable or disable, and click **Enable/Disable**.
4. On the **Admin** tab, click **Deploy Changes**.

Adding a flow source

If you add a new network interface to your appliance after the initial installation, you must add it as a flow source before you can use it to monitor network flows. After making changes to the flow sources configuration, you must deploy the changes.

Procedure

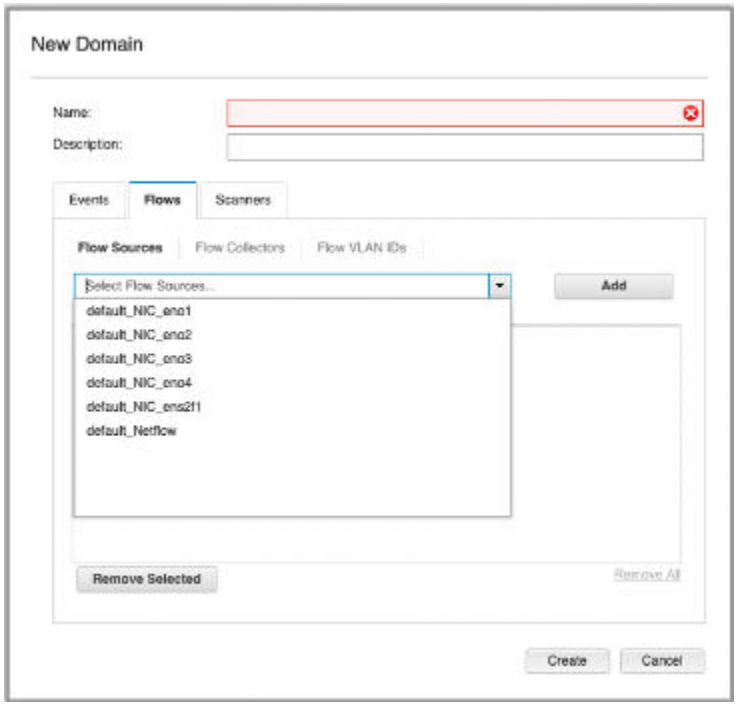
1. Log in to the QRadar Console as an administrator.

2. Click the **Admin** tab.
3. In the **Flows** section, click **Flow Sources**, and click **Add**.
4. Configure the flow source details.
   a) In the **Flow Source Name** field, type a descriptive name.
   b) In the **Target Flow Collector** field, select a flow collector or accept the value provided.
   c) In the **Flow Source Type** list, select **Netflow v.1/v.5/v.7/v.9/IPFIX**.
   d) In the **Monitoring Interface**, select the network interface that supplies the flow traffic.
   e) In the **Monitoring Port** field, select a port or accept the value provided.
   f) In the **Linking Protocol** list, select the protocol to use.
   g) To forward flows, select the **Enable Flow Forwarding** check box and configure the settings.
5. Click **Save**.
6. On the **Admin** tab, click **Deploy Changes**.

Flow source domain management

Domains are virtual buckets that you use to segregate data based on the source of the data. Segmenting your network into different domains helps to ensure that relevant information is available only to those users that need it, helping you to build a multitenant environment.
To ensure that traffic on a specific network interface is segregated from other traffic in your network, you can add the network interface to a domain.

The interface must be configured as a flow source before it appears in the Domain configuration window.



As with all domains that are based on flow sources, the data is not segregated if different domains have overlapping IP addresses. Domains that are based on Flow Collectors or Flow VLAN IDs do not have this limitation.

Viewing flow data from a specific flow source in QRadar Network Insights

Use the Network Activity tab to view flows that are received by IBM QRadar. You can apply a filter to view flows that are received from a specific flow source.

Before you begin

Ensure that the flow source is added to the deployment and that the flow source is enabled.

About this task

When you install IBM QRadar, a `default_Netflow` flow source is automatically added to the deployment. This flow source is enabled by default. New flow sources are created as you add flow collectors and flow processors.

When you add a QRadar Network Insights host, an input flow source is automatically created for all non-management interfaces that are available on the host.

With exception of Napatech network interfaces, the auto-detected flow sources are disabled by default, and must be enabled if you want to use them for monitoring network flows. Flow sources for Napatech interfaces are enabled by default, and cannot be edited, disabled, or deleted.

Procedure

1. Click the **Network Activity** tab.
2. Click **Add Filter**, and select the criteria that you want to match.

   Tip: Reduce the options in the **Parameter** list by typing keywords. For example, you can type *flow* to find all the flow parameters.

   The filter is applied, and the search results are shown. You can add more filter parameters to further reduce the result list.

Results

The **Flow Interface** column that appears in the result list might appear differently, depending on which QRadar version you are using.

In QRadar Network Insights V7.3.3 or earlier, the **Flow interface** value is a combination of `<flow_processor_component>_<hostname>:<qni_hostname>`. For example, if your flow processor hostname is *qfp1* and your QRadar Network Insights hostname is *qni1*, the **Flow interface** shows *qfp1:qni1*.

In QRadar Network Insights V7.4.0, the **Flow interface** shows the host name of the network interface on the managed host that received the flow. Using the example above, the **Flow interface** on an appliance that uses a Napatech card shows *qni1:napatech0*.

Related tasks

Adding a flow source

If you add a new network interface to your appliance after the initial installation, you must add it as a flow source before you can use it to monitor network flows. After making changes to the flow sources configuration, you must deploy the changes.

Enable flow sources

Chapter 12. Flow inspection levels

The flow inspection level determines how much data is analyzed and extracted from the network flows.

By default, the flow inspection level is a global setting that is configured in the **System Settings** on the **Admin** tab. It applies to all appliances in your deployment. For QRadar Network Insights 6200, 6600, 6610 appliances, you can override the global setting by configuring a custom flow inspection level.

In a stacked configuration, each stack can have a different inspection level, but all appliances within a stack must have the same inspection level.

Basic inspection level

The **Basic** level is the lowest level of flow inspection. This level supports the highest bandwidth, but generates the least amount of flow information.

The attributes that QRadar Network Insights captures using the basic flow inspection level are similar to what you get out of a router or network switch that does not perform deep packet inspection, and include the following types of information:

- Source and destination information
- Network protocol
- Application ID
- Byte and packet counters
- Time of first and last packets
- Quality of service
- VLAN tags

At the **Basic** inspection level, QRadar Network Insights creates a data flow that captures information about the network communication. The data flow includes payload samples, and shows the byte and packet size counters. The **Basic** inspection level collects the same information as the QRadar QFlow process.

Enriched inspection level

With the enriched inspection level, each flow is identified and inspected by one of the protocol or domain inspectors, and many kinds of attributes can be generated from that inspection.

The **Enriched** inspection level provides the following types of information:

- Usernames, email addresses, chat IDs
- Search arguments
- Host information
- HTTP, FTP, SMTP, SSL and TLS fields
- DNS queries and responses
- File name, type, size, hash, and entropy
- Last proxy, XFF, True Client IP
- Suspect content
- Web categories
- Configurable content-based suspect content (YARA rules)

At the **Enriched** and **Advanced** inspection levels, QRadar Network Insights creates both data flows and content flows. The content flow shows what was found inside the data flow with the deeper level of

inspection. Content flows do not include payload samples, and all byte and packet counters appear as zero. They are linked to the data flow by the **Flow ID** field.

You can identify content flows in the following ways:

- In the **Flow Information** window, the **Flow Type** field shows **Standard Flow (Content Flow)**.
- On the **Network Activity** tab, the tooltip for the **Flow Type** icon shows **Standard Flow (Content Flow)**.

Advanced inspection level

Advanced inspection is the highest level of inspection, and it is the default setting for new installations. Through comprehensive analysis of the application content, it builds on the flow attributes that are extracted at the Enriched inspection level.

The **Advanced** inspection level provides the following types of information:

- Content extraction
- Personal information detection
- Confidential data detection
- Embedded scripts
- Redirects
- Extra file metadata

The advanced inspection level also performs content analysis, which can yield more suspect content values than the Enriched level. For example, when set to the **Advanced** inspection level, QRadar Network Insights looks deep within files to identify suspect content such as embedded scripts in PDF or Microsoft documents.

Similar to the enriched level, a content flow is created to show what QRadar Network Insights found while doing the deeper level of inspection of the data flow.

Performance levels based on flow inspection levels

Flow inspection levels are cumulative, and each level collects more data than the level before it. You must configure the flow inspection level to suit the flow rate that you want to achieve. System performance varies based on the exact configuration and tuning of the system components. It is influenced not only by hardware, but also factors such as the search, extraction criteria, and the amount of network data.

Table 12. Performance based on flow inspection levels

Flow Inspection Level	1901 appliance	1910 appliance	1920 appliance (1)	1940 appliance(1)
Basic	~ 4 Gbps	~ 10 Gbps	~ 10 Gbps	~ 10 Gbps
Enriched	~ 3 Gbps	~ 3 Gbps	~ 6 Gbps	~ 6 Gbps
Advanced	~ 1.2 Gbps	~ 1.2 Gbps	~ 2.5 Gbps	~ 2.5 Gbps

(1) Supports appliance stacking.

Scaling performance by stacking appliances

To achieve higher flow rates, you can stack some QRadar Network Insights appliances to distribute data processing across multiple Napatech cards and CPUs.

The following appliance types can be stacked, with up to four appliances in each stack.

- QRadar Network Insights 1920 (Type 6200)
- QRadar Network Insights 1940 (Type 6600)

In a stacked configuration, the performance scales linearly according to the number of appliances in the stack. For example, a stack with three appliances can achieve up to 3x the performance, depending on the flow inspection level.

For more information, see Chapter 13, “QRadar Network Insights appliance stacking,” on page 47.

Related concepts

QRadar Network Insights appliances

QRadar Network Insights appliances connect to network TAPs, SPAN, or mirror ports to access full packet data for real-time analysis. All QRadar Network Insights appliances provide detailed analysis of network flows to extend the threat detection capabilities of QRadar.

Configuring the flow inspection level

The flow inspection level determines how much data is analyzed and extracted from the network flows. Each **Flow Inspection Level** setting provides deeper visibility and extracts more content than the preceding levels.

About this task

The following table explains the difference between each inspection level:

Table 13. Flow inspection levels

Flow Inspection Level	Description
`Basic`	Lowest level of inspection. Flows are detected by 5-tuple, and the number of bytes and packets that are flowing in each direction are counted.
`Enriched`	Each flow is identified and inspected by one of the protocol or domain inspectors, and many kinds of attributes can be generated from that inspection.
`Advanced`	The default setting. The highest level of inspection. Flows are subjected to more rigorous content extraction processes, including scanning and inspecting the content of the files that it finds.

By default, the **Flow Inspection Level** for each appliance is inherited from the global setting that is defined in the **System Settings** on the **Admin page**. When you change the global setting, the new value is inherited by all QRadar Network Insights appliances that are configured to use the global setting. This includes new appliances that you add after the setting is changed.

You can override the global setting by configuring custom settings for individual QRadar Network Insights appliances.

In a stacked configuration, each stack can have a different flow inspection level, but all appliances within a stack must have the same inspection level.

Procedure

1. Log in to QRadar as an administrator.
2. To configure the global setting, follow these steps:
   a) On the **Admin** tab, click **System Settings**.
   b) Click **QRadar Network Insights Settings**.
   c) From the **Flow Inspection Level**, select the flow rate.
   d) Click **Save**.
3. To configure the settings for individual QRadar Network Insights appliances, follow these steps:

a) On the **Admin** tab, click **System and License Management**.

b) Select the appliance that you want to modify, and click **Deployment actions** > **Edit Host Connection**.

c) Set the flow collector and the flow source connection and click **Save**.

d) Specify the **Flow Inspection Level** for the appliance.

e) Click **Next** and then click **Save**.

4. From the menu bar on the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

Warning: When you deploy the full configuration, QRadar services restart. During this time, events and flows are not collected, and offenses are not generated.

5. Refresh your web browser.

What to do next

Deploy the QRadar Network Insights Processor.

Chapter 13. QRadar Network Insights appliance stacking

You can stack QRadar Network Insights appliances to scale performance by load balancing the network packet data across multiple appliances. By distributing the data processing and analysis, stacked appliances can help you handle higher data volumes and improve flow throughput performance at the highest inspection levels.

Only the QRadar Network Insights 1920 (type 6200) and QRadar Network Insights 1940 (type 6600) appliances can be stacked. All appliances in the stack must be the same type. You cannot have both 1920 and 1940 appliances in the same stack.

You can have more than one stack in a deployment, and each stack can have a maximum of four appliances. If any of the appliances in the stack experience a failure and becomes unavailable, the entire stack is impacted. For example, if the first appliance in a stack has a hardware failure, the data is not received by the rest of the stacked appliances.

You cannot stack the QRadar Network Insights 1901 appliance, and you cannot stack appliances in a software installation.

Related concepts

QRadar Network Insights appliances

QRadar Network Insights appliances connect to network TAPs, SPAN, or mirror ports to access full packet data for real-time analysis. All QRadar Network Insights appliances provide detailed analysis of network flows to extend the threat detection capabilities of QRadar.

Stacked QRadar Network Insights 1920 appliances

You can stack the QRadar Network Insights appliances (type 6200).

Each QRadar Network Insights 1920 appliance is configured with 2 Napatech cards. The port configuration on the first Napatech card changes, depending on whether the appliance is part of a standalone configuration or a stacked configuration.

Standalone configuration

In a standalone configuration, the four ports on the first Napatech card are configured to accept inbound traffic from the network tap.

The second Napatech card is a load balancer that is configured internally. Do not use the ports on this card; if you use them, you do not get any data.

Stacked configuration

In a stacked configuration, the four ports on the first Napatech card are reconfigured, two ports for inbound traffic and two ports for outbound traffic. The ports are configured as linked pairs, so the data that comes in on port 0 goes out on port 2, and the data that comes in on port 1 goes out on port 3.

Similar to a standalone configuration, the second Napatech card cannot be used in a stacked configuration.

Single incoming TAP line

When your deployment has incoming data on one network tap only, the stacked appliances must be cabled like this:

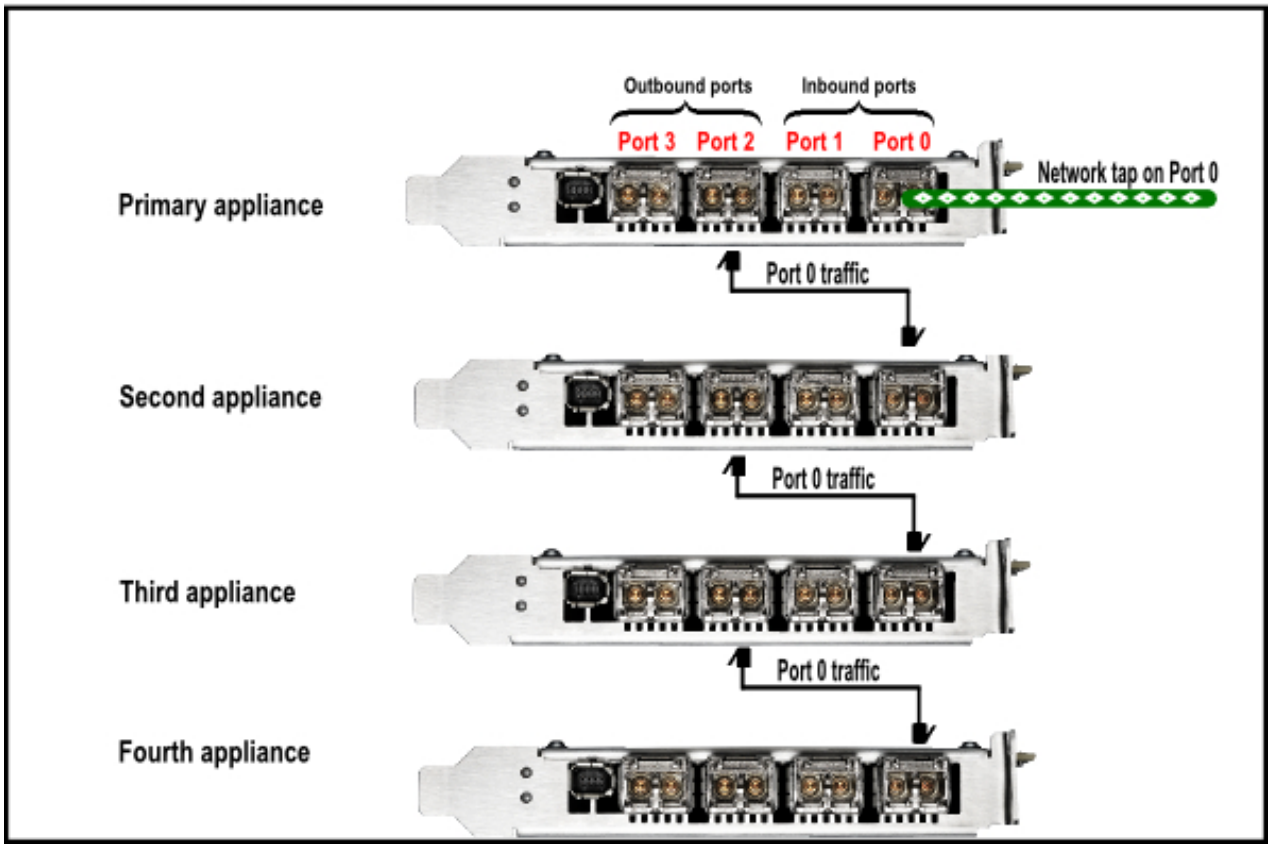


Figure 2. Cabling for stacked 1920 appliances with single network TAP

Dual incoming TAP lines

When your deployment has incoming data on two network taps, the stacked appliances must be cabled like this:

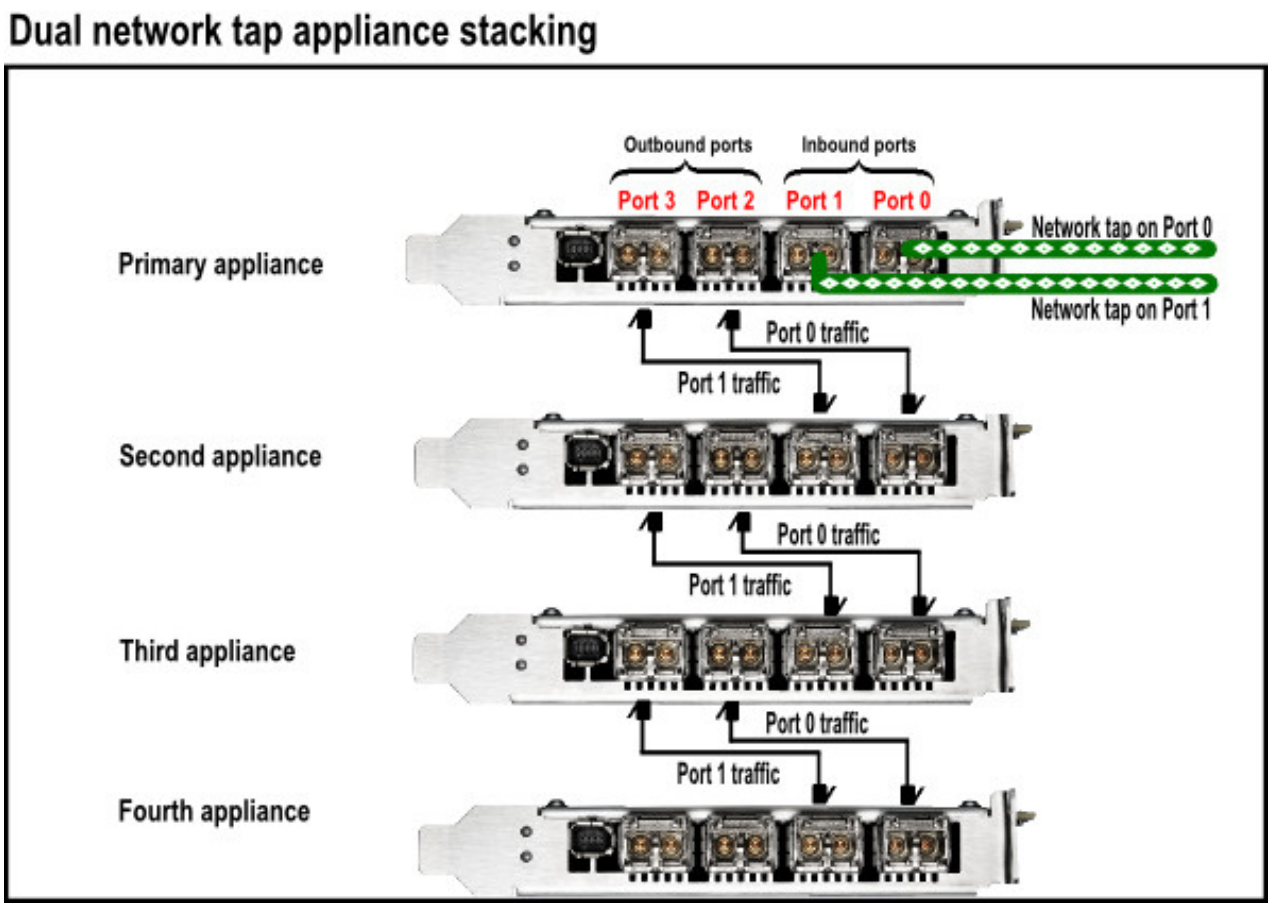


Figure 3. Cabling for stacked 1920 appliances with dual network TAP

Related tasks

Modifying an existing stack

You can edit an existing stack to add or remove QRadar Network Insights appliances, set the primary host in the stack, and set the flow inspection level and the raw payload size for all appliances in the stack.

Creating a stack

Create a stack to help you handle higher data volumes and improve flow throughput performance at the highest inspection levels. You can stack only the QRadar Network Insights 1920 (type 6200) and QRadar Network Insights 1940 (type 6600) appliances.

Stacked QRadar Network Insights 1940 appliances

You can stack the QRadar Network Insights 1940 (type 6600) appliances to distribute network packets across multiple Napatech cards. Stacking the appliances can help you handle higher data volumes and inspect more traffic.

Each QRadar Network Insights 1940 appliance is configured with two Napatech cards. The port configuration on the first Napatech card changes, depending on whether the appliance is part of a stand-alone configuration or a stacked configuration.

Stand-alone configuration

In a stand-alone configuration, the two ports on the first Napatech card are configured to accept inbound traffic from the network tap.

The second Napatech card is a load balancer that is configured internally. Do not use the ports on this card; if you use them, you do not get any data.

Stacked configuration

In a stacked configuration, the two ports on the first Napatech card are reconfigured so that one port is for inbound traffic and one port is for outbound traffic. The ports are configured so the data that comes in on port 0, and goes out on port 1.

Similar to a stand-alone configuration, the second Napatech card cannot be used in a stacked configuration.

Appliance cabling

The following image shows how to connect the cables on up to four QRadar Network Insights 1940 appliances in a stacked configuration. On the first appliance, port 0 is used for the network tap or span port. The traffic is then mirrored to Port 1 on the same card, which sends data to port 0 of the next appliance in the stack.

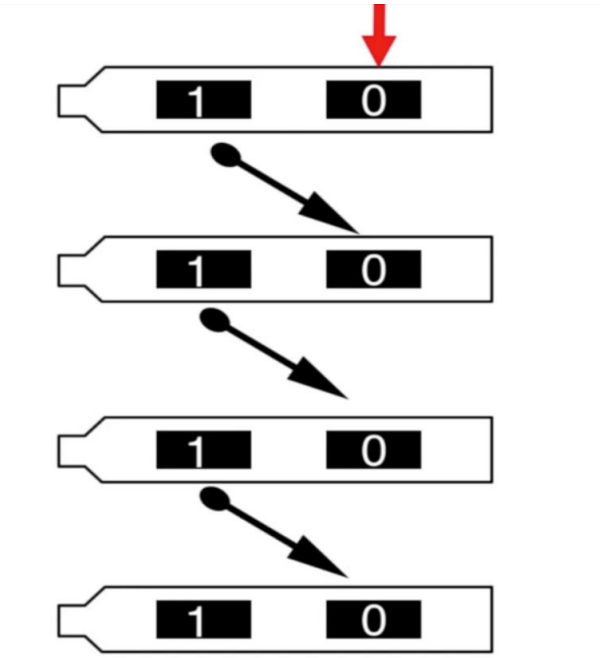


Figure 4. Cabling for stacked QRadar Network Insights 1940 appliances

Related tasks

Modifying an existing stack
You can edit an existing stack to add or remove QRadar Network Insights appliances, set the primary host in the stack, and set the flow inspection level and the raw payload size for all appliances in the stack.

Creating a stack
Create a stack to help you handle higher data volumes and improve flow throughput performance at the highest inspection levels. You can stack only the QRadar Network Insights 1920 (type 6200) and QRadar Network Insights 1940 (type 6600) appliances.

Creating a stack

Create a stack to help you handle higher data volumes and improve flow throughput performance at the highest inspection levels. You can stack only the QRadar Network Insights 1920 (type 6200) and QRadar Network Insights 1940 (type 6600) appliances.

Before you begin

Ensure that all appliances that you want to include in the stack are racked and cabled.

Ensure that the appliance and the QRadar Console used to manage it are at the same QRadar version and fix pack level.

About this task

By default, the **Flow Inspection Level** for each appliance is inherited from the global settings that are defined in the **System Settings**. You can override the global setting by configuring the flow inspection level for each appliance. In a stacked configuration, each stack can have a different inspection level, but all appliances within a stack must have the same inspection level.

The **Maximum Raw Payload Size** is also inherited from the global system settings, but you can change it for individual appliances. The default size of the payload is 64 bytes, and the maximum size is 32 768 bytes. Large payloads can impact performance. Adjust the byte size in small increments, and monitor the disk capacity to ensure that it does not fill up quickly.

Procedure

1. If required, add the QRadar Network Insights appliance to your deployment as a managed host.
   a) On the navigation menu (☰), click **Admin**.
   b) In the **System Configuration** section, click **System and License Management**.
   c) In the **Display** list, select **Systems**.
   d) On the **Deployment Actions** menu, click **Add Host**.
   e) Configure the settings for the managed host by providing the fixed IP address and the root password for the appliance.
   f) Click **Add**.

      The managed host is added and the new configuration is ready to deploy.
   g) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

      QRadar continues to collect events when you deploy the full configuration.
2. To configure the managed host as part of a QRadar Network Insights stack, edit the host connection information.
   a) On the **Admin** tab, click **System and License Management**.
   b) In the **Display** list, select **Systems**.
   c) Select the QRadar Network Insights managed host, and on the **Deployment Actions** menu, click **Edit Host Connection**.
   d) On the **Modify QRadar Network Insights Connection** page, select the QRadar Flow Collector and the NetFlow source.

      By default, the flow collector is the IP address of the QRadar Console.
   e) Click **Save**.

      The console recognizes that the managed host is a stackable appliance.
   f) In the **Host Action** field, select **Create new stack** and type a descriptive name.
   g) Change the **Flow Inspection Level** and the **Maximum Raw Payload Size**.
   h) Select **Next**.

      The **Configure QNI Ports** window shows that the ports are now reconfigured to work in a stacked configuration.
   i) Click **Save**.

      The **System and License Management** window now shows the new QRadar Network Insights stack with one QRadar Network Insights appliance.

What to do next

You must deploy the changes for the new configuration to take effect.

Related concepts

Stacked QRadar Network Insights 1920 appliances

You can stack the QRadar Network Insights appliances (type 6200).

Stacked QRadar Network Insights 1940 appliances

You can stack the QRadar Network Insights 1940 (type 6600) appliances to distribute network packets across multiple Napatech cards. Stacking the appliances can help you handle higher data volumes and inspect more traffic.

Related tasks

Upgrading QRadar Network Insights

Modifying an existing stack

You can edit an existing stack to add or remove QRadar Network Insights appliances, set the primary host in the stack, and set the flow inspection level and the raw payload size for all appliances in the stack.

Before you begin

Before you add an appliance to a stack, ensure that the appliance is deployed into your QRadar environment.

All appliances in the stack must be at the same QRadar version and fix pack level as the QRadar Console that manages them.

About this task

You can add up to four QRadar Network Insights managed hosts to an appliance stack. All appliances in the stack must be the same appliance type. The primary host appliance is the appliance that receives data from the network TAP.

By default, the stack uses the global **Flow Inspection Level** and the **Maximum Raw Payload Size** settings, as defined in the **System Settings** on the **Admin** tab. You can override the global settings by choosing a different setting in the stack configuration. The setting that you choose applies to all appliances in the stack.

Procedure

1. On the **Admin** tab, click **System and License Management**.
2. In the **Display** list, select **Systems**.
3. In the host table, select that stack that you want to configure, and click **Deployment Actions** > **Edit Stack**.
4. To set custom settings for the **Flow Inspection Level** level and the **Maximum Raw Payload Size**, click **Change** in the appropriate section.
5. To modify the number of hosts in the stack or to set the primary host, make the selections in the **Hosts in Stack** section.

   All appliances in the stack must be the same type. Appliances that do not match do not appear in the list of appliances.
6. Click **Save**.

What to do next

You must deploy the changes for the new configuration to take effect.

Related concepts

Stacked QRadar Network Insights 1920 appliances

You can stack the QRadar Network Insights appliances (type 6200).

Stacked QRadar Network Insights 1940 appliances
You can stack the QRadar Network Insights 1940 (type 6600) appliances to distribute network packets across multiple Napatech cards. Stacking the appliances can help you handle higher data volumes and inspect more traffic.

Removing stacked appliances

When you remove a stack, each managed host in the stack is re-configured as a standalone appliance.

Remember to re-cable the managed hosts as standalone appliances. For more information about how to cable the standalone appliance, see Chapter 3, “QRadar Network Insights appliances,” on page 5.

Procedure

1. On the **Admin** tab, click **System and License Management**.
2. In the **Display** list, select **Systems**.
3. To remove a single appliance from a stack, follow these steps.
   a) In the host table, select that stack that you want to configure.
   b) Click **Deployment Actions** > **Edit Stack**.
   c) In the **Hosts in Stack** section, click **Change**.
   d) Click the minus (-) symbol next to the appliance that you want to remove, and then click **Save**.
4. To remove the entire stack, follow these steps.
   a) In the host table, select that stack that you want to remove.
   b) Click **Deployment Actions** > **Unstack**.

What to do next

You must deploy the changes for the new configuration to take effect.

Chapter 14. Troubleshooting

To isolate and resolve problems with your IBM product, use the following troubleshooting and support information.

For answers to common support questions about QRadar Network Insights, see IBM Support Forums and search for *QRadar Network Insights*.

Related tasks

Upgrading QRadar Network Insights

Installing QRadar Network Insights software on a QRadar appliance

Verifying that the QRadar Network Insights appliance is receiving raw packet data

Follow these steps to verify that QRadar Network Insights appliance is receiving raw packet data from the network tap or span port.

Before you begin

- Ensure that the appliance is cabled correctly.

  Review the hardware specifications for your QRadar Network Insights appliance, and use the images to verify the cable configuration.

  If you are working with stacked appliances, ensure that the appliance is cabled correctly for the stacked configuration. For more information, see Cabling for stacked appliances.

Procedure

1. From the Console, use SSH to log in to QRadar Network Insights as the root user.
2. If your appliance uses a traditional network card, use `tcpdump` to verify that the traffic is reaching the network interface:

   ```
   tcpdump -ni <interface_name>
   ```

   For example, type `tcpdump -ni ens3f0 -c 5` to capture on *ens3f0* and stop after 5 packets.

   The results might look similar to this example:

   ```
   [root@qni ~]# tcpdump -ni ens3f0 -c 5
   tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
   listening on ens3f0, link-type EN10MB (Ethernet), capture size 262144 bytes
   14:36:43.685604 IP 10.100.30.30.ssh > 10.166.1.6.60427: Flags [P.], seq 1917025348:1917025592, ack 2328280798, win 14, options
   [nop,nop,TS val 425001723 ecr 1124311903], length 244
   14:36:43.685846 IP 10.100.30.30.ssh > 10.166.1.6.60427: Flags [P.], seq 244:472, ack 1, win 14, options [nop,nop,TS val
   425001724 ecr 1124311903], length 228
   14:36:43.685961 IP 10.100.30.30.ssh > 10.166.1.6.60427: Flags [P.], seq 472:684, ack 1, win 14, options [nop,nop,TS val
   425001724 ecr 1124311903], length 212
   14:36:43.686072 IP 10.100.30.30.ssh > 10.166.1.6.60427: Flags [P.], seq 684:896, ack 1, win 14, options [nop,nop,TS val
   425001724 ecr 1124311903], length 212
   14:36:43.686184 IP 10.100.30.30.ssh > 10.166.1.6.60427: Flags [P.], seq 896:1108, ack 1, win 14, options [nop,nop,TS val
   425001724 ecr 1124311903], length 212
   5 packets captured
   5 packets received by filter
   0 packets dropped by kernel
   [root@qni ~]#
   ```

   Figure 5. Results of tcpdump capture command
3. If your appliance uses a Napatech network interface card, type the following command to verify that the traffic is reaching the network interface:

   ```
   /opt/napatech3/bin/monitoring
   ```

   The results might look like similar to the following example:

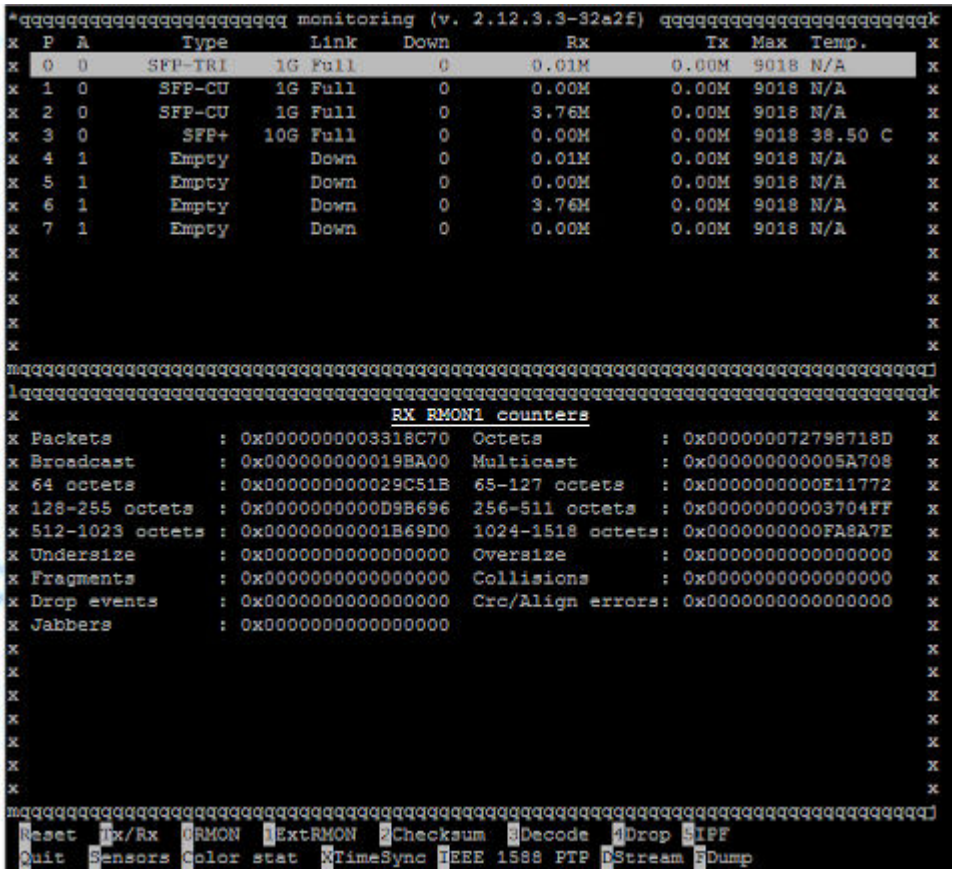


Figure 6. Napatech monitor with SFP type, Link status, and Transmission (Tx) values.

If there is no traffic that is displayed, check the **Link** column to see if the status is **Down**.

4. Make sure that you are using the correct SFP part number.
   a) To identify which SFP part numbers are in use, type the following commands to :

```
grep -i pn /var/log/messages
zgrep -i pn /var/log/messages
```

The output might look similar to the following example:

```
ntservice: Port 3: NIM info: (Vendor: FINISAR CORP., PN: FTLX1471D3BCL, SN: xxxxxx)
```

Review the hardware specifications to view the supported SFP part numbers for your appliance.

Verifying that the QRadar Network Insights appliance is sending data to the flow processor

Follow these steps to verify that the QRadar Network Insights appliance is sending IPFIX records to the flow collector or flow processor in your deployment.

Before you begin

Ensure that the flow source was added, enabled, and that the changes were deployed. For more information, see Chapter 11, “Flow sources,” on page 39.

Verify that the QRadar Network Insights appliance is receiving raw packet data.

Procedure

1. Verify that the flow source is added and enabled in QRadar.

a) Log in to the QRadar console as an admin user.

b) On the **Admin** tab, click **Flows** > **Flow Sources**.

c) Verify the flow source settings and ensure that the **Enabled** column is set to true.

d) Repeat the procedure for each QRadar Network Insights managed host.

e) If you changed the flow source configurations, on the **Admin** tab, click **Deploy Changes**.

2. Verify that the flows are being received.

a) Use SSH to log in to the QRadar Console.

b) Type the following command:

```
tailf /var/log/qradar.log | grep qflow
```

Messages like this one indicate that the Flow Processor is not receiving any flows from QRadar Network Insights:

```
IPFIX Flow Source Stats for <my_dtls_flow_source_name>: received and processed 0 packets
```

Messages like this one indicate that flows are being received:

```
IPFIX Flow Source Stats for <my_dtls_flow_source_name>: received and processed 12345 packets
```

3. If flows are not being received, check that the QRadar Network Insights managed host is configured correctly.

a) On the **Admin** tab, click **System and License Management**.

b) Select the QRadar Network Insights managed host that is not sending flow data.

c) Click **Deployment Actions** > **Edit Host Connections**.

d) Select the flow processor that you want your QRadar Network Insights appliance to send flow data to, and click **Save**.

e) Configure the QRadar Network Insights managed host, and then click **Save**.

f) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

g) Repeat the previous steps to verify that the flows are being received.

What to do next

On the QRadar Console, click the **Network Activity** tab to see the flow records.

Flow data from the QRadar Network Insights 1920 appliance does not appear

Follow these steps to determine why the flow data from your QRadar Network Insights 1920 or 1920-C appliance does not appear on the **Network Activity** tab.

Symptoms

The **Network Activity** tab doesn't show flow data from the QRadar Network Insights 1920 or 1920-C appliance.

Causes

This problem can be caused by a race condition, indicating that the system did not start in proper sequence. This problem occurs when the following Napatech configuration file is corrupted after QRadar services are restarted:

```
/opt/napatech3/config/ntservice.ini
```

Diagnosing the problem

1. Log in to the QRadar Network Insights host by using an SSH session.

2. Verify that flow data is not being received by typing the following command:

```
/opt/napatech3/bin/monitoring
```

   After the command is entered, a message displays similar to the following example:

```
ntservice not running
```

3. Search for messages that show the bonding type of the adapter by typing the following command:

```
grep -i bonding /opt/napatech3/config/ntservice.ini
```

   Messages similar to the following example indicate that the configuration file is corrupted. The corrupted file prevents the napatech3 service from starting.

```
BondingType = *Separate*
```

Resolving the problem

Follow these steps to re-create the corrupted `ntservice.ini` configuration file.

You can save the corrupted file for investigation later.

1. Log in to the QRadar Network Insights appliance by using an SSH session.
2. Move the *ntservice.ini* file to save it for later:

```
mv /opt/napatech3/config/ntservice.ini /root/
```

3. Restart the Napatech service:

```
systemctl restart napatech3
```

   Note: The `ntservice.ini` configuration file is re-created when the service restarts.

4. Test the service to confirm that it is now working:

```
grep -i bonding /opt/napatech3/config/ntservice.ini:
```

   You might see messages similar to the following examples:

```
BondingType = Master
BondingType = Slave
```

5. Rerun the following command to verify that the service is running:

```
/opt/napatech3/bin/monitoring
```

Results

The napatech3 service is started and flow data appears in QRadar on the **Network Activity** tab.

If the service is still not running, open a case with QRadar Support.

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.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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”.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr