CLAROTY

Claroty CTD – QRadar: Installation Guide

Version 7

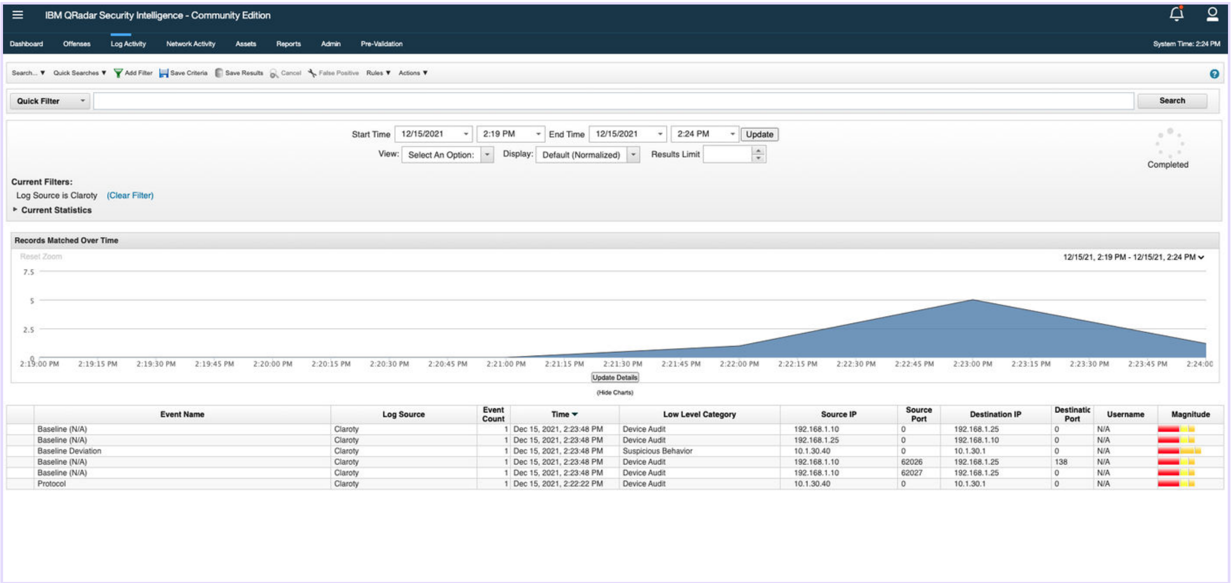
05-Jan-2022

1. Solution Overview

The Claroty Continuous Threat Detection (CTD) add-on for IBM's QRadar delivers comprehensive security, visibility, and alert management capabilities for operational technology (OT) environments. This integration enables QRadar to automatically ingest OT events, alerts and traffic baselines from Claroty CTD.

Users can monitor all assets and potential threats in their OT environment on a single pane of glass in real-time, leading to more effective and efficient OT security monitoring and stronger OT security posture. Benefits include:

- Continuous monitoring of ICS and industrial network assets - With a unified, real-time view into security threats targeting PLCs/RTs, embedded PCs, process control software and additional network assets, enterprises can identify threats early before they can impact their business.
- Single view for IT SOC teams to identify threats across both IT and OT environments -- enabling Companies to have a true enterprise view of all threats and risks across the business.

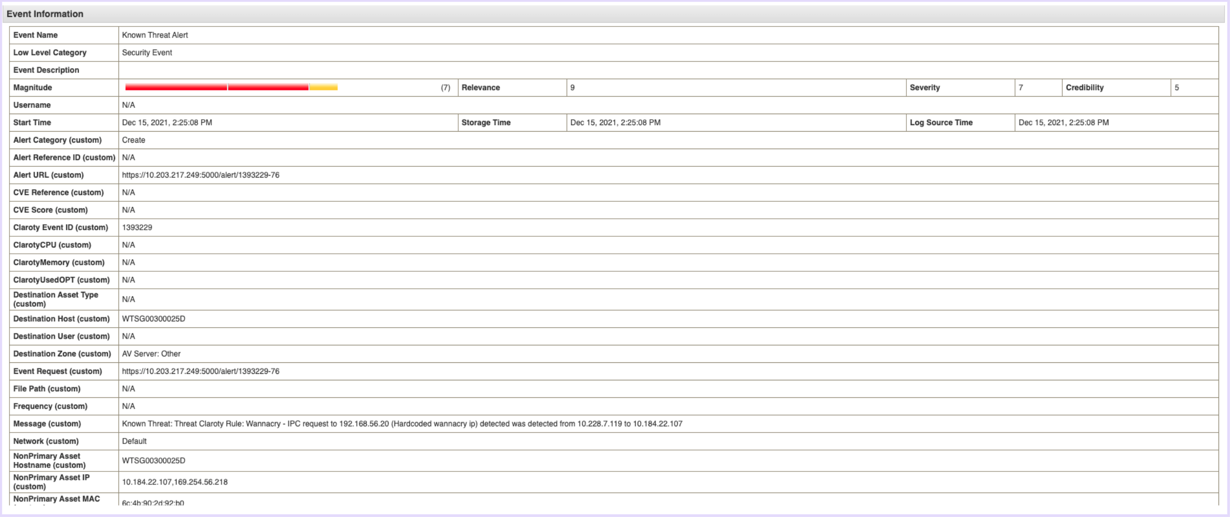


Start Time 12/15/2021 2:19 PM End Time 12/15/2021 2:24 PM

View: Select An Option: Display: Default (Normalized) Results Limit

Current Filters:
Log Source is Claroty (Clear Filter)
▸ Current Statistics

	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP	Source Port	Destination IP	Destinatic Port	Username	Magnitude
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.10	0	192.168.1.25	0	N/A	🟥🟨🟨
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.25	0	192.168.1.10	0	N/A	🟥🟨🟨
	Baseline Deviation	Claroty	1	Dec 15, 2021, 2:23:48 PM	Suspicious Behavior	10.1.30.40	0	10.1.30.1	0	N/A	🟥🟨🟨
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.10	62026	192.168.1.25	138	N/A	🟥🟨🟨
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.10	62027	192.168.1.25	0	N/A	🟥🟨🟨
	Protocol	Claroty	1	Dec 15, 2021, 2:22:22 PM	Device Audit	10.1.30.40	0	10.1.30.1	0	N/A	🟥🟨🟨



Event Information

Event Name	Known Threat Alert						
Low Level Category	Security Event						
Event Description							
Magnitude	(7)	**Relevance**	9	**Severity**	7	**Credibility**	5
Username	N/A						
Start Time	Dec 15, 2021, 2:25:08 PM	**Storage Time**	Dec 15, 2021, 2:25:08 PM	**Log Source Time**	Dec 15, 2021, 2:25:08 PM		
Alert Category (custom)	Create						
Alert Reference ID (custom)	N/A						
Alert URL (custom)	https://10.203.217.249:5000/alert/1393229-76						
CVE Reference (custom)	N/A						
CVE Score (custom)	N/A						
Claroty Event ID (custom)	1393229						
ClarotyCPU (custom)	N/A						
ClarotyMemory (custom)	N/A						
ClarotyUsedOPT (custom)	N/A						
Destination Asset Type (custom)	N/A						
Destination Host (custom)	WTSG00300025D						
Destination User (custom)	N/A						
Destination Zone (custom)	AV Server: Other						
Event Request (custom)	https://10.203.217.249:5000/alert/1393229-76						
File Path (custom)	N/A						
Frequency (custom)	N/A						
Message (custom)	Known Threat: Threat Claroty Rule: Wannacry - IPC request to 192.168.56.20 (Hardcoded wannacry ip) detected was detected from 10.228.7.119 to 10.184.22.107						
Network (custom)	Default						
NonPrimary Asset Hostname (custom)	WTSG00300025D						
NonPrimary Asset IP (custom)	10.184.22.107,169.254.56.218						
NonPrimary Asset MAC	6c:4b:90:2d:92:b0						

2. Setup and Configure

2.1. CTD Prerequisites

- CTD Version 4.2.4 or later

2.2. QRadar Prerequisites

- QRadar Version 7.3.3 or above

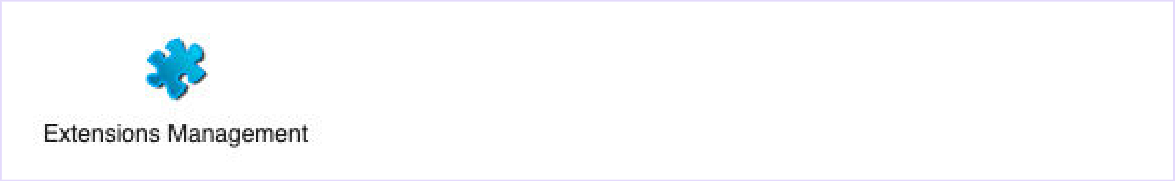
2.3. Setup Instructions

2.3.1. The DSM

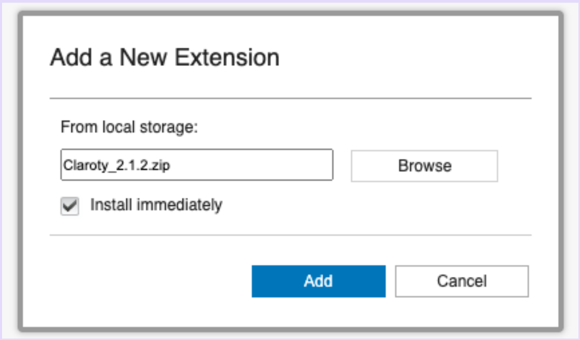
- IBM® QRadar® uses the Device Support Modules (DSMs) to log and correlate the data that is collected from external log sources, such as firewalls, switches, or routers. DSMs are regularly updated to ensure that QRadar can correctly interpret and parse security event information that is provided by external devices.
- DSMs can be updated both automatically from IBM's AppExchange and manually.
- This DSM integration supports both CTD's legacy CEF and the new CEF structure.
- See the FAQ (page 15) for the log types supported.

2.3.2. Installing the Claroty DSM in QRadar

1. Download the DSM `.zip` file from the IBM App Exchange, IBM X-Force Exchange.
2. In QRadar under the **Admin** tab go to **Extensions Management**:



3. Click **Add**.
4. Select the `.zip` file and select the **Install immediately** checkbox, then click **Add**:

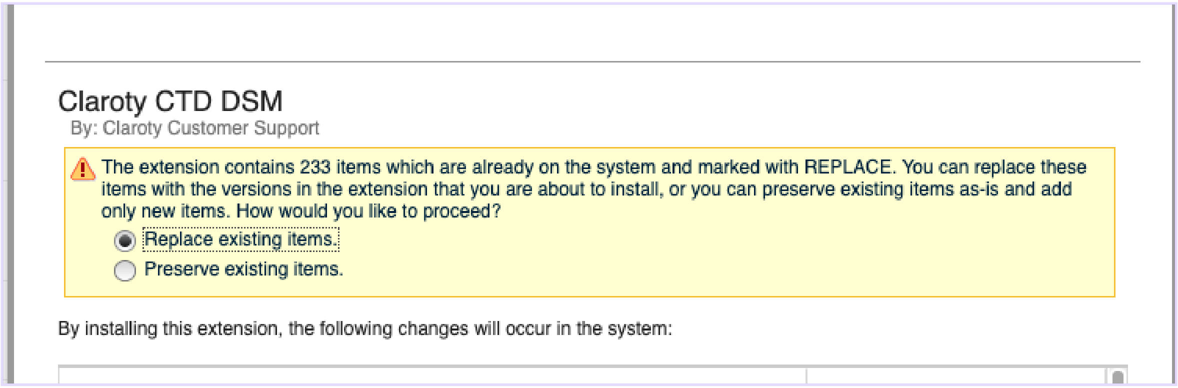


Add a New Extension

From local storage: Claroty_2.1.2.zip

☑ Install immediately

5. If you get a message like the following, select **Replace existing items**:



Claroty CTD DSM

By: Claroty Customer Support

⚠ The extension contains 233 items which are already on the system and marked with REPLACE. You can replace these items with the versions in the extension that you are about to install, or you can preserve existing items as-is and add only new items. How would you like to proceed?

● Replace existing items.

○ Preserve existing items.

By installing this extension, the following changes will occur in the system:

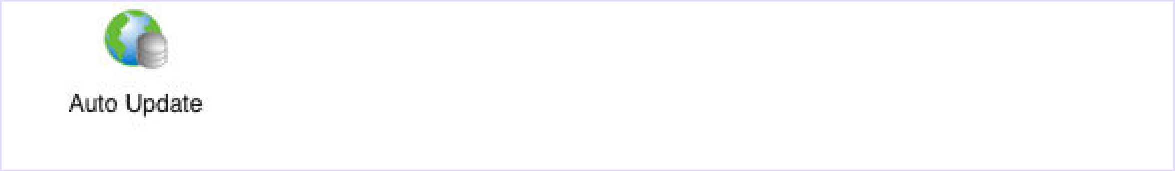
6. Follow the wizard to complete the installation.

2.3.3. Updating the Claroty DSM Version

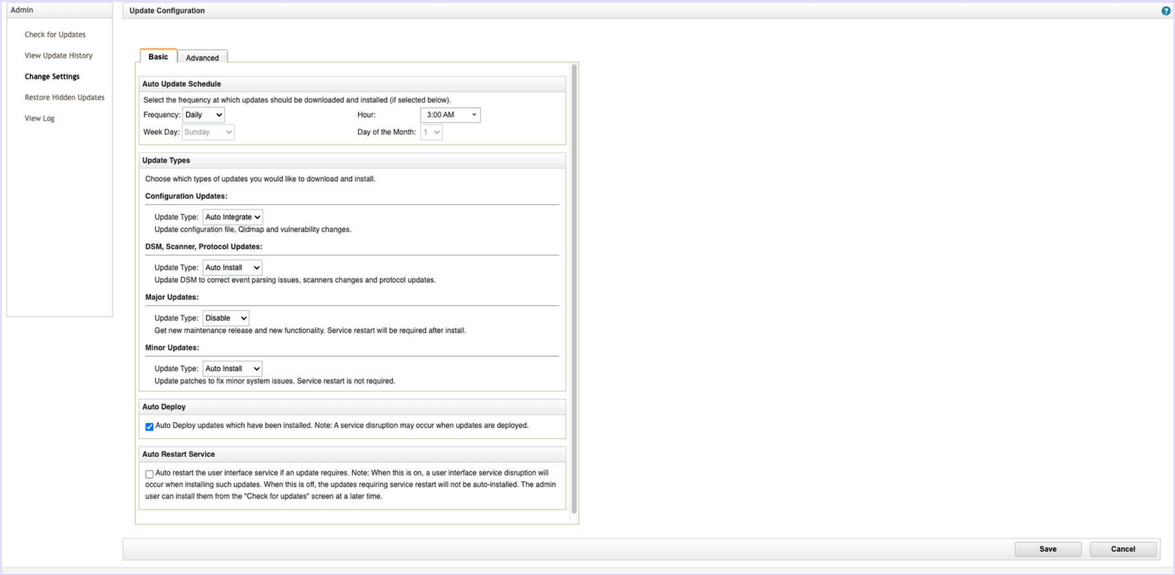
Either set all of your DSMs to be updated automatically or manually update the DSM by downloading the new version from the IBM App Exchange and following the Installing the Claroty DSM in QRadar (page 4) instructions.

To update automatically:

1. In QRadar go to **Admin > Auto Update**:



2. Click on the **Change Setting > Basic** tab.
3. Under **DSM > Scanner > Protocol Updates**, select **Auto install**:



Auto Update Schedule

Select the frequency at which updates should be downloaded and installed (if selected below).

Frequency: Daily

Hour: 3:00 AM

Week Day: Sunday

Day of the Month: 1

Update Types

Choose which types of updates you would like to download and install.

Configuration Updates:

Update Type: Auto Integrate

Update configuration file, Qidmap and vulnerability changes.

DSM, Scanner, Protocol Updates:

Update Type: Auto Install

Update DSM to correct event parsing issues, scanners changes and protocol updates.

Major Updates:

Update Type: Disable

Get new maintenance release and new functionality. Service restart will be required after install.

Minor Updates:

Update Type: Auto Install

Update patches to fix minor system issues. Service restart is not required.

Auto Deploy

☑ Auto Deploy updates which have been installed. Note: A service disruption may occur when updates are deployed.

Auto Restart Service

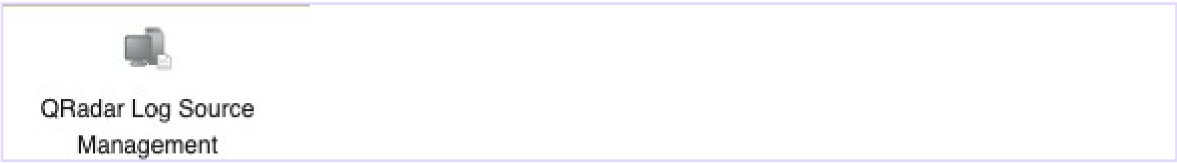
☐ Auto restart the user interface service if an update requires. Note: When this is on, a user interface service disruption will occur when installing such updates. When this is off, the updates requiring service restart will not be auto-installed. The admin user can install them from the "Check for updates" screen at a later time.

4. Select **Save**.

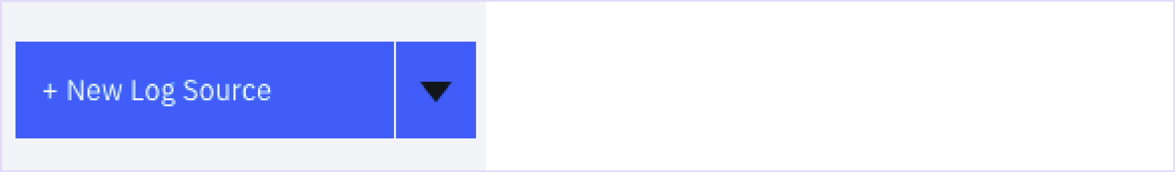
2.3.4. Setting up the Connection in QRadar

2.3.4.1. Using the QRadar Log Source Management App

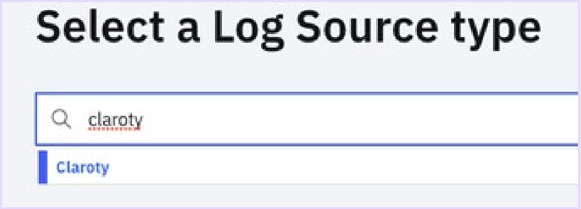
1. On the main dashboard go to **Admin** -> **QRadar Log Source Management**:



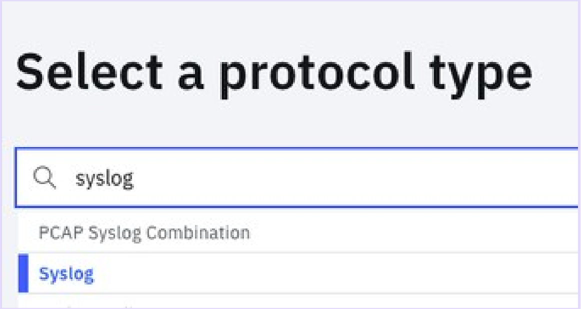
2. Click on **New Log Source**:



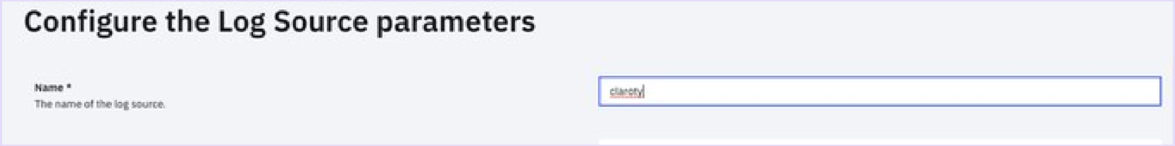
3. Select **Single Log Source**.
4. Search for **Claroty** and click on **Step 2**:



5. Select **Syslog** and click on **Step 3**:



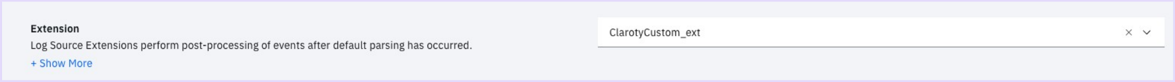
6. Give this source a name and click on **Step 4**:


Configure the Log Source parameters

Name *
The name of the log source.

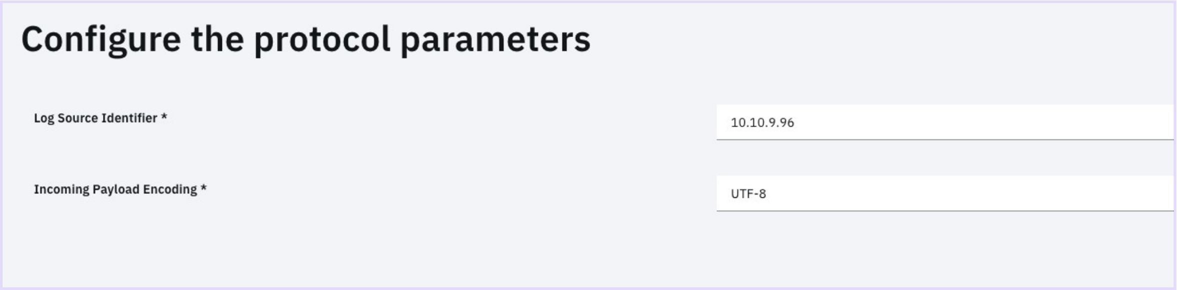
claroty

7. Select **ClarotyCustom_ext** as the Extension:


Extension
Log Source Extensions perform post-processing of events after default parsing has occurred.
+ Show More

ClarotyCustom_ext

8. Type your EMC IP address in the **Log Source Identifier** field and click on **Finish**:

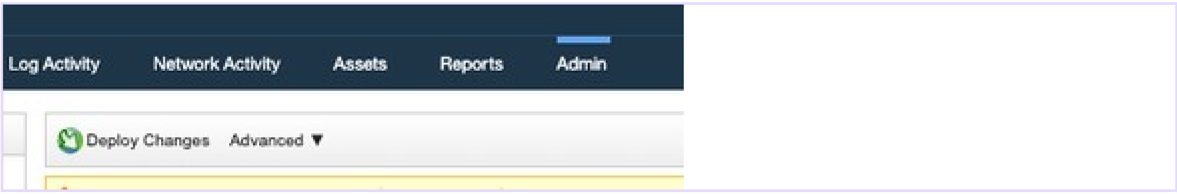


Configure the protocol parameters

Log Source Identifier * 10.10.9.96

Incoming Payload Encoding * UTF-8

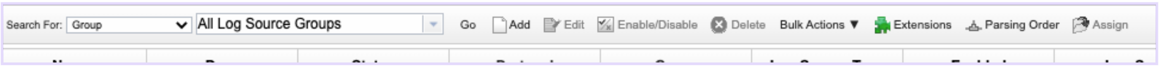
9. Go back to the **Admin** page and click on **Deploy Changes** to deploy the new changes:



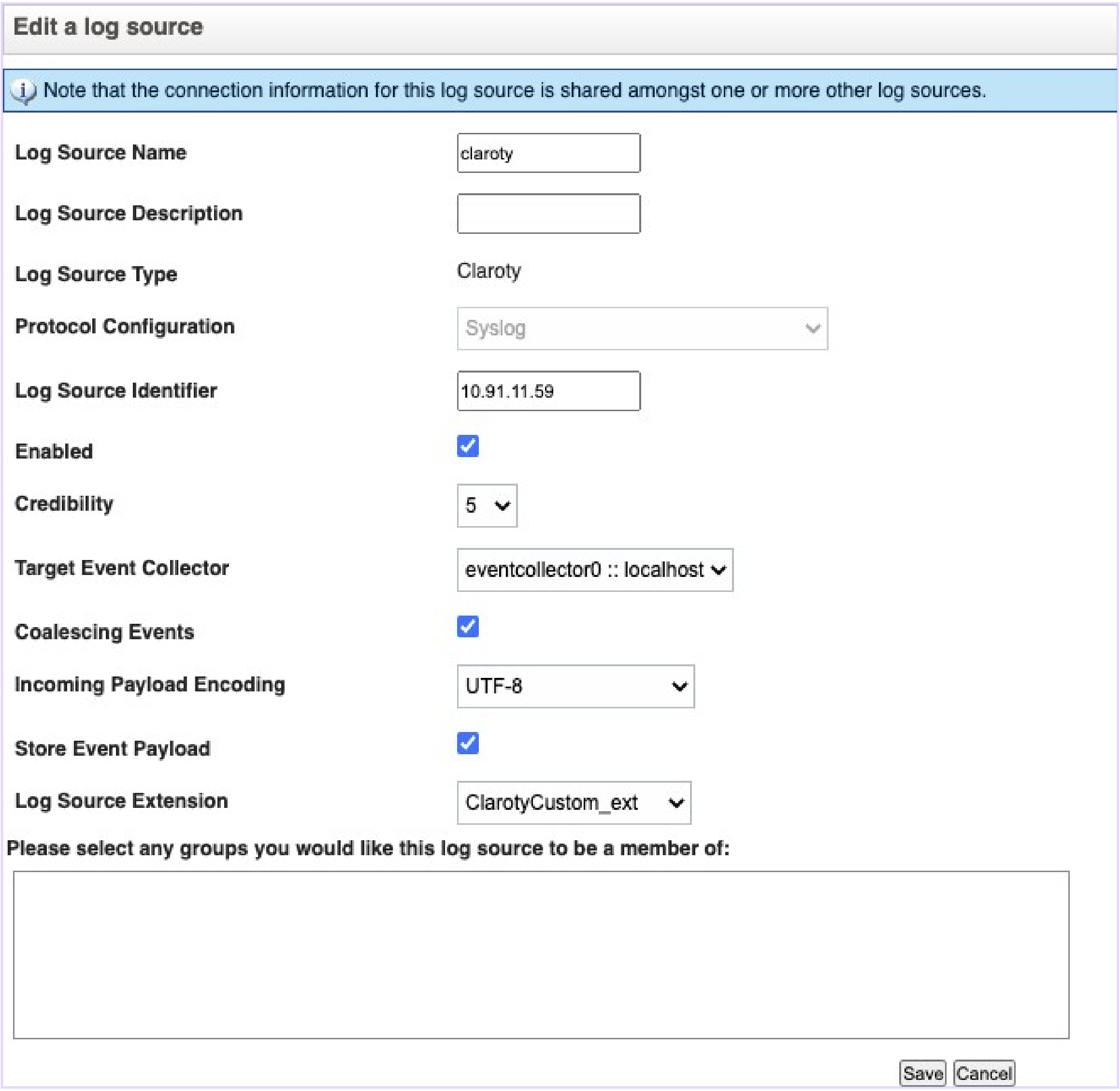
2.3.4.2. Using Log Sources

1. On the main dashboard go to **Admin > Log Sources**:

2. Click on **Add**:



3. Fill in the **Edit a Log Source** fields:



Edit a log source

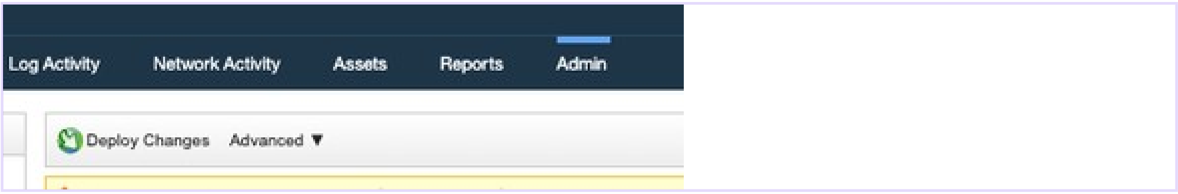
Note that the connection information for this log source is shared amongst one or more other log sources.

Log Source Name	claroty
Log Source Description	
Log Source Type	Claroty
Protocol Configuration	Syslog
Log Source Identifier	10.91.11.59
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: localhost
Coalescing Events	☑
Incoming Payload Encoding	UTF-8
Store Event Payload	☑
Log Source Extension	ClarotyCustom_ext

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

   a. **Log Source Name** - A given name for this source
   b. **Log Source Type** - Must be `Claroty`
   c. **Protocol Configuration** - Set to **Syslog**
   d. **Log Source Identifier** - Enter the IP address of the EMC machine
   e. **Log Source Extension** - Select **ClarotyCustom_ext**
   f. Click **Save**.

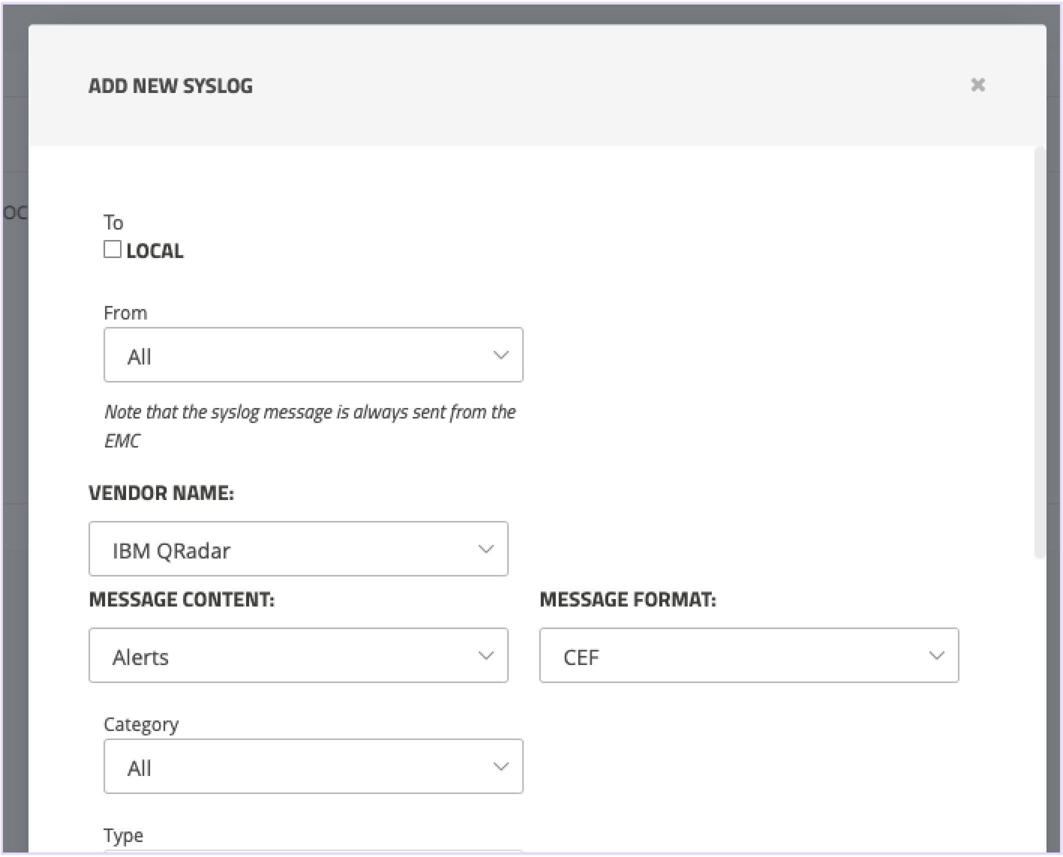
4. Go back to the **Admin** page and click **Deploy Changes** to apply your new changes:



2.3.5. Setting up the Connection in the CTD EMC

1. In the CTD EMC, click on the ⚙ gear icon and then **Integrations > SIEM Syslog**.

2. Click on the + **Add** icon.
3. Fill in the **Add New Syslog** details and click **Save**:



ADD NEW SYSLOG

To
□ LOCAL

From
All

Note that the syslog message is always sent from the EMC

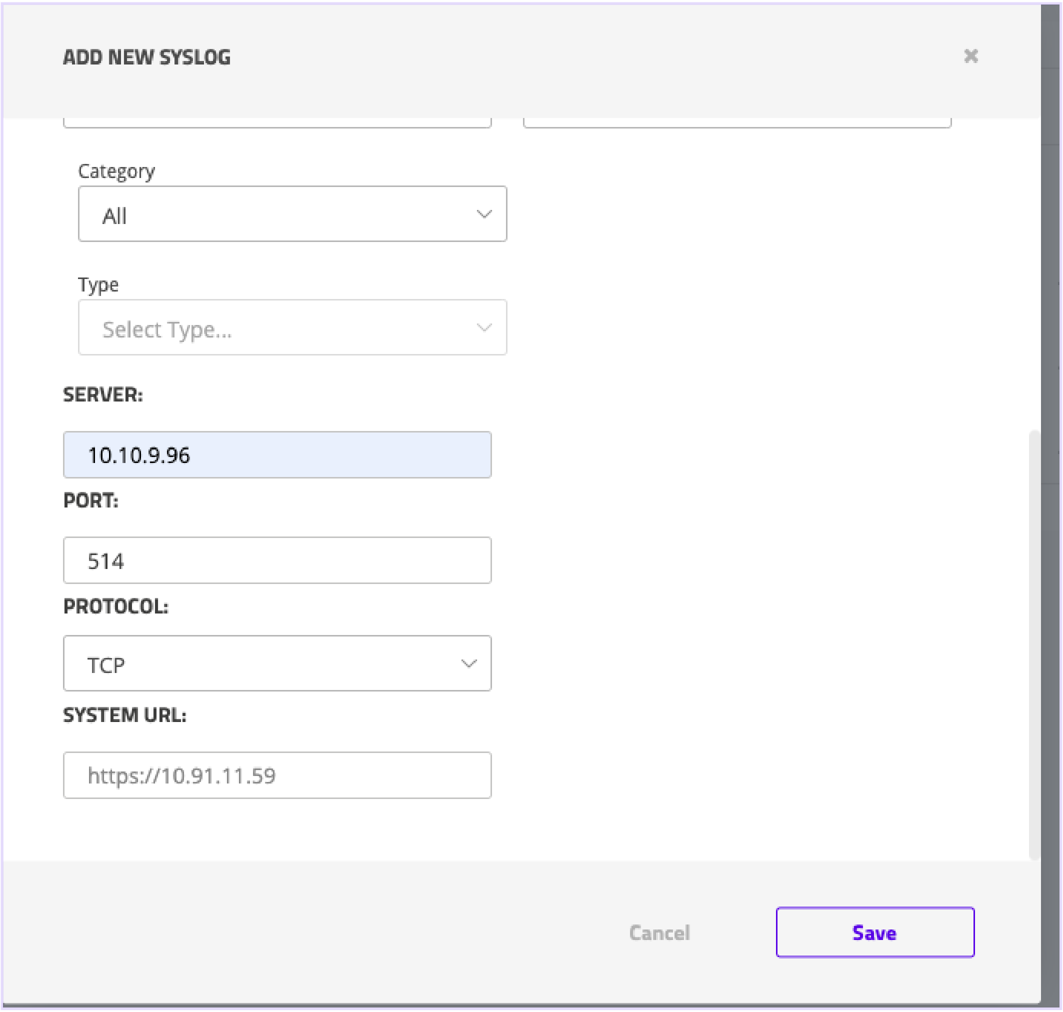
VENDOR NAME:
IBM QRadar

MESSAGE CONTENT:
Alerts

MESSAGE FORMAT:
CEF

Category
All

Type



ADD NEW SYSLOG

Category: All

Type: Select Type...

SERVER: 10.10.9.96

PORT: 514

PROTOCOL: TCP

SYSTEM URL: https://10.91.11.59

a. **To** - Unselect the **Local** checkbox
b. **From** - Select **All** or specify the sites from which data will be sent
c. **Vendor Name** - Select **IBM QRadar**
d. **Message Content** - Select the data type to be sent (one option only)
e. **Server** - The IP of the QRadar machine
f. **Port** - Enter 514
g. **Protocol** - Select **TCP/UDP**

> **IMPORTANT**
> TCP is the recommended protocol.

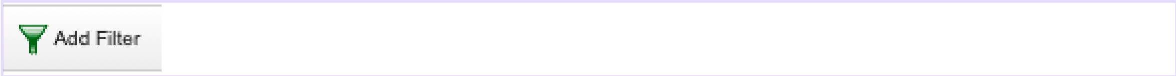
4. Click **Save**.

2.4. Displaying the Data

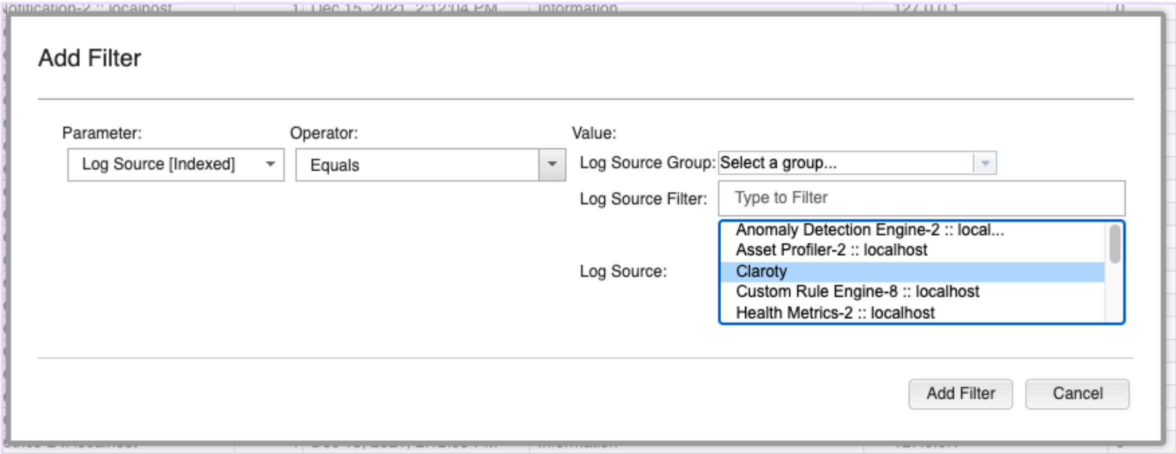
After you have installed or updated the Claroty DSM, created two way connection between QRadar and CTD and have deployed the changes, your data mapping is ready.

Go to **Log Activity** and create a new filter as follows:

1. Click on **Add Filter**:



2. Select **Log Source [Index]** as the Parameter:



Add Filter

Parameter: Log Source [Indexed]

Operator: Equals

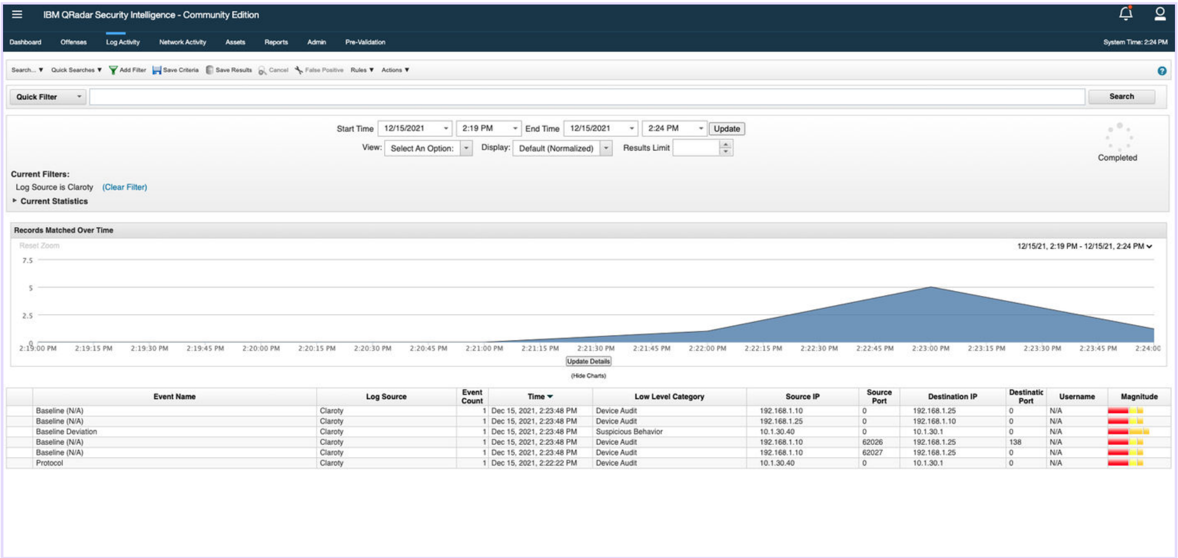
Value:

Log Source Group: Select a group...

Log Source Filter: Type to Filter

Log Source:
- Anomaly Detection Engine-2 :: local...
- Asset Profiler-2 :: localhost
- Claroty
- Custom Rule Engine-8 :: localhost
- Health Metrics-2 :: localhost

3. Select the log source name that you defined in the Log Source Management app as the Log Source.
4. Click on **Add Filter** again.
5. Select the relevant time interval for your search and you should see the mapped data:



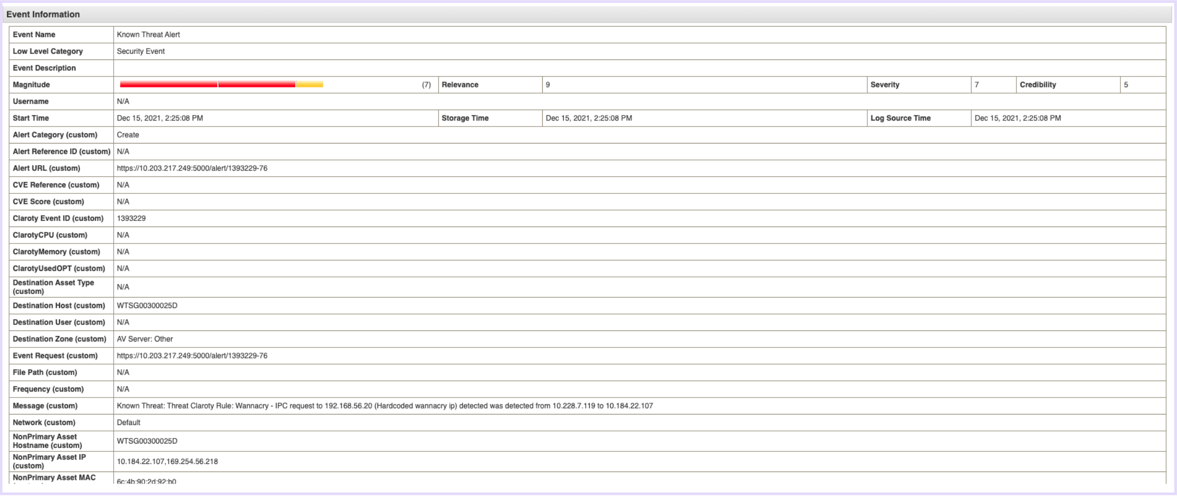
Start Time 12/15/2021 2:19 PM End Time 12/15/2021 2:24 PM

View: Select An Option: Display: Default (Normalized) Results Limit

Current Filters:
Log Source is Claroty (Clear Filter)

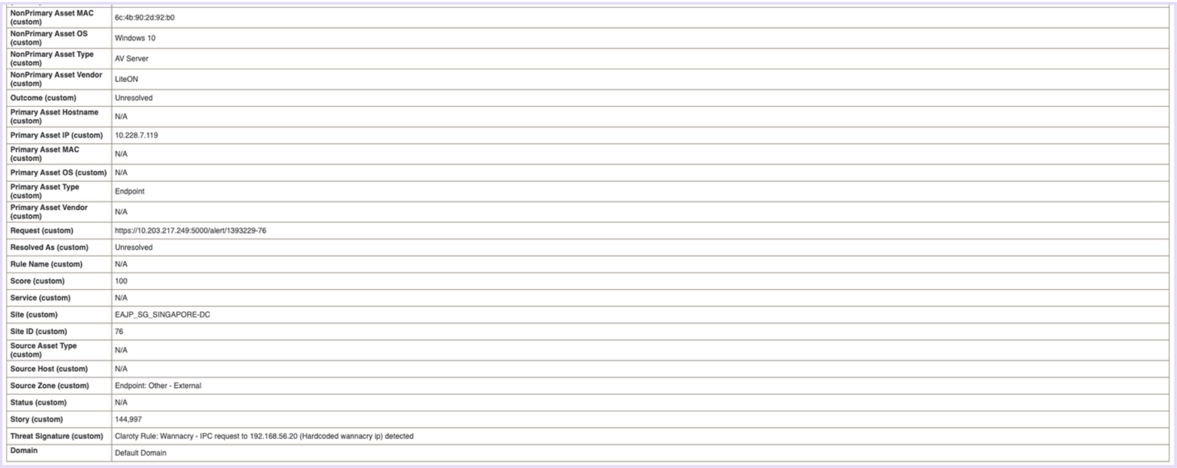
▸ Current Statistics

	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP	Source Port	Destinatic Port	Destination IP	Username	Magnitude
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.10	0	0	192.168.1.25	N/A	
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.25	0	0	192.168.1.10	N/A	
	Baseline Deviation	Claroty	1	Dec 15, 2021, 2:23:48 PM	Suspicious Behavior	10.1.30.40	0	0	10.1.30.1	N/A	
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.10	62026	138	192.168.1.25	N/A	
	Baseline (N/A)	Claroty	1	Dec 15, 2021, 2:23:48 PM	Device Audit	192.168.1.10	62027	0	192.168.1.25	N/A	
	Protocol	Claroty	1	Dec 15, 2021, 2:22:22 PM	Device Audit	10.1.30.40	0	0	10.1.30.1	N/A	

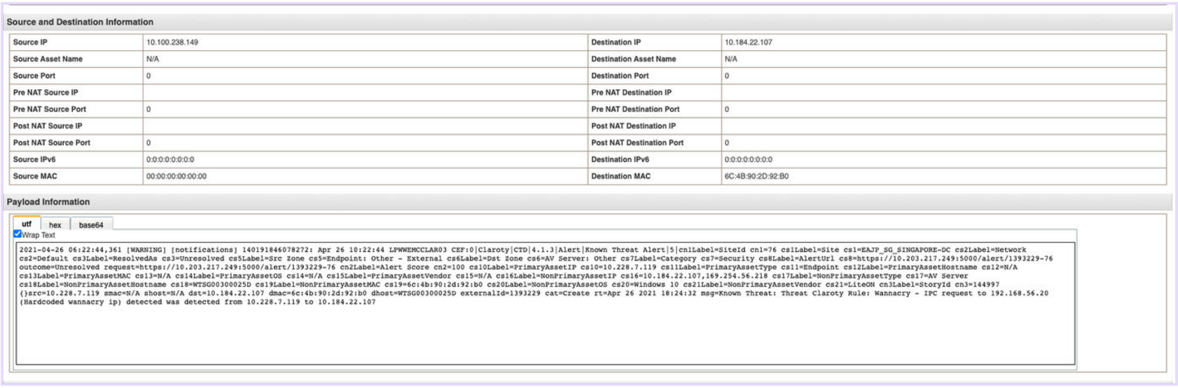


Event Information

Event Name	Known Threat Alert						
Low Level Category	Security Event						
Event Description							
Magnitude	(7)	**Relevance**	9	**Severity**	7	**Credibility**	5
Username	N/A						
Start Time	Dec 15, 2021, 2:25:08 PM	**Storage Time**	Dec 15, 2021, 2:25:08 PM	**Log Source Time**	Dec 15, 2021, 2:25:08 PM		
Alert Category (custom)	Create						
Alert Reference ID (custom)	N/A						
Alert URL (custom)	https://10.203.217.249:5000/alert/1393229-76						
CVE Reference (custom)	N/A						
CVE Score (custom)	N/A						
Claroty Event ID (custom)	1393229						
ClarotyCPU (custom)	N/A						
ClarotyMemory (custom)	N/A						
ClarotyUsedOPT (custom)	N/A						
Destination Asset Type (custom)	N/A						
Destination Host (custom)	WTSG00300025D						
Destination User (custom)	N/A						
Destination Zone (custom)	AV Server: Other						
Event Request (custom)	https://10.203.217.249:5000/alert/1393229-76						
File Path (custom)	N/A						
Frequency (custom)	N/A						
Message (custom)	Known Threat: Threat Claroty Rule: Wannacry - IPC request to 192.168.56.20 (Hardcoded wannacry ip) detected was detected from 10.228.7.119 to 10.184.22.107						
Network (custom)	Default						
NonPrimary Asset Hostname (custom)	WTSG00300025D						
NonPrimary Asset IP (custom)	10.184.22.107,169.254.56.218						



NonPrimary Asset MAC (custom)	6c:4b:90:2d:92:b0
NonPrimary Asset OS (custom)	Windows 10
NonPrimary Asset Type (custom)	AV Server
NonPrimary Asset Vendor (custom)	LiteON
Outcome (custom)	Unresolved
Primary Asset Hostname (custom)	N/A
Primary Asset IP (custom)	10.228.7.119
Primary Asset MAC (custom)	N/A
Primary Asset OS (custom)	N/A
Primary Asset Type (custom)	Endpoint
Primary Asset Vendor (custom)	N/A
Request (custom)	https://10.203.217.249:5000/alert/1393229-76
Resolved As (custom)	Unresolved
Rule Name (custom)	N/A
Score (custom)	100
Service (custom)	N/A
Site (custom)	EAJP_SG_SINGAPORE-DC
Site ID (custom)	76
Source Asset Type (custom)	N/A
Source Host (custom)	N/A
Source Zone (custom)	Endpoint: Other - External
Status (custom)	N/A
Story (custom)	144,997
Threat Signature (custom)	Claroty Rule: Wannacry - IPC request to 192.168.56.20 (Hardcoded wannacry ip) detected
Domain	Default Domain



Source and Destination Information

Source IP	10.100.238.149	**Destination IP**	10.184.22.107
Source Asset Name	N/A	**Destination Asset Name**	N/A
Source Port	0	**Destination Port**	0
Pre NAT Source IP		**Pre NAT Destination IP**	
Pre NAT Source Port	0	**Pre NAT Destination Port**	0
Post NAT Source IP		**Post NAT Destination IP**	
Post NAT Source Port	0	**Post NAT Destination Port**	0
Source IPv6	0:0:0:0:0:0:0:0	**Destination IPv6**	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	**Destination MAC**	6C:4B:90:2D:92:B0

Payload Information

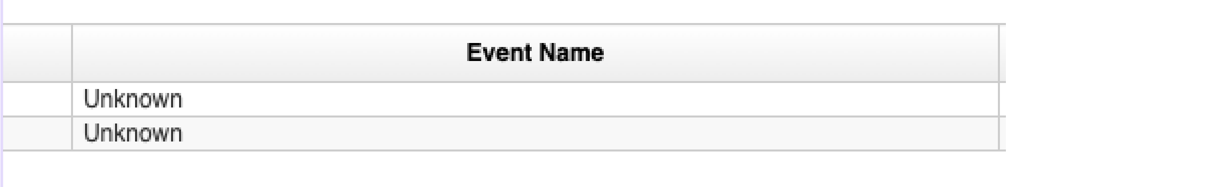
☑ Wrap Text

```
2021-04-26 06:22:44,361 [WARNING] [notifications] 140191846078272: Apr 26 10:22:44 LPWWEMCCLAR03 CEF:0|Claroty|CTD|4.1.3|Alert|Known Threat Alert|5|cn1Label=SiteId cn1=76 cs1Label=Site cs1=EAJP_SG_SINGAPORE-DC cs2Label=Network
cs2=Default cs3Label=ResolvedAs cs3=Unresolved cs5Label=Src Zone cs5=Endpoint: Other - External cs6Label=Dst Zone cs6=AV Server: Other cs7Label=Category cs7=Security cs8Label=AlertUrl cs8=https://10.203.217.249:5000/alert/1393229-76
outcome=Unresolved request=https://10.203.217.249:5000/alert/1393229-76 cn2Label=Alert Score cn2=100 cs10Label=PrimaryAssetIP cs10=10.228.7.119 cs11Label=PrimaryAssetType cs11=Endpoint cs12Label=PrimaryAssetHostname cs12=N/A
cs13Label=PrimaryAssetMAC cs13=N/A cs14Label=PrimaryAssetOS cs14=N/A cs15Label=PrimaryAssetVendor cs15=N/A cs16Label=NonPrimaryAssetIP cs16=10.184.22.107,169.254.56.218 cs17Label=NonPrimaryAssetType cs17=AV Server
cs18Label=NonPrimaryAssetHostname cs18=WTSG00300025D cs19Label=NonPrimaryAssetMAC cs19=6c:4b:90:2d:92:b0 cs20Label=NonPrimaryAssetOS cs20=Windows 10 cs21Label=NonPrimaryAssetVendor cs21=LiteON cn3Label=StoryId cn3=144997
{}src=10.228.7.119 smac=N/A shost=N/A dst=10.184.22.107 dmac=6c:4b:90:2d:92:b0 dhost=WTSG00300025D externalId=1393229 cat=Create rt=Apr 26 2021 18:24:32 msg=Known Threat: Threat Claroty Rule: Wannacry - IPC request to 192.168.56.20
(Hardcoded wannacry ip) detected was detected from 10.228.7.119 to 10.184.22.107
```

3. Troubleshooting

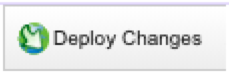
3.1. Message Event Name is Unknown

If the message event name is unknown as is shown below:



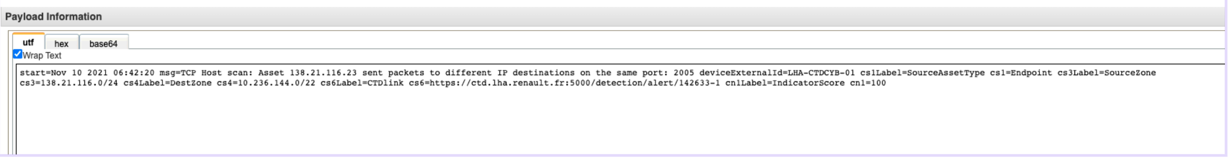
	Event Name
	Unknown
	Unknown

- Make sure you correctly defined the connection between QRadar and your EMC:
  - **Claroty** is selected as the **Log Source Type**
  - The current identifier of your EMC is correct
  - **ClarotyCustom_ext** is selected as the Log Source Extension
- Make sure you click on the **Deploy Changes** button after setting up the connection in your QRadar machine:



3.2. Syslog Message was Split into Parts

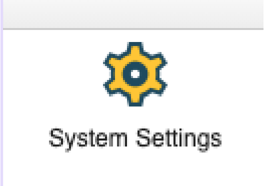
If the Syslog message was split into parts as follows:



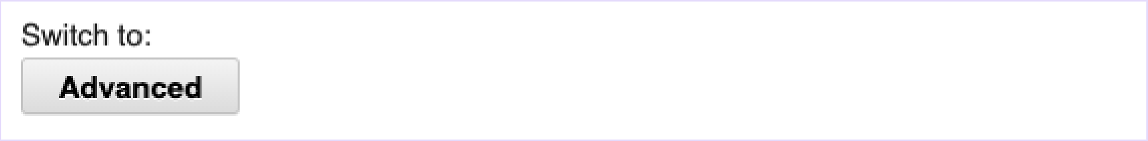
```
start=Nov 10 2021 06:42:20 msg=TCP Host scan: Asset 138.21.116.23 sent packets to different IP destinations on the same port: 2005 deviceExternalId=LHA-CTDCYB-01 cs1Label=SourceAssetType cs1=Endpoint cs3Label=SourceZone
cs3=138.21.116.0/24 cs4Label=DestZone cs4=10.236.144.0/22 cs6Label=CTDlink cs6=https://ctd.lha.renault.fr:5000/detection/alert/142633-1 cn1Label=IndicatorScore cn1=100
```

- Make sure your select **TCP** over UDP as the **Protocol** when you define the connection in your EMC
- You may need to increase the size of the TCP payload you allow on your QRadar machine:

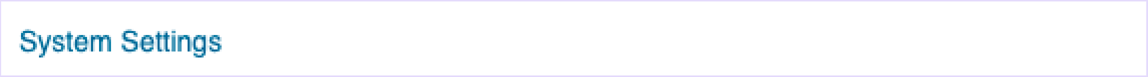
1. In your QRadar machine, go to the **Admin** tab.
2. Click on the **System Settings** icon:



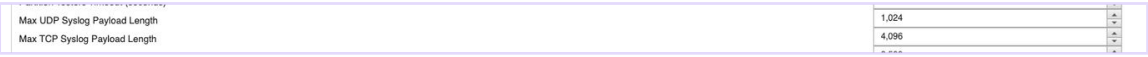
3. Click on the **Advanced** button:



4. Click on **System Settings**:



5. Look for **Max TCP Syslog Payload Length** and increase the length as needed:



Max UDP Syslog Payload Length	1,024
Max TCP Syslog Payload Length	4,096

4. FAQ & Reference

Q: What CTD data can be sent via Syslog?

A: The following entities are supported:

Log Type	CEF - Legacy	CEF - New
Alerts	Yes	Yes
Events	Yes	Yes
Baseline	Yes	No
Health Monitoring	Yes	No

Q: Which DSM Event QRadar Identifier (QIDs) are supported?

A: The following QIDs are supported:

Event	QID
Protocol	1002500003
Baseline Deviation	1002500031
Firmware Download	1002500033
Configuration Download	1002500028
Baseline (N/A)	1002500035
Known Threat Alert	1002500025
Configuration Upload Alert	1002500026
New Entity	1002500023
Asset Information Change	1002500024
New Asset	1002500019
New Conflict Asset	1002500015
Entity Conflict	1002500016
Known Threat Event	1002500012
Health Check ("HealthCheck")	1002500013
Login Event	1002500010
Alert Login	1002500011
Sniffer Status	1002500008
Alert Port Scan	1002500027
Event Port Scan	1002500029
Alert Host Scan	1002500022
Event Host Scan	1002500020
Site Status	1002500021
Suspicious File Transfer Event	1002500017
Suspicious File Transfer Alert	1002500018
NOTE The Policy Violation Event and Policy Violation Alert both have the same ID	
Policy Violation Event	1002500014
Policy Violation Alert	1002500014