

## JUNIPer QRadar Network Insights Software Installation Guide

[Home](#) » [JUNIPer](#) » JUNIPer QRadar Network Insights Software Installation Guide



Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc.

in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

QRadar Network Insights Installation Guide  
7.5.0

Copyright © 2022 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

### THE YEAR 2000 NOTICE

Juniper Networks hardware and software products are the Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing, or using such software, you agree to the terms and conditions of that EULA.

## Contents

- 1 Introduction to Installing QRadar Network Insights
- 2 What's New in QRadar Network Insights
  - 2.1 What's new for installers in QRadar Network Insights
- 3 Real-time Threat Investigations with QRadar Network Insights
- 4 Installations
  - 4.1 QRadar Network Insights Software Installations on your Own Hardware
  - 4.2 Prerequisites for Installing QRadar Network Insights on your Own Appliance
  - 4.3 QRadar Network Insights Software Installations on a Virtual Appliance
  - 4.4 Creating your Virtual Machine
- 5 Configuration
  - 5.1 Appliance Configuration
  - 5.2 Flow Sources
  - 5.3 Enabling Flow Sources
  - 5.4 Adding a Flow Source
  - 5.5 Domain Segmentation
  - 5.6 Flow Inspection Levels
  - 5.7 Enriched Inspection Level
  - 5.8 QRadar Network Insights Appliance Stacking
  - 5.9 Creating a Stack
- 6 Troubleshooting
- 7 Documents / Resources
  - 7.1 References
- 8 Related Posts

## Introduction to Installing QRadar Network Insights

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

### Intended Audience

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

### Technical Documentation

To find JSA product documentation on the web, including all translated documentation, access the JSA Series Virtual Appliance Documentation.

### Contacting Customer Support

For information, contact Juniper Customer Support.

## What's New in QRadar Network Insights

### SUMMARY

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

### What's new for installers in QRadar Network Insights

For installers, QRadar Network Insights 7.5.0 includes improvements to network inspection performance, and data segmentation and aggregation.

### Performance improvements for the QRadar Network Insights 6500 appliance

QRadar Network Insights 7.5.0 Update Pack 1 software and virtual appliance installations (appliance type 6500) now use the DPDK library to capture network traffic on appliances that use one of the following network interfaces:

- Intel x520
- Intel x710

- VMware vmxnet3

The DPDK library provides better performance than the PF\_RING library that is used in earlier versions of QRadar Network Insights. Network interface cards that DPDK uses are not visible to the operating system. You must use DPDK utilities to work with these interfaces.

Napatech-based appliances use a different library to process network data, so they are not affected by this change.

### **Data aggregation and segmentation**

QRadar Network Insights 7.5.0 includes improvements to the way that data is segmented and aggregated.

Flows that are received through any supported network interface on the same NUMA node are now aggregated together when the following properties match:

- IP address
- Ports (TCP/UDP)
- Protocol
- VLAN IDs
- VXLAN Identifier

### **Network inspection performance**

The network inspection performance at the basic and enriched inspection levels is increased in QRadar Network Insights 7.5.0.

**NOTE:** System performance and data throughput depend on many factors, including the amount of multiprogramming in the job stream, I/O configuration, storage configuration, and the workload volume that is processed. Individual performance improvements are not guaranteed.

## **Real-time Threat Investigations with QRadar Network Insights**

### **SUMMARY**

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

## **Installations**

### **QRadar Network Insights Installations**

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

### **Upgrading QRadar Network Insights**

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



### **RESTRICTION:**

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 Juniper Downloads.

1. Download the patch update file from Juniper Downloads.
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:

### **QRadar Network Insights Software Installations on your Own Hardware**

You can install QRadat 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 QRadat Network Insights installations." on page 11
2. Ensure that you have entitlement for a QRadat Software Node. To acquire entitlement to a QRadat Software Node, contact your QRadat Sales Representative.
3. "Install Red Hat Enterprise Linux (RHEL)" on page 12.
4. "Install QRadat Network Insights" on page 14

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

### **Prerequisites for Installing QRadat Network Insights on your Own Appliance**

Before you install QRadat 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 QRadat Network Insights software on your own appliance:

- You must acquire entitlement to a QRadat Software Node for a QRadat Network Insights software installation.  
To acquire entitlement to a QRadat Software Node, contact your QRadat Sales Representative.
- Do not install software other than QRadat Network Insights on your hardware.  
Unapproved RPM installations can cause dependency errors when you upgrade QRadat Network Insights software and can also cause performance issues in your deployment.
- Do not update your operating system or packages before or after QRadat Network Insights installation.

### **Minimum System Requirements**

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



**RESTRICTION:**

**Table 1: Minimum System Requirements for QRadar Network Insights Software Installations**

Requirement	Details
CPU	14C / 28T The system must use either Intel Westmere or AMD Bulldozer processors. 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: <ul style="list-style-type: none"><li>• Appliances that have a Napatech card.</li><li>• Virtual hosts such as EC2 instances and VMware guests.</li></ul>
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 management cards	One of the following network interface cards: <ul style="list-style-type: none"><li>• Napatech NT40E3</li><li>• Intel x520</li><li>• Intel x710</li></ul> Maximum of one capture card per host.

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

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 2: Red Hat Version**

QRadar version	Red Hat Enterprise Linux version
QRadar 7.5.0	Red Hat Enterprise Linux V7.9 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.

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 Juniper Secure Analytics 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 hostname.
  - 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 an 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.

### “Installing QRadar Network Insights on your Own Hardware”

You can install QRadar Network Insights 7.5.0 or later on your own hardware.

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

Download the installation file from Juniper Downloads. 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 7.5.0	Use the QRadar installation file, which looks similar to this one: <rhel_id ntifier>QRadar<build_number>.iso This file installs the QRadar Console and the managed hosts, including Q Radar Network Insights.

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:**

5. Select Software Install.
6. On the Select the Appliance ID page, choose 6500 QRadar Network Insights.

7. For the type of setup, select Normal Setup (default) or HA Recovery Setup, and set up the time.
8. Select the Internet Protocol version.
9. If you selected ipv6, select manual or auto for the Configuration type.
10. Select the bonded interface setup, if required.
11. Select the management interface.
12. In the wizard, enter a fully qualified domain name in the Hostname field.
13. In the IP address field, enter a static IP address, or use the assigned IP address.
14. Leave the root password as it is.
15. Click Finish.
16. Follow the instructions in the installation wizard to complete the installation.  
The installation process might take several minutes.
17. Add the QRadar Network Insights managed host to QRadar:
  - a. Log in to QRadar: [https://IP\\_Address\\_QRadar.com](https://IP_Address_QRadar.com)  
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.
18. 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.

### **QRadar Network Insights Software Installations on a Virtual Appliance**

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:

### QRadar Network Insights

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

**Table 4:** Requirements for Virtual Appliances

Requirement	Description
VMware Server	VMware ESXi Version 6.5+ For more information about VMWare clients, see the VMware website
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.
CPU cores	28 cores (minimum)
Memory	64 GB

### Creating your Virtual Machine

#### SUMMARY

To install a virtual appliance, you must first use VMWare ESXi to create a virtual machine.

Ensure that your virtual appliance meets the minimum system requirements. For more information, see “System Requirements for Virtual Appliance Installations for QRadar Network Insights” on page 17.

1. From the VMware vSphere Client, click File > New > Virtual Machine.
2. Add the Name and Location, and select the Datastore for the new virtual machine.
3. Use the following steps to guide you through the choices:
  - a. In the Configuration pane of the Create New Virtual Machine window, select Custom.
  - b. In the Virtual Machine Version pane, select Virtual Machine Version: 7.
  - c. For the Operating System (OS), select Linux, and select Red Hat Enterprise Linux 7.6 (64-bit) for QRadar 7.4.0 or Red Hat Enterprise Linux 7.7 (64-bit) for QRadar 7.4.1.
  - d. On the CPUs page, configure the number of virtual processors that you want for the virtual machine.
  - e. In the Memory Size field, type or select the RAM required for your deployment. Select 64 GB or more.
  - f. Use the following table to configure your network interfaces.

Table 5: Network Interface Configuration Parameters

Parameter	Description
How many NICs do you want to connect	You must attach at least two Network Interface Controllers. One controller is dedicated to network management, and at least one controller is required for network capture.
Adapter	VMXNET3

- g. In the SCSI controller pane, select VMware Paravirtual.



h. In the Disk pane, select Create a new virtual disk and use the following table to configure the virtual disk parameters.

Table 6: Settings for the Virtual Disk Size and Provisioning Policy Parameters

Property	Option
Capacity	480 GB
Disk Provisioning	Thin provision
Advanced options	Do not configure

4. On the Ready to Complete page, review the settings and click Finish.

“Install the QRadar Network Insights software on your virtual machine.” on page 19

You can install QRadar Network Insights 7.5.0 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:**

Download the installation file from [Juniper Downloads](#). 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 7.5.0	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.

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

**NOTE:**

- Log in to the virtual machine by typing root for the user name.  
The user name is case-sensitive.
- Review the End User License Agreement (EULA) and accept the license.

**TIP:**

- Select Software Install.
- On the Select the Appliance ID page, choose QRadar Network Insights Software (6500).
- For the type of setup, select normal.

- Follow the instructions in the installation wizard to complete the installation.

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

- Hostname (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.

- Add the QRadar Network Insights managed host to QRadar: a. Log in to QRadar:

[https://IP\\_Address\\_QRadar.com](https://IP_Address_QRadar.com)

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.

- 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.

## Configuration

### QRadar Network Insights Configuration

After you install QRadar Network Insights, you must add the appliance to the QRadar Console as a managed host, and then configure the data capture settings and the flow inspection level.

### 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.

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.

- Log in to the QRadar Console as an administrator.
- On the navigation menu, click Admin.
- In the System Configuration section, click System and License Management.

- In the Display list, select Systems.
- On the Deployment Actions menu, click Add Host.
- Configure the settings for the QRadar Network Insights managed host and then click Add.
- On the Admin tab, click Advanced > Deploy Full Configuration.

**NOTE:** 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 give you the option to cancel the deployment and restart the service at a more convenient time.

“Configure the QRadar Network Insights appliance.” on page 24

Optionally, you can install the “QRadar Network Insights content extension” on page 28. 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.

## Appliance Configuration

After your 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.

Configuring the Size of the Raw Payload Data Capture

You can use 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.

On initial installation, 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.

You can override the global settings by configuring custom Maximum Raw Payload Size settings for individual QRadar Network Insights appliances. 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:** If the size of the QRadar Network Insights maximum raw payload is larger than the Flow Processor content capture length, some payloads might be truncated. Ensure that the Flow Processor capture is the same size or greater than the QRadar Network Insights payload size. For more information about flows, see Flow sources.

- Log in to QRadar as an administrator.
- 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.
- 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.

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



#### **WARNING:**

QRadar

- Refresh your web browser.

### **Configuring the Flow Processor 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 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 QRadar Network Insights appliance as a managed host.



#### **IMPORTANT:**

1. Log in to QRadar: [https://QRadar\\_IP\\_Address.com](https://QRadar_IP_Address.com)

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 Flow Processor Settings menu, and in the IPFIX Additional Field Encoding field, choose the format.

Table 8: Flow Processor Format Options

Flow Processor format	Description
TLV	<p>The default setting for the flow collector format.</p> <p>Must be used when there is a QRadar Network Insights appliance in the environment.</p> <p>QRadar Network Insights V7.3.0 or later supports only TLV for content flows.</p> <p>Can be used when there is no QRadar Network Insights appliance in the environment.</p>
Payload	<p>Can be used when there is no QRadar Network Insights appliance in the environment.</p>

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



## **WARNING: QRadar**

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.

Ensure that your QRadar Network Insights appliance is attached as a managed host. For more information, see “Adding the QRadar Network Insights Appliance as a Managed Host” on page 23.

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.

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.

Download the QRadar Network Insights content extension to your local computer from the IBM Security App Exchange.

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 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.

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

### SUMMARY

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

### IN THIS SECTION

Decrypting SSL and TLS Traffic by Using a Server's Private Key | 29

For 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:

#### Diffie Hellman

#### Decrypting SSL and TLS Traffic by Using a Server's Private Key

### SUMMARY

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

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/keyloggers"/>
```

You will use the keytar and keyloggers locations in the next steps.

3. Copy one or more private keys into the keytar directory.
4. In the keytar 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`

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

## Flow Sources

### Viewing Flow Data from a Specific Flow Source in QRadar Network Insights | 34

When you install an 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 nonmanagement 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).

Add Edit Enable/Disable Delete ?			
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

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.

Add Edit Enable/Disable Delete ?			
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.

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

### SUMMARY

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.

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 forwarding flows, select the Enable Flow Forwarding check box and configure the settings.
5. Click Save.
6. On the Admin tab, click Deploy Changes.

## Domain Segmentation

Domains are virtual buckets that you use to separate 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 segmented 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.

**NOTE:** QRadar Network Insights supports traffic segmentation across multiple flow sources only if those flow sources are configured for separate domains, or they are part of separate NUMA nodes.

New Domain

Name:

Description:

Events Flows Scanners

Flow Sources Flow Collectors Flow VLAN IDs

Select Flow Sources...

- default\_NIC\_ens1
- default\_NIC\_ens2
- default\_NIC\_ens3
- default\_NIC\_ens4
- default\_NIC\_ens211
- default\_Netflow

Add

Remove Selected Remove All

Create Cancel



Consider the following information when you plan for domain segmentation in your deployment:

- For installations that use a Napatech card, all ports on the napatech0 interface are treated as a single aggregated interface.
- You can receive flows from a network tap if both halves of the tap are connected to network interface ports on the same NUMA node.
- For flows that are aggregated across multiple flow sources, the Flow interface field shows the interface that first observed the flow session.

### **Overlapping IP addresses**

If your QRadar Network Insights deployment monitors network segments that have overlapping IP addresses, you must use the domain segmentation capability to ensure that traffic remains segmented by the input flow sources. If you do not use domains, traffic that is received on Intel or virtual network interfaces on the same NUMA node are aggregated together.

Within a single domain, flow sources are aggregated together based on the following matching flow properties:

- IP address
- Ports (TCP/UDP)
- Protocol
- VLAN IDs
- VXLAN Identifier

If domains are configured based on the flow source, QRadar Network Insights ensures that different flow IDs are generated for different domains. This process ensures that the overlapping IP addresses are not aggregated back together by the Flow Processor.

### **Overlapping IP addresses**

If your QRadar Network Insights deployment monitors network segments that have overlapping IP addresses, you must use the domain segmentation capability to ensure that traffic remains segmented by the input flow sources. If you do not use domains, traffic that is received on Intel or virtual network interfaces on the same NUMA node are aggregated together.

Within a single domain, flow sources are aggregated together based on the following matching flow properties:

- IP address
- Ports (TCP/UDP)
- Protocol
- VLAN IDs
- VXLAN Identifier

If domains are configured based on the flow source, QRadar Network Insights ensures that different flow IDs are generated for different domains. This process ensures that the overlapping IP addresses are not aggregated back together by the Flow Processor.

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.

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

**TIP:****Parameterflow**

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

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 hostname 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.

**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. You can override the global setting by configuring a custom 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.

**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 Flow Processor.

**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 flow and content flows. The content flow shows what was found inside the data flow with a 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.

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 9:** 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 “QRadar Network Insights Appliance Stacking” on page 41.

### 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.

The following table explains the difference between each inspection level:

Table 10: Flow Inspection Levels

Flow Inspection Level	Description
Basic	The 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.

For the QRadar Network Insights 1920 (6200) and 1940 (6400) appliances, you can override the global setting by configuring a custom inspection level for the individual 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.

1. Log in to QRadar as an administrator.
2. To configure the global setting for all appliances, 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. For appliance types 6200 and 6400, you can configure the flow inspection level for the individual appliance.
  - 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.

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.

For the QRadar Network Insights 1920 (6200) and 1940 (6400) appliances, you can override the global setting by configuring a custom inspection level for the individual 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.

  1. Log in to QRadar as an administrator.
  2. To configure the global setting for all appliances, 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. For appliance type 6200 and 6400, you can configure the flow inspection level for the individual appliance.
    - 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.
5. From the menu bar on the Admin tab, click Advanced > Deploy Full Configuration.

## **QRadar Network Insights Appliance Stacking**

### **SUMMARY**

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.

## Stacked QRadar Network Insights 1920 Appliances

### SUMMARY

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.

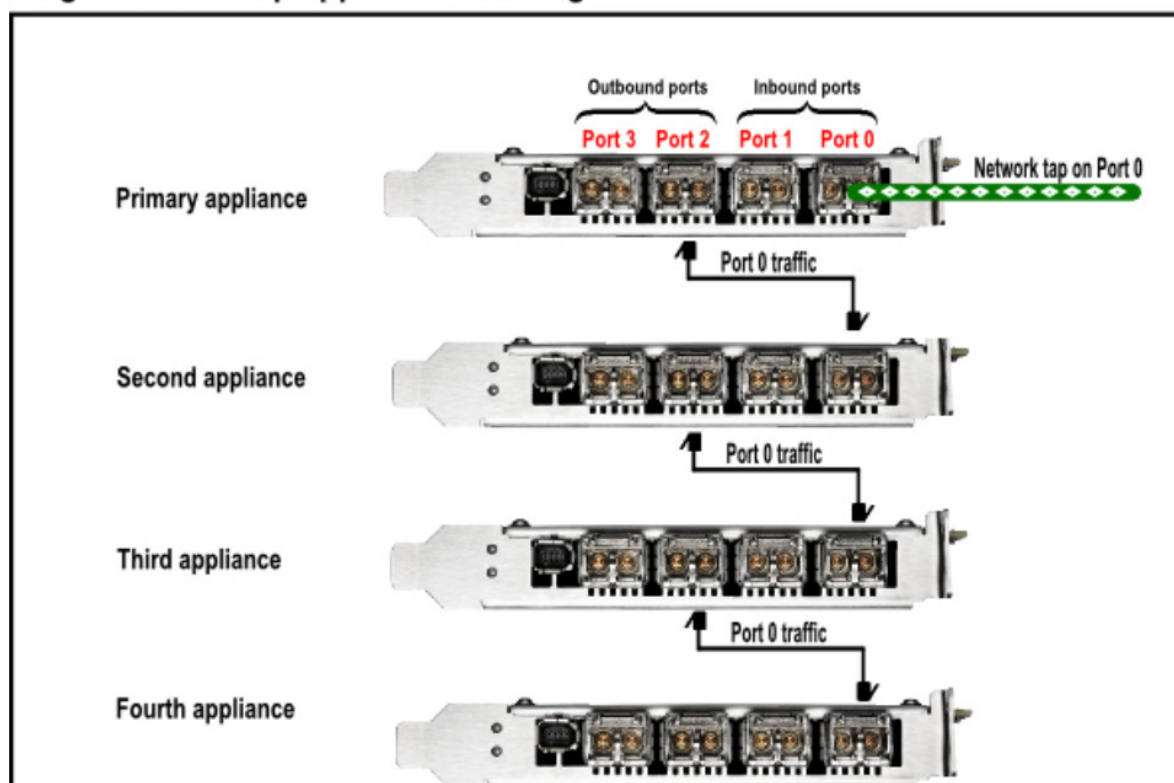
Similar to a standalone configuration, the second Napatech card cannot be used in a stacked configuration.

### Single Incoming TAP Line

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

**Figure 1: Cabling for Stacked 1920 Appliances with Single Network TAP**

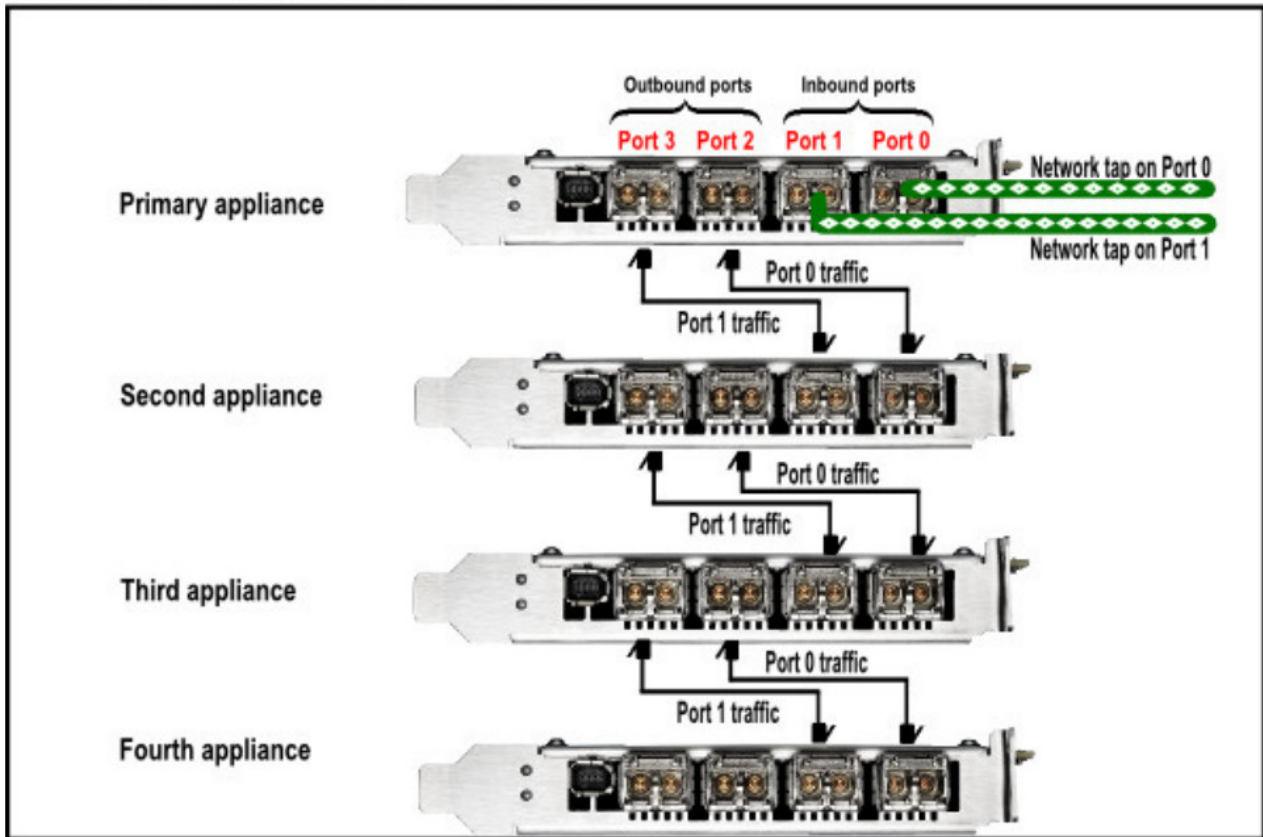
#### Single network tap appliance stacking



### Dual Incoming TAP Lines

When your deployment has incoming data on two network taps, the stacked appliances must be cabled like this:  
**Figure 2: Cabling for Stacked 1920 Appliances with Dual Network TAP**

### Dual network tap appliance stacking



### SUMMARY

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

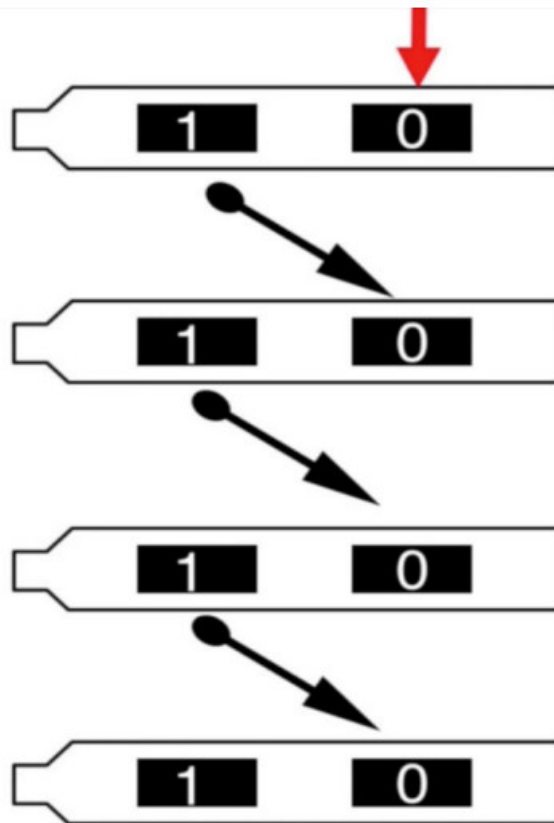
In a stacked configuration, the two ports on the first Napatech card are reconfigured so that one port is for inbound traffic and one port is for outbound traffic. The ports are configured so the data that comes in on port 0, and goes out on port 1.

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 3: Cabling for Stacked QRadar Network Insights 1940 Appliances**



### Creating a Stack

#### SUMMARY

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.

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 the pack level.

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.

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 QRadars 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 QRadars Network Insights managed host, and on the Deployment Actions menu, click Edit Host Connection.
  - d. On the Modify QRadars Network Insights Connection page, select the QRadars Flow Collector and the NetFlow source.

By default, the flow collector is the IP address of the QRadars Console.

- e. Click Save.

The console recognizes that the managed host is a stackable appliance.

- f. In the Host Action field, select Create a 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 QRadars Network Insights stack with one QRadars Network Insights appliance.

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

## Modifying an Existing Stack

### SUMMARY

You can edit an existing stack to add or remove QRadars 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 add an appliance to a stack, ensure that the appliance is deployed into your QRadars environment.

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

You can add up to four QRadars 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.

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 the 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.

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

## 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 QRadar Network Insights Appliances.

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.

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

## Troubleshooting

### SUMMARY

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

For answers to common support questions about QRadar Network Insights, see Juniper Customer Support and search for QRadar Network Insights.

### Verifying that the QRadar Network Insights Appliance is Receiving Raw Packet Data

### SUMMARY

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

#### 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.

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:

**Figure 4: Results of the tcpdump capture command**



## Verifying that the QRadar Network Insights Appliance is Sending Data to the Flow Processor

### SUMMARY

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.

Ensure that the flow source was added, enabled, and that the changes were deployed. For more information, see “Flow Sources” on page 30.

“Verify that the QRadar Network Insights appliance is receiving raw packet data” on page 51.

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: `tail/var/log/qradar.log|grep flow`  
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.

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

### SUMMARY

Follow these steps to determine why the flow data from your QRadar Network Insights 1920 or 1920C 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 Juniper Support.

### Documents / Resources

	<p><a href="#">JUNIPer QRadar Network Insights Software</a> [pdf] Installation Guide QRadar Network Insights Software, QRadar Network Insights, Software</p>
---	--

### References

-  [Juniper Networks – Leader in AI Networking, Cloud, & Connected Security Solutions](#)
-  [VMware - Delivering a Digital Foundation For Businesses](#)
-  [Red Hat Customer Portal - Access to 24x7 support and knowledge](#)
-  [IBM X-Force Exchange](#)
-  [Support](#)
-  [Downloads](#)
-  [End User License Agreement - Support - Juniper Networks](#)
-  [IBM Docs](#)

-  [JSA Series Virtual Appliance Documentation | Juniper Networks](#)

[Manuals+](#), [home](#) [privacy](#)