

IBM QRadar Network Packet Capture
7.4.3

Installation Guide



Note

Before you use this information and the product that it supports, read the information in [“Notices” on page 23](#).

Contents

- Introduction to installing QRadar Network Packet Capture..... v**
- Chapter 1. What's new.....1**
 - Previous releases..... 1
- Chapter 2. Installation overview..... 3**
- Chapter 3. Installations of QRadar Network Packet Capture on IBM appliances.....5**
 - QRadar Network Packet Capture hardware..... 5
 - Upgrading QRadar Network Packet Capture 7
 - Installing QRadar Network Packet Capture on IBM hardware..... 9
 - Configuring the appliance.....10
 - Configuring older versions of QRadar Network Packet Capture..... 12
 - Changing the root password.....12
 - Updating the license usage agreement.....13
- Chapter 4. Direct-attached storage devices..... 15**
 - Adding storage to your IBM QRadar Network Packet Capture appliance..... 15
- Chapter 5. Verify the QRadar Network Packet Capture installation..... 19**
 - Verifying the capture port..... 19
 - Verifying the time synchronization..... 20
 - Verify by using the external LEDs 21
- Notices.....23**
 - Trademarks..... 24
 - Terms and conditions for product documentation..... 24
 - IBM Online Privacy Statement..... 25
 - General Data Protection Regulation..... 25

Introduction to installing QRadar Network Packet Capture

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

Intended audience

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

Technical documentation

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

Contacting customer support

For information about contacting customer support, see [QRadar Support – Assistance 101](https://ibm.biz/qradarsupport) (<https://ibm.biz/qradarsupport>).

Statement of good security practices

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

Please Note:

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

Chapter 1. What's new in QRadar Network Packet Capture

Find out what's new or changed in IBM QRadar Network Packet Capture.

The following QRadar Network Packet Capture versions are included in this release:

- QRadar Network Packet Capture 7.4.3 Fix Pack 2 (Build 1304)
- QRadar Network Packet Capture 7.3.3 Fix Pack 8 (Build 20)

These fix packs include fixes for defects and security vulnerabilities.

Related concepts

[Installations of QRadar Network Packet Capture on IBM appliances](#)

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

What's new for installers in previous releases of QRadar Network Packet Capture

The following features and improvements were introduced in earlier versions of IBM QRadar Network Packet Capture.

Users can change their own passwords

[QRadar Network Packet Capture 7.4.3 Fix Pack 1 \(Build 1302\)](#)

[QRadar Network Packet Capture 7.3.3 Fix Pack 7 \(Build 17\)](#)

Non-administrative users can now change their own password. In previous releases, you had to be an administrator to change passwords.

 [Learn more about changing passwords as a non-administrative user...](#)

More Linux utilities installed

[QRadar Network Packet Capture 7.4.3 Fix Pack 1 \(Build 1302\)](#)

[QRadar Network Packet Capture 7.3.3 Fix Pack 7 \(Build 17\)](#)

The following Linux[®] utilities are now included in the QRadar Network Packet Capture installation:

- nc
- telnet
- nmap

For more information about how to use these utilities, refer to the Linux documentation.

License terms and conditions


[QRadar Network Packet Capture 7.4.3 \(Build 1301\)](#)

[QRadar Network Packet Capture 7.4.2 Fix Pack 1 \(Build 1203\)](#)

[QRadar Network Packet Capture 7.3.3 Fix Pack 6 \(Build 16\)](#)

Users must now review terms and conditions before they can log in to QRadar Network Packet Capture. The **Login** button appears only after you click the checkbox that indicates that you have read and accept the terms.

The terms that are shown on the login screen are populated by the `/opt/pandion/client/terms.txt` file. The file contains placeholder text, and you must edit it to include the terms and conditions that you want the user to accept. The file is a standard ASCII file, and you can use standard text editing tools to update it.

 [Learn more about updating the license usage agreement...](#)

Improved security features

QRadar Network Packet Capture 7.4.3 (Build 1301)


QRadar Network Packet Capture 7.4.2 Fix Pack 1 (Build 1203)

QRadar Network Packet Capture 7.3.3 Fix Pack 6 (Build 16)

When the QRadar Network Packet Capture installation is complete, the **Configure System** menu no longer runs on the IMM Remote Control screen.

You must authenticate in a terminal window, and run the Network Manager text user interface (`nmtui`) tool to set the IP address for the QRadar Network Packet Capture server. Then, you can log in to the QRadar Network Packet Capture graphical user interface.

The QRadar Network Packet Capture version information was removed from the **Login** screen to limit the information that is available before authentication. To view the version information after you log in, click the question mark icon in the upper right, and then select **About**.

 [Learn more about configuring the IP address...](#)

Direct-attached storage devices

QRadar Network Packet Capture 7.4.1 (Build 1107)

Expand the storage capacity of your QRadar Network Packet Capture appliance by attaching direct-attached storage (DAS) devices. Each DAS device that you connect adds 80 TB of storage capacity.

DAS devices can be used with only some QRadar Network Packet Capture appliances. The number of DAS devices that you can connect depends on which hardware you are using.

 [Learn more about adding direct-attached storage devices.....](#)

Chapter 2. Installation overview

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

You can upgrade directly to QRadar Network Packet Capture 7.4.3 from earlier versions.

Related concepts

[Installations of QRadar Network Packet Capture on IBM appliances](#)

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

Chapter 3. Installations of QRadar Network Packet Capture on IBM appliances

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

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

Related concepts

[Verify the QRadar Network Packet Capture installation](#)

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

[Installation overview](#)

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

[What's new in QRadar Network Packet Capture](#)

Find out what's new or changed in IBM QRadar Network Packet Capture.

QRadar Network Packet Capture hardware

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

QRadar Network Packet Capture appliance

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

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



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

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

The placement for the Intel X520 and Napatech NT40E3-4-PTP hardware can be seen in the following diagram, which shows the rear panel of the packet capture device:

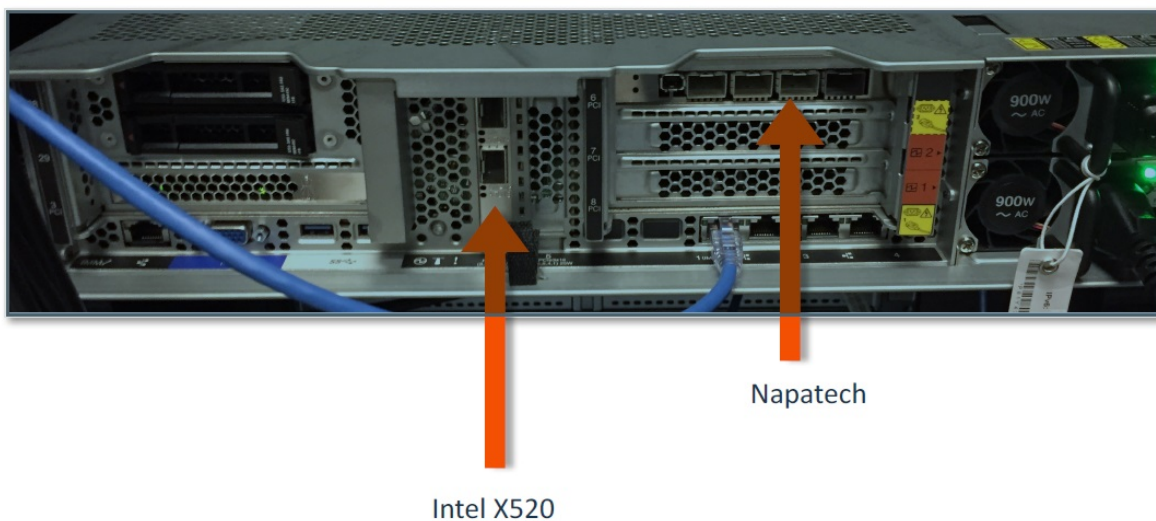


Figure 2. Rear panel of the QRadar Network Packet Capture appliance

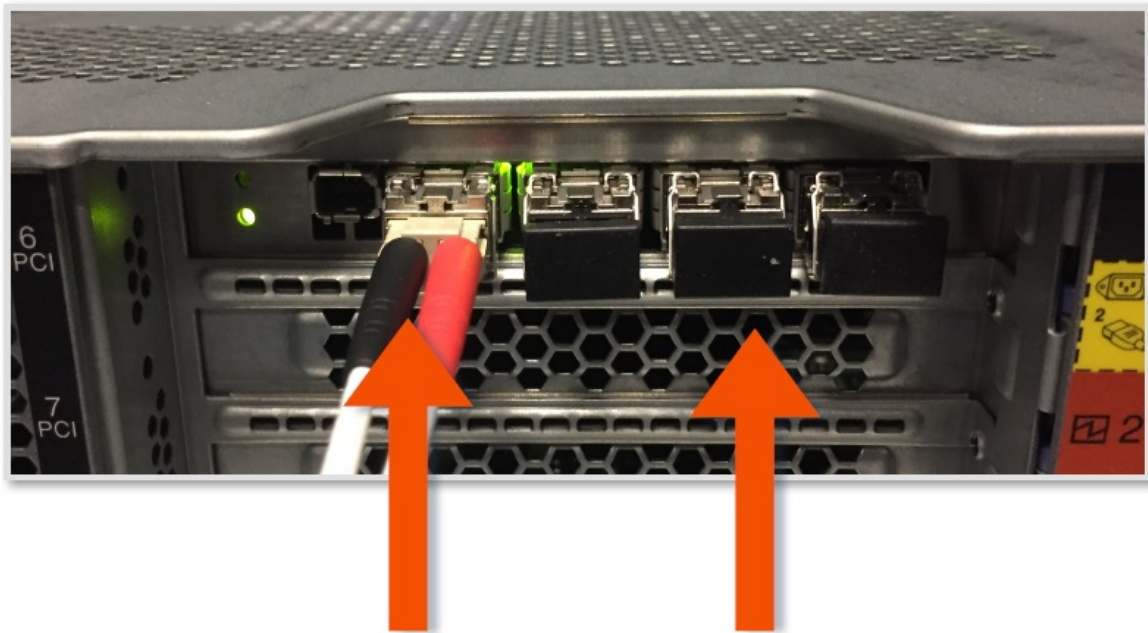
Napatech NT40E3-4-PTP SmartNIC

The Napatech NT40E3-4-PTP SmartNIC provides full packet capture and analysis with zero packet loss. You can capture data from up to four capture port sources with a single appliance. Capture ports can be reconfigured to enable port forwarding, that is you can capture on one port and mirror out another port.

Dual rate ports 10G/1G supports:

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

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



Fiber installed

Four SR SFP+ modules installed

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

The Napatech card is shipped with two sets of SFP+ modules. One set (four pieces) is Transceiver Dual SFP+ short range, and one set (four pieces) is Transceiver Dual SFP+ long range.

The following SFP+ modules are approved for use with the Napatech card:

- IBM D10E7LL 10G LR Avago (Included: 4 pieces)
- IBM D10E8LL 10G SR Avago (Included: 4 pieces)
- Napatech 802-0039-01-01 10G SR Finisar
- Napatech 10G LR 802-0039-01-01 Finisar

The following SFP+ modules are approved for use with the Intel X520 card:

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

Upgrading QRadar Network Packet Capture on IBM hardware

When you upgrade IBM QRadar Network Packet Capture, both the QRadar Network Packet Capture software and Red Hat Enterprise Linux operating system are upgraded. The configuration files and packet capture files remain unchanged.

Before you begin

Ensure that the following requirements are met:

- You are logged in to the QRadar Network Packet Capture appliance as an administrator.
- You are using an IBM-supplied QRadar Network Packet Capture appliance.

- The computer that you use to mount the .iso file must be on the same network as the appliance that you want to upgrade.

Network and internet latency across networks can cause the upgrade to fail.

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

If your deployment includes QRadar Network Packet Capture appliances that are in a stacked or grouped configuration, complete the following tasks before you upgrade:

- Ensure that traffic capture is stopped.

For more information, see [Starting or stopping packet capture](#).

- Remove the appliances from the group or stack.

After all your appliances are upgraded to the same version, you can re-create the group or stack. By upgrading each appliance individually and then rebuilding the stack and group configuration, the packet capture data is preserved during the upgrade process.

For more information, see [Stacked appliances](#) and [Grouped appliances](#).

Procedure

1. Download the .iso image from [IBM Fix Central](http://www.ibm.com/support/fixcentral) (www.ibm.com/support/fixcentral).

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

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

For example, if you are upgrading to QRadar Network Packet Capture 7.4.3 Fix Pack 2, select *7.4.3-QRadar-NETPCAP-Upgrade-1304*.

2. To use IMM2 to mount the .iso image, follow these steps:

- a) Log in to the IMM2 management module.

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

- b) Click **Remote Control**.

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

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

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

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

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

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

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

To watch a video tutorial about mounting an .iso by using the IMM2 management module, see [QRadar: Mounting ISOs Using IMM](https://www-01.ibm.com/support/docview.wss?uid=swg21974632) (<https://www-01.ibm.com/support/docview.wss?uid=swg21974632>).

3. Alternatively, you can copy the .iso to a bootable USB flash drive.

For more information, see [Creating a bootable USB flash drive with Red Hat Linux](#).

4. Restart the appliance.

5. On the **Boot Devices Manager** window, select the **Upgrade** option to start the upgrade process.



Warning: The upgrade process ensures that your configuration files and captured data remain intact. Choosing any other option might reset your configuration and delete your capture data.

6. After the upgrade is completed, restart the appliance.

Results

QRadar Network Packet Capture is upgraded.

Installing QRadar Network Packet Capture on IBM hardware

IBM QRadar Network Packet Capture appliances already have the QRadar Network Packet Capture software pre-installed. You might need to reinstall the software if, for example, you want to add Direct-Attached Storage devices or if you are recovering from a hardware failure.

Before you begin

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

- You are using an IBM-supplied QRadar Network Packet Capture appliance.
- You are logged in to the appliance as an administrator.
- The computer that you use to mount the .iso file must be on the same network as the appliance that you want to install on.

Network and internet latency across networks can cause the installation to fail.

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

About this task



Warning: QRadar Network Packet Capture configurations are lost when reinstalling the appliance. For more information about the impact on your configuration and capture data, see [Chapter 2, “Installation overview,”](#) on page 3.

Procedure

1. Download the .iso image from [IBM Fix Central](http://www.ibm.com/support/fixcentral) (www.ibm.com/support/fixcentral).

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

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

For example, if you want to do a clean installation of QRadar Network Packet Capture 7.4.1 and remove capture data that was previously collected, download *7.4.1-QRADAR-NETPCAPFULL-1110*.

If you want to reinstall or upgrade to QRadar Network Packet Capture 7.4.1 and keep captured data, select *7.4.1-QRADAR-NETPCAP-Upgrade-1110*.

2. To use IMM2 to mount the .iso image, follow these steps:

a) Log in to the IMM2 management module.

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

b) Click **Remote Control**.

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

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

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

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

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

- h) Locate the .iso image that you want to use, and click **Open**.
- i) Select the **Mapped** checkbox next to the drive to mount, and click **Mount Selected**.

To watch a video tutorial about mounting an .iso by using the IMM2 management module, see [QRadar: Mounting ISOs Using IMM](https://www-01.ibm.com/support/docview.wss?uid=swg21974632) (https://www-01.ibm.com/support/docview.wss?uid=swg21974632).

3. Alternatively, you can copy the .iso to a bootable USB flash drive.

For more information, see [Creating a bootable USB flash drive with Red Hat Linux](#).

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

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

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

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



Warning: When you choose **Install**, existing capture data is deleted. If you want to keep existing capture data, you must use the upgrade .iso, and select **Reinstall**.

7. After the installation is completed, restart the appliance.

Results

QRadar Network Packet Capture is installed. You can now configure the IP and network settings, and update the license usage agreement.

Related concepts

[Direct-attached storage devices](#)

[Verify the QRadar Network Packet Capture installation](#)

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

Related tasks

[Configuring the appliance](#)

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

[Changing the root password](#)

[Updating the license usage agreement](#)

Configuring the appliance

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

Before you begin

If your QRadar Network Packet Capture appliance is a member of a group, do not change the network configuration settings. In this case, unregister from the group, change the network configuration, and

reregister with the group. Use a full DHCP infrastructure, which assigns QRadar Network Packet Capture devices an IP address and hostname from DHCP.

About this task

New This process applies to the following versions of QRadar Network Packet Capture:

- QRadar Network Packet Capture 7.4.3 (Build 1301).
- QRadar Network Packet Capture 7.4.2 Fix Pack 1 (Build 1203).
- QRadar Network Packet Capture 7.3.3 Fix Pack 6 (Build 16)

Before you can set the IP address of the server, you must use the Network Manager Text User Interface (`nmtui`) tool to authenticate. Unlike older versions of QRadar Network Packet Capture, you cannot configure the appliance until you authenticate.

If you are using older versions of QRadar Network Packet Capture and you want to configure the appliance without authenticating, see [“Configuring older versions of QRadar Network Packet Capture”](#) on page 12.

Procedure

1. Log in to the PCAP server as the root user.
The default password is `napatech10`.
2. On the command line, run the Network Manager Text User Interface Tool by typing `nmtui`.
3. Select **Edit a connection**.
4. Select the management interface connection for your PCAP server, and click **Edit**.
5. In the **IPv4 Configuration** field, select **Manual**.

6. Edit the configuration settings.

You must use CIDR notation to specify the IP address.

You can leave the **DNS** field blank. A DNS infrastructure is not required for QRadar Network Packet Capture.

Tip: Use the following keystrokes to navigate the fields:

- To move forward, use the arrow keys or press the Tab key.
- To move backwards, press Shift-Tab.
- To select an option, press Enter.
- To toggle the status of a checkbox, press the space bar.

7. When you finish editing the configuration, select **OK**, and press Enter.
8. On the **Ethernet** screen, select **Back**, and press Enter.
9. On the **NetworkManager TUI** screen, select **OK** to save the configuration changes.
10. To apply the changes, you must deactivate and then reactivate the management interface.
 - a) On the **NetworkManager TUI** screen, select **Activate a connection**.
 - b) Select the interface that you updated the IP address, and select **Deactivate**.
 - c) Select the interface again, and select **Activate**.
11. If the **USB Ethernet** interface is active, select the interface and press Enter to deactivate it.
An active interface is indicated by a ***** next to the interface name.
12. Select **Back** and then select **Quit** to exit.

What to do next

To improve the security of the QRadar Network Packet Capture server, consider changing the root password. You can also set the terms and conditions for using the software.

Related concepts

[Verify the QRadar Network Packet Capture installation](#)

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

Related tasks

[Changing the root password](#)

[Updating the license usage agreement](#)

[Installing QRadar Network Packet Capture on IBM hardware](#)

IBM QRadar Network Packet Capture appliances already have the QRadar Network Packet Capture software pre-installed. You might need to reinstall the software if, for example, you want to add Direct-Attached Storage devices or if you are recovering from a hardware failure.

Configuring older versions of QRadar Network Packet Capture

You can configure your IBM QRadar Network Packet Capture appliance by making changes directly on the appliance or you can use the web interface.

About this task

This procedure is applicable to older versions of QRadar Network Packet Capture. Newer versions of QRadar Network Packet Capture require authentication before you can configure the appliance.

If you are using the following versions of QRadar Network Packet Capture, you must use the `nmtui` tool to authenticate before you can configure the appliance.

- QRadar Network Packet Capture 7.4.3 (Build 1301).
- QRadar Network Packet Capture 7.4.2 Fix Pack 1 (Build 1203).
- QRadar Network Packet Capture 7.3.3 Fix Pack 6 (Build 16)

For more information about using the `nmtui` tool, see [“Configuring the appliance” on page 10](#).

Procedure

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

Changing the root password

To improve the security of the QRadar Network Packet Capture server, consider changing the root password.

Procedure

1. To change the root password, type the following command on the console:

```
passwd root
```

2. Type the new password.

3. After the password is set, type `exit` to log out.

Related tasks

Configuring the appliance

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

Installing QRadar Network Packet Capture on IBM hardware

IBM QRadar Network Packet Capture appliances already have the QRadar Network Packet Capture software pre-installed. You might need to reinstall the software if, for example, you want to add Direct-Attached Storage devices or if you are recovering from a hardware failure.

Updating the license usage agreement

New IBM QRadar Network Packet Capture now includes a license usage agreement.

The license usage agreement was introduced in the following versions:

- QRadar Network Packet Capture 7.4.3 (Build 1301)
- QRadar Network Packet Capture 7.4.2 Fix Pack 1 (Build 1203)
- QRadar Network Packet Capture 7.3.3 Fix Pack 6 (Build 16)

About this task

Before users can log in to IBM QRadar Network Packet Capture, they must accept the terms and conditions that apply to the software use.

The initial IBM QRadar Network Packet Capture installation includes a stub file that contains place holder text for the terms and conditions. You must update the text file to include the terms and conditions that are specific to your organization.

Procedure

Edit the `/opt/pandion/client/terms.txt` file to include the terms and conditions that you want users to accept before they log in.

The `terms.txt` file is a standard ASCII file, and you can use standard text editing tools to update it.

Related tasks

Configuring the appliance

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

Installing QRadar Network Packet Capture on IBM hardware

IBM QRadar Network Packet Capture appliances already have the QRadar Network Packet Capture software pre-installed. You might need to reinstall the software if, for example, you want to add Direct-Attached Storage devices or if you are recovering from a hardware failure.

Chapter 4. Direct-attached storage devices

New in 7.4.1

IBM offers direct-attached storage (DAS) devices to expand the storage of some IBM QRadar Network Packet Capture appliances.

Upon delivery, the QRadar Network Packet Capture appliance is configured to recognize internal storage only. To use DAS devices, you must reconfigure the storage array by reinstalling the software, using IBM QRadar Network Packet Capture 7.4.1 (Build 1110) or later.

During the installation, the storage array is rebuilt and automatically includes the connected DAS devices.



Warning: The existing storage array on your QRadar Network Packet Capture appliance is destroyed. All packet capture data is lost.

Dell-based appliances

The QRadar Network Packet Capture-C Direct Attached Storage (MTM 4654-D2S) (DAS) device is based on the Dell MD 1400. It is intended for use with the IBM QRadar Network Packet Capture-C 40 GB (MTM 4654-F3D) appliance. You cannot connect this DAS device to other Dell-based IBM QRadar Network Packet Capture appliances.

You can attach up to three DAS devices. Each device adds 80 TB of storage capacity, and increases the capture rate by 10 Gbps.

Lenovo-based appliances

The QRadar Network Packet Capture Direct Attached Storage (MTM 4563-D1S) (DAS) device is based on the Lenovo D1212. It is intended for use with the IBM QRadar Network Packet Capture 10 GB (MTM 4563-F3C) appliance. You cannot connect this DAS device to other Lenovo-based IBM QRadar Network Packet Capture appliances.

You can attach up to eight DAS devices in a daisy-chain configuration. Each device adds 80 TB of storage capacity. Adding DAS devices to your Lenovo appliance does not increase the capture rate.

Related tasks

[Installing QRadar Network Packet Capture on IBM hardware](#)

IBM QRadar Network Packet Capture appliances already have the QRadar Network Packet Capture software pre-installed. You might need to reinstall the software if, for example, you want to add Direct-Attached Storage devices or if you are recovering from a hardware failure.

Adding storage to your IBM QRadar Network Packet Capture appliance

New in 7.4.1

Follow these steps to add direct-attached storage (DAS) devices to your IBM QRadar Network Packet Capture appliance.

1. Back up the configuration of your packet capture appliance.
2. Attach the DAS devices.
3. Reinstall the QRadar Network Packet Capture software.

You must install IBM QRadar Network Packet Capture 7.4.1 (Build 1110) or later.

4. Restore the configuration backup.
5. Verify that the increased storage appears as expected in QRadar Network Packet Capture.

Failure to follow these procedures might result in the loss of configuration data on the appliance, or the appliance might not be able to use the new DAS devices.



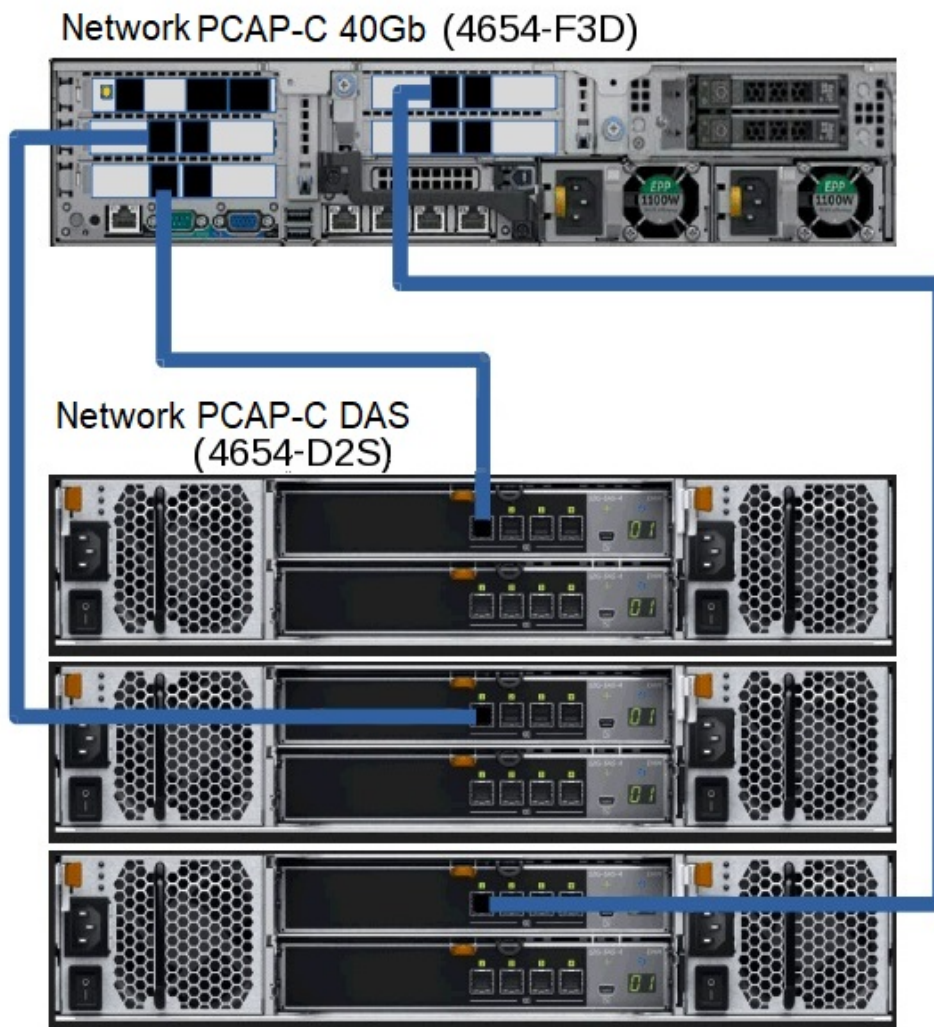
Warning: When you reinstall the software, the existing storage array is destroyed, and all packet capture data is lost. The packet capture data is not included in the configuration backup and cannot be restored.

Procedure

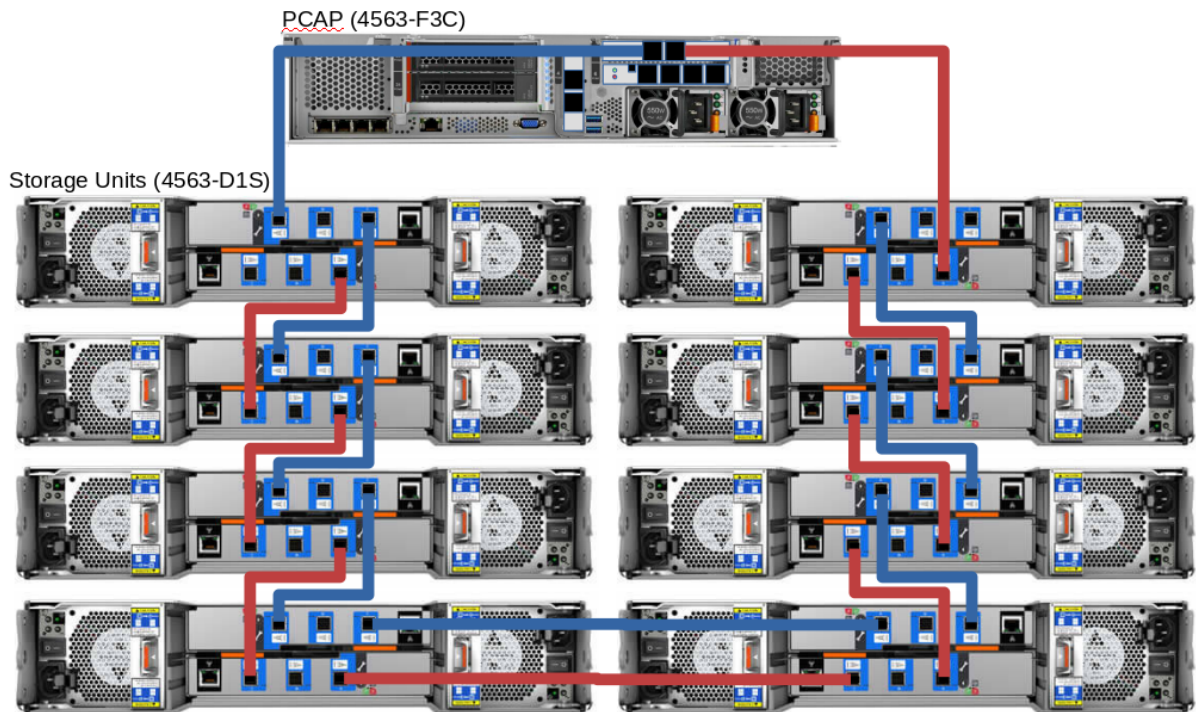
1. Back up the configuration files for the appliance.
 - a) Log in to the QRadar Network Packet Capture appliance.
 - b) Click **ADMIN**.
 - c) Click **Backup**.

A .json file is created that includes all of the custom configuration changes that were made to the system. The file is automatically downloaded to your local computer.
2. Connect the DAS devices to the server.

The following image shows a QRadar Network Packet Capture-C 40 GB appliance with three attached DAS devices.



The following image shows a QRadar Network Packet Capture 10 GB appliance with eight DAS devices attached. The blue cables are required to connect the devices. The red cables provide cable redundancy, therefore, they are optional.



3. Install the QRadar Network Packet Capture software.
 For more information, see [“Installing QRadar Network Packet Capture on IBM hardware”](#) on page 9.
 The installation process automatically includes the DAS storage when it builds the new RAID-5 storage array.
4. Restore the configuration from the backup file.
 - a) Log in to the QRadar Network Packet Capture appliance.
 - b) Click **ADMIN**.
 - c) Click **Restore** and select the configuration backup file.
5. Log in to the appliance and verify that the increased storage capacity is shown.
 The total storage capacity depends on the number of DAS devices that are connected. The storage capacity in your deployment may be different than what is shown in the following image.

IBM DASHBOARD SEARCH ADMIN

GROUP VIEW

Unknown QRadar Network Packet Capture 0.00 Mbit/s

UNIT VIEW (UNKNOWN)

Current retention	N/A
Estimated max retention	N/A
Updated at	2020-24-10 19:19:14 localtime (UTC-0400)

Health status
The system is healthy.

<p>SmartNIC</p> <p>Health: Healthy</p> <p>Port 0: Up at 40G</p> <p>Port 1: Down</p> <p>Temperature: 44.4 °C</p> <p>Fan speed: 6465 RPM</p>	<p>System</p> <p>Version: 7.4.2-1201</p> <p>Product name: QRadar Network Packet Capture</p> <p>Health: Healthy</p> <p>Uptime: 16 days 2 hours 28 mins 51 secs</p> <p>System time: 2020-24-10 23:19:14 (UTC)</p> <p>Retention: N/A</p> <p>Packets dropped: 0</p> <p>Capturing: No</p>	<p>Storage</p> <p>Health: Healthy</p> <p>Storage: 320TB</p>
---	---	--

Figure 4. Increased storage capacity shown on the Network Packet Capture dashboard

Chapter 5. Verify the QRadar Network Packet Capture installation

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

To verify the installation on your custom appliance, [use the external LED lights](#).

Related concepts

[Installations of QRadar Network Packet Capture on IBM appliances](#)

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

Related tasks

[Installing QRadar Network Packet Capture on IBM hardware](#)

IBM QRadar Network Packet Capture appliances already have the QRadar Network Packet Capture software pre-installed. You might need to reinstall the software if, for example, you want to add Direct-Attached Storage devices or if you are recovering from a hardware failure.

[Configuring the appliance](#)

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

Verifying the capture port

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

Procedure

1. In a browser window, log in to the QRadar Network Packet Capture appliance as an administrator.

The default password for the ADMIN account is `pandion`.

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

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

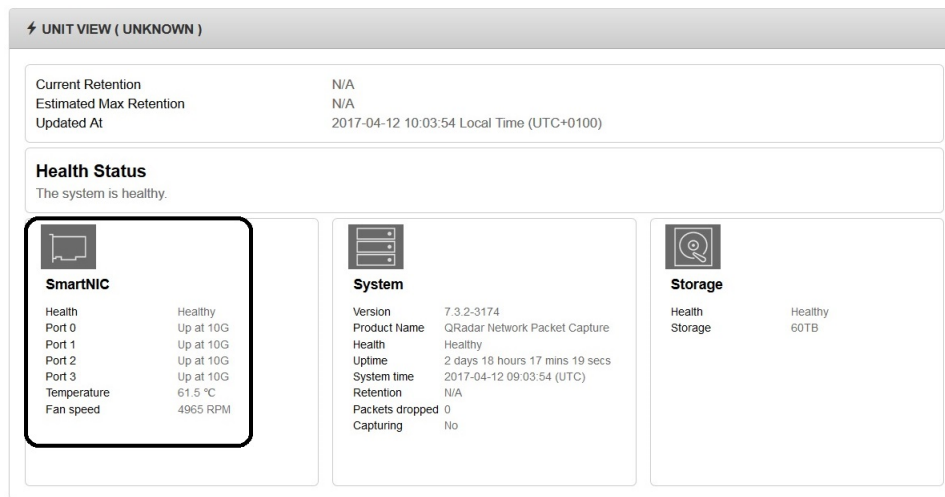


Figure 5. **UNIT VIEW** widget.

Verifying the time synchronization

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

About this task

If the appliance is not supplied by IBM, you can use the [external LED lights](#) to verify external time synchronization.

Procedure

1. In a browser window, log in to the QRadar Network Packet Capture appliance as an administrator.

The default password for the ADMIN account is `pandion`.

2. On the **Admin** tab, review the logs for a general message that indicates that the time synchronization source changed, or that the SmartNIC obtained or released the lock against the time source.

The following syntax is representative of a general entry:

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

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

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

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

The following syntax is representative of a PTP entry:

```
Adapter < number > PTP time-sync status:
PTP Time: "--" | < PTP clock time > [ "(TAI)" ]
Port: < IPv4_address > | < IPv6_address > | "IEEE 802.3"
Link Status: < Down | 10M | 100M >
IPv4 Subnet Mask: < IPv4_address >
IPv4 Gateway: < IPv4_address >
DHCP Enabled: "Yes" | "No"
Profile Id: < six_times_2_hex_digits >
Profile: < Default | Telecom | Power >
Clock Id: < six_times_2_hex_digits >
Domain: < number > | "--"
VLAN: < number >
Delay Mechanism: "E2E", "P2P", "N/A"
PTP Filter: "Min", "PDV", "None", "N/A"
DelayAssemetry: < number >
Clock State: "Faulty" | "INACTIVE" | "SLAVE" | "--"
Mean Path Delay: <number>
GM Clock Identity: < 16_hex_digits >
```

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

```
Adapter 0 time-sync status:
Adapter 0 PTP time-sync status:
PTP Time: Thu 26-May-2016 12:44:03.123456789 (TAI)
Port: 192.168.3.77
Link Status: 100M
IPv4 Subnet Mask: 192.168.3.0
IPv4 Gateway: 192.168.3.1
DHCP Enabled: Yes
Profile Id: 00:1b:19:00:01:00
```

```

Profile: Default
Clock Id: 00:0d:e9:03:a2:aa
Domain: 0
VLAN: 0
Delay Mechanism: E2E
PTP Filter: None
Delay Assemetry: 0
Clock State: SLAVE
Mean Path Delay: 0
GM Clock Identity: 000de9fffe03a2aa

```

Verify by using the external LEDs

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

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

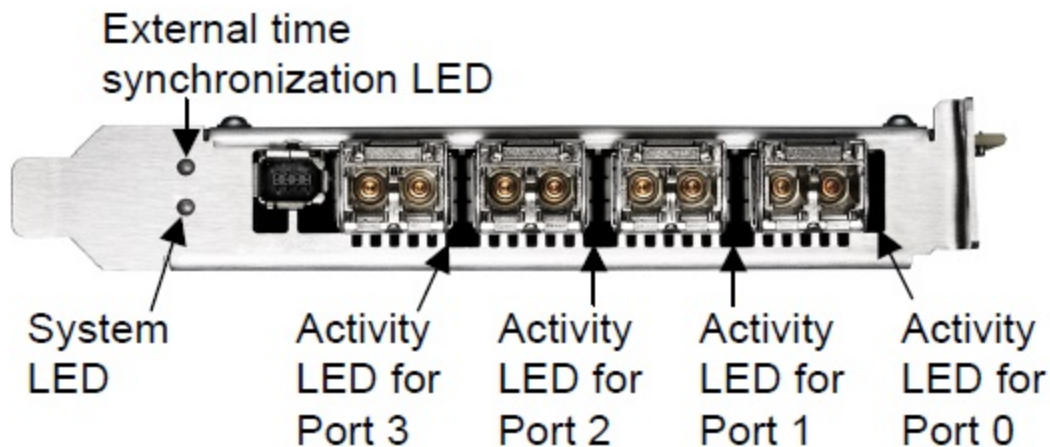


Figure 6. Location of the external LEDs

Tip:

If you are using an IBM-supplied appliance, you can also verify the time synchronization and status of the capture network interface card by reviewing the SYSLOGS messages. For more info, see [“Verifying the time synchronization”](#) on page 20.

Activity LEDs

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

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

System LED

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

Table 3. System LED and operating status of the appliance.

State and Color	Condition
Off	The power is off.
Constant red	During start-up and the power is on, the SmartNIC is checking the power supplies.
Flashing red	After start-up and the power is on, there is an unrecoverable hardware error.
Constant yellow	During start-up the power is on, and the power supplies are working.
Flashing yellow	There is a new entry in the hardware log.
Constant green	The FPGA is loaded, and the system is running.

External time synchronization LED

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

Table 4. External time synchronization LED and the operating status of the appliance.

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

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Trademarks

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

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

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

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

IBM Online Privacy Statement

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

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

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

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

General Data Protection Regulation

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

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

