QRadar Custom Event Properties for IBM z/OS
Version 7.1.0 MR1

Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 13.

CONTENTS

1 CUSTOM EVENT PROPERTIES FOR IBM Z/OS

Custom event properties allow users to provide additional regex fields for specific IBM z/OS-based events to make these fields more visible in searches and reports.

Creating custom event properties allows you to expand QRadar SIEM searching and reporting by normalizing important event data for a log source, making the important data more visible in your system searches and reports. By default, QRadar SIEM includes a number of default custom event properties, but depending on the information that is important to you, a unique custom event property might be required. This technical note describes how to create IBM z/OS specific custom event properties and provides the regex patterns required to parse z/OS specific events.

QRadar SIEM collects events from IBM z/OS using IBM Security zSecure Audit for standard auditing, authorization, and security events. However, depending on your configuration, the event payload might contain a specialized information, which is important to your administrators, but not searchable or available for reports by default. This is because QRadar SIEM stores the event, but the entire event payload is not normalized. The amount of event normalization varies from DSMs in QRadar SIEM.

For example, the following is a sample IBM z/OS event payload to QRadar SIEM in LEEF format.

LEEF:1.0|IBM|z/OS|1.13|14|eventTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSZ eventTime=2012-06-11T15:34:41.12+01:00 usrName=JEFFADMN name= job=EEND 11 Jun 2012 15:34:40.97 JEFFADMN terminal=TEST99 desc= class=DATASET res=EEND.ISPF.ISPLLIB prof= vol=EENDSY CO73 *SMS* Z180R2 Z180R1 dsn=EEND.ISPF.ISPLLIB own= box=ASSET75-D358 ASSET75-BA48 ASSET75-0000000 ASSET75-D335 ASSET75-D334 sum=JEFFADMN Input activity for concatenation starting with EEND.ISPF.ISPLLIB

Each line of the event log contains the event payload, such as timestamp, user, description, source, destination, and other event payload information corresponding to the LEEF format, if present in the event payload. These LEEF events are normalized and searchable in QRadar SIEM. However, the event payload also contains events specific to IBM z/OS, which are outside of the LEEF specification and not normalized. These fields in the event payload are specific to IBM z/OS, but contain important information, such as the DD name, job name, job ID, terminal, class, dsn, sum, or member name. You can create a custom event

property to extract this information from the logs, and then use the event property in event searches and reports.

QRadar SIEM supports log sources from IBM z/OS images for the following products:

- IBM z/OS
- IBM Resource Access Control Facility (RACF)
- IBM DB2
- IBM Customer Information Control System (CICS)
- CA Technologies Access Control Facility (ACF2)
- CA Technologies Top Secret

Before you begin

To create custom event properties, you must have the User Defined Event Properties permission.

Check with your administrator to ensure you have the correct permissions. For more information on permissions, see the *IBM Security QRadar SIEM Administration Guide*.

Creating a Regex-based custom event property

A custom event property can be associated with one or multiple regular expressions.

About this task

When an event is parsed, each regex pattern is tested on the event until a regex pattern matches the payload. The first regex pattern to match the event payload determines the data to be extracted for the custom event.

Custom event properties window parameters

Table 1-1 Custom event properties window parameters

Parameter	Description
Test Field	Type the unnormalized event from your z/OS DSM that you'd like to normalize from the payload. For example, terminal=TEST99.
Property definition	
Existing Property	To select an existing property, select this option and then select a previously saved property name from the list box.
New Property	To create a new property, select this option and then type a unique name for this custom event property. ***Note:*** *The new property name cannot use the name of an existing normalized event property, such as Username, Source IP, or Destination IP.*

Table 1-1 Custom event properties window parameters (continued)

Parameter	Description
Optimize parsing for rules, reports, and searches	To parse and store the property the first time QRadar SIEM receives the event, select this check box. When you select the check box, the property does not require additional parsing for reporting, searching, or rule testing. If you clear this check box, the property is parsed each time a report, search, or rule test is performed. By default, this option is disabled.
Field Type	From the list box, select the field type. The field type determines how the custom event property is displayed in QRadar SIEM and which options are available for aggregation. The field type options are: • Alpha-Numeric • Numeric • IP • Port The default is Alpha-Numeric.
Description	Type a description of this custom event property.
Property expression definition	
Log Source Type	From the list box, select the type of log source to which this custom event property applies.
Log Source	From the list box, select the log source to which this custom event property applies. If there are multiple log sources associated with this event, this field specifies the term Multiple and the number of log sources.
Event Name	To specify an event name to which this custom event property applies, select this option. Click **Browse** to access the Event Browser and select the QRadar SIEM Identifier (QID) for the event name you want applied to this custom event property. By default, this option is enabled.
Category	To specify a low-level category to which this custom event property applies, select this option. To select a low-level category: **1** From the **High Level Category** list box, select the high-level category. The **Low Level Category** list updates to include only the low-level categories associated with the selected high-level category. **2** From the **Low Level Category** list box, select the low-level category to which this custom event property applies.

Table 1-1 Custom event properties window parameters (continued)

Parameter	Description
RegEx	Type the regular expression you want to use for extracting the data from the payload. Regular expressions are case-sensitive. The following regex patterns are available for IBM z/OS-based event sources: • For CA ACF2 regex patterns, see **Creating CA ACF2 custom event properties**. • For CA Top Secret regex patterns, see **Creating CA Top Secret custom event properties**. • For IBM z/OS, see **Creating IBM z/OS custom event properties**. • For IBM RACF, see **Creating IBM RACF custom event properties**. • For IBM DB2, see **Creating IBM DB2 custom event properties**. • For IBM CICS, see **Creating IBM CICS custom event properties**. ***Note:*** *Capture groups must be enclosed in parenthesis.*
Capture Group	Type the capture group you want to use if the regex contains more than one capture group. Capture groups treat multiple characters as a single unit. In a capture group, characters are grouped inside a set of parentheses.
Test	Click **Test** to test the regular expression against the payload.
Enabled	Select this check box to enable this custom event property. If you clear the check box, this custom event property does not display in event search filters or column lists and the event property is not parsed from payloads.

Procedure to create a custom event property

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

Step 3 In the **Data sources** window, click the **Custom Event Properties** icon.

Step 4 Click **Add**.

Step 5 In the Property Type Selection pane, select the **Regex Based** option.

Step 6 Configure the custom event property parameters. Refer to **Table 1-1** in About this task section.

Step 7 Click **Test** to test the regular expression against the payload.

Step 8 Click **Save**.

Results

The custom event property is now displayed as an option in the list of available columns when you search for events using the **Log Activity** tab in QRadar SIEM.

Note: Custom event properties are not automatically included in event listings. To include a custom event property in an events list, you must select the custom event property from the list of available columns when creating a search.

Creating CA ACF2 custom event properties

Regex patterns are available for CA Technologies Access Control Facility (ACF2) custom event properties in QRadar SIEM.

Table 1-2 CA Technologies ACF2 Regex patterns

Description	Regex for custom event property
Event summary	sum=([^\t]+)
Access intent	intent=([^\t]+)
Data set name	dsn=([^\t]+)
Log string	logstr=([^\t]+)
Person name	name=([^\t]+)
Physical DASD box serial	box=([^\t]+)
SAF class	class=([^\t]+)
SNA terminal name	terminal=([^\t]+)
Volume serial	vol=([^\t]+)
System SMF id	job=([^\t]{4})
Job name	job=[^\t]{29}([^\t]{8})
Resource sensitivity	sens=([^\t]+)
Sensitive user permissions	usrPriv=([^\t]+)
Sensitive groups	usrGroups=([^\t]+)

Creating CA Top Secret custom event properties

Regex patterns are available for CA Technologies Top Secret custom event properties in QRadar SIEM.

Table 1-3 CA Technologies Top Secret Regex patterns

Description	Regex for custom event property
Event summary	sum=([^\t]+)
Data set name	dsn=([^\t]+)
Descriptor	desc=([^\t]+)
Physical DASD box serial	box=([^\t]+)
Private / Owned data set	own=([^\t]+)
SAF class	class=([^\t]+)

Table 1-3 CA Technologies Top Secret Regex patterns (continued)

Description	Regex for custom event property
SAF resource name	res=([^\t]+)
SNA terminal name	terminal=([^\t]+)
System / Job	job=([^\t]+)
Volume serial	vol=([^\t]+)
System SMF id	job=([^\t]{4})
Job name	job=[^\t]{29}([^\t]{8})
Resource sensitivity	sens=([^\t]+)
Sensitive user permissions	usrPriv=([^\t]+)
Sensitive groups	usrGroups=([^\t]+)

Creating IBM z/OS custom event properties

Regex patterns are available for IBM z/OS custom event properties in QRadar SIEM.

Table 1-4 IBM z/OS Regex patterns

Description	Regex for custom event property
Event summer	sum=([^\t]+)
Access intent	intent=([^\t]+)
Catalog	catalog=([^\t]+)
Command	cmd=([^\t]+)
Completion code	compCode=([^\t]+)
Completion status	compStat=([^\t]+)
Data set name	dsn=([^\t]+)
DD name	dd=([^\t]+)
Descriptor	desc=([^\t]+)
Function code	function=([^\t]+)
JES line	line=([^\t]+)
JES remote terminal line	rmt=([^\t]+)
Job number	jobid=([^\t]+)
Member name	member=([^\t]+)
NJE node name	node=([^\t]+)
Old data set name	oldda=([^\t]+)
Person name	name=([^\t]+)
Physical DASD box serial	box=([^\t]+)
Port of entry	poe=([^\t]+)
Private / owned data set	own=([^\t]+)
Program	program=([^\t]+)

Table 1-4 IBM z/OS Regex patterns (continued)

Description	Regex for custom event property
RACF profile	prof=([^\t]+)
SAF class	class=([^\t]+)
SAF resource name	res=([^\t]+)
SNA terminal name	terminal=([^\t]+)
Step name	stepname=([^\t]+)
Submitted by	submitby=([^\t]+)
System / job	job=([^\t]+)
UNIX path name	path=([^\t]+)
Volume serial	vol=([^\t]+)
System SMF id	job=([^\t]{4})
Job name	job=[^\t]{29}([^\t]{8})
Resource sensitivity	sens=([^\t]+)
Sensitive user privileges	usrPriv=([^\t]+)
Sensitive groups	usrGroups=([^\t]+

Creating IBM RACF custom event properties

Regex patterns are available for IBM Resource Access Control Facility (RACF) custom event properties in QRadar SIEM.

Table 1-5 IBM RACF Regex Patterns

Description	Regex for custom event property
Event summer	sum=([^\t]+)
Access intent	intent=([^\t]+)
Application name	appl=([^\t]+)
Command	cmd=([^\t]+)
Data set name	dsn=([^\t]+)
Descriptor	desc=([^\t]+)
Identity context name	ICTXname=([^\t]+)
Identity context registry	ICTXreg=([^\t]+)
Log string	logstr=([^\t]+)
RACF authority used	auth=([^\t]+)
Person name	name=([^\t]+)
Physical DASD box serial	box=([^\t]+)
Port of entry	poe=([^\t]+)
Private / owned data set	own=([^\t]+)
RACF profile	prof=([^\t]+)
SAF class	class=([^\t]+)

Table 1-5 IBM RACF Regex Patterns (continued)

Description	Regex for custom event property
SAF resource name	res=([^\t]+)
SNA terminal name	terminal=([^\t]+)
Submitted by	submitby=([^\t]+)
System / job	job=([^\t]+)
UNIX path name	path=([^\t]+)
Volume serial	vol=([^\t]+)
System SMF id	job=([^\t]{4})
Job name	job=[^\t]{29}([^\t]{8})
Resource sensitivity	sens=([^\t]+)
Sensitive user privileges	usrPriv=([^\t]+)
Sensitive groups	usrGroups=([^\t]+

Creating IBM DB2 custom event properties

Regex patterns are available for IBM DB2 custom event properties in QRadar SIEM.

Table 1-6 IBM DB2 Regex patterns

Description	Regex for custom event property
Event summer	sum=([^\t]+)
Access intent	intent=([^\t]+)
Data set name	dsn=([^\t]+)
Person name	name=([^\t]+)
Port of entry	poe=([^\t]+)
Submitted by	submitby=([^\t]+)
System / job	job=([^\t]+)
System SMF id	job=([^\t]{4})
Job name	job=[^\t]{29}([^\t]{8})
Resource sensitivity	sens=([^\t]+)
Sensitive user privileges	usrPriv=([^\t]+)
Sensitive groups	usrGroups=([^\t]+
Current SQL id	SQLid=([^\t]+)
Object types	objtyp=([^\t]+)
Object names	obj=([^\t]+)
Plan	plan=([^\t]+)
Subsystem name	subsys=([^\t]+)
Command	cmd=([^\t]+)

Creating IBM CICS custom event properties

Regex patterns are available for IBM Customer Information Control System (CICS) custom event properties in QRadar SIEM.

Table 1-7 IBM CICS Regex patterns

Description	Regex for custom event property
Event summary	sum=([^\t]+)
Application name	appl=([^\t]+)
CICS terminal id	CICStrm=([^\t]+)
Completion status	compStat=([^\t]+)
Person name	name=([^\t]+)
Remote network	netrmt=([^\t]+)
SNA global network name	net=([^\t]+)
SNA terminal name	terminal=([^\t]+)
System / Job	job=([^\t]+)
Transaction name	tran=([^\t]+)
System SMF id	job=([^\t]{4})
Job name	job=[^\t]{29}([^\t]{8})
Resource sensitivity	sens=([^\t]+)
Sensitive user permissions	usrPriv=([^\t]+)
Sensitive groups	usrGroups=([^\t]+)

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*.

UNIX is a registered trademark of The Open Group in the United States and other countries.