IBM QRadar

Log Event Extended Format (LEEF) Version 2

Note

Before using this information and the product that it supports, read the information in "Notices" on page 11.

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.2.1 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to QRadar LEEF

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

Intended audience

This guide is intended for all QRadar users who are responsible for investigating and managing network security. To use this information, you must have access to QRadar products and a knowledge of your corporate network and networking technologies.

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 QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

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. LEEF overview

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

Any vendor can use this documentation to generate LEEF events.

QRadar can integrate, identify, and process LEEF events. LEEF events must use UTF-8 character encoding.

You can send events in LEEF output to QRadar by using the following protocols:

- Syslog
- File import with the Log File Protocol

Important: Before QRadar can use LEEF events, you must complete Universal LEEF configuration tasks. For more information about configuring the log file protocol to collect Universal LEEF events, see the *DSM Configuration Guide*.

The method that you select to provide LEEF events determines whether the events can be automatically discovered in QRadar. When events are automatically discovered the level of manual configuration that is needed in QRadar is reduced.

As LEEF events are received, QRadar analyzes the event traffic in an attempt to identify the device or appliance. This process is referred to as *traffic analysis*. It typically takes at least 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 and the event name is set as *Unknown Log Event*. After the event traffic is identified, QRadar creates a log source to properly categorize and label any events that are forwarded from your appliance or software. Events that are sent from your device are viewable in QRadar on the **Log Activity** tab.

Important: When a log source cannot be identified after 1,000 events, 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.

LEEF event components

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

Syslog header

The syslog header contains the timestamp and IPv4 address or host name of the system that is providing the event. The syslog header is an optional component of the LEEF format. If you include a syslog header, you must separate the syslog header from the LEEF header with a space. The syslog header must conform to the formats specified in RFC 3164 or RFC 5424.

RFC 3164 header format:

Note: The priority tag is optional for QRadar.

<priority tag><timestamp> <IP address or hostname>

The priority tag, if present, must be 1 - 3 digits and must be enclosed in angle brackets. For example, <13>.

Examples of RFC 3164 header:

- <13>Jan 18 11:07:53 192.168.1.1
- Jan 18 11:07:53 myhostname

RFC 5424 header format:

Note: The priority tag is required.

<priority tag>1 <timestamp> <IP address or hostname>

The priority tag must be 1 - 3 digits and must be enclosed in angle brackets. For example, <13>. The timestamp must be in the format: yyyy-MM-ddTHH:mm:ss.SSSZ.

Note:

- The 'T' must be a literal T character.
- The 'Z' can be a literal Z or it can be a timezone value in the following format: -04:00

Examples of RFC 5424 header:

- <13>1 2019-01-18T11:07:53.520Z 192.168.1.1
- <133>1 2019-01-18T11:07:53.520+07:00 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|
- LEEF:2.0|Lancope|StealthWatch|1.0|41|^|

Event attributes

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

Example:

- key=value<tab>key=value<tab>key=value<tab>key=value<tab>.
- src=192.0.2.0 dst=172.50.123.1 sev=5 cat=anomaly srcPort=81 dstPort=21 usrName=joe.black

Use the `DelimiterCharacter` in the LEEF 2.0 header to specify an alternate delimiter to the attributes. You can use a single character or the hex value for that character. The hex value can be represented by the prefix 0x or x, followed by a series of 1-4 characters (0-9A-Fa-f).

Table 1. Attribute Delimiter Character examples for LEEF 2.0

Delimiter	**Header**
Caret (^)	`LEEF:2.0|Vendor|Product|Version|EventID|^|`
Caret (hex value)	`LEEF:2.0|Vendor|Product|Version|EventID|x5E|`
Broken vertical bar (¦)	`LEEF:2.0|Vendor|Product|Version|EventID|xa6|`

The following table provides descriptions for LEEF formats.

Table 2. LEEF format descriptions

Type	Entry	Delimiter	Description
Syslog Header	IP address	Space	The IP address or the host name of the software or appliance that provides the event to QRadar. **Example:** 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, 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 that is 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 that sends the syslog events in LEEF format. For example, LEEF:1.0|Microsoft|Product|Version|EventID| 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 that sends the event log to QRadar. For example, LEEF:1.0|Microsoft|MSExchange|Version|EventID| 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 that sends the event log. For example, LEEF:1.0|Microsoft|MSExchange|4.0 SP1|EventID|
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.
LEEF Header	Delimiter Character	Pipe	Use the `DelimiterCharacter` in the LEEF 2.0 header to specify an alternate delimiter to the attributes. You can use a single character or the hex value for that character. The hex value can be represented by the prefix 0x or x, followed by a series of 1-4 characters (0-9A-Fa-f).

Table 2. LEEF format descriptions (continued)			
Type	**Entry**	**Delimiter**	**Description**
Event Attributes	Predefined Key Entries	Tab Delimiter Character	Event attribute is a set of key value pairs that provide detailed information about the security event. Each event attribute must be separated by tab or the delimiter character, 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.

LEEF uses a specific list of name-value pairs that are predefined LEEF event attributes. These keys outline fields that are identifiable to IBM Security QRadar. Use these keys on your appliance when possible, but your event payloads are not limited by this list. LEEF is extensible and you can add more keys to the event payload for your appliance or application.

The following table describes the predefined event attributes.

Table 3. Pre-defined event attributes			
Key	**Value type**	**Normalized event field? Yes or No**	**Description**
cat	String	Yes	An abbreviation for event category is used to extend the EventID field with more specific information about the LEEF event that is forwarded to QRadar. 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. **Restriction:** The value of the event category must be 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. The value in the **cat** field must not be translated when the language of your appliance or application is altered.

cat (continued)	String	Yes	Example 1: Use the **cat** key to extend the EventID with additional information to describe the event. If the EventID is defined as a User Login event, use the category to further categorize the event, such as a success or failed login. You can define your EventIDs further with the **cat** key, and the extra detail from the event can be used to distinguish between events when the same EventID is used for similar event types, for example,
			`LEEF:1.0|Microsoft|Exchange|2013|Login Event|cat=Failed`
			`LEEF:1.0|Microsoft|Exchange|2013|Login Event|cat=Success`
			Example 2: Use the **cat** key to define a high-level event category and use the EventID to define the low-level. This situation can be important when the EventID doesn't match any value in the QID map. When the EventID doesn't match any value in the QID map, QRadar can use the category and other keys to further determine the general nature of the event. This "fallback" prevents events from being identified as unknown and QRadar can categorize the events based on the known information from the key attribute fields of the event payload, for example,
			`LEEF:1.0|Microsoft|Endpoint|2015|`
			`Conficker_worm|cat=Detected`

devTime	Date	Yes	The raw event date and time that is generated by your appliance or application that provides the LEEF event. QRadar uses the **devTime** key, along with **devTimeFormat** to identify and properly format the event time from your appliance or application. If the **devTime** value is an epoch value of 10 or 13 digits, a **devTimeFormat** string is not required. Otherwise, the **devTime** and **devTimeFormat** keys must be used together to ensure that 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 time stamp. The syslog header date and time stamp is a fallback identifier, but **devTime** is the preferred method for event time identification.

Table 3. Pre-defined event attributes (continued)

Key	Value type	Normalized event field? Yes or No	Description
devTimeFormat	String	No	Applies formatting to the raw date 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" on page 9.
proto	Integer or Keyword	Yes	Identifies the transport protocol of the event. For a list of keywords or integer values, see the Internet Assigned Numbers Authority website, http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml
sev	Integer	Yes	Indicates the severity of the event. 1 is the lowest event severity. 10 is the highest event severity. Attribute Limits: 1-10
src	IPv4 or IPv6 Address	Yes	The IP address of the event source.
dst	IPv4 or IPv6 Address	Yes	The IP address of the event destination.
srcPort	Integer	Yes	The source port of the event. Attribute Limits: 0 - 65535
dstPort	Integer	Yes	The destination port of the event. Attribute Limits: 0 - 65535
srcPreNAT	IPv4 or IPv6 Address	Yes	The source IP address of the event message before Network Address Translation (NAT).
dstPreNAT	IPv4 or IPv6 Address	Yes	The destination address for the event message before Network Address Translation (NAT).
srcPostNAT	IPv4 or IPv6 Address	Yes	The source IP address of the message after Network Address Translation (NAT) occurred.
dstPostNAT	IPv4 or IPv6 Address	Yes	The destination IP address of the message after Network Address Translation (NAT) occurred.
usrName	String	Yes	The user name that is associated with the event. Attribute Limits: 255
srcMAC	MAC Address	Yes	The MAC address of the event source in hexadecimal. The MAC address is made up of six groups of two hexadecimal digits, which are colon-separated, for example, `11:2D:1a:2b:3c:4d`
dstMAC	MAC Address	Yes	The MAC address of the event destination in hexadecimal. The MAC address is composed of six groups of two hexadecimal digits, which are colon-separated, for example, `11:2D:1a:2b:3c:4d`
srcPreNATPort	Integer	Yes	The port number of the event source before Network Address Translation (NAT). Attribute Limits: 0 - 65535
dstPreNATPort	Integer	Yes	The port number of the event destination before Network Address Translation (NAT). Attribute Limits: 0 - 65535
srcPostNATPort	Integer	Yes	The port number of the event source after Network Address Translation (NAT). Attribute Limits: 0 - 65535
dstPostNATPort	Integer	Yes	The port number of the event destination after Network Address Translation (NAT). Attribute Limits: 0 - 65535

Table 3. Pre-defined event attributes (continued)

Key	Value type	Normalized event field? Yes or No	Description
identSrc	IPv4 or IPv6 Address	Yes	Identity source represents an extra IPv4 or IPv6 address that can connect an event with a true user identify or true computer identity. Example 1: Connecting a person to a network identity. User X logs in from their notebook 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 more 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 bob.smith. The following identity keys depend on **identSrcs** presence in the event payload: **identHostName** **identNetBios** **identGrpName** **identMAC**
identHostName	String	Key	Host name information that is associated with the **identSrc** to further identify the true host name that is tied to an event. The **identHostName** parameter is usable by QRadar only when your device provides both the **identSrc** key and **identHostName** together in an event payload. Attribute Limits: 255
identNetBios	String	Yes	NetBIOS name that is associated with the **identSrc** to further identify the identity event with NetBIOS name resolution. The **identNetBios** parameter is usable by QRadar only when your device provides both the **identSrc** key and **identNetBios** together in an event payload. Attribute Limits: 255
identGrpName	String	Yes	Group name that is associated with the **identSrc** to further identify the identity event with Group name resolution. The **identGrpName** parameter is usable by QRadar only when your device provides both the **identSrc** key and **identGrpName** together in an event payload. Attribute Limits: 255
identMAC	MAC Address	Yes	Reserved for future use in the LEEF format.
vSrc	IPv4 or IPv6 Address	No	The IP address of the virtual event source.
vSrcName	String	No	The name of the virtual event source. Attribute Limits: 255
accountName	String	No	The account name that is associated with the event. Attribute Limits: 255
srcBytes	Integer	No	Indicates the byte count from the event source.
dstBytes	Integer	No	Indicates the byte count to the event destination.
srcPackets	Integer	No	Indicates the packet count from the event source.
dstPackets	Integer	No	Indicates the packet count to the event destination.
totalPackets	Integer	No	Indicates the total number of packets that are transmitted between the source and destination.
role	String	No	The type of **role** that is associated with the user account that created the event, for example, Administrator, User, Domain Admin.
realm	String	No	The **realm** that is associated with the user account. Depending on your device, can be a general grouping or based on region, for example, accounting, remote offices.
policy	String	No	A **policy** that is associated with the user account. This **policy** is typically the security policy or group policy that is tied to the user account.

Table 3. Pre-defined event attributes (continued)

Key	Value type	Normalized event field? Yes or No	Description
resource	String	No	A **resource** that is associated with the user account. This **resource** is typically the computer name.
url	String	No	**URL** information that is included with the event.
groupID	String	No	The **groupID** that is associated with the user account.
domain	String	No	The **domain** that is associated with the user account.

isLoginEvent	Boolean string	No	Identifies if the event is related to a user login, for example,
			`isLoginEvent=true`
			`isLoginEvent=false`
			This key is reserved in the LEEF specification, but not implemented in QRadar.
			Attribute Limits: true or false

isLogoutEvent	Boolean string	No	Identifies if the event is related to a user logout, for example,
			`isLogoutEvent=true`
			`isLogoutEvent=false`
			This key is reserved in the LEEF specification, but not implemented in QRadar.
			Attribute Limits: true or false

identSecondIp	IPv4 or IPv6 Address	No	Identity second IP address represents an IPv4 or IPv6 address that is 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. This key is reserved in the LEEF specification, but not implemented in QRadar.

calLanguage
Attribute Limits: 2
	String	No	Identifies the language of the device time (**devTime**) key to allow translation and to ensure that QRadar correctly parses the date and time of events that are generated in translated 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, for example,
			`calLanguage=fr devTime=avril 09 2014 12:30:55`
			`calLanguage=de devTime=Di 30 Jun 09 14:56:11`
			This key is reserved in the LEEF specification, but not implemented currently in QRadar.
			Attribute Limits: 2

calCountryOrRegion	String	No	Extends the **calLanguage** key to provide more translation information that can 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, for example,
			`calLanguage=de calCountryOrRegion=DE devTime=Di 09 Jun 2014 12:30:55`
			`calLanguage=en calCountryOrRegion=US devTime=Tue 30 Jun 09`
			This key is reserved in the LEEF specification, but not implemented in QRadar.
			Attribute Limits: 2

Note: Non-normalized predefined LEEF event attributes are not automatically parsed for all log source types. However, QRadar provides custom properties (either built-in or from the IBM Security App Exchange) for some of these keys. You can configure custom properties for non-normalized keys to parse by using Regex. To configure a key to parse, the input is *key*=`([^\t]+)`.

The following examples show Regex inputs for non-normalized predefined keys, where the delimiter that follows the caret (^) is a horizontal tab in LEEF V1.0:

- The input for **vSrc** is `vSrc=([^\t]+)`.
- The input for **vSrcName** is `vSrcName=([^\t]+)`.

- The input for **accountName** is `accountName=([^\t]+)`.

The following examples show Regex inputs for non-normalized predefined keys, where the delimiter that follows the caret (^) is a customized separator character in LEEF V2.0:

- If you use # as the delimiter, the input for **vSrc** is `vSrc=([^#]+)`.
- If you use | as the delimiter, the input for **vSrc** is `vSrc=([^|]+)`.

QRadar V7.3.2 or later includes property auto-detection for custom properties of both predefined and custom LEEF event attributes. Property auto-detection makes it easier to configure custom properties, without the use of Regex.

Custom event keys

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

Use custom key value-pair attributes in an event payload when there is no default key to represent information about an event for your appliance. Create custom event attributes only when there is no acceptable mapping to a predefined event attribute. For example, if your appliance monitors access, you can require the file name that is accessed by a user where no file name attribute exists in LEEF by default.

Note: Event attribute keys and values can appear one time only in each payload. Using a key-value pair twice in the same payload can cause IBM Security 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, you 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 about creating a custom event property, see the *IBM QRadar Administration Guide*.

Best practices Guidelines for LEEF events

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

Items that are marked `Allowed` can be included in a key or value, and is not in violation of LEEF but these items are not good practice when you create custom event keys.

The following list contains custom key and value general guidelines:

- 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` - file name=pic07720.gif
  - `Allowed` - file name=pic07720.gif
  - `Allowed` - file name =pic07720.gif
- A user-defined key cannot use the same name as a LEEF predefined key. For more information, see “Predefined LEEF event attributes” on page 4.
- Key values must be human readable, if possible, to help you to investigate event payloads.
  - `Correct` - deviceProcessHash=value
  - `Correct` - malwarename=value
  - `Allowed` - EBFDFBE14D4=value

Custom event date format

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

Use the **devTimeformat** to format the **devTime** event attribute to display the event in IBM Security QRadar. The suggested **devTimeFormat** patterns are listed in the following table:

Table 4. devTimeFormat suggested patterns

devTimeFormat Pattern	Result
devTimeFormat=MMM dd yyyy HH:mm:ss	Jun 06 2015 16:07:36
devTimeFormat=MMM dd yyyy HH:mm:ss.SSS	Jun 06 2015 16:07:36.300
devTimeFormat=MMM dd yyyy HH:mm:ss.SSS z	Jun 06 2015 02:07:36.300 GMT

For more information about specifying a date format, see the SimpleDateFormat information on the Java Web Page (http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html).

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

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

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

IBM Online Privacy Statement

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

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

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

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

General Data Protection Regulation

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

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

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.

Glossary

This glossary provides terms and definitions for the IBM QRadar SIEM software and products.

The following cross-references are used in this glossary:

- *See* refers you from a nonpreferred term to the preferred term or from an abbreviation to the spelled-out form.
- *See also* refers you to a related or contrasting term.

For other terms and definitions, see the IBM Terminology website (opens in new window).

A

accumulator
A register in which one operand of an operation can be stored and subsequently replaced by the result of that operation.

active system
In a high-availability (HA) cluster, the system that has all of its services running.

Address Resolution Protocol (ARP)
A protocol that dynamically maps an IP address to a network adapter address in a local area network.

administrative share
A network resource that is hidden from users without administrative privileges. Administrative shares provide administrators with access to all resources on a network system.

anomaly
A deviation from the expected behavior of the network.

application signature
A unique set of characteristics that are derived by the examination of packet payload and then used to identify a specific application.

ARP
See Address Resolution Protocol.

ARP Redirect
An ARP method for notifying the host if a problem exists on a network.

ASN
See autonomous system number.

asset
A manageable object that is either deployed or intended to be deployed in an operational environment.

autonomous system number (ASN)
In TCP/IP, a number that is assigned to an autonomous system by the same central authority that assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

behavior
The observable effects of an operation or event, including its results.

bonded interface
See link aggregation.

burst
A sudden sharp increase in the rate of incoming events or flows such that the licensed flow or event rate limit is exceeded.

C

CIDR
See Classless Inter-Domain Routing.

Classless Inter-Domain Routing (CIDR)
A method for adding class C Internet Protocol (IP) addresses. The addresses are given to Internet Service Providers (ISPs) for use by their customers. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

client
A software program or computer that requests services from a server.

cluster virtual IP address
An IP address that is shared between the primary or secondary host and the HA cluster.

coalescing interval
The interval at which events are bundled. Event bundling occurs in 10 second intervals and begins with the first event that does not match any currently coalescing events. Within the coalescing interval, the first three matching events are bundled and sent to the event processor.

Common Vulnerability Scoring System (CVSS)
A scoring system by which the severity of a vulnerability is measured.

console
A display station from which an operator can control and observe the system operation.

content capture
A process that captures a configurable amount of payload and then stores the data in a flow log.

credential
A set of information that grants a user or process certain access rights.

credibility
A numeric rating between 0-10 that is used to determine the integrity of an event or an offense. Credibility increases as multiple sources report the same event or offense.

CVSS
See Common Vulnerability Scoring System.

D

database leaf object
A terminal object or node in a database hierarchy.

datapoint
A calculated value of a metric at a point in time.

Device Support Module (DSM)
A configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output.

DHCP
See Dynamic Host Configuration Protocol.

DNS
See Domain Name System.

Domain Name System (DNS)
The distributed database system that maps domain names to IP addresses.

DSM
See Device Support Module.

duplicate flow
Multiple instances of the same data transmission received from different flow sources.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

E

encryption
In computer security, the process of transforming data into an unintelligible form in such a way that the original data either cannot be obtained or can be obtained only by using a decryption process.

endpoint
The address of an API or service in an environment. An API exposes an endpoint and at the same time invokes the endpoints of other services.

external scanning appliance
A machine that is connected to the network to gather vulnerability information about assets in the network.

F

false positive
An event or flow that the user can decide should not create an offense, or an offense that the user decides is not a security incident.

flow
A single transmission of data passing over a link during a conversation.

flow log
A collection of flow records.

flow sources
The origin from which flow is captured. A flow source is classified as internal when flow comes from hardware installed on a managed host or it is classified as external when the flow is sent to a flow collector.

forwarding destination
One or more vendor systems that receive raw and normalized data from log sources and flow sources.

FQDN
See fully qualified domain name.

FQNN
See fully qualified network name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com.

fully qualified network name (FQNN)
In a network hierarchy, the name of an object that includes all of the departments. An example of a fully qualified network name is CompanyA.Department.Marketing.

G

gateway
A device or program used to connect networks or systems with different network architectures.

H

HA
See high availability.

HA cluster
A high-availability configuration consisting of a primary server and one secondary server.

Hash-Based Message Authentication Code (HMAC)
A cryptographic code that uses a cryptic hash function and a secret key.

high availability (HA)
Pertaining to a clustered system that is reconfigured when node or daemon failures occur so that workloads can be redistributed to the remaining nodes in the cluster.

HMAC
See Hash-Based Message Authentication Code.

host context
A service that monitors components to ensure that each component is operating as expected.

I

ICMP
See Internet Control Message Protocol.

identity
A collection of attributes from a data source that represent a person, organization, place, or item.

IDS
See intrusion detection system.

Internet Control Message Protocol (ICMP)
An Internet protocol that is used by a gateway to communicate with a source host, for example, to report an error in a datagram.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network. See also Transmission Control Protocol.

Internet service provider (ISP)
An organization that provides access to the Internet.

intrusion detection system (IDS)
Software that detects attempts or successful attacks on monitored resources that are part of a network or host system.

intrusion prevention system (IPS)
A system that attempts to deny potentially malicious activity. The denial mechanisms could involve filtering, tracking, or setting rate limits.

IP
See Internet Protocol.

IP multicast
Transmission of an Internet Protocol (IP) datagram to a set of systems that form a single multicast group.

IPS
See intrusion prevention system.

ISP
See Internet service provider.

K

key file
In computer security, a file that contains public keys, private keys, trusted roots, and certificates.

L

L2L
See Local To Local.

L2R
See Local To Remote.

LAN
See local area network.

LDAP
See Lightweight Directory Access Protocol.

leaf
In a tree, an entry or node that has no children.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

link aggregation
The grouping of physical network interface cards, such as cables or ports, into a single logical network interface. Link aggregation is used to increase bandwidth and network availability.

live scan
A vulnerability scan that generates report data from the scan results based on the session name.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

Local To Local (L2L)
Pertaining to the internal traffic from one local network to another local network.

Local To Remote (L2R)
Pertaining to the internal traffic from one local network to another remote network.

log source
Either the security equipment or the network equipment from which an event log originates.

log source extension
An XML file that includes all of the regular expression patterns required to identify and categorize events from the event payload.

M

Magistrate
An internal component that analyzes network traffic and security events against defined custom rules.

magnitude
A measure of the relative importance of a particular offense. Magnitude is a weighted value calculated from relevance, severity, and credibility.

N

NAT
See network address translation.

NetFlow
A Cisco network protocol that monitors network traffic flow data. NetFlow data includes the client and server information, which ports are used, and the number of bytes and packets that flow through the switches and routers connected to a network. The data is sent to NetFlow collectors where data analysis takes place.

network address translation (NAT)
In a firewall, the conversion of secure Internet Protocol (IP) addresses to external registered addresses. This enables communications with external networks but masks the IP addresses that are used inside the firewall.

network hierarchy
A type of container that is a hierarchical collection of network objects.

network layer
In OSI architecture, the layer that provides services to establish a path between open systems with a predictable quality of service.

network object
A component of a network hierarchy.

O

offense
A message sent or an event generated in response to a monitored condition. For example, an offense will provide information on whether a policy has been breached or the network is under attack.

offsite source
A device that is away from the primary site that forwards normalized data to an event collector.

offsite target
A device that is away from the primary site that receives event or data flow from an event collector.

Open Source Vulnerability Database (OSVDB)
Created by the network security community for the network security community, an open source database that provides technical information on network security vulnerabilities.

open systems interconnection (OSI)
The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information.

OSI
See open systems interconnection.

OSVDB
See Open Source Vulnerability Database.

P

parsing order
A log source definition in which the user can define the order of importance for log sources that share a common IP address or host name.

payload data
Application data contained in an IP flow, excluding header and administrative information.

primary HA host
The main computer that is connected to the HA cluster.

protocol
A set of rules controlling the communication and transfer of data between two or more devices or systems in a communication network.

Q

QID Map
A taxonomy that identifies each unique event and maps the events to low-level and high-level categories to determine how an event should be correlated and organized.

R

R2L
See Remote To Local.

R2R
See Remote To Remote.

recon
See reconnaissance.

reconnaissance (recon)
A method by which information pertaining to the identity of network resources is gathered. Network scanning and other techniques are used to compile a list of network resource events which are then assigned a severity level.

reference map
A data record of direct mapping of a key to a value, for example, a user name to a global ID.

reference map of maps
A data record of two keys mapped to many values. For example, the mapping of the total bytes of an application to a source IP.

reference map of sets
A data record of a key mapped to many values. For example, the mapping of a list of privileged users to a host.

reference set
A list of single elements that are derived from events or flows on a network. For example, a list of IP addresses or a list of user names.

reference table
A table where the data record maps keys that have an assigned type to other keys, which are then mapped to a single value.

refresh timer
An internal device that is triggered manually or automatically at timed intervals that updates the current network activity data.

relevance
A measure of relative impact of an event, category, or offense on the network.

Remote To Local (R2L)
The external traffic from a remote network to a local network.

Remote To Remote (R2R)
The external traffic from a remote network to another remote network.

report
In query management, the formatted data that results from running a query and applying a form to it.

report interval
A configurable time interval at the end of which the event processor must send all captured event and flow data to the console.

routing rule
A condition that when its criteria are satisfied by event data, a collection of conditions and consequent routing are performed.

rule
A set of conditional statements that enable computer systems to identify relationships and run automated responses accordingly.

S

scanner
An automated security program that searches for software vulnerabilities within web applications.

secondary HA host
The standby computer that is connected to the HA cluster. The secondary HA host assumes responsibility of the primary HA host if the primary HA host fails.

severity
A measure of the relative threat that a source poses on a destination.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SNMP
See Simple Network Management Protocol.

SOAP
A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet.

standby system
A system that automatically becomes active when the active system fails. If disk replication is enabled, replicates data from the active system.

subnet
See subnetwork.

subnet mask
For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address.

subnetwork (subnet)
A network that is divided into smaller independent subgroups, which still are interconnected.

sub-search
A function that allows a search query to be performed within a set of completed search results.

superflow
A single flow that is comprised of multiple flows with similar properties in order to increase processing capacity by reducing storage constraints.

system view
A visual representation of both primary and managed hosts that compose a system.

T

TCP
See Transmission Control Protocol.

Transmission Control Protocol (TCP)
A communication protocol used in the Internet and in any network that follows the Internet Engineering Task Force (IETF) standards for internetwork protocol. TCP provides a reliable host-to-host protocol in packet-switched communication networks and in interconnected systems of such networks. See also Internet Protocol.

truststore file
A key database file that contains the public keys for a trusted entity.

V

violation
An act that bypasses or contravenes corporate policy.

vulnerability
A security exposure in an operating system, system software, or application software component.

W

whois server
A server that is used to retrieve information about a registered Internet resources, such as domain names and IP address allocations.