IBM Security QRadar
LEEF 1.0

Log Event Extended Format (LEEF) Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 19.

CONTENTS

ABOUT THIS GUIDE

The *IBM Security QRadar Log Event Extended Format (LEEF) Guide* provides information on how to construct and implement syslog events for QRadar products in Log Event Extended Format (LEEF).

Unless otherwise noted, all references to QRadar refer to IBM Security QRadar and IBM Security QRadar Log Manager.

Intended audience

This guide is intended for appliance vendors, software developers, and product managers. This guide assumes that you have access to QRadar software through the IBM PartnerWorld program or have been invited to join the IBM Security QRadar SIEM DSM Beta program.

About IBM Programs

The LEEF format is supported by IBM Partner World and the Ready for IBM Security Intelligence Program

For information about the Ready for IBM Security Intelligence Program, you can send an email to *SIPP@ca.ibm.com* or visit one of the following websites:

- Ready for IBM Security Intelligence Program: *http://www.ibm.com/partnerworld/rfisi*
- IBM Partner World: *http://www.ibm.com/partnerworld*

Ready for IBM Security Intelligence Program

The Ready for IBM Security Intelligence Program™ is an open enrollment program for vendors of security products, such as software or hardware manufacturers. The program relies on shared tools to enable development, testing, troubleshooting, and advanced integrations techniques that allow security products and QRadar to communicate events effectively.

The Ready for IBM Security Intelligence offering helps promote a vibrant ecosystem to nurture and support business partner products that extend the core value of IBM Security solutions for the design, development, and delivery of software and systems to support new security capabilities for our customers.

The Ready for IBM Security Intelligence Program is intended as a joint commitment to collaborate and support security and event integrations for the

benefit of shared customers. The program provides an avenue for sellers, product managers, engineers, and documentation personnel to communicate and resolve integration issues, answer questions, share documentation, or test security integrations. The LEEF format was designed under the Ready for IBM Security Intelligence Program to allow for integration of security events with QRadar.

IBM PartnerWorld

IBM PartnerWorld is an IBM global marketing and enablement program designed to create new market opportunities and help generate new revenue for IBM Business Partners. PartnerWorld can provide support for partners and their sales force by providing content to articulate value to shared customers, such as solution briefs, marketing messages, and webinars. PartnerWorld provides access to the resources you need to begin building and selling IBM-based solutions, products and services.

Documentation conventions

The following conventions are used throughout this guide:

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING: *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical documentation

For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***.
(http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)

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 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.

1 LOG EVENT EXTENDED FORMAT (LEEF)

The Log Event Extended Format (LEEF) is a customized event format for IBM Security QRadar.

About LEEF event collection in QRadar

LEEF events can be created by any vendor with this documentation to have their product generate events.

Appliances or applications that generate LEEF events allow QRadar to easily integrate, identify, and process LEEF formatted events provided to QRadar. LEEF events require UTF-8 character encoding.

Events in LEEF format can be provided to QRadar with the following protocols:

- Syslog
- File import with the Log File protocol
- Other protocol collection methods (requires engineering support)

The method you select to provide LEEF events determines if the events can be automatically discovered in QRadar. Automatically discovered events provide ease of configuraton for customers as it reduces the amount of manual configuration required in QRadar.

As LEEF events are received, QRadar analyzes the event traffic in an attempt to identify the device or appliance. This process is referred to internally as traffic analysis. It typically takes at minimum 25 LEEF events to identify and create a new log source in QRadar. Until traffic analysis identifies the event source, the initial 25 events are categorized as SIM Generic Log DSM events with the event name set as Unknown Log Event. After the event traffic is identified, then QRadar creates a log source to properly categorize and label any events forwarded from your appliance or software. Events sent from your device are viewable in QRadar on the **Log Activity** tab.

Note: If a log source cannot be identified after 1,000 events, then QRadar creates a system notification and removes the log source from the traffic analysis queue. QRadar is still capable of collecting the events, but a user must intervene and create a log source manually to identify the event type.

Components of LEEF events

The Log Event Extended Format (LEEF) is a customized event format for IBM Security QRadar that contains readable and easily processed events for QRadar. The LEEF format consists of the following components.

Syslog header

The syslog header is an optional field. The syslog header contains the timestamp and IPv4 address or host name of the system providing the event. The syslog header is an optional component of the LEEF format. If you include the syslog header, you must separate the syslog header from the LEEF header with a space.

Examples:

- Date<space>IP address
- Jan 18 11:07:53 192.168.1.1
- Jan 18 11:07:53 myhostname

LEEF header

The LEEF header is a required field for LEEF events. The LEEF header is a pipe delimited (|) set of values that identifies your software or appliance to QRadar.

Examples:

- LEEF:Version|Vendor|Product|Version|EventID|
- LEEF:1.0|Microsoft|MSExchange|4.0 SP1|15345|

Event attributes

The event attributes identify the payload information of the event produced by your appliance or software. Every event attribute is a key and value pair with a tab separating individual payload events. The LEEF format contains a number of predefined event attributes, which allow QRadar to categorize and display the event.

Examples:

- key=value<tab>key=value<tab>key=value<tab>key=value<tab>
- src=7.5.6.6 dst=172.50.123.1 sev=5 cat=anomaly srcPort=81 dstPort=21 usrName=joe.black

Note: If your appliance is not capable of using tab separators in the Event attritubes as a delimiter, then a substitution can be made. In special cases, we can substitute caret (^) or pipe (|) characters as delimiters. If your appliance or software requires an alternate delimiter, please contact us for engineering support.

Table 1-1 LEEF format description

Type	Entry	Delimiter	Description
Syslog Header	Date	Space	The date and timestamp of the host providing the event to QRadar. The date field should conform to the mmm dd hh:mm:ss format: For example, Jan 18 11:07:53. A space must separate the date and IP address fields.

Table 1-1 LEEF format description (continued)

Type	Entry	Delimiter	Description
Syslog Header	IP address	Space	The IP address or the host name of the software or appliance providing the event to QRadar. Examples: • 192.168.1.1 • myhostname The IP address of the syslog header is used by QRadar to route the event to the correct log source in the event pipeline. It is not recommended that your syslog header contain an IPv6 address. QRadar cannot route an IPv6 address present in the syslog header for the event pipeline. Also, an IPv6 address might not display properly in the Log Source Identifier field of the user interface. When an IP address of the syslog header cannot be understood by QRadar, then the system defaults to the packet address to properly route the event.
LEEF Header	LEEF:version	Pipe	The LEEF version information is an integer value that identifies the major and minor version of the LEEF format used for the event. For example, LEEF:1.0|Vendor|Product|Version|EventID|
LEEF Header	Vendor or manufacturer name	Pipe	Vendor is a text string that identifies the vendor or manufacturer of the device sending the syslog event in LEEF format. For example, LEEF:1.0|Microsoft|Product|Version|EventID| ***Note:*** *The Vendor and Product fields must contain unique values when specified in the LEEF header.*
LEEF Header	Product name	Pipe	The product field is a text string that identifies the product sending the event log to QRadar. For example, LEEF:1.0|Microsoft|MSExchange|Version|EventID| ***Note:*** *The Vendor and Product fields must contain unique values when specified in the LEEF header.*
LEEF Header	Product version	Pipe	Version is a string that identifies the version of the software or appliance sending the event log. For example, LEEF:1.0|Microsoft|MSExchange|4.0 SP1|EventID|

Table 1-1 LEEF format description (continued)

Type	Entry	Delimiter	Description
LEEF Header	EventID	Pipe	EventID is a unique identifier for an event in the LEEF header. The purpose of the EventID is to provide a fine grain, unique identifier for an event without the need to examine the payload information. An EventID can contain either a numeric identified or a text description. Examples: • LEEF:1.0|Microsoft|MSExchange|2007|7732| • LEEF:1.0|Microsoft|MSExchange|2007|Logon Failure| Restrictions: The value of the event ID must be a consistent and static across products that support multiple languages. If your product supports multi-language events, you can use a numeric or textual value in the EventID field, but it must not be translated when the language of your appliance or application is altered. The EventID field cannot exceed 255 characters.
Event Attributes	Predefined Key Entries	Tab	Event attribute is a set of key value pairs that provide detailed information about the security event. Each event attribute must be separated by a tab delimiter, but the order of attributes is not enforced. For example, src=172.16.77.100

Predefined LEEF event attributes

The Log Event Extended Format (LEEF) supports a number of predefined event attributes for the event payload.

The LEEF format uses a specific list of name and value pairs that have been predefined as LEEF event attributes. These keys outline fields identifiable to QRadar and the use of the field for the LEEF format. It is recommended that your appliance use these keys when possible, but your event payloads are not limited by this list. The LEEF format is extensible and allows for additional keys to be added to the event payload for your appliance or application.

Table 1-2 Predefined event attributes

Key	Value Type	Attribute Limits	Normalized Event Field	Description
cat	String		Yes	Cat is an abbrevation for event category and is used to extend the EventID field with more specific information about the LEEF event forwarded to QRadar. The event attribute cat and the EventID field in the LEEF header help map your appliance event to a QRadar Identifier (QID) map entry. The EventID represents the first column and the category represents the second column of the QID map. Restrictions: The value of the event category must be a consistent and static across products that support multiple languages. If your product supports multi-language events, you can use a numeric or textual value in the cat field, but it must not be translated when the language of your appliance or application is altered. Examples: • Case 1: The cat key can be used to extend the EventID with additional information to describe the event. If the EventID is defined as a User Login event, the category can be used to further categorize the event, such as a success or failed login. This allows you to further define your EventIDs or distinguish between events when your appliance uses the same EventID for similar event types. LEEF:1.0|Microsoft|Exchange|2007|Login Event|cat=Failed or LEEF:1.0|Microsoft|Exchange|2007|Login Event|cat=Success • Case 2: The cat key can be used in a traditional role where it defines a high-level event category and the EventID is used to define the low-level, fine grained event. This can be important when the EventID does not match any value in the QID map. When this occurs, QRadar can fall back to the category and other keys to further determine the general nature of the event. This prevents events from identifying as unknown and allows QRadar to categorize events based on the known information from the key attribute fields of the event payload. LEEF:1.0|Microsoft|Endpoint|2012|Conficker_worm|cat=Detected

Table 1-2 Predefined event attributes (continued)

Key	Value Type	Attribute Limits	Normalized Event Field	Description
devTime	Date		Yes	The device time is the raw event date and time generated by your appliance or application providing the LEEF event. QRadar uses the devTime key, along with devTimeFormat to identify and properly format the event time from your appliance or application. The devTime and devTimeFormat keys must be used together to ensure the time of the event is accurately parsed by QRadar. When present in the event payload, devTime is used to identify the event time, even when the syslog header contains a date and timestamp. The syslog header date and timestamp is a fallback identifier, but devTime is the preferred method for event time identification.
devTimeFormat	String		No	The devTimeFormat key applies formatting to the raw data and time of the devTime key. The devTimeFormat key is required if your event log contains devTime. For more information, see **Custom Event Date Format**.
proto	Integer or Keyword		Yes	Identifies the transport protocol of the event.
	Note: *For a list of keywords or integer values, see http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml*			
sev	Integer	1-10	Yes	A numeric value that indicates the severity of the event. • 1 is the lowest event severity. • 10 is the highest event severity.
src	IPv4 or IPv6 Address		Yes	The IP address of the event source.
dst	IPv4 or IPv6 Address		Yes	IP address of the event destination.
srcPort	Integer	0 to 65535	Yes	Source port of the event.
dstPort	Integer	0 to 65535	Yes	Destination port of the event.
srcPreNAT	IPv4 or IPv6 Address		Yes	Source address for the event message before Network Address Translation (NAT).
dstPreNAT	IPv4 or IPv6 Address		Yes	Destination address for the event message before Network Address Translation (NAT).
srcPostNAT	IPv4 or IPv6 Address		Yes	Source address for the message after Network Address Translation (NAT) occurred.

Table 1-2 Predefined event attributes (continued)

Key	Value Type	Attribute Limits	Normalized Event Field	Description
dstPostNAT	IPv4 or IPv6 Address		Yes	Destination address for the message after Network Address Translation (NAT) occurred.
usrName	String	255	Yes	Username associated with the event.
srcMAC	MAC Address		Yes	MAC address of the event source in hexadecimal. The MAC address is comprised of six groups of two hexadecimal digits, which are colon-separated. For example, **`11:2D:67:BF:1A:71`**
dstMAC	MAC Address		Yes	MAC address of the event destination in hexadecimal. The MAC address is comprised of six groups of two hexadecimal digits, which are colon-separated. For example, **`11:2D:67:BF:1A:71`**
srcPreNATPORT	Integer	0 to 65535	Yes	Port number of the event source before Network Address Translation (NAT).
dstPreNATPORT	Integer	0 to 65535	Yes	Port number of the event destination before Network Address Translation (NAT).
srcPostNATPORT	Integer	0 to 65535	Yes	Port number of the event source after Network Address Translation (NAT).
dstPostNATPORT	Integer	0 to 65535	Yes	Port number of the event destination after Network Address Translation (NAT).
identSrc	IPv4 or IPv6 Address		Yes	Identity source represents an additional IPv4 or IPv6 address that can connect an event with a true user identify or true computer identity. Examples: • Case 1: Connecting a person to a network identity. For example, user X logs in from their laptop and then connects to a shared system on the network. When their activity generates an event, then the identSrc in the payload can be used to include additional IP address information. QRadar uses the identSrc information in the event along with the payload information, such as username to identify that user X is in reality bob.smith. The following identity keys are dependant on identSrc being present in the event payload: • identHostName • identNetBios • identGrpName • identMAC

Table 1-2 Predefined event attributes (continued)

Key	Value Type	Attribute Limits	Normalized Event Field	Description
identHostName	String	255	Yes	Host name information associated with the identSrc to further identify the true hostname tied to an event. The identHostName parameter is only usable by QRadar if your device provides both the identSrc key and identHostName together in an event payload.
identNetBios	String	255	Yes	NetBIOS name associated with the identSrc to further identify the identity event with NetBIOS name resolution. The identNetBios parameter is only usable by QRadar if your device provides both the identSrc key and identNetBios together in an event payload.
identGrpName	String	255	Yes	Group name associated with the identSrc to further identify the identity event with Group name resolution. The identGrpName parameter is only usable by QRadar if your device provides both the identSrc key and identGrpName together in an event payload.
identMAC	MAC Address		Yes	***Note:*** *The identMAC key is reserved for future use in the LEEF format.*
vSrc	IPv4 or IPv6 Address		No	IP address of the virtual event source.
vSrcName	String	255	No	Name of the virtual event source.
accountName	String	255	No	The account name associated with the event.
srcBytes	Integer		No	A numeric value indicating the byte count from the event source.
dstBytes	Integer		No	A numeric value indicating the byte count to the event destination.
srcPackets	Integer		No	A numeric value indicating the packet count from the event source.
dstPackets	Integer		No	A numeric value indicating the packet count to the event destination.
totalPackets	Integer		No	A numeric value indicating the total number of packets transmitted between the source and destination.
role	String		No	Role type associated with the user account that created the event. For example, Administrator, User, Domain Admin.

Table 1-2 Predefined event attributes (continued)

Key	Value Type	Attribute Limits	Normalized Event Field	Description
realm	String		No	Realm associated with the user account. Depending on your device, this could be a general grouping or based on region. For example, accounting, remote offices.
policy	String		No	Policy associated with the user account. This is typically the security policy or group policy tied to the user account.
resource	String		No	Resource associated with the user account. This is typically the computer name.
url	String		No	URL information that is included with the event.
groupID	String		No	GroupID that is associated with the user account.
domain	String		No	Domain associated with the user account.
isLoginEvent	Boolean string	true or false	No	Identifies if the event is related to a user login. Examples: • isLoginEvent=true • isLoginEvent=false ***Note:*** *This key is reserved in the LEEF specification, but not implemented at this time in QRadar.*
isLogoutEvent	Boolean string	true or false	No	Identifies if the event is related to a user logout. Examples: • isLogoutEvent=true • isLogoutEvent=false ***Note:*** *This key is reserved in the LEEF specification, but not implemented at this time in QRadar.*
identSecondIp	IPv4 or IPv6 Address		No	Identity second IP address represents an IPv4 or IPv6 address used to associate a device event that includes a secondary IP address. Secondary IP addresses can be in events by routers, switches, or virtual LAN (VLAN) device events. ***Note:*** *This key is reserved in the LEEF specification, but not implemented at this time in QRadar.*

Table 1-2 Predefined event attributes (continued)

Key	Value Type	Attribute Limits	Normalized Event Field	Description
calLanguage	String	2	No	Identifies the language of the device time (devTime) key to allow localization and ensure QRadar correctly parses the date and time of events generated in localized languages. The calLanaguage field can include two alphanumeric characters to represent the event language for the device time of your event. All calLanguage alphanumeric characters follow the ISO 639-1 format. Examples: • calLanguage=fr devTime=avril 09 2006 12:30:55 • calLanguage=de devTime=Di 30 Jun 09 14:56:11 ***Note:*** *This key is reserved in the LEEF specification, but not implemented at this time in QRadar.*
calCountryOrRegion	String	2	No	Extends the calLanguage key to provide additional localization information to include the country or region for the event device time (devTime). The key calCountryOrRegion must be used with the calLanguage key. The calCountryOrRegion field can include two alphanumeric characters to represent the event country or region for the device time of your event. All calCountryOrRegion alphanumeric characters follow the ISO 3166 format. Examples: • calLanguage=de calCountryOrRegion=DE devTime=Di 09 Jun 2006 12:30:55 • calLanguage=en calCountryOrRegion=US devTime=Tue 30 Jun 09 14:56:11 ***Note:*** *This key is reserved in the LEEF specification, but not implemented at this time in QRadar.*

Custom event keys

Vendors and partners have the option to define their own custom event keys and include them in the payload of the LEEF format.

A custom key value pair attributes can be used in an event payload when there is no default key to represent information about an event for your appliance. Custom event attributes should only be created when there is no acceptable mapping to a predefined event attribute. For example, if your appliance monitors access, you might require the filename accessed by a user where no filename attribute exists in LEEF by default.

CAUTION: *Event attribute keys and values can only appear once per payload. Using a key value pair twice in the same payload can cause QRadar to ignore the value of the duplicate key.*

Custom event keys are non-normalized, which means that any specialized key value pairs you include in your LEEF event are not displayed by default on the **Log Activity** tab of QRadar. To view custom attributes and non-normalized events on the **Log Activity** tab of QRadar, the QRadar user must create a custom event property. Non-normalized event data is still part of your LEEF event, is searchable in QRadar, and is viewable in the event payload. For more information on creating a custom event property, see the *QRadar Administration Guide*.

Best practices

LEEF is very flexible and allows you to create custom key value pairs for events, but you should follow some best practices to avoid potential parsing issues.

Note: Items marked allowed can be included in a key or value, but is not in violation of the LEEF format nor is it a best practice when creating custom event keys.

The following list contains custom key and value best practices:

- Use alphanumeric (A-Z, a-z, and 0-9) characters, but avoid tab, pipe, or caret delimiters in your event payload keys and values (key=value).
  - **Correct** - usrName=Joe.Smith
  - **Incorrect** - usrName=Joe<tab>Smith
- Contain a single word for the key attribute (key=value).
  - **Correct** - filename=pic07720.gif
  - **Allowed** - file name=pic07720.gif
  - **Allowed** - filename =pic07720.gif
- A user defined key cannot use the same name as a LEEF predefined key. For more information, see **Table 1-2**.

- Key values should be human readable, if possible, as your customers might need to investigate event payloads.
  - **Correct** - deviceProcessHash=value
  - **Correct** - malwarename=value
  - **Allowed** - EBFDFBE14D4=value

Custom Event Date Format

The create a customized event format, your device must supply the raw date format using the devTime event attribute in the payload of the event.

The devTime event attribute requires formatting using devTimeFormat to display the event in QRadar. The suggested devTimeFormat patterns are listed as follows:

Table 1-3 devTimeFormat suggested patterns

devTimeFormat Pattern	Result
devTimeFormat=MMM dd yyyy HH:mm:ss	Jun 06 2010 16:07:36
devTimeFormat=MMM dd yyyy HH:mm:ss.SSS	Jun 06 2010 16:07:36.300
devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z	Jun 06 2010 02:07:36.300 GMT

For further information on specifying a date format, visit the SimpleDateFormat page at: http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

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 *http:\\www.ibm.com/legal/copytrade.shtml*.

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

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.