

QRadar™ Open Mic: Custom Properties

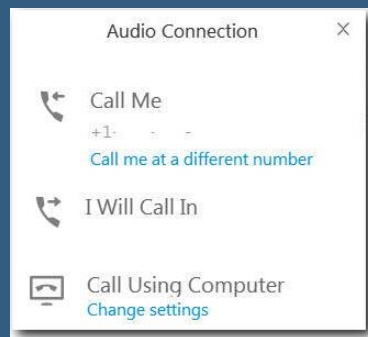
IBM SECURITY SUPPORT OPEN MIC

To hear the WebEx audio, **select an option** in the Audio Connection dialog or by access the Communicate > Audio Connection menu option. To ask a question by voice, you must either Call In or have a microphone on your device.

You will not hear sound until the host opens the audio line.

For more information, visit:

http://ibm.biz/WebExOverview_SupportOpenMic



Slides and additional dial in numbers:

<http://ibm.biz/JoinQRadarOpenMic>

NOTICE: BY PARTICIPATING IN THIS CALL, YOU GIVE YOUR IRREVOCABLE CONSENT TO IBM TO RECORD ANY STATEMENTS THAT YOU MAY MAKE DURING THE CALL, AS WELL AS TO IBM'S USE OF SUCH RECORDING IN ANY AND ALL MEDIA, INCLUDING FOR VIDEO POSTINGS ON YOUTUBE. IF YOU OBJECT, PLEASE DO NOT CONNECT TO THIS CALL.

Announcements

- QRadar 7.3.0 Patch 6 is released and includes 57 resolved issues.
- An interim fix 01 for 7.3.0 Patch 6 is being posted today for a list of release notes, see <https://ibm.biz/qradarsoftware>.
- QRadar Community Edition is now available for all users. QRadar Support does not do phone support for QRadar Community Edition. Administrators can use the tag 'qradarce' in the forums to ask questions about QRadar Community Edition.

For questions, see <https://ibm.biz/qradarceforums>

For the software, see <https://ibm.biz/qradarce>

- User Behavior Analytics v2.4.0 is now on the IBM App Exchange.



A Quick Introduction



Log Sources

- The primary method for how QRadar gets data from event sources.
- A log source is made up of two components: The Protocol and the DSM.
- The Protocol is how the data gets into QRadar.
- The DSM concerns how the data is parsed.

Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources. Because this log source was auto-discovered, its connection information is not modifiable.

Log Source Name	Pix @ 172.16.158.160
Log Source Description	Pix device
Log Source Type	Cisco PIX Firewall
Protocol Configuration	Syslog
Log Source Identifier	172.16.158.160
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: BIZDEV
Coalescing Events	<input checked="" type="checkbox"/>
Incoming Payload Encoding	UTF-8
Store Event Payload	<input checked="" type="checkbox"/>

Please select any groups you would like this log source to be a member of:

SaveCancel

Device Support Modules (DSMs)

- The parsing component of the log source.
- Normalizes event data to fit into the QRadar Normalized Event Model.
- Custom properties are not part of the DSM to process normalized events.

Return to Event List Offense Map Event False Positive Extract Property Previous Next Print Obfuscation

Event Information

Event Name	Built TCP connection							
Low Level Category	Firewall Session Opened							
Event Description	A TCP connection slot between two hosts was created.							
Magnitude	<div><div></div></div>	(5)	Relevance	9	Severity	2	Credibility	5
Username	N/A							
Start Time	Sep 16, 2016, 11:23:34 AM	Storage Time	Sep 16, 2016, 11:23:34 AM		Log Source Time	Sep 16, 2016, 11:23:42 AM		
Domain	Default Domain							

Source and Destination Information

Source IP	172.16.150.147	Destination IP	192.168.1.1
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	47915	Destination Port	3260
Pre NAT Source IP	172.16.150.147	Pre NAT Destination IP	192.168.1.1
Pre NAT Source Port	47915	Pre NAT Destination Port	3260
Post NAT Source IP	156.34.252.10	Post NAT Destination IP	192.168.1.1
Post NAT Source Port	63945	Post NAT Destination Port	3260
IPv6 Source	0:0:0:0:0:0:0:0	IPv6 Destination	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf hex base64

☐ Wrap Text

*PIX-6-302013: Built outbound TCP connection 7787953 for outside:192.168.1.1/3260 (192.168.1.1/3260) to inside:172.16.150.147/47915 (156.34.252.10/63945)

Normalized Event Data vs Custom Properties

Normalized events are the standard values that we populate in the user interface that present a common and make data which is broadly applicable available in a consistent presentation. Data like the date and time an event occurred, the user involved in the event, and information about endpoints/assets involved in the event (IP addresses, ports, MAC addresses) are almost universally relevant to all events and so these values are considered normalized event data.

Normalized event fields include:

- Source IP
- Destination IP
- MAC Address
- Username
- Port
- Protocol
- Pre-NAT values (source, dest, ports)
- Post-NAT values (source, dest, ports)
- HostName (identity-related)
- GroupName (identity-related)
- NetBIOSName (identity-related)
- ExtraIdentityData (identity-related)

Custom Properties are used to parse values from event payloads which do not align with the Normalized event fields. These allow administrators to display information in the user interface as '**name(custom)**' to be used across QRadar.

Event Information	
Event Name	Success Audit: Successful login with administrative or special privileges
Low Level Category	Admin Login Successful
Event Description	Success Audit: Successful login with administrative or special privileges
Magnitude	<div><div></div><div></div><div></div><div></div></div> (2)
Username	Administrator
Start Time	Nov 29, 2017, 1:58:06 AM
Accesses (custom)	N/A
AccountDomain (custom)	N/A
AccountID (custom)	N/A
AccountName (custom)	Administrator
ChangedAttributes (custom)	N/A
EventID (custom)	4672
GroupID (custom)	N/A

Normalized Event Data vs Custom Properties (continued)

You can think of custom properties as a quick reference for a value that falls outside of normalized data, such as source zone, destination zone, policy, or server name. As this data might be important and administrators might want to be able to provide these filters to users to assist with searches.

For example, let's look at a payload from a IDP event.

```
<26> 1 2011-05-01T22:43:12 10.10.150.3 Jnpr Syslog 32743 1
[syslog@juniper.net dayId="20170501" recordId="659" timeRecv="2017/05/01
22:43:12" timeGen="2017/05/02 03:13:12" domain="" devDomVer2="751"
device_ip="10.10.150.3" cat="Predefined" attack="HTTP:XSS:X-FORWARDED-FOR-
INJ" srcZn="DMZ" srcIntf="NULL" srcAddr="193.5.216.100" srcPort="47255"
natSrcAddr="169.5.216.100" natSrcPort="47255" dstZn="TRUSTED" dstIntf="NULL"
dstAddr="169.128.28.10" dstPort="80" natDstAddr="10.100.127.1"
natDstPort="80" protocol="TCP" servername="CardServer15" ruleVer="0"
policy="31" rulebase="IDS"
```

In this example you will see common values that are part of our normalized data for the event, such as IP, port information, NAT, etc. This payload also contains a number of highlighted values that might be important to the administrator where a custom property might provide useful data.

Types of Custom Properties

Custom **Event** Properties allow for event payload information to be extracted and presented in its own field in the Log Activity user interface.

Custom **Flow** Properties allow for flow information to be extracted and presented in its own field in the Network Activity user interface.

Custom **Asset** Properties allow administrators to assign a name to an asset group, which can then be leveraged in Asset tab searches. These are not regex-based values, but manually assigned definitions, which can then be searched.

AQL Custom Properties (coming soon)



Custom Properties and the User Interface



Custom Event Properties

- Allows users to define event properties not covered by the Normalized Event Fields.
- Divided into three parts: The test field, property definition and the expression definition.
- Custom Properties can be associated with specific log source types, log sources, high level categories, low level categories, or even specific QIDmap entries. This ensures not all Custom Properties are applied to all events that are received by QRadar and allows the admin to decide on usage.

Test Field

<158>Nov 16 2006 14:04:11: %PIX-6-302014: Teardown TCP connection 117396798 for DMZ-1:10.141.9.175/3010 to inside:10.130.9.31/6000 duration 0:00:01 bytes 462 TCP FINs

Property Definition

☒ Existing Property: Bytes☐ New Property: ☐ Optimize parsing for rules, reports, and searchesField Type: NumericDescription: Default custom extraction of Bytes from DSM payload.

Property Expression Definition

Enabled: ☐

Selection

Log Source Type: Cisco PIX FirewallLog Source: All☐ Event Name: Please browse for an event

Browse

☒ Category: High Level Category AnyLow Level Category Any

Extraction

Regex: bytes (ld+)Capture Group: 1

Test

Format

Extracted Number Format:

1,234,567.89 English (United States)

10 IBM Security

Custom Properties in the DSM Editor (continued)

- To add a custom property to the DSM simply click the plus above the normalized properties.
- Once selected, you can set the property expression like any of the normalized fields.
- You can Change the Selectivity so that the property only fires on certain events rather than all the time
- You can also set to have the property enabled or disabled by default. Custom Properties are calculated in a brute force fashion so customers often like having them disabled to start out, and then turn on the ones they see as important.

The screenshot displays the DSM Editor interface. The 'Properties' tab is active, showing a list of properties. A 'Filter' input field is at the top. Below it, the 'Property Configuration' section is visible, showing 'Expressions (1)' with a green plus icon. A modal dialog titled 'Expression' is open, showing the configuration for a custom property. The 'Regex' field contains 'sensorName=\"\"([^\"]*)\"\"'. The 'Capture Group' is set to '1'. The 'Selectivity' is set to 'Edit'. The 'Enabled' checkbox is checked, and the button is labeled 'Enabled'. 'Ok' and 'Cancel' buttons are at the bottom right of the dialog.

Below the dialog, the 'Identity Extended Field' section is visible, showing 'Text'.

On the right side, the 'Log Activity Preview' section shows a preview of the payloads in configuration. It includes a table with columns 'Hostname (custom)' and 'Destination'.

Hostname (custom)	Destination
Sensor-1	198.1
Sensor-1	198.1
Sensor-1	127.0
Sensor-1	127.0

Multiple Custom Properties in the DSM Editor (continued)

Multiple custom properties are represented by Expressions (#) and can be used to deal with variations in format. It is recommended that multiple expressions be used, instead of complex regex when the data differs drastically.

Log Source Type

Microsoft Windows Security Event Log

Change

Properties

Event Mappings

Filter

+

Property Configuration

Expressions (2)

Expression

Regex

EventID=(id+)

Capture Group

1

Edit

Expression

Regex

\\d{1,2}\\:\\d{1,2}\\:\\d{1,2}\\s+\\d{1,4}\\s+(\\d{3,5})

Capture Group

1

Workspace

Use sample event payloads to help fine tune the behavior of this Log Source Type. Matches in the payload are highlighted in the workspace. Note: System properties that have not been overridden cannot be highlighted in the workspace.

☒ Wrap Content

<13>Nov 29 04:07:43 WIN2K12 AgentDevice=WindowsLog AgentLogFile=on=7.2.7.20 Source=Microsoft-Windows-Security-Auditing ComputerName=lab OriginatingComputer=WIN2K12 User= Domain= EventID=4624 EventType=8 EventCategory=12544 RecordNumber=481262142853 TimeWritten=1511942853 Level=0 Keywords=0 Task=0 Opcode=0 account was successfully logged on. Subject: Security ID: NULL SII count Domain: - Logon ID: 0x0 Logon Type: 3 New Logon: Security

Log Activity Preview

A preview of the payloads in the Workspace as they would appear in the Log Activity viewer using the current configuration.

Accesses (custom)	AccountDomain (custom)	AccountID (custom)	AccountName (custom)	Call Trace (custom)
			-	



1

2

Custom Properties in the DSM Editor

- It is highly recommended to base a custom property on an existing one if something similar already exists in the list.
- Custom Properties are made up of 2 parts. The property itself and an expression. There is only ever one property so that it can be shared across DSMs, but each can have its own expression.
- A DSM can also have multiple expressions for a given property if some event sets give the same information in slightly different ways.
- Properties can be set to be optimized for Rules or indexes can be enabled for searches.

Choose a Custom Property Definition to Express

Select an existing Custom Property Definition to express. Make a selection from the list or create a new Custom Property Definition. Definitions can be expressed across multiple Log Source Types.

<input type="checkbox"/>	ACF2 rule key Text Optimized admin
<input type="checkbox"/>	AVT-App-Category Text admin
<input type="checkbox"/>	AVT-App-Name Text admin AVT-App-Name
<input type="checkbox"/>	AVT-App-VolumeBytes Number admin
<input type="checkbox"/>	Access allowed Text Optimized admin
<input type="checkbox"/>	Access intent Text Optimized admin
<input type="checkbox"/>	Accesses Text admin

Selected: None

Create New

Select

Cancel



Optimizing & Indexing



Optimized Custom Properties

Optimized means that the custom properties are part of the event record written to disk, and therefore any reports and searches run after initial processing that depend on those properties can simply retrieve them, rather than having to parse them out of the payload on demand. Custom Properties which are not optimized parse out the values on demand when something attempts to access the event record. When you optimize, the values are pre-parsed and the data is stored and allows it to run without having to run the regex to retrieve the values.

Only check off 'Optimize' if you actually need the properties for rules.

If you have a property used often, optimizing it will help with other parts of the product, such as reports, searches, and dashboards as the pre-parsed data is faster than running the regex. However, using optimization for gaining speed outside of rules should be considered carefully.

Indexed Custom Properties

When you want to leverage certain properties for faster searching in QRadar, administrators can enable an index for a custom property, which requires you to optimize the value. This allows you to use custom properties in searches to get quick results from the indexed values.

✓ Enable Index ✗ Disable Index

Display: Last 30 Days

View: All

Database: Events

Show: Custom

Index management allows you to control database indexing, which can optimize search performance for frequently

WARNING : Enabling indexing on too many properties, can have a negative impact on system performance. It is in

Indexed	Property
●	Action (custom)
●	EventID (custom)
	UserType (custom)
	SHA1 Hash (custom)
	Parent (custom)
	Submitted by (custom)
	Flows per Second - Average 15 Min (custom)
	ParentImage (custom)



Tips and Best Practices



Best practices

- Content packs from the X-Force App Exchange contain custom properties that might be useful for popular event sources.
- Look for existing regular expressions to use as examples.
- Consolidate common properties for data that has structured format where you can.
- Create multiple custom properties to deal with variations in the data format, instead of trying to create complex regex.

AccountName	Microsoft Windows Security Event Log	New Account Name: (.*)
AccountName	Microsoft Windows Security Event Log	Account Name:\s*(.+) \s+(Additional Information Account Domain Service Infor...
AccountName	Microsoft Windows Security Event Log	Account Name:\s*(.+) \s+(Additional Information Account Domain Service Infor...
AccountName	Microsoft Windows Security Event Log	Target Account Name: (.*)

- Only optimize when you need to use a custom property in a rule.

Rule

Apply AWS Cloud: Multiple Failed Console Logins from Different Source IPs on events which are detected by the Local system
and when the event(s) were detected by one or more of Amazon AWS CloudTrail
and when the event category for the event is one of the following Audit.General Audit Event
and when any of Action (custom) match Failure
and when at least 25 events are seen with the same Destination IP and different Source IP in 2 minutes

Common mistakes with custom properties

- Do not use greedy regular expressions.

Using greedy quantifiers (.?) or (.+?) by themselves. If you use them, you are wild card matching against the payload to identify these values. If you know what content you are looking for, then it is better use \d or \w.

- Combining different formats in to a single property, for example CSV format with name=value pairs in a single custom property regular expression.
- Trying to do too much in a single property, such as large numbers of capture groups. We specifically limit regex to 10 capture groups in the DSM Editor.
- Optimizing too many properties
- Extremely rigid patterns can cause you issues



Using Custom Properties in Advanced Searches



Using Custom Properties in AQL statements

Custom properties can be used throughout your AQL statement. In most cases, you can call the custom property directly, unless it contains spaces where you would require double-quotes.

NOTE: The custom property must be enabled to be used in an AQL statement.

```
SELECT Bluecoat-cs-host, sourceip, Bluecoat-cs-uri FROM events
WHERE LOGSOURCEGROUPNAME(devicegroupname)
ILIKE '%Proxies%' AND Bluecoat-cs-host ILIKE '%facebook.com%'
GROUP BY sourceip
```

Bluecoat-cs-host = Hostname from the client's requested URL.

Bluecoat-cs-uri = The original URL requested.

```
SELECT "Changed User" from events where "Changed User" = 'admin'
```



New Custom Property Features in QRadar 7.3.1



JSON Support in Custom Properties

- In QRadar 7.3.1 a new feature is being provided to assist users with improved JSON property support. This new JSON support allows users to configure parsing of both standard/normalized and custom properties from JSON events without needing to use regex. This makes JSON data easier to consume when there is no DSM available and runs more efficiently for the system than using regex, which is typically a brute-force match for the regex to the payload values.
- In Log Source Extensions, users can now put a JSON keypath expression in their <pattern> elements, as long as they set the “type” attribute to “JsonKeypath”. They can then reference these patterns inside their <match-group> elements by using <json-matcher> elements instead of the original <matcher> elements. No capture-group value is necessary because the JSON keypath specifies a particular JSON value (or set of values, if multiple values are used)

JSON Keypaths in the User Interface

DSM Editor JSON Expression Interface

The screenshot shows the 'Properties' tab of the DSM Editor. A 'Filter' input field is at the top. Below it, the 'Property Configuration' section has a checked 'Override system behavior' checkbox and an 'Expressions (1)' section with a green plus icon. An 'Expression' dialog box is open, showing a dropdown menu for 'Expression Type' with options 'Regex', 'JSON', and 'Capture Group'. A red arrow points to the 'JSON' option. The dialog also has 'Ok' and 'Cancel' buttons.

Custom Property JSON Expression Interface

The screenshot shows the 'Property Expression Definition' dialog. It has an 'Enabled' checkbox which is checked. Under the 'Selection' section, there are fields for 'Log Source Type' (a dropdown), 'Log Source' (a dropdown with 'All' selected), and 'Event Name' (radio button selected) with a 'Browse' button. There are also 'High Level Category' and 'Low Level Category' dropdowns. At the bottom, the 'Extraction using' section has two radio buttons: 'Regex' and 'JSON Keypath' (which is selected). Below this is a text input field for the 'JSON Keypath'. A red arrow points to this section. A 'Save' button is at the bottom right.

Using JSON Keypaths (continued)

Given the JSON data on the right, the examples on the left show how to reference different fields

- To capture the “action” value, the expression is:

`/"action"`

- To capture the “username” value, the expression is:

`/"client"/"username"`

- To capture the 1st “address” value, the expression is:

`/"client"/"address"`

- To capture the 2nd “address” value, the expression is:

`/"target"/"address"`

- To capture the “port” value, the expression is:

`/"target"/"port"`

```
{
  "action": "login",
  "client":
  {
    "username": "Bruce",
    "address": "10.0.2.15"
  },
  "target":
  {
    "address": "10.100.100.90",
    "port": 80
  }
}
```

Automatic Custom Property Discovery in the DSM Editor

The DSM Editor can support automatic creation of custom properties for JSON event data. This is toggled using an “Enable Auto Property Discovery” feature.

Work flow for users

1. Launch the DSM Editor.
2. Create (or select an existing) log source type with has JSON-formatted event data
3. Go to the Configuration tab in the left-side pane of the DSM Editor
4. Click the “Enable Auto Property Discovery” toggle to show additional property discovery configuration
5. Select a “Property Discovery Format” as JSON
6. Toggle the “Enable Properties for use in Rules and Search Indexing” switch if you want discovered properties to be optimized by default.
7. If desired, adjust the Discovery Completion Threshold value. This number represents the number of consecutive events received by this log source type without new properties being discovered that should trigger discovery to turn itself off. The idea being that if X events go by without any new properties, then stop trying to auto create values.
8. After events for this log source type enter the system, the properties will automatically get created. The user may choose to go into the DSM Editor at any time to remove or modify any autodiscovered properties they want to get rid of or adjust.



AQL Custom Property Feature in QRadar 7.3.1



AQL Custom Properties

With AQL-based custom event or custom flow properties, you can use an AQL expression to extract data that IBM QRadar does not typically normalize and display from the event or flow payload. For example, users can create an AQL-based property when they want to combine multiple extraction and calculation-based properties, such as URLs, virus names, or secondary user names, into a single property. The new property can be used in custom rules, searches, reports, or they can use it for indexing offenses.

AQL custom properties are used like any other custom property and can enrich user information, or concatenate multiple properties in to a single value.

The screenshot displays the IBM QRadar Rule Wizard interface, specifically the 'Offense Indexing' tab. The interface is divided into several sections:

- Rule Wizard:** Contains options for indexing offenses, such as 'Index offense based on', 'Annotate this offense', and 'Include detected events'.
- Rule Response:** Allows users to choose the response(s) to make when an offense is detected, including 'Dispatch New Event'.
- Event Details:** Provides fields for event information, including 'Event Name', 'Event Description', 'Severity', 'Credibility', and 'High-Level Category'.
- Advanced View Definition:** Features a search bar and a list of available columns for filtering, including 'Source IP', 'Destination IP', 'Username', and various bandwidth manager filters.

A search bar is visible in the center, and a 'Rule Wizard - Google Chrome' window is open in the background, showing a URL: <https://172.16.184.59/console/do/rule>.

AQL Custom Properties (continued)

For example, in a multi domain environment, an IP address on its own does not hold much meaning for the SOC analyst and should include information about the domain.

AQL custom properties allow users to chain together unique properties, such as:

property 1, property 2, property 3,

That can then be called using a single custom property value.

Custom Event Properties

In the AQL Expression field, type the event or flow properties, separated by a comma, that you want to include in the custom property. When two or more properties are specified, the result is shown as concatenated text. You can specify a delimiter to make the results easier to read.

For example, type `property1,'|',property2,'|',property3`.

Do not type SELECT, FROM, or the database name in the AQL expression. Aggregate functions and AQL properties are not supported.

Note: Custom fields are not indexed and may increase the time it takes to run searches and reports.

Property Definition

Tenant:

Ricks Company

Property Name:

Source IP with Domain

Description:

AQL Property Definition

AQL Expression:

`sourceip,':',sourceport,'-',DOMAINNAME(domainid)`

Enabled:

☒

Save

AQL Custom Properties (continued)

Other scenarios for concatenation of values to a single property could be to leverage:

- Hostname and Username
- Source IP and Username
- Username and URL
- Complex calculation through AQL function

Advanced Search

Search

Viewing real time events (Paused) View: Select An Option: Display: Custom

Current Filters:
Domain is not Default Domain (Clear Filter)

	Event Name	Log Source	Event Count	Start Time	Low Level Category	Source IP with Domain (custom)
	Deny inbound	Pix @ apop...	1	Oct 12, 2017, 4:41:1...	Firewall Deny	172.183.107.237:0-Ricks Company Domain
	Deny inbound	Pix @ apop...	1	Oct 12, 2017, 4:41:1...	Firewall Deny	62.246.132.111:0-Ricks Company Domain
	No translation group ...	Pix @ apop...	1	Oct 12, 2017, 4:41:1...	No Translatio...	172.16.151.2:47190-Ricks Company Domain
	Deny protocol src	Pix @ apop...	1	Oct 12, 2017, 4:41:1...	Firewall Deny	172.16.151.2:47190-Ricks Company Domain

All Offenses > Offense 63 (Summary)

Offense 63

Magnitude	1	Status	Relevance	4	Severity	2	Credibility	2
Description	DELETED SCAN FIN	Offense Type	Source IP with Domain (custom)					
		Event/Flow count	1 events and 0 flows in 1 categories					
Source IP(s)	172.16.60.171	Start	May 9, 2016, 11:24:12 AM					
Destination IP(s)	172.16.210.84	Duration	0s					
Network(s)	Net-10-172-192-Net-172_16_0_0	Assigned to	Unassigned					
Offense Source Summary								
Custom property value	172.16.60.171:47190-Ricks Company							
Offenses	1						Events/Flows	1



Troubleshooting & Support



Troubleshooting

Custom properties will generate notifications for Expensive Custom Properties. There are also messages in /var/log/qradar.log that have data about custom properties and their performance.

For example: QID = 38750138. Performance degradation was detected in the event pipeline. Expensive custom properties were found.

```
Nov 22 16:01:30 127.0.0.1 [Timer-63]
com.q1labs.semsources.filters.normalize.DSMFilter: [WARN]
[NOT:0080014100][10.10.10.10/- -] [-/- -]Expensive Log Source or Log
Source Extensions Based On Average Throughput in the last 60 seconds
(most to least expensive) - (.+?)=19.0eps, (\w+)/\S+=1136.0eps
```




Questions



Questions for the panel

Now is your opportunity to ask questions of our panelists.

To ask a question now:

Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

Type a question in the box below the Ask drop-down menu in the Q&A panel.

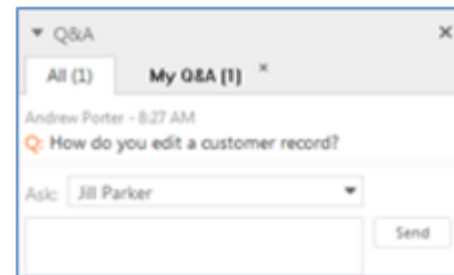
Select *All Panelists* from the Ask drop-down-menu.

Click Send. Your message is sent and appears in the Q&A panel.

To ask a question after this presentation:

You are encouraged to participate in the dW Answers forum:

<https://ibm.biz/qradarforums>





THANK YOU

FOLLOW US ON:



<https://www.facebook.com/IBM-Security-Support/>



QRadar Forums: <https://ibm.biz/qradarforums>



[youtube/user/ibmsecuritysupport](https://youtube.com/user/ibmsecuritysupport)



[@askibmsecurity](https://twitter.com/askibmsecurity)



securityintelligence.com



xforce.ibmcloud.com

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.