Engineering
Simplicity

Juniper Secure Analytics Network Insights Installation Guide

Published
2023-07-25

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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.

Juniper Secure Analytics Network Insights Installation Guide
7.5.0

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

YEAR 2000 NOTICE

Juniper Networks hardware and software products are 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.

Table of Contents

About This Guide

Use this guide to understand how to install, configure, and troubleshoot JSA Network Insights.

1

CHAPTER

Introduction to Installing Network Insights

Introduction to Installing Network Insights

IN THIS SECTION

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

2

CHAPTER

What's New in Network Insights

What's New in Network Insights

IN THIS SECTION

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

What's new for installers in Network Insights 7.5.0

IN THIS SECTION

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

Performance improvements for the Network Insights 6500 appliance

JSA 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 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

JSA 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 Non-Uniform Memory Architecture (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 JSA 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.

3

CHAPTER

Real-time Threat Investigations with Network Insights

Real-time Threat Investigations with Network Insights

SUMMARY

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

4

CHAPTER

Installations

Network Insights Installations

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

Upgrading Network Insights

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

> **NOTE**: Resizing logical volumes is not supported.

Custom changes that you make to JSA 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 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:

```
umount /media/updates
```

Network Insights Software Installations on your Own Hardware

IN THIS SECTION

You can install 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 Network Insights installations." on page 10

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

3. "Install Red Hat Enterprise Linux (RHEL)" on page 12.

4. "Install Network Insights" on page 14

You cannot stack appliances in a Network Insights software installation.

Prerequisites for Installing Network Insights on your Own Appliance

IN THIS SECTION

Before you install 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 Network Insights software on your own appliance:

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

  To acquire entitlement to a JSA Software Node, contact your Juniper Sales Representative.

- Do not install software other than Network Insights on your hardware.

  Unapproved RPM installations can cause dependency errors when you upgrade Network Insights software and can also cause performance issues in your deployment.

- Do not update your operating system or packages before or after Network Insights installation.

Minimum System Requirements

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

RESTRICTION: Resizing logical volumes is not supported.

Table 1: Minimum System Requirements for 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: • Appliances that have a Napatech card. • Virtual hosts such as EC2 instances and VMware guests.

Table 1: Minimum System Requirements for Network Insights Software Installations *(Continued)*

Requirement	Details
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 Network Insights.
Network management cards	One of the following network interface cards: • Napatech NT40E3 • Intel x520 • Intel x710 Maximum of one capture card per host.

Installing RHEL on your Hardware

SUMMARY

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

JSA version	Red Hat Enterprise Linux version
JSA 7.5.0	Red Hat Enterprise Linux V7.9 64-bit

You must acquire entitlement to a JSA Software Node for a Network Insights software installation. To acquire entitlement to a JSA Software Node, contact your Juniper 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 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.

"Installing Network Insights on your Own Hardware" on page 14

Installing Network Insights on your Own Hardware

You can install JSA Network Insights 7.5.0 or later on your own hardware.
Software installations for earlier versions of 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 Network Insights that you want to install.

Table 3: Network Insights Installation Files

Installation version	Installation file
JSA Network Insights 7.5.0	Use the JSA installation file, which looks similar to this one: ***<rhel_identifier>*JSA*<build_number>*.iso** This file installs the JSA Console and the managed hosts, including JSA 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**: 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. Select **Software Install**.
6. On the **Select the Appliance ID** page, choose **Network Insights**.
7. Select the Internet Protocol version.
8. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
9. Select the bonded interface setup, if required.
10. Select the management interface.
11. In the wizard, enter a fully qualified domain name in the **Hostname** field.
12. In the **IP address** field, enter a static IP address, or use the assigned IP address.
13. Set the root password.
14. Click **Finish**.
15. Add the Network Insights managed host to JSA:

    a. Log in to JSA:

       https://*IP_Address_JSA*

       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**.

f. Click **Deploy License Changes**.

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

Network Insights Software Installations on a Virtual Appliance

IN THIS SECTION

You can install Network Insights software on a VMWare ESXi virtual machine.
A virtual appliance provides the same visibility and function in your virtual network infrastructure that 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 Network Insights software on the virtual machine.
- Add the virtual appliance to your JSA deployment.

You cannot stack virtual Network Insights appliances.

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

NOTE: Do not install software other than JSA Network Insights on the virtual machine.

System Requirements for Virtual Appliance Installations for Network Insights

Before you install 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 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 V7.9 64-bit** for JSA 7.5.0.

   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

Table 6: Settings for the Virtual Disk Size and Provisioning Policy Parameters *(Continued)*

Property	Option
Advanced options	Do not configure

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

"Install the Network Insights software on your virtual machine." on page 19

Installing Network Insights Software on a Virtual Machine

You can install JSA Network Insights 7.5.0 or later on a virtual machine. Installing earlier versions of Network Insights is not supported.

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

NOTE: Resizing logical volumes is not supported.

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

Table 7: Network Insights Installation Files

Installation version	Installation file
JSA Network Insights 7.5.0	Use the JSA installation file, which looks similar to this one: ***<rhel_identifier>*JSA*<build_number>*.iso** This file installs the JSA Console and the managed hosts, including JSA Network Insights.

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 **Network Insights Software**.
13. 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.

14. Add the Network Insights managed host to JSA:

    a. Log in to JSA:

       https://*IP_Address_JSA*

       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**.

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**.

f. Click **Deploy License Changes**.

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

5

CHAPTER

Configuration

Network Insights Configuration

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

Adding the Network Insights Appliance as a Managed Host

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

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

Add the Network Insights managed host to JSA as per the instructions mentioned in Step 17 of "Installing Network Insights on your Own Hardware" on page 14.

NOTE: JSA continues to collect events when you deploy the full configuration. When the event collection service must restart, JSA 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.

"Configure the Network Insights appliance." on page 23

Optionally, you can install the "Network Insights content extension" on page 27. The content extension includes custom rule engine content, including rules, searches, reports, and custom property extractions, that provide analysis, alerts, and reports for Network Insights.

Appliance Configuration

IN THIS SECTION

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

On initial installation, 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 Network Insights to extract raw payload data. The **Maximum Raw Payload Size** for each appliance is inherited from the Network Insights global settings.

On initial installation, 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 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 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: 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 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 Network Insights payload size. For more information about flows, see Flow sources.

1. Log in to JSA as an administrator.
2. To configure the global settings, follow these steps:
   a. On the **Admin** tab, click **System Settings**.

   b. Click **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 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, JSA services restart. During this time, events and flows are not collected, and offenses are not generated.

5. 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 JSA.

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 JSA Console with a Network Insights appliance attached as a managed host.
- Perform a full deployment after you attach the Network Insights appliance as a managed host.

NOTE: 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.

1. Log in to JSA: **https://*JSA_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 8: QFlow Format Options

Flow Processor format	Description
TLV	Default setting for the flow collector format. Must be used when there is a Network Insights appliance in the environment. Network Insights V7.3.0 or later supports only TLV for content flows. Can be used when there is no Network Insights appliance in the environment.
Payload	Can be used when there is no 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, JSA 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 Network Insights managed host. This encrypts the IPFIX connection between the Network Insights managed host and the Flow Processor that receives the traffic.

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

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

You can have more than one 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 Flow Processor or flow source of any JSA 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 Network Insights Connection** page, select the Flow Processor and flow source.
4. Click **Save**.
5. Specify whether to configure the 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 Network Insights Content Extension

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 Network Insights deployments.

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

1. Log in to the JSA 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**.

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 Network Insights

SUMMARY

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

IN THIS SECTION

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

If you do not want to deploy a man-in-the-middle solution, limited decryption capabilities are available within JSA 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 **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.

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 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
```

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

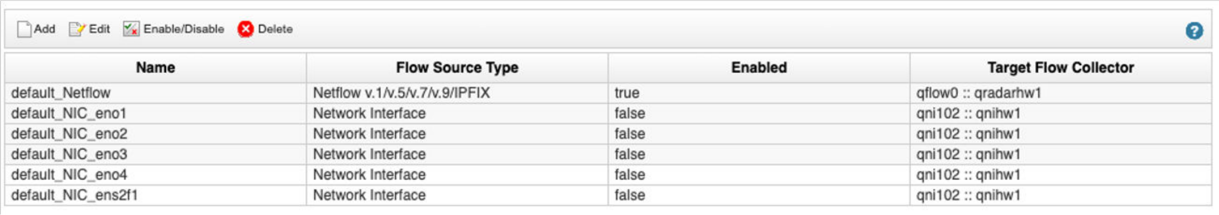
Flow Sources

IN THIS SECTION

When you install an Network Insights host, two types of flow sources are required. A 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 JSA deployment.

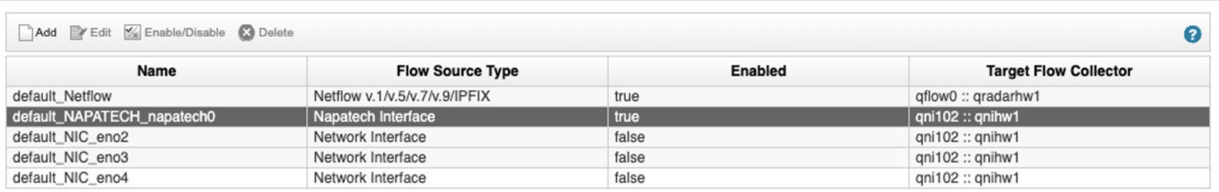
On Network Insights hosts, an input flow source is automatically created for all non-management interfaces that are available on the host. Except for Napatech interfaces, these flow sources are disabled by default, so you must enable the flow source if you want to use it for monitoring network flows.

In the following example, a Network Insights host *(qnihw1)* is connected to a JSA 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 Network Insights to export its flows to. By default, default_NetFlow sources are automatically created for JSA 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 JSA 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**.

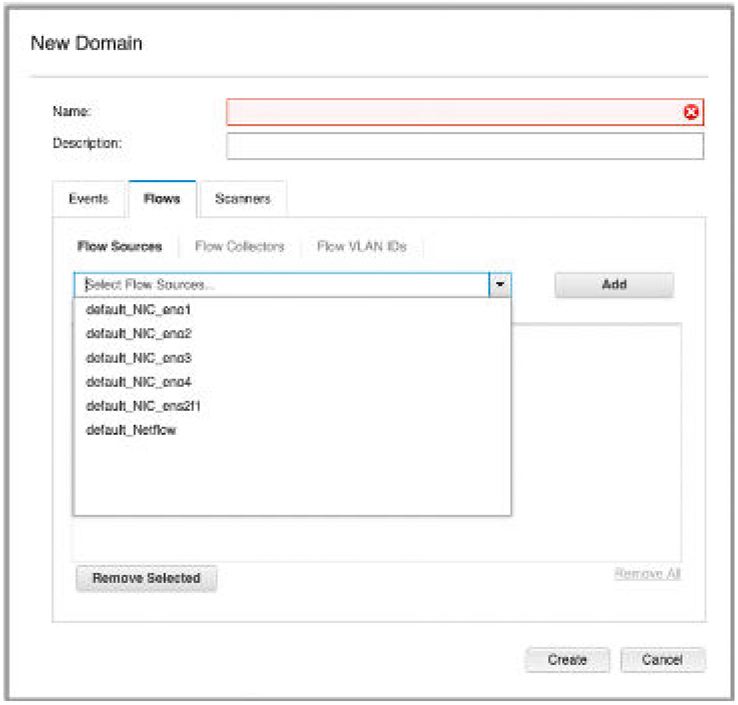
Domain Segmentation

IN THIS SECTION

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: 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.



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 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, 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 QFlow process.

Viewing Flow Data from a Specific Flow Source in Network Insights

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

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

When you install JSA, 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 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**: 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.

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

RELATED DOCUMENTATION

Adding a Flow Source | 31

Enabling Flow Sources | 31

Flow Inspection Levels

IN THIS SECTION

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.

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 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, 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 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, 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, 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 Network Insights found while doing the deeper level of inspection of the data flow.

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 9: 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 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 Network Insights appliances, you can override the global setting by configuring a custom inspection level for the individual appliances.

1. Log in to JSA 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 **Network Insights Settings**.

   c. From the **Flow Inspection Level**, select the flow rate.

   d. Click **Save**.
3. From the menu bar on the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

   ⚠ **WARNING**: When you deploy the full configuration, JSA services restart. During this time, events and flows are not collected, and offenses are not generated.
4. Refresh your web browser.

Deploy the Network Insights Processor.

6

CHAPTER

Troubleshooting

Troubleshooting

SUMMARY

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

IN THIS SECTION

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

Verifying that the Network Insights Appliance is Receiving Raw Packet Data

SUMMARY

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

- Ensure that the appliance is cabled correctly.

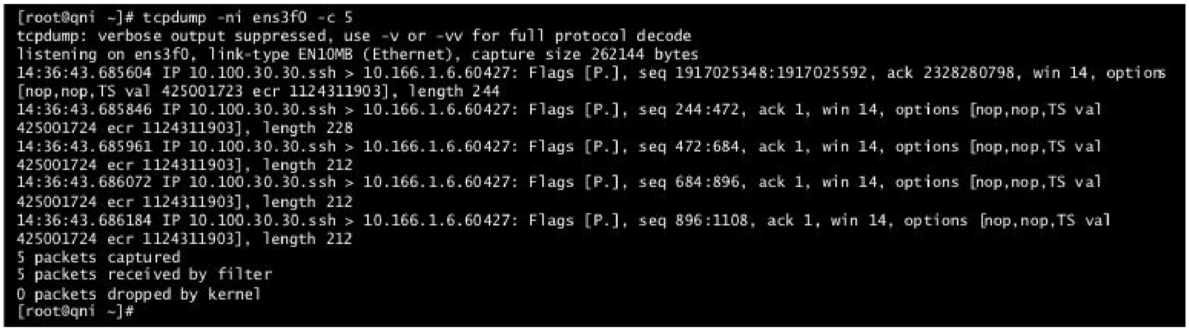
1. From the Console, use SSH to log in to JSA Network Insights as the root user.
2. If your appliance uses a traditional network card, use `tcpdump` to verify that the traffic is reaching the network interface:

   ```
   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 1: Results of tcpdump capture command



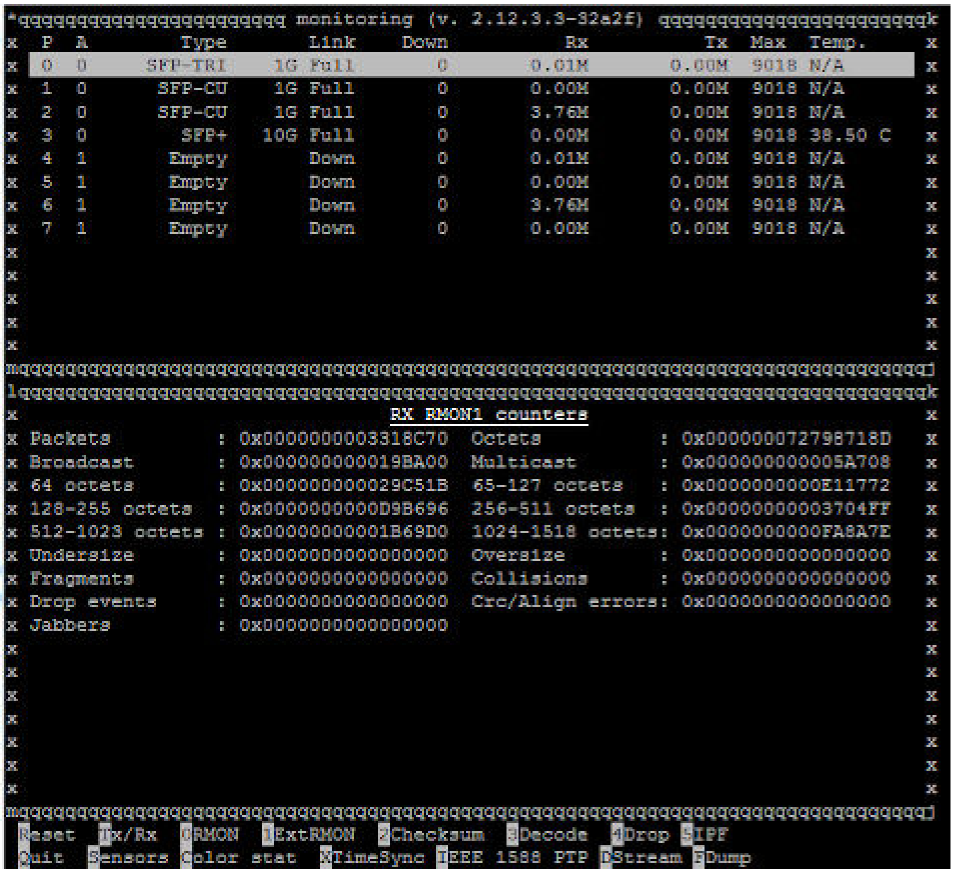
```
[root@qni ~]# tcpdump -ni ens3f0 -c 5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3f0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:36:43.685604 IP 10.100.30.30.ssh > 10.166.1.6.60427: Flags [P.], seq 1917025348:1917025592, ack 2328280798, 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 ~]#
```

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 2: Napatech Monitor with SFP Type, Link Status, and Transmission (Tx) Values.



```
*qqqqqqqqqqqqqqqqqqqqqqqq monitoring (v. 2.12.3.3-32a2f) qqqqqqqqqqqqqqqqqqqqqqqqk
x  P  A        Type       Link     Down            Rx           Tx  Max  Temp.     x
x  0  0    SFP-TRI    1G Full         0         0.01M        0.00M  9018 N/A       x
x  1  0     SFP-CU    1G Full         0         0.00M        0.00M  9018 N/A       x
x  2  0     SFP-CU    1G Full         0         3.76M        0.00M  9018 N/A       x
x  3  0       SFP+   10G Full         0         0.00M        0.00M  9018 38.50 C   x
x  4  1      Empty       Down         0         0.01M        0.00M  9018 N/A       x
x  5  1      Empty       Down         0         0.00M        0.00M  9018 N/A       x
x  6  1      Empty       Down         0         3.76M        0.00M  9018 N/A       x
x  7  1      Empty       Down         0         0.00M        0.00M  9018 N/A       x
x                                                                                  x
x                                                                                  x
x                                                                                  x
x                                                                                  x
x                                                                                  x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x                                  RX RMON1 counters                               x
x Packets          : 0x0000000003318C70  Octets            : 0x000000072798718D   x
x Broadcast        : 0x000000000019BA00  Multicast         : 0x000000000005A708   x
x 64 octets        : 0x000000000029C51B  65-127 octets     : 0x0000000000E11772   x
x 128-255 octets   : 0x0000000000D9B696  256-511 octets    : 0x00000000003704FF   x
x 512-1023 octets  : 0x00000000001B69D0  1024-1518 octets: 0x0000000000FA8A7E   x
x Undersize        : 0x0000000000000000  Oversize          : 0x0000000000000000   x
x Fragments        : 0x0000000000000000  Collisions        : 0x0000000000000000   x
x Drop events      : 0x0000000000000000  Crc/Align errors: 0x0000000000000000   x
x Jabbers          : 0x0000000000000000                                           x
x                                                                                  x
x                                                                                  x
x                                                                                  x
x                                                                                  x
x                                                                                  x
x                                                                                  x
x                                                                                  x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
 Reset  Tx/Rx  0RMON  1ExtRMON  2Checksum  3Decode  4Drop 5IPF
 Quit  Sensors Color stat  XTimeSync IEEE 1588 PTP DStream FDump
```

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)
   ```

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

SUMMARY

Follow these steps to verify that the Network Insights appliance is sending IPFIX records to the 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 Network Insights appliance is receiving raw packet data" on page 40.

1. Verify that the flow source is added and enabled in JSA.
   a. Log in to the JSA 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 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 JSA 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 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 Network Insights managed host is configured correctly.
   a. On the **Admin** tab, click **System and License Management**.
   b. Select the 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 Network Insights appliance to send flow data to, and click **Save**.

e. Configure the 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 JSA Console, click the **Network Activity** tab to see the flow records.

Flow data from the Network Insights does not Appear

SUMMARY

Follow these steps to determine why the flow data from your Network Insights does not appear on the **Network Activity** tab.

IN THIS SECTION

Symptoms

The **Network Activity** tab doesn’t show flow data from the Network Insights.

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 JSA services are restarted:

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

Diagnosing the Problem

1. Log in to the JSA 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 JSA 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 JSA on the **Network Activity** tab.

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