IBM Security QRadar Incident Forensics
Version 7.2.6

Installation Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 33.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to installing IBM Security QRadar Incident Forensics

Information about installing IBM® Security QRadar® Incident Forensics and integrating the product with IBM Security 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 Security 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 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.

Note

IBM Security QRadar Incident Forensics is designed to help companies improve their security environment and data. More specifically, IBM Security 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 Security 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 Security QRadar Incident Forensics.

Chapter 1. Upgrading QRadar Incident Forensics

You must upgrade all of your IBM Security QRadar products in your deployment to the same version. You upgrade IBM Security QRadar Incident Forensics V7.2.5 to V7.2.6 by using an upgrade installer. During the upgrade, the version of RedHat Enterprise Linux is upgraded to version 6.7.

If you want to upgrade from QRadar Incident Forensics V7.2.4 or earlier versions and want to keep your data, contact your IBM sales representative. Otherwise, if you want to upgrade from QRadar Incident Forensics V7.2.4 or earlier versions, but don't want to keep your data, you upgrade directly to V7.2.6 by doing a new installation.

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

Procedure

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

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

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

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

   The first time that you run the patch installer script, there might be a delay before the first patch installer menu is displayed.
8. Provide answers to the pre-installation questions based on your deployment.
9. 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.
10. 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 Security QRadar Packet Capture Quick Reference Guide*.

Chapter 2. 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 Security QRadar Incident Forensics components on one appliance (*all-in-one*) or on multiple appliances.

Installation options

Depending on the components that you install, not all of the security capabilities are available. For example, if you install QRadar Incident Forensics on one appliance, only network forensics is available. However, if you install a QRadar Incident Forensics managed host, more security capabilities are available. For most installations, you install the QRadar Console, at least one QRadar Incident Forensics Processor, and one or more QRadar Packet Capture appliances.

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

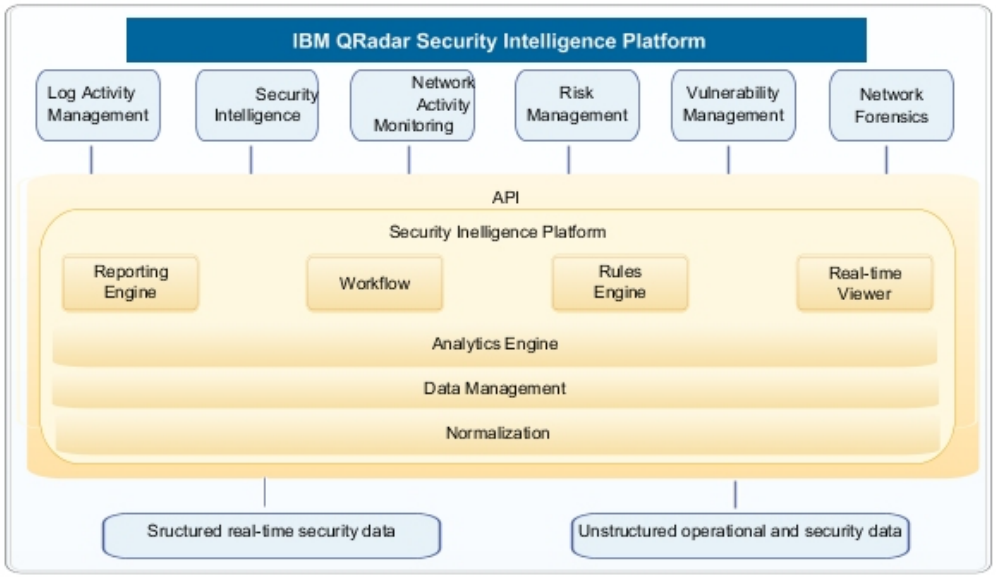


Figure 1. QRadar security intelligence architectural overview

All-in-one deployments

In stand-alone or all-in-one deployments, you install the IBM Security QRadar Incident Forensics Standalone software. These single appliance deployments are similar to installing the QRadar Console and QRadar Incident Forensics managed host on one appliance, but without log management, network activity monitoring, or other security intelligence features. For a stand-alone network forensics solution, install the QRadar Incident Forensics Standalone in small to midsize deployments.

As shown in the following diagram, you can attach QRadar Packet Capture appliances to the IBM Security QRadar Incident Forensics Standalone.

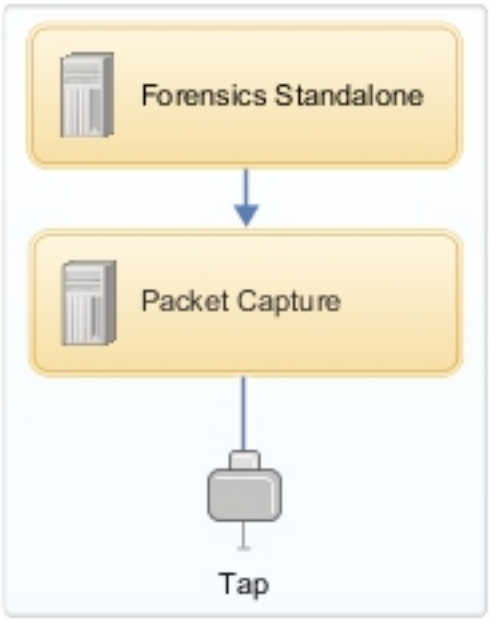


Figure 2. IBM Security QRadar Incident Forensics Standalone deployment example

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

Distributed deployments

In deployments where you need both network forensics analysis and other security intelligence capabilities, or when you need to distribute the workload for forensics recoveries, you install the QRadar Console and one or more QRadar Incident Forensics managed hosts. The QRadar Console provides information and event management (SIEM), log management, anomaly detection, risk management, and vulnerability management.

In a distributed deployment, there are three appliances:

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

Software versions for all IBM Security 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 Packet Capture devices to the QRadar Incident Forensics managed hosts (QRadar Incident Forensics Processor).

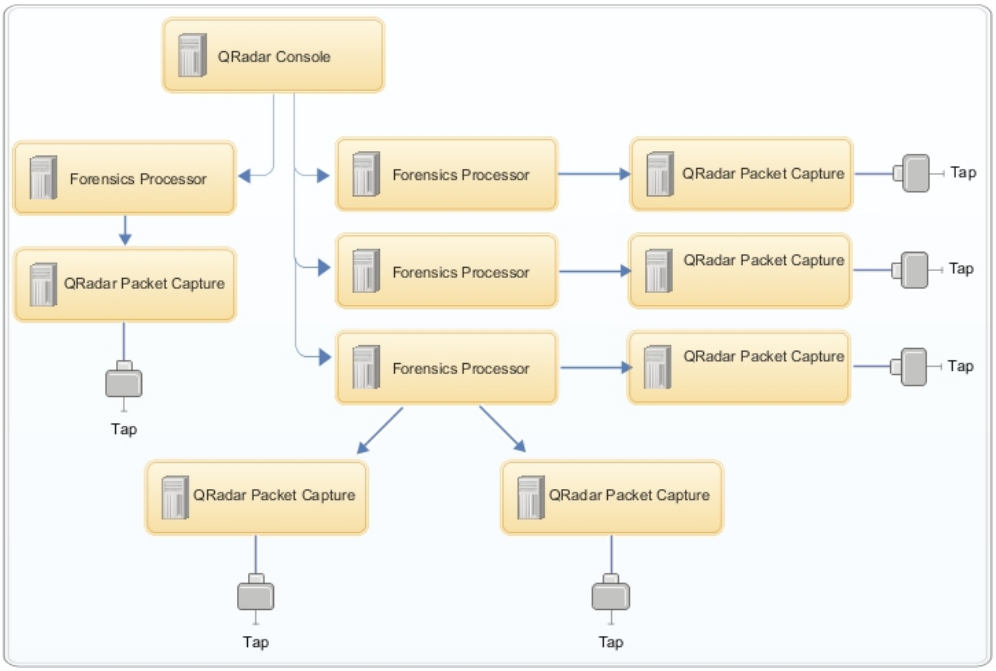


Figure 3. Distributed deployment example

QRadar Incident Forensics components

QRadar deployments can include the following components:

QRadar Console

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

In distributed deployments, use the QRadar Console to manage multiple QRadar Incident Forensics Processor hosts.

QRadar Incident Forensics Processor

Provides the QRadar Incident Forensics product 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 add QRadar Incident Forensics Processor as a managed host before you can use the security intelligence forensics capability.

QRadar Incident Forensics Standalone

Provides the QRadar Incident Forensics product user interface. Installing QRadar Incident Forensics Standalone provides the tools that you need to do forensics investigations. Only forensics investigative and the related administrative functions are available.

QRadar Packet Capture

You can install an optional QRadar Packet Capture appliance. If no other network packet capture (PCAP) device is deployed, you can use this appliance to store data that is used by QRadar Incident Forensics. 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.

Chapter 3. QRadar Incident Forensics installation overview

You install QRadar Incident Forensics software on your own appliance or on a virtual appliance. QRadar Incident Forensics appliances have the QRadar Incident Forensics software installed

QRadar Incident Forensics must be installed on a Red Hat Enterprise Linux operating system.

Appliance ID selection

For most QRadar Incident Forensics, you install at least two ISO images:

- QRadar Console

  QRadar products use the same installation software image. The *activation key* determines the appliance type and the components to install. When you enter in the activation key, you are prompted to identify the appliance type. You must install QRadar Console
- 6000 QRadar Incident Forensics Processor (manged host)

  Due to export controls, QRadar Incident Forensics components are installed from a different ISO image. You must install the QRadar Incident Forensics managed host and configure it to connect to the QRadar Console

For all-in-one installations, you install only the 6100 QRadar Incident Forensics ISO image and select the QRadar Incident Forensics Standalone component.

When you install QRadar Incident Forensics, a default license key provides you with access for five weeks. Before the default license expires, you must allocate a license key to your system.

Installation steps

For distributed installations, use these steps to guide you through the installation process.

1. Review the hardware and software requirements.
2. Install the QRadar Console software.
3. Install the QRadar Incident Forensics managed host.
4. Deploy the QRadar Incident Forensics managed host.
5. Add packet capture devices.

Activation keys and license keys

When you install IBM Security 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 Security 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 key

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 default license expires.

Prerequisite hardware accessories and desktop software for QRadar installations

Before you install IBM Security 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

Supported web browsers

The following table lists the supported web browsers:

Table 1. Supported web browsers for QRadar products

Web browser	Supported versions
Mozilla Firefox	38.0 Extended Support Release
32-bit or 64-bit Microsoft Internet Explorer, with document mode or browser mode enabled.	10.0
64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled.	11.0
Google Chrome	Version 46

If you use Microsoft Internet Explorer, you must enable document mode and browser mode:

1. In your Internet Explorer web browser, press F12 to open the Developer Tools window.
2. Click **Browser Mode** and select the version of your web browser.
3. Click **Document Mode**.
   - For Internet Explorer V9.0, select **Internet Explorer 9 standards**.
   - For Internet Explorer V10.0, select **Internet Explorer 10 standards**.

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 2. Open ports between hosts

Port	Description
443	Required for artifact analysis.
28080	Required for distributed search

Chapter 4. QRadar Incident Forensics software installations on your own appliance

To ensure a successful installation of IBM Security 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 Security QRadar, you install two ISO files:

- QRadar

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

  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 3. System requirements for RHEL installations on your own appliance

Requirement	Details
Supported software version	Version 6.7
Bit version	64-bit
Kickstart disks	Not supported
Memory (RAM) for Forensics processor	Minimum 128 GB **Important:** You must upgrade your system memory before you install QRadar.
Free disk space for Forensics processor	Minimum 5% of total disk space **Important:** 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 **Important:** 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 appliance

If you use your own appliance, 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.

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

Table 4. Partition guide for RHEL

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
/boot	System boot files	/boot	EXT4	200 MB	Yes	SDA
swap	Used as memory when RAM is full.	empty	swap	Systems with 4 to 8 GB of RAM, the size of the swap partition must match the amount of RAM Systems with 8 to 24 GB of RAM, configure the swap partition size to be 75% of RAM, with a minimum value of 8 GB and a maximum value of 24 GB.	No	SDA
/	Installation area for QRadar, the operating system, and associated files.	/	EXT4	20000 MB	No	SDA
/store/tmp	Storage area for QRadar temporary files	/store/tmp	EXT4	20000 MB	No	SDA
/var/log	Storage area for QRadar and system log files	/var/log	EXT4	20000 MB	No	SDA

Table 4. Partition guide for RHEL (continued)

Partition	Description	Mount point	File system type	Size	Forced to be primary	SDA or SDB
/store	Storage area for QRadar data and configuration files	/store	XFS	[1]On Console appliances: approximately 80% of the available storage. On managed hosts other than QFlow Collectors and Store and Forward Event Collectors: approximately 90% of the available storage.	No	SDA If 2 disks, SDB
/store/transient	Storage area for ariel database cursor	/store/transient	XFS on Consoles EXT4 on managed hosts	[1]On Console appliances: 20% of the available storage. On managed hosts other than QFlow Collectors and Store and Forward Event Collectors: 10% of the available storage.	No	SDA If 2 disks, SDB
[1]The /store and /store/transient together take 100% of the disk space that remains after you create the first 5 partitions.						

Restrictions

Future software upgrades might fail if you reformat any of the following partitions or their sub-partitions:

- /store
- /store/tmp
- /store/ariel
- /store/transient

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.

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 Security 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

Chapter 7, “Installing QRadar Console,” on page 21

Chapter 5. QRadar Incident Forensics software installation on a QRadar Incident Forensics appliance

IBM Security QRadar Incident Forensics appliances are preinstalled with a Red Hat Enterprise Linux operating system and QRadar software.

For new software installations that integrate QRadar Incident Forensics with IBM Security QRadar , you configure the two preloaded ISO files:

- QRadar

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

- QRadar Incident Forensics

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

For new software installations where you need only forensics capabilities, install the QRadar Incident Forensics Standalone from the QRadar Incident Forensics ISO.

Chapter 6. Virtual appliance installations for QRadar Incident Forensics

You can install IBM Security 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 ESX 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 Security 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 5. 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 ESX 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 **Red Hat Enterprise Linux 6 (64-bit)**.
   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 6. 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 7. 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 Security 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 8. 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 Security QRadar Incident Forensics Standalone, see Chapter 9, “Adding a QRadar Incident Forensics managed host to QRadar Console,” on page 25.

Chapter 7. Installing QRadar Console

For distributed installations, install the QRadar Console on an appliance and the IBM Security 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.
- A keyboard and monitor are connected by using the VGA connection.
- The activation key is available.
- If you want to configure bonded network interfaces, see www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).

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. 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 To QRadar**.
c. Click the **Admin** tab.
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.

Chapter 8. Installing QRadar Incident Forensics

For distributed installations, install the QRadar Console on an appliance and the IBM Security QRadar Incident Forensics managed host (QRadar Incident Forensics Processor) on another appliance. For stand-alone deployments, install only the QRadar Incident Forensics Standalone component.

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.

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

__ • The activation key is available.

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

Procedure

1. For installations on your own hardware or on virtual machines, 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 distributed installation, select **6000 QRadar Incident Forensics Processor**
   - For stand-alone deployments, select **6100 QRadar Incident Forensics Standalone**

   Restriction: The following configuration choices are not supported for QRadar Incident Forensics:
   - On the Choose the type of setup page, the **HA Recovery Setup** option
   - On the Select if you want to use bonded interface configuration mode page, the **Use bonded interface configuration mode** option

   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 the login.

c. Click the **Admin** tab.

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 you license key.

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

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

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

For each distributed installation (6000) into an existing IBM Security QRadar SIEM environment, you may require a license for each Forensics managed host (6000) and a single license to enable the **Forensics** tab on the console. If your existing QRadar Console license key is allocated for access to the **Forensics** tab, you only need the install license key. If your existing QRadar Console license key is not allocated for access to the **Forensics** tab, you need the install license key as well as an updated Forensics enablement key.

What to do next

Deploy QRadar Incident Forensics Processor managed host. For more information, see Chapter 9, "Adding a QRadar Incident Forensics managed host to QRadar Console," on page 25.

Chapter 9. Adding a QRadar Incident Forensics managed host to QRadar Console

For distributed installations, you must add IBM Security 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.

Restriction: Using the Deployment Editor to add or remove QRadar Incident Forensics managed hosts is not supported. You must use the System and License Management tool.

Before you begin

You must install the QRadar Console software first. For more information, see Chapter 7, "Installing QRadar Console," on page 21.

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. Click the **Admin** tab.
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: The **Encrypt Host** and **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 IBM Security QRadar Packet Capture device to the QRadar Incident Forensics Processor. For more information, see "Adding packet capture devices to QRadar Incident Forensics hosts" on page 31.

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 Security 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.

Restriction: Using the Deployment Editor to add or remove QRadar Incident Forensics managed hosts is not supported. You must use the System and License Management tool.

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. Click the **Admin** tab.
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 10. Connections between packet capture devices and QRadar Incident Forensics

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

Packet capture master system

Depending on your network and packet capture requirements, you can connect up to five packet capture devices to a QRadar Incident Forensics appliance. When you submit a recovery, separate jobs are submitted for each packet capture device on each QRadar Incident Forensics appliance. For example, if you install two QRadar Incident Forensics managed hosts, and each has two packet capture, four jobs are submitted.

The following diagrams show that you can connect multiple packet capture devices to a QRadar Incident Forensics managed host (QRadar Incident Forensics Processor) or QRadar Incident Forensics Standalone appliances.

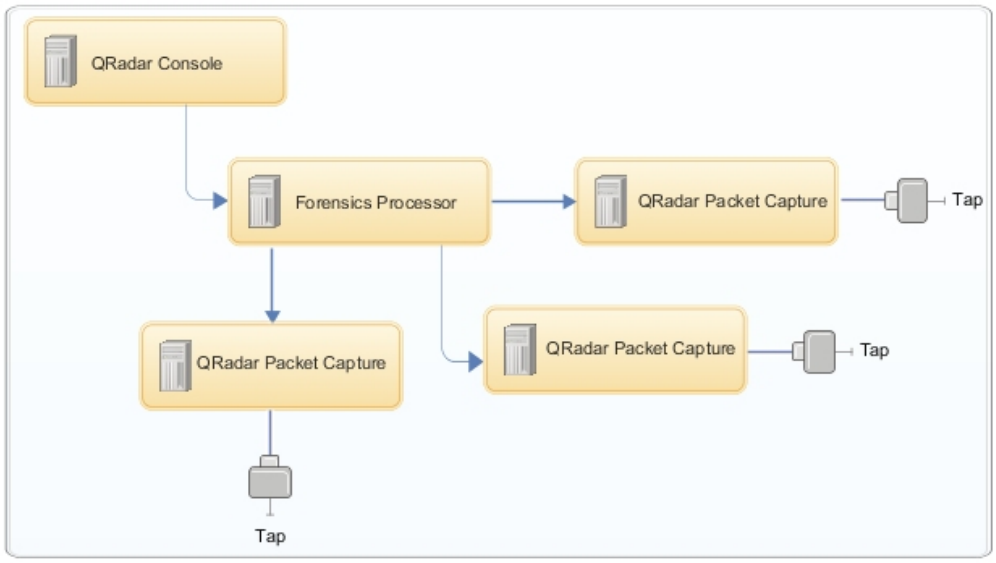


Figure 4. Example of multiple packet capture devices connected to a QRadar Incident Forensics managed host

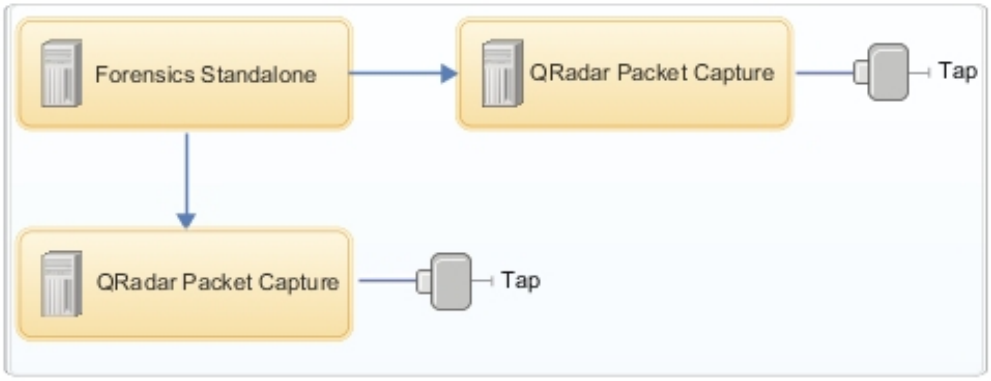
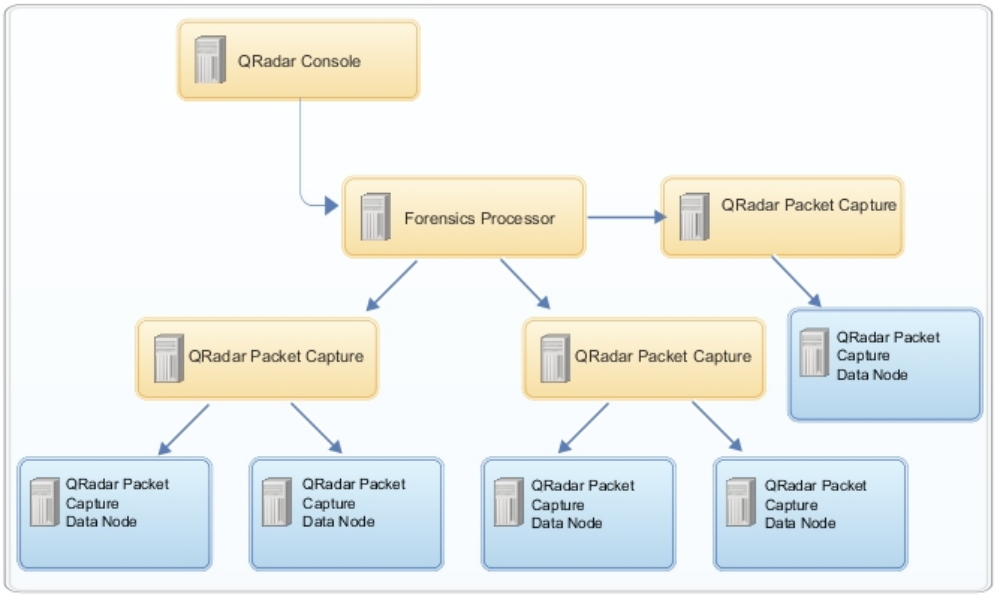


Figure 5. Example of multiple packet capture devices connected to a QRadar Incident Forensics Standalone host.

QRadar Packet Capture Data Node appliances

For extra storage capacity, you can connect up to two QRadar Packet Capture Data Node appliances to each QRadar Packet Capture master system. Each PCAP Data Node appliance provides 37 TB of extra storage.



After you connect the QRadar Packet Capture Data Node appliances to the master system, you can configure the cluster in the QRadar Packet Capture user interface.

For more information about the physical connections from the master appliance to the QRadar Packet Capture Data Node appliance, see the *QRadar Packet Capture Quick Reference Guide*. For more information about configuring the packet capture cluster, see the *QRadar Packet Capture User Guide*.

Installing QRadar Packet Capture software on your own appliance

To ensure a successful installation of IBM Security QRadar Packet Capture on your own appliance, you must install the Red Hat Enterprise Linux operating system and the QRadar Packet Capture software. You must also ensure that your appliance meets the system requirements.

Important: The system on which the QRadar Packet Capture software is installed must be dedicated to QRadar Packet Capture. Do not install RPM packages that are not approved by IBM. Unapproved RPM installations can cause dependency errors when you upgrade and can also cause performance issues in your deployment. Do not use YUM to update your operating system or install unapproved software on QRadar Packet Capture systems.

Restriction: Software installations on a virtual machine are not supported.

Before you begin

Ensure that your appliance meets the following system requirements:

Table 9. System requirements for a QRadar Packet Capture software installation

Specification	Description
Processors	Intel E5 series processors V2 or V3. V4 versions require 6 cores or more.
Processor BIOS settings	Must support the Intel AES and AVX standards introduced by Intel in 2011. Configure your BIOS system settings to ensure that Hyper threading is disabled.
Memory	24 GB
Hardware RAID controller and capture and extraction store	RAID configuration (using a combination of RAID 0, 1 or 5) across a minimum 4 hard disk drives, where each hard disk drive is at least 7200 RPM performance and a minimum 1 TB per drive
Operating system drive	500 GB minimum 7200 RPM enterprise class hard disk drive SATA or SAS
Operating system	Red Hat Enterprise Linux V6.7 **Note:** 1G SFS installer should be installed on the system where the 1G PCAP is installed as a dedicated PCAP appliance. It should not be used for any purpose other than packet capture.
Minimum total disk space	4 TB
Quad Port Server Adapter	Intel E1G44ET2BLK quad port Ethernet PCI Express adaptor http://ark.intel.com/products/49187/Intel-Gigabit-ET2-Quad-Port-Server-Adapter supporting 1 capture port Intel 82576 Gigabit Ethernet Controller http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller

Table 9. System requirements for a QRadar Packet Capture software installation (continued)

Specification	Description
PCAP UI network interface	Any 1G or (optionally 10G) network interface, for example, eth0.

Before you install QRadar Packet Capture software on your own appliance, we suggest that you set up and configure three separate virtual drives. These virtual drives are for the OS, extraction and storage. The storage drive should be the largest of the three, and a minimum requirement for this is 4000 GB.

See the following example:

Table 10. Example of RAID configuration for a QRadar Packet Capture software installation

Virtual Drive	RAID Level	Size
0	RAID 1	128 GB
1	RAID 1	3587 GB
2	RAID 5	33527 GB

Procedure

1. Insert the Red Hat Enterprise Linux operating system disk into your appliance and restart your appliance.
2. 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. On the **IPv4 Settings** tab, from the **Method** list, select **Manual**.
   d. On the Which type of installation would you like page, select **Use All Space** and then select the smallest partition (boot partition) for the operating system to be installed on.
   e. Select only **Base System** option to install.
3. When the installation is complete, click **Reboot**.
4. Copy the QRadar Packet Capture SFS file to your appliance.
5. Mount the QRadar Packet Capture SFS file.
   a. Create the `/tmp/qpc_install` directory by typing the following command:
      ```
      mkdir -p /tmp/qpc_install
      ```
   b. Mount the QRadar Packet Capture SFS file by typing the following command:
      ```
      mount -o loop -t squashfs <QRadar_Packet_Capture_file.sfs>
      /tmp/qpc_install
      ```
   c. Go to the `/tmp/qpc_install` directory.
      ```
      cd /tmp/qpc_install
      ```
6. To run the installation script, type the following command:
   ```
   sh installer.sh
   ```
7. At the `Capture port number` prompt, type the appropriate response. The default capture port number is `0`.
8. Confirm your response by typing uppercase letters: `Y` or `N`. This is case sensitive, and the patch might not progress if a lowercase letter is used.

9. Type the RAID device name (not the OS drive) when prompted. For example, /dev/sdc.
10. Confirm the entry displayed is correct by typing uppercase letters: Y or N. This is case sensitive, and the patch might not progress if a lowercase letter is used.

Adding packet capture devices to QRadar Incident Forensics hosts

To provide investigators access to packet capture information, you can connect up to five packet capture devices to an IBM Security QRadar Incident Forensics managed host or IBM Security QRadar Incident Forensics Standalone host. The attached package capture devices process the captured files for forensics recoveries.

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

Restriction: Using the Deployment Editor to add packet capture devices is not supported. You must use the System and License Management tool.

Before you begin

You must install and deploy a QRadar Incident Forensics manged host or install a QRadar Incident Forensics Standalone host. For more information, see Chapter 8, “Installing QRadar Incident Forensics,” on page 23 and Chapter 9, “Adding a QRadar Incident Forensics managed host to QRadar Console,” on page 25.

The following interactive diagram shows the main steps in the installation process for distributed installations. The installation process is the same for stand-alone deployments, but you don't deploy a managed host.

By default, the time zone for QRadar Packet Capture device is set to UTC (Coordinated Universal Time).

Important: If you change the default time zone on the QRadar Packet Capture device, the rest of the QRadar environment might not function properly.

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. Click the **Admin** tab.
3. In the **System Configuration** pane, click **System and License Management**.
4. From the host table, select the QRadar Incident Forensics Processor (**Appliance Type** 6000) or the QRadar Incident Forensics Standalone host (**Appliance Type** 6100) and click **Deployment Actions** > **Edit Managed Host**
5. Click **Component Management**.
6. To add packet capture devices, click the add icon (+) and enter the information about the device.

   Tip: The default user name for the QRadar Packet Capture device is continuum.
7. Click **Save**.

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All 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 the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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.

The following terms are trademarks or registered trademarks of other companies:

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.

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

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

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

Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

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.

Printed in USA