IBM Security QRadar Risk Manager
Version 7.2.6

Installation Guide

Note
Before using this information and the product that it supports, read the information in "Notices" on page 29.

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This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.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

This information is intended for use with IBM® Security QRadar® Risk Manager. QRadar Risk Manager is an appliance that is used to monitor device configurations, simulate changes to your network environment, and prioritize risks and vulnerabilities in your network.

This guide contains instructions for installing QRadar Risk Manager and adding QRadar Risk Manager as a managed host on an IBM Security QRadar SIEM Console.

QRadar Risk Manager appliances are preinstalled with software and a Red Hat Enterprise Linux operating system. You can also install QRadar Risk Manager software on your own hardware.

Intended audience

This guide is intended for network administrators that are responsible for installing and configuring QRadar Risk Manager systems in your network.

Administrators need a working knowledge of networking and Linux 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.

Chapter 1. Prepare to install IBM Security QRadar Risk Manager

You install an IBM Security QRadar Risk Manager appliance as a managed host on your IBM Security QRadar SIEM Console. Only one QRadar Risk Manager can exist on a QRadar Console.

QRadar Console and QRadar Risk Manager use the same installation process and ISO image. After you install the QRadar Console and QRadar Risk Manager, you add QRadar Risk Manager as a managed host by using the **System and License Management** tool on the **Admin** tab. A QRadar Risk Manager appliance is preinstalled with the QRadar Risk Manager software and a Red Hat Enterprise Linux operating system.

Chapter 2. Before you install

You must complete the installation process for an IBM Security QRadar SIEM Console before you install IBM Security QRadar Risk Manager. It is a good practice to install QRadar SIEM and QRadar Risk Manager on the same network switch.

For information about installing QRadar SIEM, including hardware and software requirements, see *IBM Security QRadar SIEM Administration Guide*.

Since QRadar Risk Manager is a 64-bit appliance, make sure that you download the correct installation software for your operating system.

Identify network settings

You must gather information about your network settings before starting the installation process.

Gather the following information for your network settings:

- Host name
- IP address
- Network mask address
- Subnet mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server (optional) address
- Public IP address for networks that use Network Address Translation (NAT) email server name
- Email server name
- Network Time Protocol (NTP) server (Console only) or time server name

Configure port access on firewalls

Firewalls between the IBM Security QRadar SIEM Console and IBM Security QRadar Risk Manager must allow traffic on certain ports.

Ensure that any firewall located between the QRadar SIEM Console and QRadar Risk Manager allows traffic on the following ports:

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Time)

Unsupported features in IBM Security QRadar Risk Manager

It is important to be aware of the features that are not supported by QRadar Risk Manager.

The following features are not supported in QRadar Risk Manager:

- High availability (HA)

- Dynamic Routing for Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP)
- IPv6
- Non-contiguous network masks
- Load-balanced routes
- Reference maps
- Store and Forward

Chapter 3. Additional hardware requirements

Additional hardware is required before you can install IBM Security QRadar Risk Manager.

Before you install QRadar Risk Manager systems, you need access to the following hardware components:

- Monitor and keyboard
- Uninterrupted Power Supply (UPS)

Protect your QRadar Risk Manager installations that store data by using an Uninterrupted Power Supply (UPS). Using a UPS ensures that your QRadar Risk Manager data, such as the data that is stored on consoles, event processors, and QRadar QFlow Collectors, is preserved during a power failure.

Chapter 4. Additional software requirements

Additional software is required before you can install IBM Security QRadar Risk Manager.

The following software must be installed on the desktop system that you use to access the QRadar Risk Manager user interface:

- Java™ Runtime Environment
- Adobe Flash, version 10 or higher

Chapter 5. Supported web browsers

For the features in IBM Security QRadar products to work properly, you must use a supported web browser.

When you access the QRadar system, you are prompted for a user name and a password. The user name and password must be configured in advance by the administrator.

The following table lists the supported versions of web browsers.

Table 1. Supported web browsers for QRadar products

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

Enabling document mode and browser mode in Internet Explorer

If you use Microsoft Internet Explorer to access IBM Security QRadar products, you must enable browser mode and document mode.

Procedure

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**, and select the **Internet Explorer standards** for your Internet Explorer release.

Chapter 6. Install IBM Security QRadar Risk Manager appliances

An IBM Security QRadar Risk Manager deployment includes an IBM Security QRadar SIEM Console and QRadar Risk Manager appliance as a managed host.

Installing QRadar Risk Manager involves the following steps:

1. Preparing your appliance.
2. Installing QRadar Risk Manager.
3. Adding QRadar Risk Manager to QRadar.

Preparing your appliance

You must prepare your appliance before you install an IBM Security QRadar Risk Manager appliance.

Before you begin

You must install all necessary hardware and you need an activation key. The activation key is a 24-digit, 4-part, alphanumeric string that you receive from IBM. You can find the activation key:

- Printed on a sticker that is placed on your appliance.
- Included with the packing slip, where all appliances are listed along with their associated keys.

To avoid typing errors, the letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

If you do not have an activation key for your QRadar Risk Manager appliance, contact Customer Support (www.ibm.com/support/).

For information about your appliance, see the *IBM Security QRadar Hardware Installation Guide*.

Procedure

1. Connect a keyboard and monitor to their respective ports.
2. Power on the system and log in. The user name, which is case-sensitive, is root.
3. Press **Enter**.
4. Read the information in the window. Press the Space bar to advance each window until you reach the end of the document.
5. Type `yes` to accept the agreement, and then press Enter.
6. Type your activation key, and then press Enter.

Access the IBM Security QRadar Risk Manager user interface

IBM Security QRadar Risk Manager uses default login information for the URL, user name, and password.

You access QRadar Risk Manager through the IBM Security QRadar SIEM Console. Use the information in the following table when you log in to your QRadar Console.

Table 2. Default login information for QRadar Risk Manager

Login information	Default
URL	`https://<IP address>`, where *<IP address>* is the IP address of the QRadar Console.
User name	admin
Password	The password that is assigned to QRadar Risk Manager during the installation process.
License key	A default license key provides access to the system for 5 weeks.

Network parameter information for IPv4

Network information for Internet Protocol version 4 (IPv4) network settings is required when you install IBM Security QRadar Risk Manager or when you change network settings.

Network information is required when you install or reinstall QRadar Risk Manager, or when you need to change network settings.

The Public IP network setting is optional. This secondary IP address is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured by using the Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network.

Installing IBM Security QRadar Risk Manager

You can install IBM Security QRadar Risk Manager after you prepare your appliance.

Before you begin

You must complete the preparation steps before you install QRadar Risk Manager.

Procedure

1. Select normal for the type of setup. Select **Next** and press Enter.
2. Select your time zone continent or area. Select **Next** and press Enter.
3. Select your time zone region. Select **Next** and press Enter.
4. Select an Internet Protocol version. Select **Next** and press Enter.
5. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
6. Type your host name, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server. For network parameter information, see "Network parameter information for IPv4."
7. Select **Next** and press Enter.
8. Type a password to configure the QRadar Risk Manager root password.
9. Select **Next** and press Enter.

10. Retype your new password to confirm. Select **Finish** and press Enter. This process typically takes several minutes.

Adding IBM Security QRadar Risk Manager to IBM Security QRadar SIEM Console

You must add IBM Security QRadar Risk Manager as a managed host to IBM Security QRadar SIEM Console.

Before you begin

If you want to enable compression, then the minimum version for each managed host must be QRadar Console V7.1 or QRadar Risk Manager V7.1.

To add a managed host that is not NATed to your deployment where the Console is NATed, you must change the QRadar Console to a NATed host. You must change the console before you add the managed host to your deployment. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

Procedure

1. Open your web browser.
2. Type the URL, `https://<IP Address>`, where *<IP Address>* is the IP address of the QRadar Console.
3. Type your user name and password.
4. Click the **Admin** tab.
5. In the System Configuration pane, click **System and License Management**.
6. In the System and License Management window, click **Deployment Actions**, and then select **Add Host**.
7. Click **Next**.
8. Enter values for the following parameters:

Option	Description
Host IP	The IP address of QRadar Risk Manager.
Host Password	The root password for the host.
Confirm Host Password	Confirmation for your password.
Encrypt Host Connections	Creates an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running QRadar Console V7.1 or QRadar Risk Manager V7.1.
Encryption Compression	Enables data compression between 2 managed hosts.
Network Address Translation	To enable NAT for a managed host, the NATed network must be using static NAT translation. For more information, see the *IBM Security QRadar SIEM Administration Guide*.

9. If you select the **Network Address Translation** check box, then you must enter values for the NAT parameters:

Option	Description
NAT Group	The network that you want this managed host to use. If the managed host is on the same subnet as the QRadar Console, select the console of the NATed network. If the managed host is not on the same subnet as the QRadar Console, select the managed host of the NATed network.
Public IP	The public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks that use NAT.

10. Click **Add**. This process can take several minutes to complete. If your deployment includes changes, then you must deploy all changes.
11. From the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

What to do next

Clear your web browser cache and then log in to QRadar Console. The **Risks** tab is now available.

Clearing web browser cache

You must clear the web browser cache before you can access the **Risks** tab in IBM Security QRadar SIEM Console.

Before you begin

Ensure that only one web browser is open. If you have multiple browsers open, the cache can fail to clear properly.

If you are using a Mozilla Firefox web browser, you must clear the cache in your Microsoft Internet Explorer web browser too.

Procedure

1. Open your web browser.
2. Clear your web browser cache. For instructions, see your web browser documentation.

Chapter 7. Risk Manager user role

You must assign the Risk Manager user role for users that require access to the **Risks** tab.

A user account defines the default password, and email address for a user. You need to assign a user role and security profile for each new user account.

Before you allow users in your organization to have access to IBM Security QRadar Risk Manager functions, you must assign the appropriate user role permissions. By default, QRadar Console provides a default administrative role, which provides access to all areas of QRadar Risk Manager.

For information about creating and managing user roles, see the *IBM Security QRadar SIEM Administration Guide*.

Assigning the Risk Manager user role

You can assign the Risk Manager user role to users that need access to the **Risk** tab.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. In the **User Management** pane, click the **User Roles** icon.
4. Click the **Edit** icon next to the user role you want to edit.
5. Select the **Risk Manager** check box.
6. Click **Next**. If you add Risk Manager to a user role that has Log Activity permission, then you must define the log sources that the user role can access. You can add an entire log source group by clicking the **Add** icon in the **Log Source Group** pane. You can select multiple log sources by holding the Ctrl key while you select each log source you want to add.
7. Click **Return**.
8. From the **Admin** tab menu, click **Deploy Changes**.

Chapter 8. Troubleshoot the Risks tab

You can troubleshoot if the **Risks** tab does not display properly or is inaccessible.

When the Risks tab is not displaying properly or is inaccessible, you remove and re-add IBM Security QRadar Risk Manager as a managed host.

Removing a managed host

You can remove your IBM Security QRadar Risk Manager managed host from IBM Security QRadar SIEM Console to change network settings or if there is a problem with the **Risks** tab.

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 Risk Manager 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 9. Re-adding IBM Security QRadar Risk Manager as a managed host

You can re-add IBM Security QRadar Risk Manager as a managed host after it is removed.

Procedure

1. On the **Admin** tab, click **System and License Management** > **Deployment Actions** > **Add Host**.
2. Enter the host IP address and password.
3. Click **Add**.

   You must wait several minutes while the managed host is added.
4. Close the System and License Management window.
5. On the **Admin** tab toolbar, click **Advanced** > **Deploy Full Configuration**.
6. Click **OK**.

Chapter 10. Reinstall IBM Security QRadar Risk Manager from the recovery partition

When you reinstall IBM Security QRadar Risk Manager from the IBM Security QRadar SIEMIBM Security QRadar SIEM Console ISO on the recovery partition, your system is restored back to factory default configuration. This means that your current configuration and data files are overwritten.

This information applies to new QRadar Risk Manager installations or upgrades from new QRadar Risk Manager on QRadar Risk Manager appliances. When you install QRadar Risk Manager, the installer (QRadar Console ISO) is copied into the recovery partition. From this partition, you can reinstall QRadar Risk Manager, which restores QRadar Risk Manager to factory defaults.

Note: If you upgrade your software after you install QRadar Risk Manager, then the ISO file is replaced with the newer version.

When you reboot your QRadar Risk Manager appliance, you are presented with the option to reinstall the software. Since QRadar Console and QRadar Risk Manager use the same ISO installation file, the QRadar Console ISO name displays.

If you do not respond to the prompt after 5 seconds, the system reboots as normal, which maintains your configuration and data files. If you choose to reinstall QRadar Console ISO, a warning message is displayed and you must confirm that you want to reinstall the software. After confirmation, the installer runs and you can follow the prompts through the installation process.

After a hard disk failure, you cannot reinstall from the recovery partition because it is no longer available. If you experience a hard disk failure, contact customer support for assistance.

Reinstalling IBM Security QRadar Risk Manager by using Factory re-install

You can restart and reinstall your IBM Security QRadar Risk Manager appliance by using the factory installation option.

Before you begin

Ensure that you have your activation key, which is a 24-digit, 4-part, alphanumeric string that you receive from IBM. You can find the key in these places:

- Printed on a sticker that is placed on your appliance.
- Included with the packing slip, where all appliances are listed along with their associated keys.

To avoid typing errors, the letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

If you do not have an activation key for your QRadar Risk Manager appliance, contact Customer Support (www.ibm.com/support/).

Software activation keys do not require serial numbers.

Procedure

1. Reboot your QRadar Risk Manager appliance.
2. Select **Factory re-install**.
3. Type `flatten` to continue. The hard disk is partitioned and reformatted, the OS is installed, and then QRadar Risk Manager is reinstalled. You must wait for the flatten process to complete. This process can take up to several minutes, depending on your system.
4. Type `SETUP`.
5. Log in to QRadar Risk Manager as the root user.
6. Read the information in the window. Press the Space bar to advance each window until you reach the end of the document. Type `yes` to accept the agreement, and then press Enter.
7. Type your activation key and press `Enter`.
8. Follow the instructions in the wizard.

   This process typically takes several minutes.
9. Press `Enter` to select `OK`.
10. Press `Enter` to select `OK`.

Chapter 11. Change network settings

You can change the network settings of an IBM Security QRadar Risk Manager appliance that is attached to an IBM Security QRadar SIEM Console.

If you need to change the network settings, then you must complete these tasks in the following order:

1. Remove QRadar Risk Manager as a managed host.
2. Change network settings.
3. Re-add QRadar Risk Manager as a managed host.

Removing a managed host

You can remove your IBM Security QRadar Risk Manager managed host from IBM Security QRadar SIEM Console to change network settings or if there is a problem with the **Risks** tab.

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 Risk Manager 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.

Changing network settings

You can change the network settings of an IBM Security QRadar Risk Manager appliance that is attached to an IBM Security QRadar SIEM Console.

Before you begin

You must remove the QRadar Risk Manager managed host from QRadar Console before you change the network settings.

Procedure

1. Using SSH, log in to QRadar Risk Manager as the root user.
2. Type the command, `qchange_netsetup`.
3. Select an Internet Protocol version. Select **Next** and press Enter. Depending on your hardware configuration, the window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.
4. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.

5. Enter information for your host name, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server. For network information, see "Network parameter information for IPv4" on page 12.
6. Type your password to configure the QRadar Risk Manager root password.
7. Select **Next** and press Enter.
8. Retype your new password to confirm. Select **Finish** and press Enter. This process typically takes several minutes.

Re-adding IBM Security QRadar Risk Manager as a managed host

You can re-add IBM Security QRadar Risk Manager as a managed host after it is removed.

Procedure

1. On the **Admin** tab, click **System and License Management** > **Deployment Actions** > **Add Host**.
2. Enter the host IP address and password.
3. Click **Add**.

   You must wait several minutes while the managed host is added.
4. Close the System and License Management window.
5. On the **Admin** tab toolbar, click **Advanced** > **Deploy Full Configuration**.
6. Click **OK**.

Chapter 12. Data back up and restore

You can use a command-line interface (CLI) script to back up data that is stored on IBM Security QRadar SIEM Console managed hosts.

You can use the CLI script to restore IBM Security QRadar Risk Manager after a data failure or hardware failure on the appliance.

A backup script is included in QRadar Risk Manager, which can be scheduled by using crontab. The script automatically creates a daily archive of QRadar Risk Manager data at 3:00 AM. By default, QRadar Risk Manager keeps the last five backups. If you have network or attached storage, you must create a cron job to copy QRadar Risk Manager back archives to a network storage location.

The backup archive includes the following data:

- QRadar Risk Manager device configurations
- Connection data
- Topology data
- Policy Monitor questions
- QRadar Risk Manager database tables

For information about migrating from QRadar Risk Manager Maintenance Release 5 to this current release, see the *IBM Security QRadar Risk Manager Migration Guide*.

Prerequisites for backing up and restoring data

You must understand how data is backed up, stored, and archived before you back up and restore your data.

Data backup location

Data is backed up in the `/store/qrm_backups` local directory. Your system might include a mount `/store/backup` from an external SAN or NAS service. External services provide long-term offline retention of data. Long-term storage might be required for compliance regulations, such as Payment Card Industry (PCI) standards.

Appliance version

The version of the appliance that created the backup in the archive is stored. A backup can be restored only in an IBM Security QRadar Risk Manager appliance if it is the same version.

Data backup frequency and archival information

Daily data backups are created at 3:00 AM. Only the last five backup files are stored. A backup archive is created if there is enough free space on QRadar Risk Manager.

Format of backup files

Use the following format to save backup files:

```
backup-<target date>-<timestamp>.tgz
```

Where, <target date> is the date that the backup file was created.

The format of the target date is <day>_<month>_<year>. <timestamp> is the time that the backup file was created.

The format of the time stamp is <hour>_<minute>_<second>.

Backing up your data

Automatic backup occurs daily, at 3:00 AM, or you can start the backup process manually.

Procedure

1. Using SSH, log in your IBM Security QRadar SIEM Console as the root user.
2. Using SSH from the QRadar Console, log in to QRadar Risk Manager as the root user.
3. Start a QRadar Risk Manager backup by typing the following command:
   ```
   /opt/qradar/bin/dbmaint/risk_manager_backup.sh
   ```

Results

The script that is used to start the backup process might take several minutes to start.

The following message is an example of the output that is displayed, after the script completes the backup process:

```
Fri Sep 11 10:14:41 EDT 2015
- Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2015-09-11-10-14-39.tgz
```

Restoring data

You can use a restore script to restore data from a QRadar Risk Manager backup.

Before you begin

The QRadar Risk Manager appliance and the backup archive must be the same version of QRadar Risk Manager. If the script detects a version difference between the archive and the QRadar Risk Manager managed host, an error is displayed.

About this task

Use the restore script to specify the archive that you are restoring to QRadar Risk Manager. This process requires you to stop services on QRadar Risk Manager. Stopping services logs off all QRadar Risk Manager users and stops multiple processes.

The following table describes the parameters that you can use to restore a backup archive.

Table 3. Parameters used to restore a backup archive to QRadar Risk Manager

Option	Description
-f	Overwrites any existing QRadar Risk Manager data on your system with the data in the restore file. Selecting this parameter allows the script to overwrite any existing device configurations in Configuration Source Management with the device configurations from the backup file.
-w	Do not delete directories before you restore QRadar Risk Manager data.
-h	The help for the restore script.

Procedure

1. Using SSH, log in your IBM Security QRadar SIEM Console as the root user.
2. Using SSH from the QRadar SIEM Console, log in to QRadar Risk Manager as the root user.
3. Stop `hostcontext` by typing `service hostcontext stop`.
4. Type the following command to restore a backup archive to QRadar Risk Manager:

   `/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>`.

   Where `<backup>` is the QRadar Risk Manager archive that you want to restore.

   For example, `backup-2012-09-11-10-14-39.tgz`.
5. Start `hostcontext` by typing `service hostcontext start`.

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.

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.

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