IBM Security QRadar Incident Forensics
Version 7.2.6

# *IBM Security QRadar Packet Capture Setup for the Dell PowerEdge R730 System*

**Note**

Before using this information and the product that it supports, read the information in “Notices” on page 17.

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This document applies to IBM QRadar Security Intelligence Platform V7.2.6 and subsequent releases unless superseded by an updated version of this document.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

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

## Intended audience

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

## Technical documentation

To find IBM Security QRadar product documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (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. QRadar Packet Capture on a PowerEdge R730 system

For the setup, you must start the system from an external DVD or Preboot Execution Environment server that has the .iso image files for the Standalone and IBM Security QRadar Packet Capture Data Node. Use this process to set up an individual Dell PowerEdge system as either a stand-alone system or master. You can also use this process to set up a Data Node in a cluster of 2 or 3 Dell systems or to set up a single system packet capture solution. Each cluster must contain a master and 1 or 2 Data Nodes.

*Table 1. System Requirements*

| Description | Value |
|---|---|
| System | Dell PowerEdge R730 |
| CPU | E5-2650 V3 |
| RAID Controller | PERC H730P Mini RAID Controller |
| RAM | Minimum 64 GB per CPU (128 GB) |
| HDD | Twelve 4 TB near-line SAS front-mounted hard disks connected to the RAID Controller |
| NIC | 2 Intel X520 NICs with 10 Gb/s SFP+ modules |
| Monitor | External monitor plugged into VGA port |
| Optical Cables | 2 or 3 optical cables for testing packet capture |

You must install two Intel X520 10 Gbit/s NICs in the exact slots shown in the diagrams. You can use a single X520 NIC that is for a stand-alone setup or an individual Data Node. You must install the single NIC where Interface 0 is marked on the diagram.

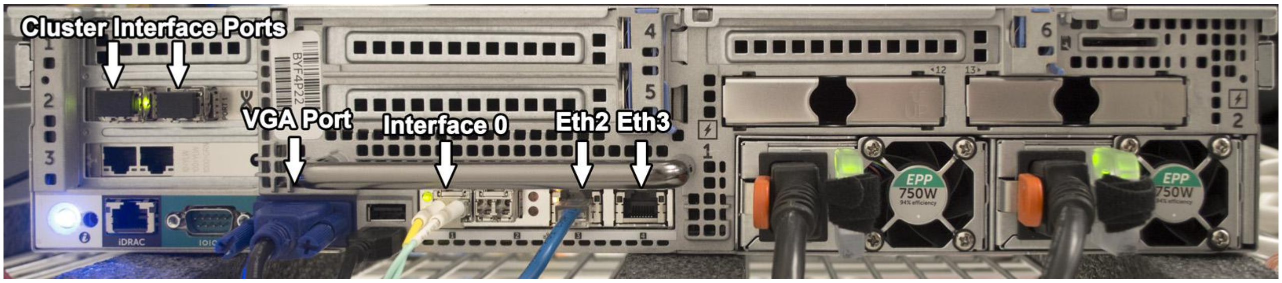

*Figure 1. Cluster Master or Stand-Alone System*

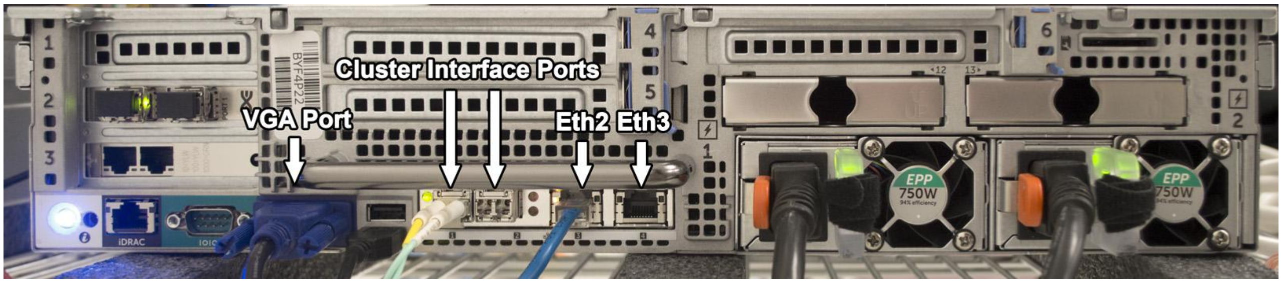

*Figure 2. Cluster Data Node*

# Chapter 2. Configuring system BIOS on a Linux PowerEdge R730 system

Use the BIOS to configure your system settings. These settings are based on system BIOS version 1.04. If your BIOS is newer, you must verify that the same settings in your version exist as shown here.

## Procedure

1. To access the BIOS system setup, press the F2 key while the system is powering on.
2. From the Main menu screen, select **System BIOS**.
3. Load the default settings by selecting **Default**.
4. Configure your system BIOS settings by using the following values:

*Table 2. Processor Settings*

| **Setting** | **Value** |
|---|---|
| Logical Processor | Disabled |
| QPI Speed | 9.6 GT/s |

*Table 3. System Profile Settings*

| **Setting** | **Value** |
|---|---|
| System Profile | Custom |
| CPU Power® Management | OSDBPM |
| Memory Frequency | Max Performance |
| Turbo Boost | Disabled |
| Energy Efficiency Policy | Performance |

5. Press the Esc key to return to the **System BIOS** screen.
6. Save changes when prompted.

# Chapter 3. Configuring a virtual disk for the Dell PowerEdge R730 system

Create a 128 GB operating system that has a RAID 1 configuration on the first two disk drives. Then create an extraction RAID 1 virtual partition on the remaining space of the same two disks that are used to configure the operating system virtual disk. Finally, create a RAID 5 capture partition for the remaining 10 disk drives. Use these settings to create the RAID arrays. Double-check your settings as you progress because some settings change dynamically. An incorrect RAID configuration can cause performance or system failures later.

## Procedure

1. Create an operating system virtual disk.
   a. To access the BIOS system setup, press the F2 key while powering on the system.
   b. From the Main menu screen, select **Device Settings**.
   c. Select **Integrated RAID Controller 1: Dell Perc <PERC H730P Mini> Configuration Utility**.
   d. From the Main menu, select **Configuration Management** > **Create Virtual Disk**. Use the following table to configure the virtual disk settings:

*Table 4. Configuration Management - Create Virtual Disk*

| Setting | Value |
|---|---|
| Select RAID Level | RAID1 |
| Secure Virtual Disk | Disable |
| Use Data Protection | Disable |

   e. Select the **Select Physical Disks** menu, and use the following table to configure the physical disk parameters:

*Table 5. Select Physical Disks*

| Setting | Value |
|---|---|
| Select Media Type | HDD |
| Select Interface Type | SAS |
| Logical Sector | 512 B |

   f. Select **Unconfigured Physical Disks** > **RAID 1**, select the first two disks, which are identified as **`00:01:00`** and **`00:01:01`** and then select **Apply Changes**.
   g. Select **Configure Virtual Disk Parameters** and use the following table to configure the virtual disk parameters:

*Table 6. Configure Virtual Disk Parameters*

| Setting | Value |
|---|---|
| Virtual Disk Name | default |
| Virtual Disk Size | 128 |
| Virtual Disk Size Unit | GB |
| Strip Element Size | 256 KB |
| Read Policy | Read Ahead |
| Write Policy | Force Write Back |
| Disk Cache | Enable |
| Default Initialization | Fast |

   h. Check **Confirm** to create the virtual disk.

2. Create an extraction virtual disk.
   a. From the Main menu, select **Configuration Management**.
   b. Verify or adjust these settings in the Create Virtual Disk menu:

*Table 7. Configuration Management - Create Virtual Disk*

| Setting | Value |
|---|---|
| Select RAID Level | RAID1 |
| Secure Virtual Disk | Disable |
| Use Data Protection | Disable |
| Select Physical Disks From | Free Capacity |
| Select/Check [x] | Disk Group 0: RAID1 |
| Verify - Free Space | 3597 GB |
| Verify (RAID1) | Associated Physical Disks: Physical Disk 00:01:00: HDD, SAS, 3725GB, Online, (512B)<br>Associated Physical Disks: Physical Disk 00:01:01: HDD, SAS, 3725GB, Online, (512B) |

   c. Select **Create Virtual Disks** to save the configuration.
   d. Select **Confirm** to create the virtual disk.

3. Create a capture virtual disk.
   a. From the System Setup Main menu, select **Configuration Management** > **Create Virtual Disk**, and configure the following virtual disk settings:

*Table 8. Configuration Management - Create Virtual Disk*

| Setting | Value |
|---|---|
| Select RAID Level | RAID5 |
| Secure Virtual Disk | Disable |
| Use Data Protection | Disable |

b. Select **Unconfigured Capacity** > **Select Physical Disks** and use the following table to configure the physical disk parameters:

*Table 9. Configuration Management - Select Physical Disks*

| Setting | Value |
|---|---|
| Media Type | HDD |
| Interface Type | SAS |
| Logical Sector | 512 B |

c. Select **Unconfigured Physical Disks**, and select **Check All** for each of the 11 disks.

d. Select **Apply Changes**.

e. Use the following table to configure the virtual disk parameters:

*Table 10. Configuration Management - Virtual Disk Parameters*

| Setting | Value |
|---|---|
| Virtual Disk Name | Leave default |
| Virtual Disk Size | 33529 |
| Virtual Disk Size Unit | GB |
| Strip Element Size | 1 MB |
| Read Policy | Read Ahead |
| Write Policy | Force Write Back |
| Disk Cache | Enable |
| Default Initialization | Fast |

f. Select **Create Virtual Disk** to save the configuration.

g. Select **Confirm** to create the virtual disk.

h. Press the Esc key twice to return to the **Integrated RAID Controller Main menu**.

i. Select **Virtual Disk Management** from the **Integrated RAID Controller Main menu** and verify that all of the virtual disks were created as shown in the following table:

*Table 11. Virtual Disk Management*

| **Virtual Disk** | **RAID Level** | **Virtual Disk Size** | **Status** |
|---|---|---|---|
| Virtual Disk 0 | RAID1 | 128 GB | Ready |
| Virtual Disk 1 | RAID1 | 3597 GB | Ready |
| Virtual Disk 2 | RAID5 | 33529 GB | Optimal |

j. Press the Esc key several times to return to the **System Setup Main menu**.

k. Select **Device Settings** from the **System Setup Main menu.**

l. Select **Integrated NIC 1 Port 3**: Intel Gigabit 4P x520/I350 rNDC.

m. Select **NIC Configuration** and change **Legacy Boot Protocol** to PXE.

n. Press the Esc key several times to return to the **System Setup Main menu**, and press the Esc key to exit.

o. Select **Yes** to confirm the exit, and restart the system.

# Chapter 4. Deploying a QRadar Packet Capture image on a PowerEdge R730 system

Each cluster setup consists of one master, and 1 or 2 IBM Security QRadar Packet Capture Data Nodes. Make sure that you boot from the appropriate image source, depending on the final system configuration that you want. A stand-alone system uses the same image as a cluster system.

## Procedure

1. Plug in an external DVD drive to one of the rear USB ports on the server that has the image DVD inserted into the drive or connect a network cable provided from a PXE server, depending upon your installation source. Make sure that you do not have any additional USB devices or network and packet capture cables plugged into the system during this setup.
2. Restart the system after RAID configuration is complete. At POST, press F11, and then choose One-Shot BIOS Boot Menu, followed by selecting your DVD drive from the list.
3. For the Preboot Execution Environment (PXE), plug into ETH2 as physically shown in the following diagram, and restart the system by using the most recent image provided.

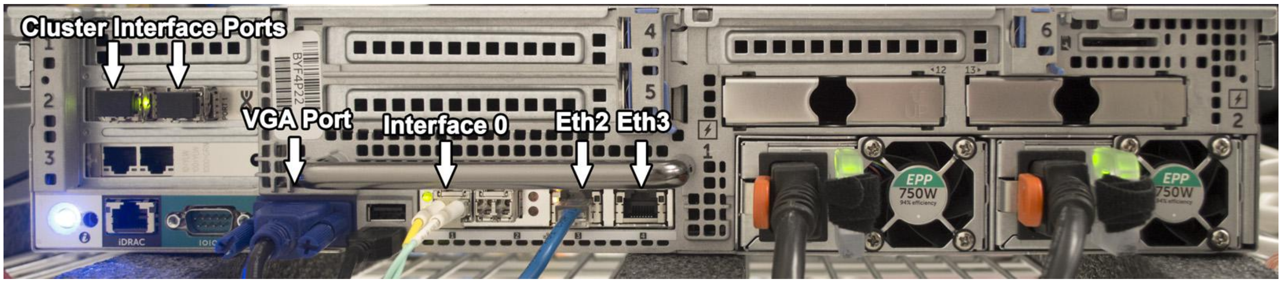

*Figure 3. Cluster Master or Stand-Alone System*

4. For DVD installations, when the image DVD starts, select the default menu option at the top.

   For PXE installations, this step might be automated.
5. For DVD installations, select y to the: **Are you sure you want to continue?** prompt.
6. For DVD installations, select y again to the: **Let me ask you again. Are you sure you want to continue?** prompt.
7. Make sure that the imaging process completes successfully.
8. Select **Power Off** from the menu after imaging completes.
9. Disconnect the DVD drive or PXE Ethernet cable from the system.
10. Turn on the system.
11. Log in as the root user.

    The Default password is `P@ck3t08.`.
12. Change to the `/root` directory and then run the following command:
    `./Reset_Interfaces.sh`

13. Log in as root user after the system restarts and run the following command: `df -h .`
    a. On the line that begins with `/dev/sdc`, check that the size of the `/storage0` partition is 33 TB.
    b. On the line that begins with `/dev/sdb1`, check that the size of the `/extraction` partition is 3.5 TB.
    c. If these `/dev/sdc` and `/dev/sdb1` configurations are not the correct size, retrace your steps. Make sure that the operating system, extraction, and capture RAID arrays were created correctly, and in the correct order before you deployed the image. Verify that no steps were missed.
    d. The sizes of `sdc` and `sdb1` are based on using all 4 TB hard disks in the system. If different disks are used, the relative sizes of the `sdc` and `sdb` increase or decrease with the size of the hard disks. The operating system partition `sda` is always fixed because it was set up in the RAID configuration.

# Chapter 5. 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 12. 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.<br>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<br>**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 |

*Table 12. System requirements for a QRadar Packet Capture software installation (continued)*

| **Specification** | **Description** |
|---|---|
| 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<br>Intel 82576 Gigabit Ethernet Controller http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller |
| 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 13. 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.

# Chapter 6. Customizing the setup on a PowerEdge R730 system

After you set up IBM Security QRadar Packet Capture, you can configure the date and time, change the IP address of the NIC cards, and change the default passwords.

## Procedure

1. Change the UTC time.
   a. At the shell prompt, change the date and time to current UTC time by using the date command at the prompt.

      The format for the date command is month (02), day (25), hour (15), minutes (07), and year (2016). In this example, the date is in the format *022515072016*.

   b. Set the BIOS clock by using the `hwclock` command:

      ```
      /sbin/hwclock --systohc
      ```

   **Important:** In the default configuration, the Network Time Protocol (NTP) service uses public servers. If you want to use an internal server, you must edit the `/etc/ntp.conf` file and change the lines that begin with "server" to your server.

2. Change the IP addresses of the NIC.
   a. Check which network interfaces are available by using the following command:

      ```
      ifconfig | grep eth
      ```

   b. Note the hardware address `/etc/sysconfig/nework-scripts/ifcfg-eth*`.
   c. Edit the `/etc/sysconfig/nework-scripts/ifcfg-eth*` files to configure the standard Ethernet interfaces that are used to communicate remotely with the system.

      `eth*` represents ETH4, ETH5, ETH6, and so on. Ensure that you do not change the preconfigured 10G static interfaces (1.1.1.X or 2.2.2.X), because they are used for master and data node connectivity.

      To set a static IP address, use the following table and replace the values with information that is specific to your deployment.

*Table 14. IP address configuration*

| Setting | Value |
|---|---|
| DEVICE | ETH0 |
| HWADDR | 34:40:B5:A3:9F:F7 |
| BOOTPROTO | Static |
| GATEWAY | 23.30.187.174 |
| IPADDR | 23.30.187.169 |
| NETMASK | 255.255.255.240 |
| NM_CONTROLLED | Yes |
| ONBOOT | Yes |

If DHCP is used, no IP address configuration is required.

d. Test the system packet capture by using QRadar Packet Capture.

   **Important:** To connect the master and data node systems together and test the packet capture, see the *QRadar Packet Capture Quick Start Guide*.

3. Use SSH and port `4477` to log in as the `root` user.

   The default password for the `root` user is `P@ck3t08.`.
4. To change the passwords for the `root` user account, use the **`passwd`** command.
5. To change the Packet Capture Web User Interface Account passwords as required upon first login, use the following steps:

   a. Log in to the UI `https://pcap-IP_Address:41390`.

   b. Click on the **Admin** tab.

   c. Under **User Management**, edit the current user account password as required, and click **Save**.

   **Note:** Passwords need to be at least 8 characters long. They must have one or more upper case and lower case letters, and one or more special characters ($,%,*).

# 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.

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