IBM QRadar Incident Forensics
7.4.0

Installation Guide

IBM

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 27.

Contents

Introduction to installing IBM QRadar Incident Forensics

Information about installing IBM® QRadar® Incident Forensics and integrating the product with IBM QRadar. QRadar Incident Forensics appliances contain preinstalled software and the Red Hat Enterprise Linux operating system. You can also install QRadar Incident Forensics software on your own hardware.

Intended audience

Network administrators that are responsible for installing and configuring QRadar Incident Forensics systems.

Administrators require a working knowledge of networking and Linux® operating systems.

Technical documentation

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

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

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

Please Note:

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

Note

IBM QRadar Incident Forensics is designed to help companies improve their security environment and data. More specifically, IBM QRadar Incident Forensics is designed to help companies investigate and better understand what happened in network security incidents. The tool allows companies to index and search captured network packet data (PCAPs) and includes a feature that can reconstruct such data back into its original form. This reconstruction feature can reconstruct data and files, including email messages, file and picture attachments, VoIP phone calls and websites. Additional information

regarding the Program's features and functions and how they may be configured are contained within the manuals and other documentation accompanying the Program. Use of this Program may implicate various laws or regulations. including those related to privacy, data protection, employment, and electronic communications and storage. IBM QRadar Incident Forensics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM QRadar Incident Forensics.

Chapter 1. What's new in QRadar Incident Forensics

Stay up to date with the new features that are available in IBM QRadar Incident Forensics.

What's new in QRadar Incident Forensics 7.4.0

QRadar Incident Forensics 7.4.0 introduces changes to the files that are used to install and upgrade your deployment.

To view the complete list of new features, see What's new in QRadar Incident Forensics 7.4.0.

Isolated installation file for QRadar Incident Forensics

In previous releases, the QRadar Incident Forensics installation and upgrade files included QRadar Network Insights. In 7.4.0, each product has a separate .iso file for new installations.

The process to upgrade your deployment does not change. Only a single file is required, but you must ensure that you download the .sfs file that includes QRadar Incident Forensics.

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

- New QRadar Incident Forensics installations:

  Rhe764forensics*<build_version>*.stable-*<identifier>*.iso
- Upgrades to existing QRadar installations that include QRadar Incident Forensics:

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

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

ⓘ Learn more about installing and upgrading QRadar Incident Forensics...

Chapter 2. QRadar Incident Forensics installation overview

The security capabilities that are available to you in IBM QRadar Incident Forensics depends on the type of installation that have.

For example, in a stand-alone deployment, a single QRadar Incident Forensics Standalone (6100) appliance provides only network forensics capabilities.

In a distributed deployment, a QRadar Incident Forensics Processor (6000) appliance is connected to a QRadar Console (3199) as a managed host, which provides more security capabilities than a stand-alone deployment.

You can also install QRadar Incident Forensics software on your own appliance or on a virtual appliance. QRadar Incident Forensics must be installed on a Red Hat® Enterprise Linux operating system.

The following diagram summarizes the multiple security capabilities and architectural framework of the IBM QRadar Security Intelligence Platform.
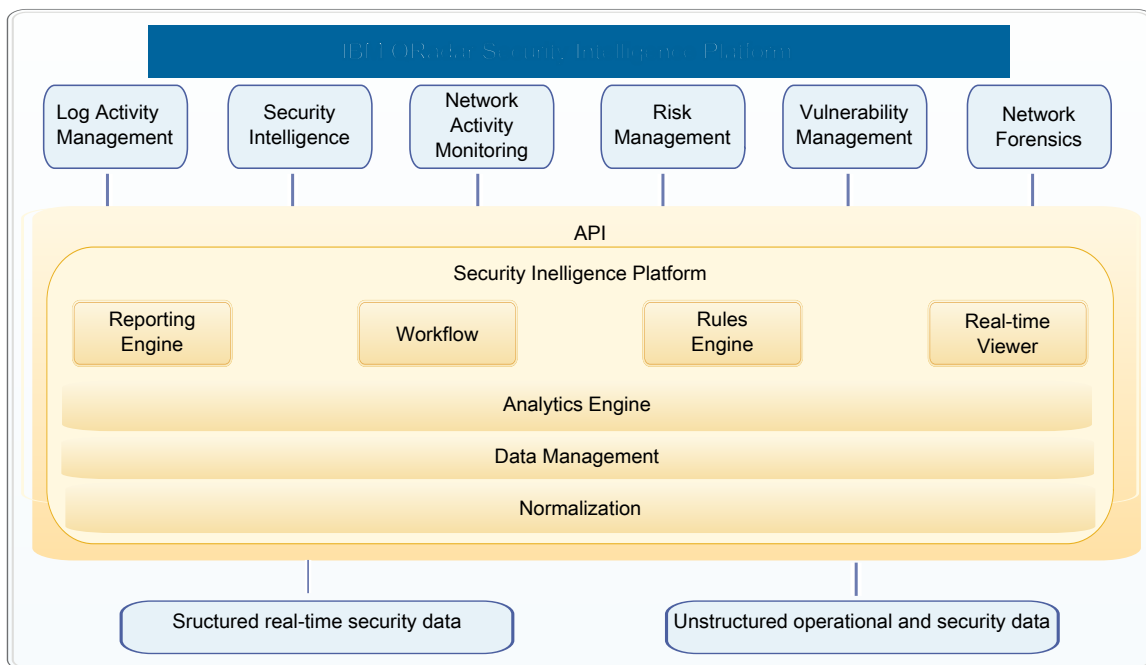

Figure 1. QRadar security intelligence architectural overview

For most installations, you install the QRadar Console, at least one QRadar Incident Forensics Processor, and one or more QRadar Network Packet Capture appliances.

QRadar Incident Forensics stand-alone deployments

IBM QRadar Incident Forensics Standalone is a single appliance deployment that is similar to installing the QRadar Console and QRadar Incident Forensics managed host on one appliance. Commonly referred to as an all-in-one deployment, this network forensics solution does not include log management or network activity monitoring capabilities.

You install QRadar Incident Forensics Standalone (appliance ID 6100) from the QRadar Incident Forensics ISO image.

As shown in the following diagram, you can attach packet capture appliances to the IBM QRadar Incident Forensics Standalone appliance.
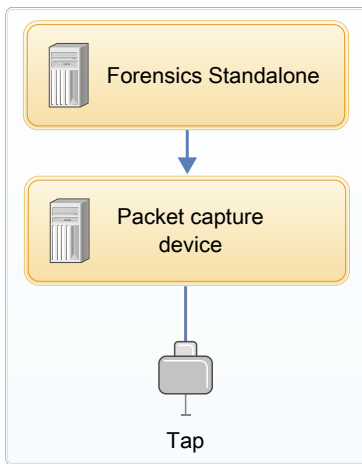
Figure 2. IBM QRadar Incident Forensics Standalone deployment example

Restriction: You can't add managed hosts to the QRadar Incident Forensics Standalone nor can you attach the QRadar Incident Forensics Standalone to a QRadar Console.

QRadar Incident Forensics distributed deployments

A distributed deployment of QRadar Incident Forensics includes a QRadar Console and one or more QRadar Incident Forensics managed hosts. This type of deployment includes event and log management, anomaly detection, risk management, vulnerability management and also gives you the ability to distribute the workload for forensics recoveries.

In a distributed deployment, there are three appliances:

- QRadar Console
- QRadar Incident Forensics managed host (Forensics processor)
- QRadar Network Packet Capture (optional)

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

The following diagram shows that you can attach multiple QRadar Incident Forensics managed hosts to the QRadar Console. You can attach QRadar Network Packet Capture devices to the QRadar Incident Forensics managed hosts (QRadar Incident Forensics Processor).
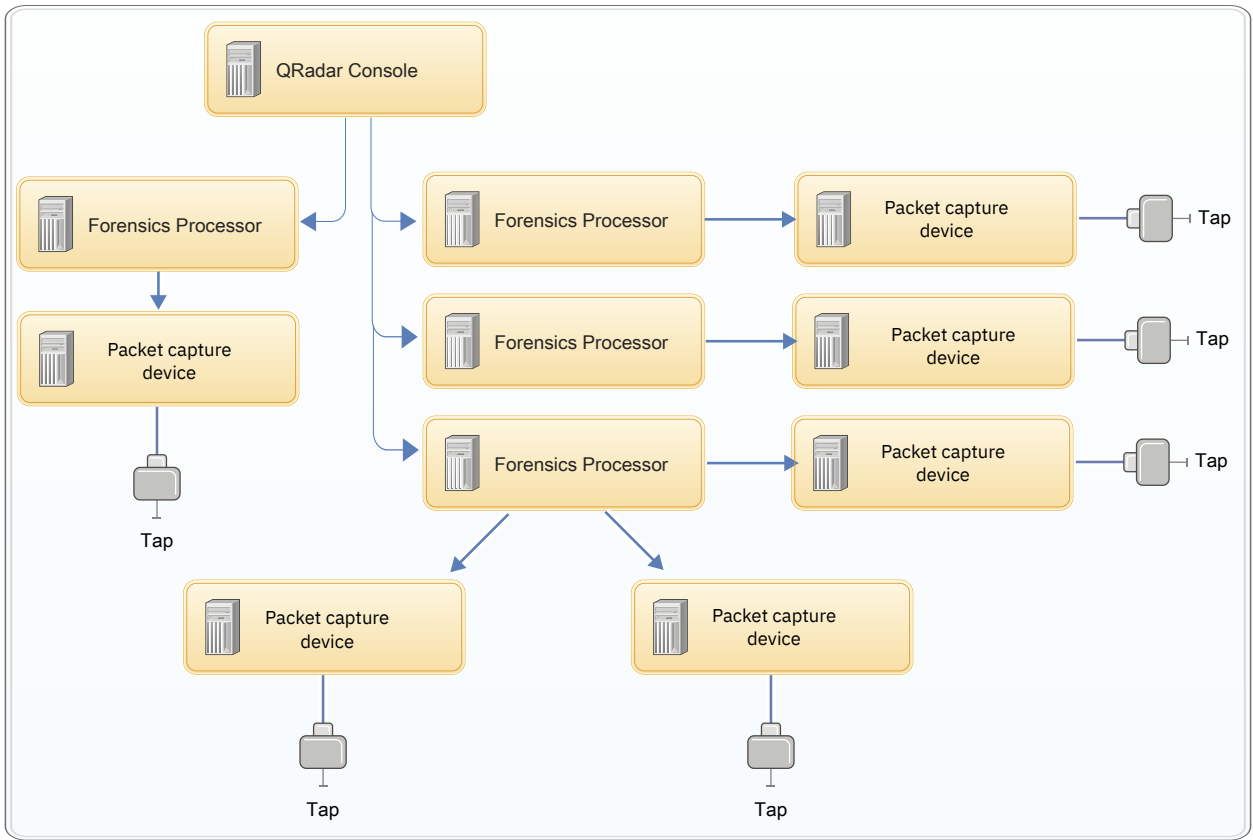
Figure 3. Distributed deployment example

Distributed installations

New software installations that integrate QRadar Incident Forensics with IBM QRadar requires installation components from at least 2 ISO files. Each installation requires an *activation key* which determines the appliance type that is installed.

The following table shows which ISO file to use to install each of the components in a QRadar Incident Forensics distributed deployment.

Table 1. Components of a QRadar Incident Forensics distributed deployment	
ISO file	**Installed component**
QRadar ISO	Choose appliance type 3199 to install the QRadar Console.
	This ISO image is also used to install every QRadar product except for QRadar Incident Forensics and IBM QRadar Network Insights. The activation key determines the type of appliance that is installed.
QRadar Incident Forensics ISO	Choose appliance type 6000 to install the QRadar Incident Forensics Processor.
	You cannot attach QRadar Incident Forensics Standalone (appliance type 6100) to a QRadar Console.

QRadar Incident Forensics installation components

QRadar Incident Forensics is integrated into the scalable architecture of IBM QRadar Security Intelligence Platform. Depending on your requirements, you can install IBM QRadar Incident Forensics components on a stand-alone appliance (*all-in-one* deployment) or on multiple appliances (distributed deployment).
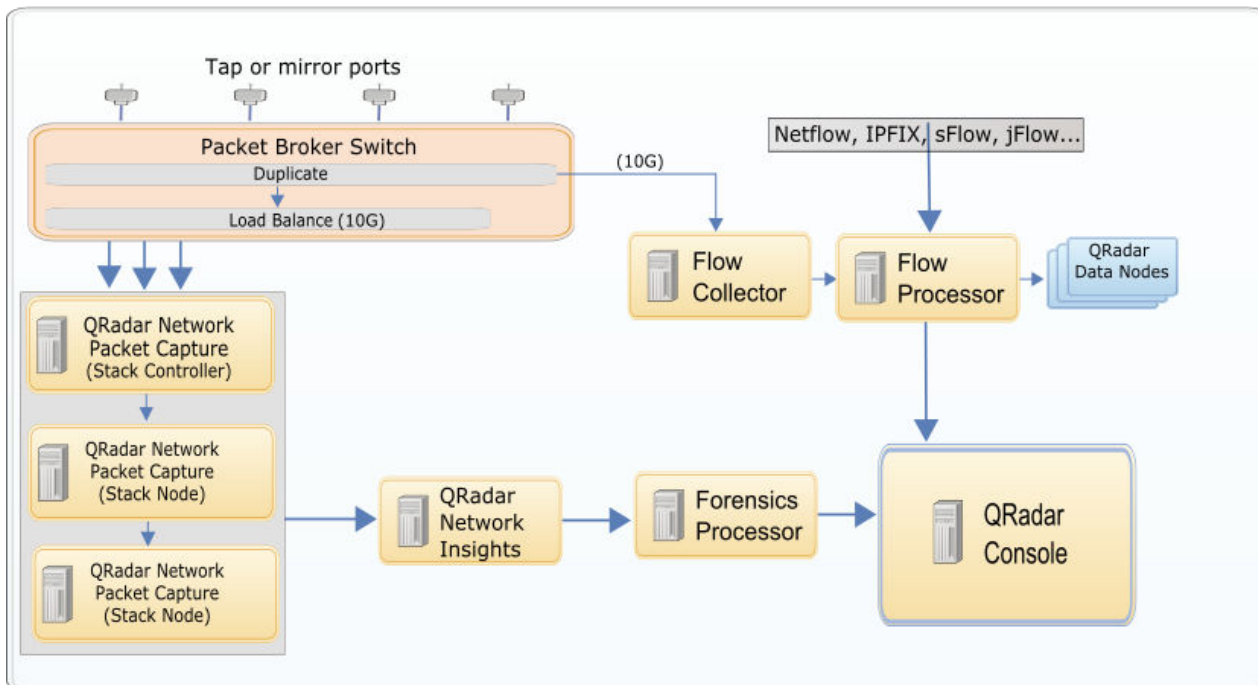
QRadar deployments can include the following components:

QRadar Console

> The QRadar Console provides the product user interface, and real-time event and flow views, reports, offenses, asset information, and administrative functions.

> In distributed QRadar deployments, use the QRadar Console to administer otherQRadar managed hosts.

QRadar Flow Processor

> Processes flows from one or more QRadar QFlow Collector appliances. The Flow Processor appliance can also collect external network flows such as NetFlow, J-Flow, and sFlow directly from routers in your network. You can use the Flow Processor appliance to scale your QRadar deployment to manage higher flows per minute (FPM) rates.

QRadar Data Node

> Data Nodes enable new and existing QRadar deployments to add storage and processing capacity on demand as required. Data Nodes help to increase the search speed in your deployment by providing more hardware resources to run search queries on.

QRadar QFlow Collector

> The IBM QRadar QFlow Collector collects flows by connecting to a SPAN port, or a network TAP. The appliance also supports the collection of external flow-based data sources, such as NetFlow from routers.

QRadar Incident Forensics Processor
> Provides the QRadar Incident Forensics product user interface. The interface delivers tools to retrace the step-by-step actions of cyber criminals, reconstruct raw network data that is related to a security incident, search across available unstructured data, and visually reconstruct sessions and events.

You must attach the QRadar Incident Forensics Processor as a managed host to a QRadar Console before you can use the security intelligence forensics capability.

You can connect up to five packet capture devices to a QRadar Incident Forensics Processor or a QRadar Incident Forensics Standalone appliance.

Note: If you install QRadar Incident Forensics Standalone, a QRadar Console is not required. This offering provides only the tools and administrative capabilities that are required to do a forensics investigation.

QRadar Network Packet Capture

Use these optional packet capture appliances to store and manage data that is used by QRadar Incident Forensics when no other packet capture device is deployed in your environment. You can install any number of these appliances as a network tap or subnetwork to collect the raw packet data. If no packet capture device is attached, you can manually upload the packet capture files in the user interface or by using FTP.

You can extend the storage that is available for capture data by connecting multiple QRadar Network Packet Capture appliances together in a ring topology to create a stack. The stack allows the distribution of capture data across each of the connected appliances. It can connect up to 16 devices, but appears and behaves like a single entity that captures data from one TAP of a single 10GB port.

QRadar Network Insights
The QRadar Network Insights appliance provides real-time analysis of network data and an advanced level of threat detection and analysis. You can use QRadar Network Insights to detect and analyze malware, phishing, insider threats, lateral movement attacks, data exfiltration, and compliance gaps.

Activation keys and license keys

When you install IBM QRadar appliances, you must type an activation key. After you install, you must apply your license keys. To avoid typing the wrong key in the installation process, it is important to understand the difference between the keys.

Activation key

The activation key is a 24-digit, 4-part, alphanumeric string that you receive from IBM. All installations of QRadar products use the same software. However, the activation key specifies which software modules to apply for each appliance type. For example, use the IBM QRadar QFlow Collector activation key to install only the QRadar QFlow Collector modules.

You can obtain the activation key from the following locations:

- If you purchased an appliance that is preinstalled with QRadar software, the activation key is included in a document on the enclosed CD.
- If you purchased QRadar software or virtual appliance download, a list of activation keys is included in the *Getting Started* document. The *Getting Started* is attached to the confirmation email.

License keys

Your system includes a temporary license key that provides you with access to QRadar software for five weeks. After you install the software and before the default license key expires, you must add your purchased licenses.

When you purchase a QRadar product, an email that contains your permanent license key is sent from IBM. These license keys extend the capabilities of your appliance type and define your system operating parameters. You must apply your license keys before your temporary license expires.

In a stand-alone deployment (6100), you must allocate two license keys to the IBM QRadar Incident Forensics Standalone appliance. One license is for QRadar Incident Forensics Standalone and the other license is for access to the **Forensics** tab.

In a distributed deployment (6000), you might need to have a license for each Forensics managed host and also a single license to enable the **Forensics** tab on the console.

- If your existing QRadar Console license key allows access to the **Forensics** tab, you only need the license key for the QRadar Incident Forensics installation.
- If your existing QRadar Console license key does not allow access to the **Forensics** tab, you need the licence for the QRadar Incident Forensics installation as well as an updated Forensics enablement key.

Prerequisite hardware and software

Before you install IBM QRadar products, ensure that you have access to the required hardware accessories and desktop software.

Hardware accessories

Ensure that you have access to the following hardware components:

- Monitor and keyboard
- Uninterruptible power supply (UPS) for all systems that store data, such as QRadar Console, Event Processor components, or QRadar QFlow Collector components

Important: QRadar products support hardware-based Redundant Array of Independent Disks (RAID) implementations, but do not support software-based RAID installations.

Desktop software requirements

Ensure that following applications are installed on all desktop systems that you use to access the QRadar product user interface:

- Java™ Runtime Environment (JRE) version 1.7 or IBM 64-bit Runtime Environment for Java V7.0
- Adobe Flash version 10.x

Red Hat Enterprise Linux

The following table describes the version of Red Hat Enterprise Linux used with the IBM QRadar version.

Table 2. Red Hat version	
IBM QRadar version	**Red Hat Enterprise Linux version**
IBM QRadar 7.4.0	Red Hat Enterprise Linux V7.6 64-bit
IBM QRadar 7.4.1	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.2	Red Hat Enterprise Linux V7.7 64-bit
IBM QRadar 7.4.3	Red Hat Enterprise Linux V7.7 64-bit

Supported web browsers

The following table lists the supported versions of web browsers:

Table 3. Supported web browsers for QRadar products	
Web browser	**Supported versions**
64-bit Mozilla Firefox	60 Extended Support Release and later
64-bit Microsoft Edge	38.14393 and later

Table 3. Supported web browsers for QRadar products (continued)	
Web browser	**Supported versions**
64-bit Google Chrome	Latest

The Microsoft Internet Explorer web browser is no longer supported as of QRadar 7.4.3.

Communication between QRadar Incident Forensics hosts require open ports

The following table lists the ports that must be open between QRadar Incident Forensics hosts:

Table 4. Open ports between hosts	
Port	**Description**
443	Required for artifact analysis.
28080	Required for distributed search.

Chapter 3. Upgrading QRadar Incident Forensics

Upgrade to IBM QRadar Incident Forensics 7.4.3 by using an upgrade installer. You must upgrade all of your IBM QRadar products in your deployment to the same version.

Before you begin

Download the QRadar Incident Forensics patch file from IBM Fix Central (www.ibm.com/support/fixcentral). The patch file is named similar to this one: `<identifier>_Forensics_patchupdate-<build_number>.sfs`.

About this task

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

During the upgrade, the Red Hat Enterprise Linux version might also be upgraded. The following table shows the Red Hat Enterprise Linux version that is used with IBM QRadar.

Table 5. Red Hat version

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

QRadar Incident Forensics supports custom certificates. When you upgrade to 7.4.3, custom certificates that are already in use on the QRadar Console are migrated as part of the upgrade.

Restriction: Resizing logical volumes by using a logical volume manager (LVM) is not supported.

If you want to upgrade from QRadar Incident Forensics V7.2.4 or earlier versions, but don't want to keep your data, you can upgrade directly to 7.4.3 by doing a new installation. If you want to keep your data, contact your IBM sales representative.

Procedure

1. Use SSH to log in to your system as the root user.
2. Copy the patch file to the `/tmp` directory or to another location that has sufficient disk space.
3. To create the `/media/updates` directory, type the following command:

   ```
   mkdir -p /media/updates
   ```

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

   ```
   mount -o loop -t squashfs <identifier>_Forensics_patchupdate-<build_number>.sfs /media/
   updates
   ```

6. 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.

7. Provide answers to the pre-installation questions based on your deployment.
8. Use the upgrade installer to upgrade all hosts in your deployment.

   If you do not select **Patch All**, you must upgrade systems in the following order:

   • QRadar Console
   • QRadar Incident Forensics

   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.
9. After the upgrade is complete, unmount the software update by using the following command:

```
umount /media/updates
```

What to do next

Upgrade your packet capture devices. For more information, see the IBM QRadar Network Packet Capture documentation.

Chapter 4. QRadar Incident Forensics installations

You can install IBM QRadar Incident Forensics as a stand-alone deployment or as a distributed installation.

For stand-alone deployments, install QRadar Incident Forensics Standalone (appliance type 6100) on a single appliance.

For distributed installations, install the QRadar Console (appliance type 3199) on one appliance and QRadar Incident Forensics Processor(appliance type 6000) on another appliance. After the installation, you deploy the QRadar Incident Forensics Processor as a managed host.

Installing QRadar Console

For distributed installations, install the QRadar Console on an appliance and the IBM QRadar Incident Forensics managed host on another appliance.

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

Before you begin

Ensure that the following requirements are met:

- The required hardware is installed.
- You have the required license key for your appliance.
- A keyboard and monitor are connected by using the VGA connection.
- If you want to configure bonded network interfaces, see the topic titled *Configuring bonded management interfaces* in the *IBM QRadar Installation Guide*.

Procedure

1. For installations on your own hardware or on virtual machines, add the QRadar Console ISO image in the root directory.

    a) Create the `/media/dvd` directory by typing the following command:

        mkdir /media/dvd

    b) Mount the QRadar Console ISO image by typing the following command:

        mount -o loop <QRadar_ISO> /media/dvd

2. Use the setup script to start the installation.

    a) Change the working directory by typing the command:

        cd /media/dvd

    b) Start the setup script by typing the command:

        setup.sh

3. Follow the instructions in the installation wizard.

    - In the **Enter your activation key below**, when you are prompted for the activation key, enter the 24-digit, 4-part, alphanumeric string that you received from IBM.

      The letter I and the number 1 (one) are treated the same. The letter O and the number 0 (zero) are also treated the same.

    - In the **Enter the network information to use** page, if you do not have an email server, enter `localhost` in the **Email server name** field.

    - In the **Root password field**, create a password that meets the following criteria:

       – Contains at least 5 characters.

       – Contains no spaces.

       – Can include the following special characters: @, #, ^, and *.

    The installation process might take several minutes.

4. If you are installing a Console, apply your license key.

    a) Log in to QRadar as the `admin` user:

       `https://<IP_Address_QRadar>`

    b) Click **Login**.

    c) On the navigation menu (☰), click **Admin**.

    d) In the navigation pane, click **System Configuration**.

    e) Click the **System and License Management** icon.

    f) From the **Display** list box, select **Licenses**, and upload your license key.

    g) Select the unallocated license and click **Allocate System to License**.

    h) From the list of systems, select a system, and click **Allocate System to License**.

What to do next

You can now install QRadar Incident Forensics.

Installing QRadar Incident Forensics

Follow these steps to install an IBM QRadar Incident Forensics managed host in your QRadar environment.

For stand-alone deployments, install only the QRadar Incident Forensics Standalone component.

For distributed installations, install the QRadar Console on an appliance and install the IBM QRadar Incident Forensics managed host on another appliance.

Before you begin

Ensure that the following requirements are met:

__ • The required hardware is installed.

__ • A keyboard and monitor are connected using the VGA connection.

__ • The activation key and all required license keys are available.

    For more information, see "Activation keys and license keys" on page 7.

__ • All appliances in the deployment have the same QRadar software version and fix level.

    Deployments that use different versions of QRadar software are not supported.

Restriction: The following limitations apply to the deployment:

• Resizing logical volumes by using a logical volume manager (LVM) is not supported.

• In a high-availability (HA) deployment, you can install multiple QRadar Incident Forensics appliances, but you cannot configure the appliances as an HA cluster. Creating an HA cluster by using appliance type 6000 and type 500 is not supported.

Procedure

1. For installations on your own hardware, add the QRadar Incident Forensics ISO image in the root directory.

    a) Create the `/media/dvd` directory by typing the following command:

```
mkdir /media/dvd
```

    b) Mount the QRadar Console ISO image by typing the following command:

```
mount -o loop <QRadar_Incident_Forensics_ISO>/media/dvd
```

2. Use the setup script to start the installation.

    a) Change the working directory by typing the command:

```
cd /media/dvd
```

    b) Start the setup script by typing the command:

```
setup.sh
```

3. Follow the instructions in the installation wizard.

On the **Select the Appliance ID** page, choose the QRadar Incident Forensics component to install.

For stand-alone deployments, select **6100 QRadar Incident Forensics Standalone**.

Restriction: The following configuration options are not supported for QRadar Incident Forensics:

- On the **Choose the type of setup** page, the **HA Recovery Setup** option is not supported.
- On the **Select if you want to use bonded interface configuration mode** page, the **Use bonded interface configuration mode** option is not supported.

If you install the QRadar Incident Forensics Processor, the installation process might take several minutes.

4. Apply your license key.

    a) Log in to QRadar:

```
https://IP_Address_QRadar
```

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

    b) Click **Login**.

    c) On the navigation menu (☰), click **Admin**.

    d) Click **System Configuration**.

    e) Click the **System and License Management** icon.

    f) From the **Display** list box, select **Licenses**, and upload you license key.

    g) Select the unallocated license and click **Allocate System to License**.

    h) From the list of licenses, select the appropriate license, and click **Allocate License to System**.

What to do next

Deploy the QRadar Incident Forensics managed host. For more information, see "Adding a QRadar Incident Forensics managed host to QRadar Console" on page 15.

Adding a QRadar Incident Forensics managed host to QRadar Console

For distributed installations, you must add IBM QRadar Incident Forensics Processor as a managed host to the QRadar Console.

A *managed host* is every non-console QRadar appliance in the deployment. To distribute processing, you can add more than one QRadar Incident Forensics Processor as a managed host.

Before you begin

You must install the QRadar Console software first. For more information, see "Installing QRadar Console " on page 13.

Procedure

1. Log in to QRadar Console as an administrator:

   `https://IP_Address_QRadar`

   The default user name is `admin`. The password is the password of the root user account that was entered during the installation.

2. On the navigation menu (☰), click **Admin**.
3. In the **System Configuration** pane, click **System and License Management**.
4. From the host table, click the QRadar Console host, and click > **Deployment Actions** > **Add Host**.
5. Enter the information for the QRadar Incident Forensics Processor appliance and then click **Add**.

   Restriction: Network Address Translation properties are not supported.
6. From the **Admin** tab menu bar, click **Deploy Changes**.
7. Refresh your web browser.

   The **Forensics** tab is now visible.

What to do next

You can add an QRadar Network Packet Capture device to the QRadar Incident Forensics Processor. For more information, see "Adding packet capture devices to QRadar Incident Forensics hosts" on page 18.

Removing a QRadar Incident Forensics managed host

To change network configuration settings or if there is an issue with seeing the **Forensics** tab, you can remove the QRadar Incident Forensics managed host (IBM QRadar Incident Forensics Processor) from the QRadar deployment.

If the QRadar Incident Forensics managed host was responsible for forensics recoveries, the data is lost when you re-add the QRadar Incident Forensics Processor.

If you don't remove the QRadar Incident Forensics managed host, but instead it becomes temporarily unresponsive because of power failure or other issue, jobs for the managed host are still scheduled and are processed when the managed host comes back online.

Procedure

1. Log in to QRadar Console as an administrator:

   `https://IP_Address_QRadar`

   The default user name is `admin`. The password is the password of the root user account that was entered during the installation.

2. On the navigation menu (☰), click **Admin**.
3. In the **System Configuration** pane, click **System and License Management**.
4. From the host table, click the QRadar Incident Forensics Processor host that you want to remove, and click > **Deployment Actions** > **Remove Host**.
5. From the **Admin** tab menu bar, click **Deploy Changes**.
6. Refresh your web browser.

Chapter 5. Packet capture connections

To retrieve packet capture data, you must connect one or more packet capture devices to an IBM QRadar Incident Forensics managed host or QRadar Incident Forensics Standalone appliance. If no packet capture device is attached, you can manually upload the packet capture files in the user interface or by using FTP.

IBM QRadar Network Packet Capture connections

If you are using IBM QRadar Network Packet Capture to capture packet data, you can extend the storage by connecting multiple appliances together in a ring topology to create a stack.

The stack allows the distribution of capture data across each of the connected appliances. It can connect up to 16 devices, but appears and behaves like a single entity that captures data from one TAP of a single 10GB port.

The *Stack Controller* is the appliance that receives the traffic that is being monitored, also known as the TAP point. The Stack Controller manages the overall configuration for the stack, therefore, there can be only one controller in each stack. The *Stack Node* is the appliance that is used as storage for the capture data. You can have up to 15 nodes in a stack.

QRadar Network Packet Capture (stacked configuration)
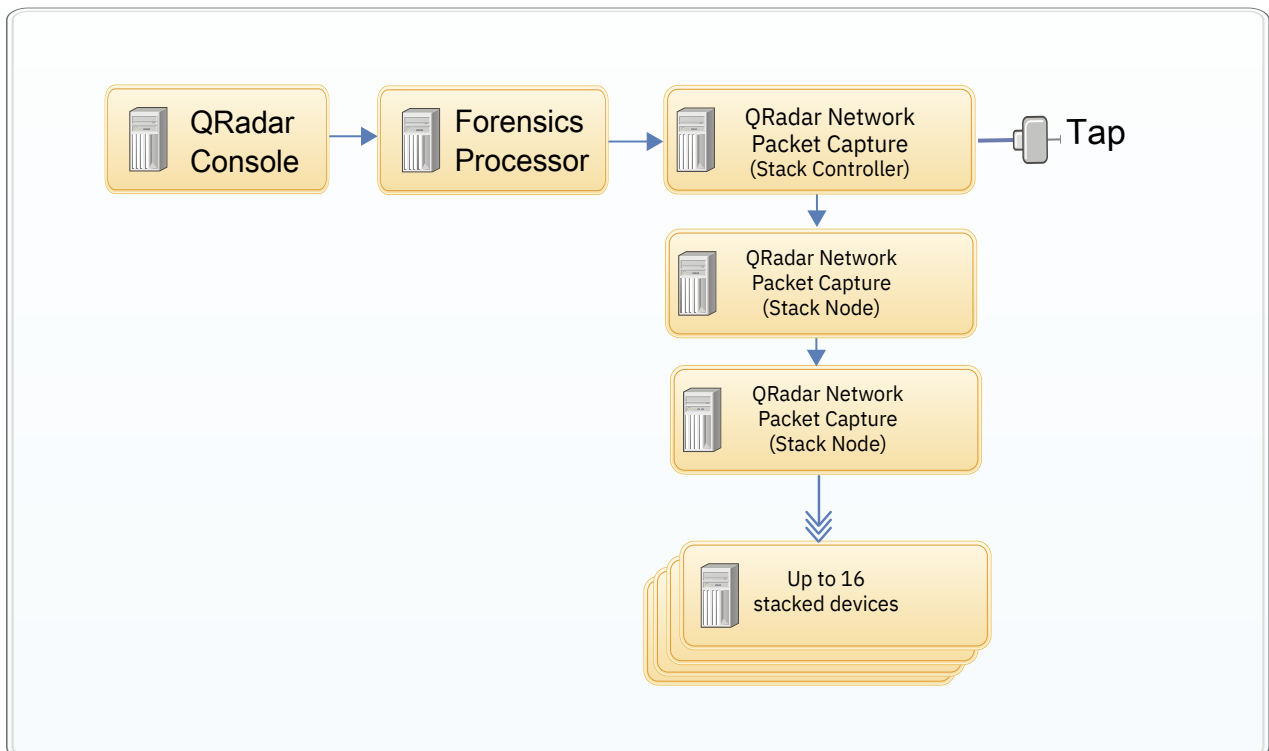
When you configure the stack in QRadar, add only the IP address for the stack controller. Do not add the IP addresses for each of the stack nodes.

Adding packet capture devices to QRadar Incident Forensics hosts

Packet capture devices process captured packet data for forensics recoveries. You can connect packet capture devices to an IBM QRadar Incident Forensics managed host or IBM QRadar Incident Forensics Standalone host.

If no packet capture device is attached, you can manually upload the packet capture files in the user interface or by using FTP.

Before you begin

You must have QRadar Incident Forensics installed.

- For distributed installations, install the QRadar Console on one appliance and QRadar Incident Forensics Processor on another appliance.
- For stand-alone deployments, install only the QRadar Incident Forensics Standalone component.

For more information, see "Installing QRadar Incident Forensics " on page 14.

Procedure

1. Log in to QRadar Console as an administrator:

   `https://IP_Address_QRadar`

   The default user name is `admin`. The password is the password of the root user account that was entered during the QRadar installation.

2. On the navigation menu (☰), click **Admin**.
3. In the **System Configuration** pane, click **System and License Management**.
4. From the host table, select the QRadar Incident Forensics appliance.

   In a distributed deployment, the QRadar Incident Forensics Processor has **Appliance Type** 6000.

   In a stand-alone deployment, the QRadar Incident Forensics Standalone host has **Appliance Type** 6100.

5. Click **Deployment Actions** > **Edit Host**.
6. Click **Component Management**.
7. To add packet capture devices, click the add icon (+) and enter the information about the device.

   For stacked configurations in QRadar Network Packet Capture, add only the Stack Controller. Don't add the IP addresses for each Stack Node.

8. Click **Save**.
9. To deploy changes from the current session, go to the **Admin** tab, and select **Advanced** > **Deploy Changes**.

   Alternatively, you can deploy all configuration changes that were made since the last deployment.

   Go to the **Admin** tab, and select **Advanced** > **Deploy Full Configuration**.

Chapter 6. QRadar Incident Forensics software installations on your own appliance

To ensure a successful installation of IBM QRadar Incident Forensics on your own appliance, you must install the Red Hat Enterprise Linux operating system, the QRadar Console, and QRadar Incident Forensics managed host.

For new software installations that integrate QRadar Incident Forensics with IBM QRadar, you install two ISO files:

- QRadar ISO image

  A single ISO is used to install every QRadar product except for QRadar Incident Forensics and IBM QRadar Network Insights. The activation key that you enter determines the QRadar appliance type that is installed.

- QRadar Incident Forensics ISO image

  This ISO image contains the QRadar Incident Forensics Processor and the QRadar Incident Forensics Standalone. You must install the QRadar Incident Forensics Processor.

Prerequisites for installing QRadar Incident Forensics on your own appliance

Before you install the Red Hat Enterprise Linux (RHEL) operating system on your own appliance, ensure that your system meets the system requirements.

The following table describes the system requirements:

Table 6. System requirements for RHEL installations on your own appliance

Requirement	Details
Supported software version	The RHEL version is dependent on the QRadar version that you are installing. View the supported RHEL versions here.
Bit version	64-bit
Kickstart disks	Not supported
Memory (RAM) for Forensics processor	Minimum 128 GB You must upgrade your system memory before you install QRadar.
Free disk space for Forensics processor	Minimum 5% of total disk space For optimal performance, ensure that an extra 2-3 times of the minimum disk space is available.
Firewall configuration	WWW (http, https) enabled SSH enabled Before you configure the firewall, disable the SELinux option. The QRadar installation includes a default firewall template that you can update in the **System Setup** window.

Restriction: Resizing logical volumes by using a logical volume manager (LVM) is not supported.

Linux operating system partition properties for QRadar installations on your own system

If you use your own appliance hardware, you can delete and re-create partitions on your Red Hat Enterprise Linux operating system rather than modify the default partitions.

Use the values in following table as a guide when you re-create the partitioning on your Red Hat Enterprise Linux operating system. You must use these partition names. Using other partition names can cause the installation to fail and other issues.

The file system for each partition is XFS.

Table 7. Partitioning guide for RHEL		
Mount Path	**LVM supported?**	**Size**
`/boot`	No	1 GB
`/boot/efi`	No	200 MB
`/var`	Yes	5 GB
`/var/log`	Yes	15 GB
`/var/log/audit`	Yes	3 GB
`/opt`	Yes	13 GB
`/home`	Yes	1 GB
`/storetmp`	Yes	15 GB
`/tmp`	Yes	3 GB
`swap`	N/A	Swap formula: Configure the swap partition size to be 75 per cent of RAM, with a minimum value of 12 GiB and a maximum value of 24 GiB.
`/`	Yes	Up to 15 GB
`/store`	Yes	80% of remaining space
`/transient`	Yes	20% of remaining space

For more information about the swap partition, see https://www.ibm.com/support/pages/node/6348712 (https://www.ibm.com/support/pages/node/6348712).

Console partition configurations for multiple disk deployments

For systems with multiple disks, configure the following partitions for QRadar:

Disk 1
    boot, swap, OS, QRadar temporary files, and log files

Remaining disks

- Use the default storage configurations for QRadar appliances as a guideline to determine what RAID type to use.
- Mounted as `/store`
- Store QRadar data

The following table shows the default storage configuration for QRadar appliances.

Table 8. Default storage configurations for QRadar appliances

QRadar host role	Storage configuration
Flow collector QRadar Network Insights (QNI)	RAID1
Data node Event processor Flow processor Event and flow processor All-in-one console	RAID6
Event collector	RAID10

Installing RHEL on your own appliance

You can install the Red Hat Enterprise Linux operating system on your own appliance for use with QRadar Incident Forensics.

For information about which Red Hat Enterprise Linux versions are supported, see "Prerequisite hardware and software" on page 8.

Procedure

1. Copy the Red Hat Enterprise Linux operating system DVD ISO to one of the following portable storage devices:

    - Digital Versatile Disk (DVD)
    - Bootable USB flash drive

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

2. Insert the portable storage device into your appliance and restart your appliance.
3. From the starting menu, select one of the following options.

    - Select the USB or DVD 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. To prevent an issue with Ethernet interface address naming, on the **Welcome** page, press the Tab key and at the end of the `Vmlinuz initrd=initrd.image` line add `biosdevname=0`.
6. Follow the instructions in the installation wizard to complete the installation:

    a) Select the **Basic Storage Devices** option.
    b) When you configure the host name, the **Hostname** property can include letters, numbers, and hyphens.
    c) When you configure the network, in the **Network Connections** window, select **System eth0** and then click **Edit** and select **Connect automatically**.
    d) On the **IPv4 Settings** tab, from the **Method** list, select **Manual**.
    e) In the **DNS servers** field, type a comma-separated list.
    f) Select **Create Custom Layout** option.
    g) Configure EXT4 for the file system type for the `/boot` partition.

h) Reformat the swap partition with a file system type of swap.

i) Select **Basic Server**.

7. When the installation is complete, click **Reboot**.

8. Ensure that your onboard network interfaces are named `eth0`, `eth1`, `eth2`, and `eth3`.

What to do next

"Installing QRadar Console " on page 13

Chapter 7. Virtual appliance installations for QRadar Incident Forensics

You can install IBM QRadar Incident Forensics on a virtual appliance. Ensure that you use a supported virtual appliance that meets the minimum system requirements.

A virtual appliance is a QRadar Incident Forensics system that consists of QRadar Incident Forensics software that is installed on a VMWare ESXi virtual machine.

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

Installation process

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

__ • Create a virtual machine.

__ • Install IBM QRadar Incident Forensics software on the virtual machine.

__ • If you installed QRadar Incident Forensics Processor, add your virtual appliance to the deployment.

System requirements for virtual appliances

Before you install your virtual appliance, ensure that the following minimum requirements are met:

Table 9. Requirements for virtual appliances

Requirement	Description
VMware client	VMware ESXi Version 5.0 VMware ESXi Version 5.1 VMware ESXi Version 5.5 For more information about VMWare clients, see the VMware website (www.vmware.com)
Virtual disk size	Minimum: 256 GB **Important:** For optimal performance, ensure that an extra 2-3 times the minimum disk space is available.

Creating your virtual machine

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

Procedure

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 the Red Hat Enterprise Linux version.

d) On the **CPUs** page, configure the number of virtual processors that you want for the virtual machine. Select 40 or more.

e) In the **Memory Size** field, type or select the RAM required for your deployment. Select 128 GB or more.

f) Use the following table to configure you network connections.

Table 10. Descriptions for network configuration parameters

Parameter	Description
How many NICs do you want to connect	You must add at least one Network Interface Controller (NIC)
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 11. Settings for the virtual disk size and provisioning policy parameters

Property	Option
Capacity	2 or higher (TB)
Disk Provisioning	Thin provision
Advanced options	Do not configure

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

What to do next

Install the QRadar software on your virtual machine.

Installing the QRadar Incident Forensics software on a virtual machine

After you create your virtual machine, you must install the IBM QRadar software on the virtual machine.

Restriction: Resizing logical volumes by using a logical volume manager (LVM) is not supported.

Procedure

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

   The user name is case-sensitive.
10. Ensure that the **End User License Agreement** (EULA) is displayed.

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

11. On the **Select the Appliance ID** page, choose the QRadar Incident Forensics component to install.

- For distributed installation, select **6000 QRadar Incident Forensics Processor**.
- For stand-alone deployments, select **6100 QRadar Incident Forensics Standalone**.

12. For the type of setup, select **normal**.
13. Follow the instructions in the installation wizard to complete the installation.

The following table contains descriptions and notes to help you configure the installation.

Table 12. Description of network settings

Network Setting	Description
Host name	Fully qualified domain name
Secondary DNS server address	Optional
Public IP address for networks that use Network Address Translation (NAT)	Not supported
Email server name	If you do not have an email server, use `localhost`.
Root password	The password must meet the following criteria: • Contain at least 5 characters • Contain no spaces • Can include the following special characters: @, #, ^, and *.

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

What to do next

If you aren't installing IBM QRadar Incident Forensics Standalone, see "Adding a QRadar Incident Forensics managed host to QRadar Console" on page 15.

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.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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.

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

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

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

IBM Online Privacy Statement

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

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

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

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details/ the section entitled "Cookies, Web Beacons and Other Technologies".

General Data Protection Regulation

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

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