WALLIX QRADAR QUICK INSTALL
OCTOBER 2018

WALLIX
250 bis rue du Faubourg Saint-Honoré 75008 Paris
Tél : +331 53 42 12 90 – Fax : + 33 1 43 87 66 38
SARL au capital de 50 000 Euros – RCS PARIS B 450 401 153 – FR67 450 401 153

VERSION	1.1

Release

Table des matières

I. INTRODUCTION

I.1 OBJECT

The purpose of this document is to help in the integration of the WALLIX Bastion DSM in QRadar

II. PREREQUISITES

II.1 WALLIX BASTION

Supported WALLIX Bastion versions :

- 5.0.x
- 6.0.x
- 6.1.x

II.2 QRADAR

Supported QRadar versions:

- 7.3.x

III. WALLIX BASTION DSM

III.1 INSTALLATION

The WALLIX Bastion DSM is in a ZIP format, transfer it first in the /tmp folder of QRadar system with SCP or SFTP.

Connect to the QRadar system through SSH or console and acquire root priviledges.

Use the contentManagement script to import the WALLIX Bastion DSM:

/opt/qradar/bin/contentManagement.pl -a import –f WALLIXBastion6.zip

The end of the import should be note with this line :

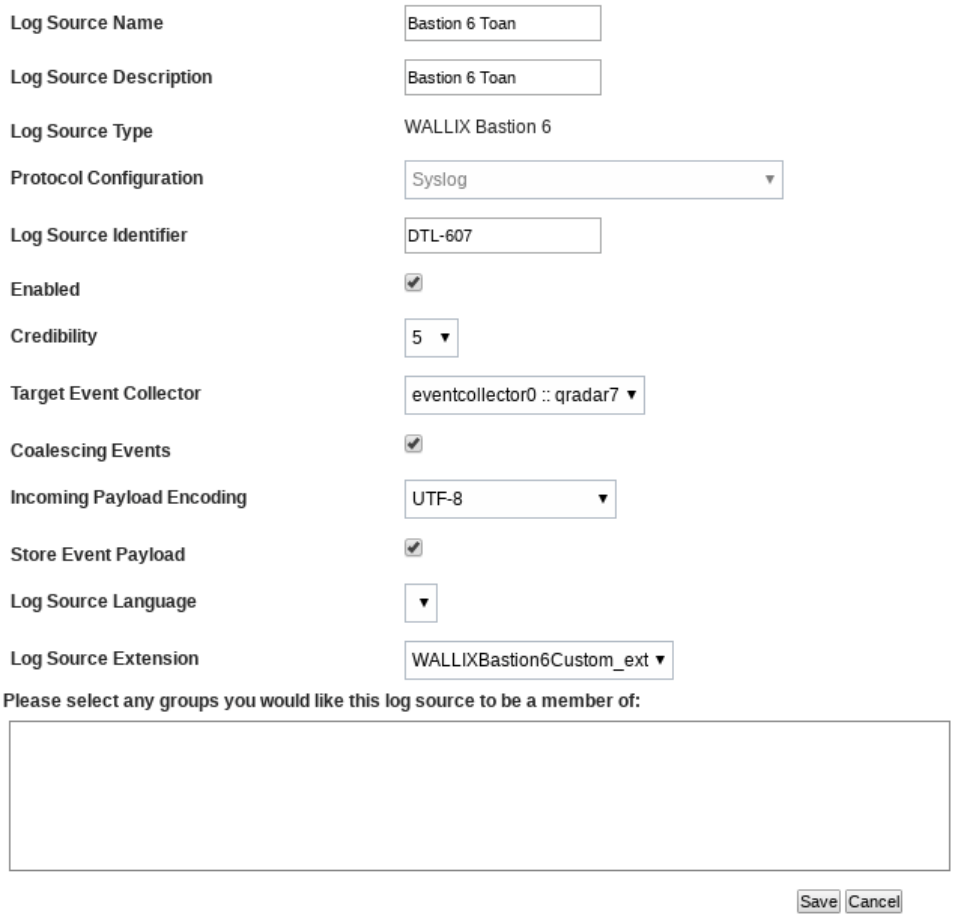
[INFO] FINISHED: The import process is completed. Please check the summary for status and allow several minutes for components to finish reloading.

III.2 CONFIGURATION

III.2.A QRADAR

Once imported, you should notice on the web interface of QRadar a new Log Source Extension named : WALLIXBastion6Custom_ext

Import then a new Log source for the Bastion if not already created :

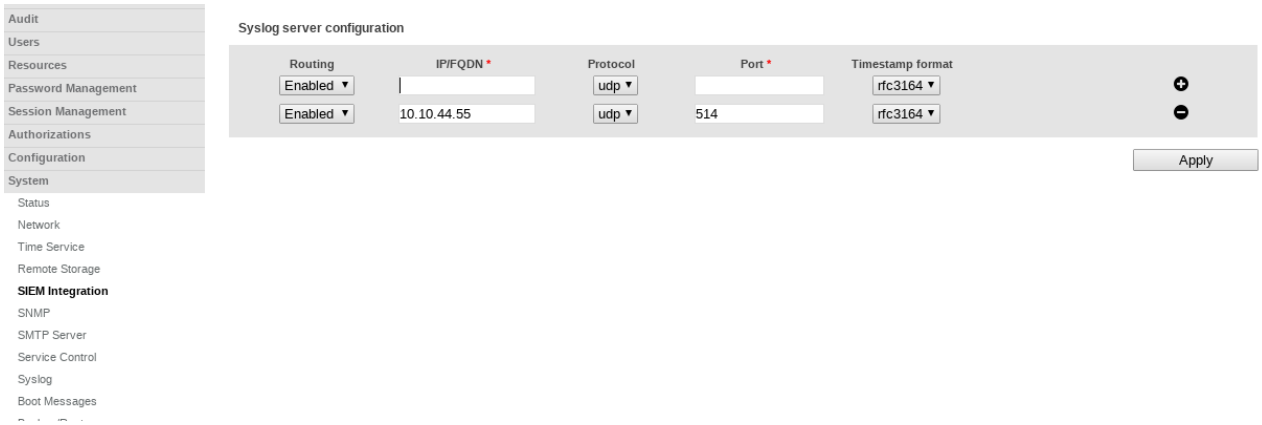


Note : the Log Source Identifier should be identical to the hostname of the Bastion.

Don't forget to click on "Deploy changes" to apply your modification.

III.2.B WALLIX BASTION

In the WALLIX Bastion, declare your QRadar in the web interface :

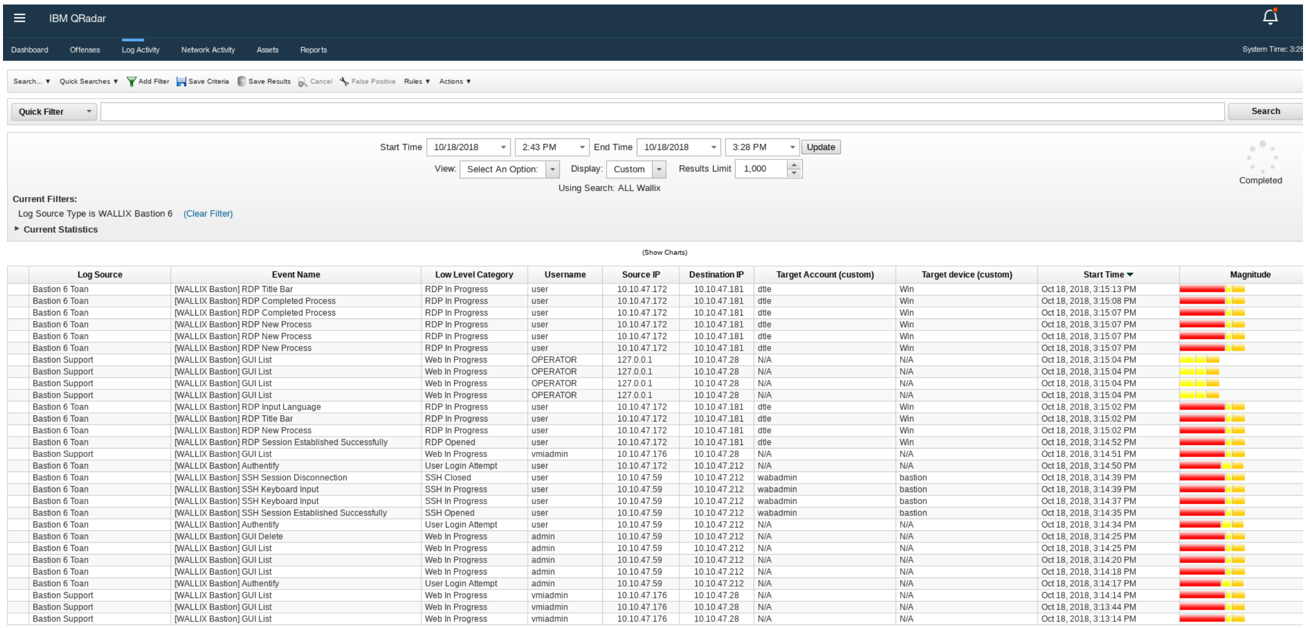


Note : since version 6.0, a license is needed to access this feature.

III.3 LOG ANALYSIS

After configuring both WALLIX Bastion and QRadar, you can check the Log Activity and filter on the Log Source Type : WALLIX Bastion 6

Logs should be automatically parsed (check below), if not please contact WALLIX Support.



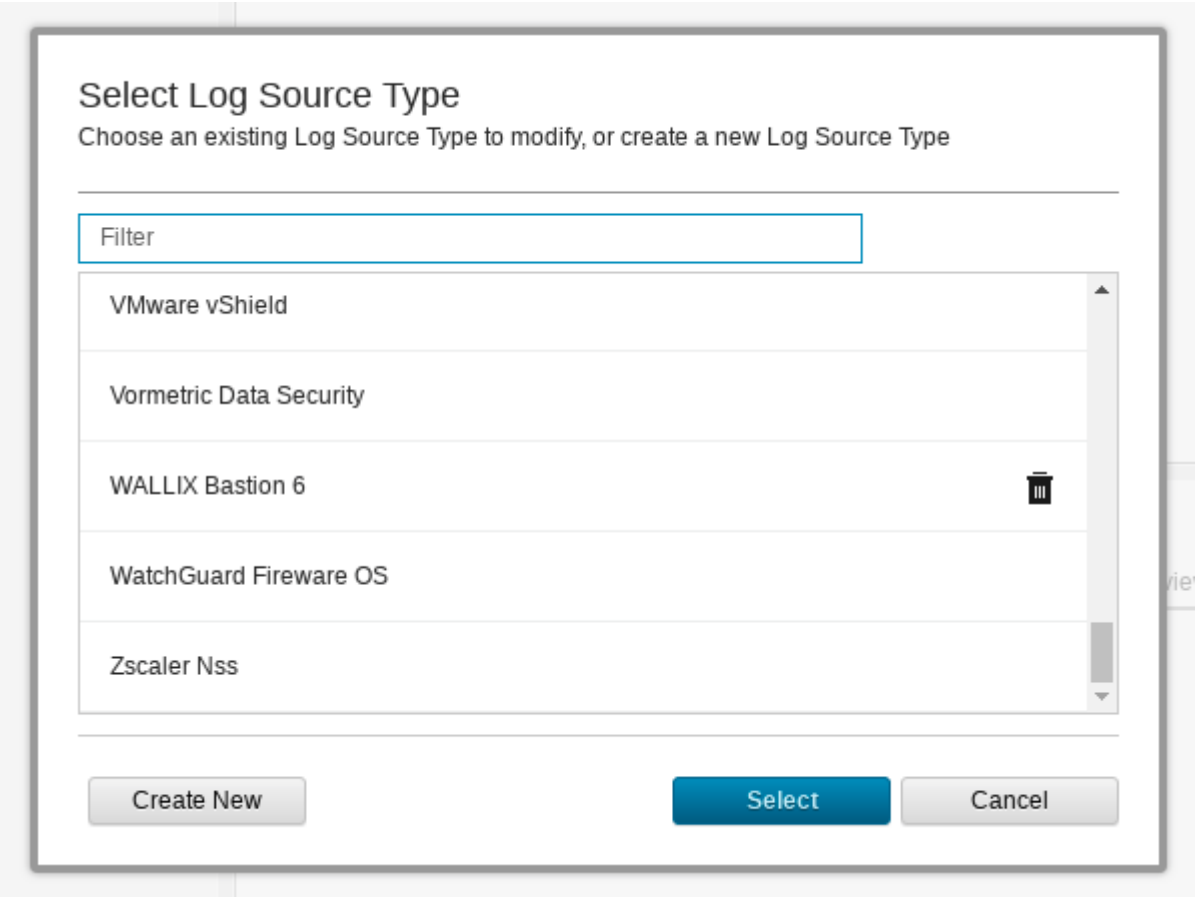
Log Source	Event Name	Low Level Category	Username	Source IP	Destination IP	Target Account (custom)	Target device (custom)	Start Time	Magnitude
Bastion 6 Toan	[WALLIX Bastion] RDP Title Bar	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:13 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP Completed Process	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:08 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP Completed Process	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:07 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP New Process	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:07 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP New Process	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:07 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP New Process	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:07 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	OPERATOR	127.0.0.1	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:15:04 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	OPERATOR	127.0.0.1	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:15:04 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	OPERATOR	127.0.0.1	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:15:04 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	OPERATOR	127.0.0.1	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:15:04 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP Input Language	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:02 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP Title Bar	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:02 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP New Process	RDP In Progress	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:15:02 PM	
Bastion 6 Toan	[WALLIX Bastion] RDP Session Established Successfully	RDP Opened	user	10.10.47.172	10.10.47.181	dtle	Win	Oct 18, 2018, 3:14:52 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	vmiadmin	10.10.47.176	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:14:51 PM	
Bastion 6 Toan	[WALLIX Bastion] Authentify	User Login Attempt	user	10.10.47.172	10.10.47.212	N/A	N/A	Oct 18, 2018, 3:14:50 PM	
Bastion 6 Toan	[WALLIX Bastion] SSH Session Disconnection	SSH Closed	user	10.10.47.59	10.10.47.212	wabadmin	bastion	Oct 18, 2018, 3:14:39 PM	
Bastion 6 Toan	[WALLIX Bastion] SSH Keyboard Input	SSH In Progress	user	10.10.47.59	10.10.47.212	wabadmin	bastion	Oct 18, 2018, 3:14:39 PM	
Bastion 6 Toan	[WALLIX Bastion] SSH Keyboard Input	SSH In Progress	user	10.10.47.59	10.10.47.212	wabadmin	bastion	Oct 18, 2018, 3:14:37 PM	
Bastion 6 Toan	[WALLIX Bastion] SSH Session Established Successfully	SSH Opened	user	10.10.47.59	10.10.47.212	wabadmin	bastion	Oct 18, 2018, 3:14:35 PM	
Bastion 6 Toan	[WALLIX Bastion] Authentify	User Login Attempt	user	10.10.47.59	10.10.47.212	N/A	N/A	Oct 18, 2018, 3:14:34 PM	
Bastion 6 Toan	[WALLIX Bastion] GUI Delete	Web In Progress	admin	10.10.47.59	10.10.47.212	N/A	N/A	Oct 18, 2018, 3:14:25 PM	
Bastion 6 Toan	[WALLIX Bastion] GUI List	Web In Progress	admin	10.10.47.59	10.10.47.212	N/A	N/A	Oct 18, 2018, 3:14:25 PM	
Bastion 6 Toan	[WALLIX Bastion] GUI List	Web In Progress	admin	10.10.47.59	10.10.47.212	N/A	N/A	Oct 18, 2018, 3:14:20 PM	
Bastion 6 Toan	[WALLIX Bastion] GUI List	Web In Progress	admin	10.10.47.59	10.10.47.212	N/A	N/A	Oct 18, 2018, 3:14:18 PM	
Bastion 6 Toan	[WALLIX Bastion] Authentify	User Login Attempt	admin	10.10.47.59	10.10.47.212	N/A	N/A	Oct 18, 2018, 3:14:17 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	vmiadmin	10.10.47.176	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:14:14 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	vmiadmin	10.10.47.176	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:13:44 PM	
Bastion Support	[WALLIX Bastion] GUI List	Web In Progress	vmiadmin	10.10.47.176	10.10.47.28	N/A	N/A	Oct 18, 2018, 3:13:14 PM	

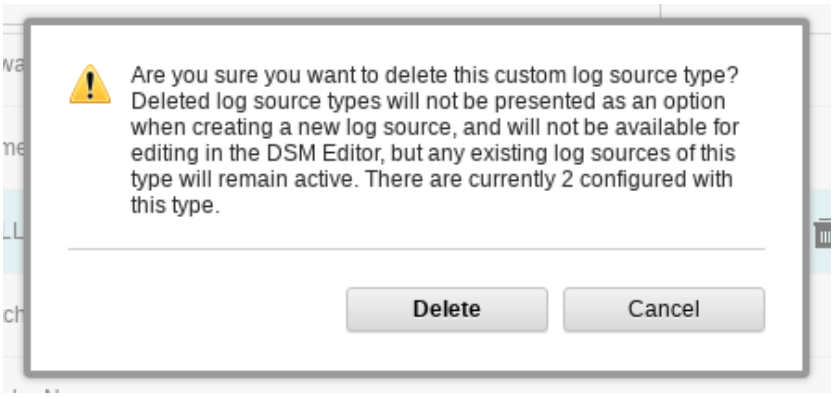
IV. DELETING WALLIX BASTION DSM

IV.1 DELETING FROM WEB INTERFACE

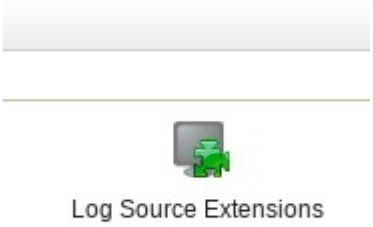
To delete WALLIX Bastion DSM, open the web interface as admin, then click on the DSM Editor :

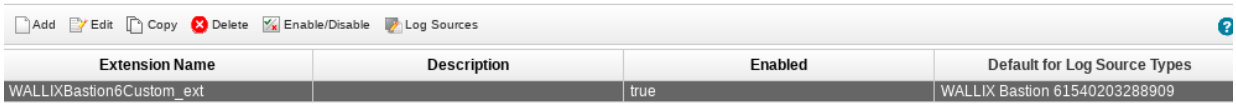
Find the WALLIX Bastion DSM then click on the bin icon





Then click on Log Source Extensions and delete the WALLIX Bastion Extension.





IV.2 DELETING FROM THE DATABASE

As mentionned by Qradar, deleting from the web interface doesn't completely delete the DSM from the database.

If you want to erase completely all data of the WALLIX Bastion DSM, you will need to go in console and use PostgreSQL commands :

Retrieving SensorDeviceType ID of the WALLIXBastion :

psql -U qradar -tA -c "select * from qradar.public.sensordevicetype;" | grep Bastion

result :

4001|WALLIXBastion6Custom|WALLIX Bastion 61540203288909|5||6||f|0|1|4000|

The SensorDeviceType ID is the ID of the WALLIX Bastion DSM, you will need it for all of the following commands. In this example, the ID is 4001.

A this stage, if you try to delete it, you will get an error :

psql -U qradar -tA -c "delete from qradar.public.sensordevicetype where id=4001;"

ERROR: update or delete on table "sensordevicetype" violates foreign key constraint "fk1940479ccaa923eb" on table "dsmevent"

DETAIL: Key (id)=(4001) is still referenced from table "dsmevent".

Delete reference from dsmevent table :

The error state that it is still referenced in the table « dsmevent », so you need to delete the reference from this table :

psql -U qradar -tA -c "delete from qradar.public.dsmevent where devicetypeid=4001;"

DELETE 51

If you try again to delete the SensorDeviceType, you will have another error :

psql -U qradar -tA -c "delete from qradar.public.sensordevicetype where id=4001;"

ERROR: update or delete on table "sensordevicetype" violates foreign key constraint "fkedfa8feb64c304c5" on table "sensordeviceprotocols"

DETAIL: Key (id)=(4001) is still referenced from table "sensordeviceprotocols".

Delete reference from sensordeviceprotocols table :

psql -U qradar -tA -c "delete from qradar.public.sensordeviceprotocols where sensordevicetypeid=4001;"

DELETE 68

Then again :

psql -U qradar -tA -c "delete from qradar.public.sensordevicetype where id=4001;"

ERROR: update or delete on table "sensordevicetype" violates foreign key constraint "sensordevicedevicetype_fkey" on table "sensordevice"

DETAIL: Key (id)=(4001) is still referenced from table "sensordevice".

Delete reference from sensordevice table :

psql -U qradar -tA -c "delete from qradar.public.sensordevice where devicetypeid=4001;"

DELETE 2

Delete sensordevicetype :

After that, you should be able to delete the sensordevicetype :

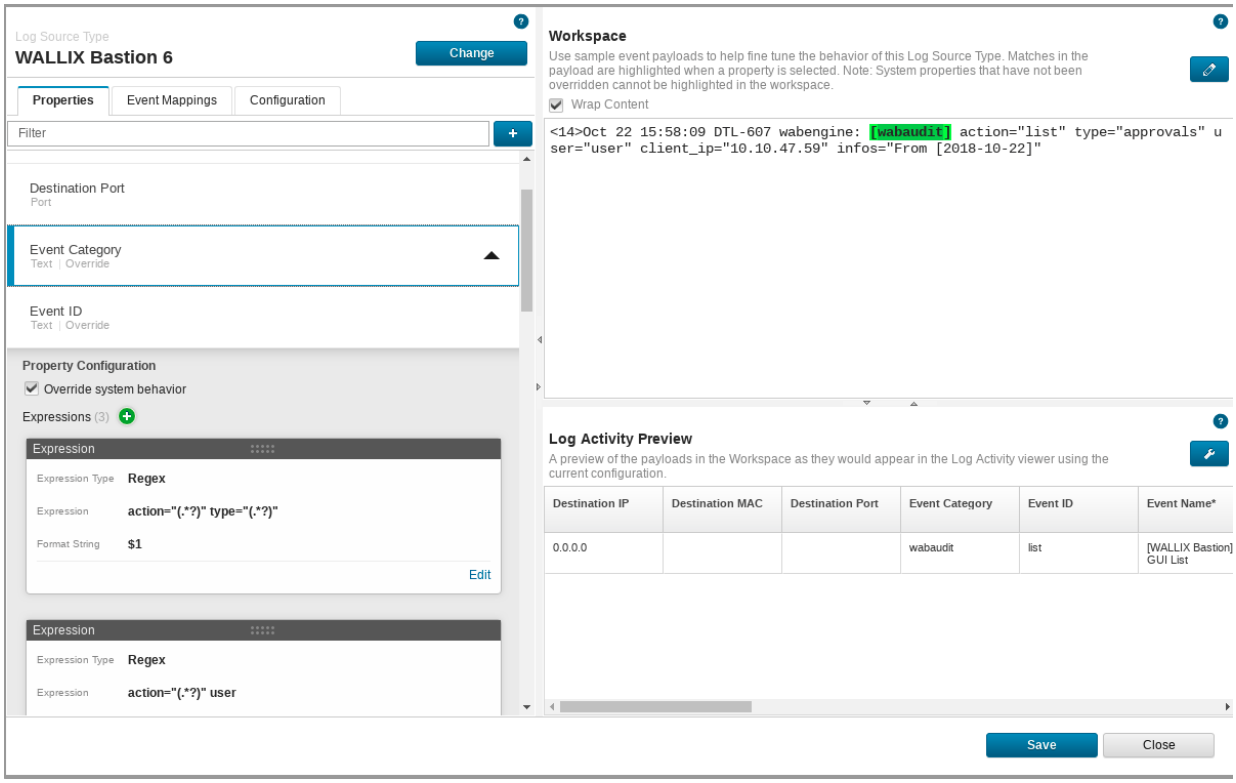
psql -U qradar -tA -c "delete from qradar.public.sensordevicetype where id=4001;"

DELETE 1

V. EVENTS MAPPING NOT WORKING

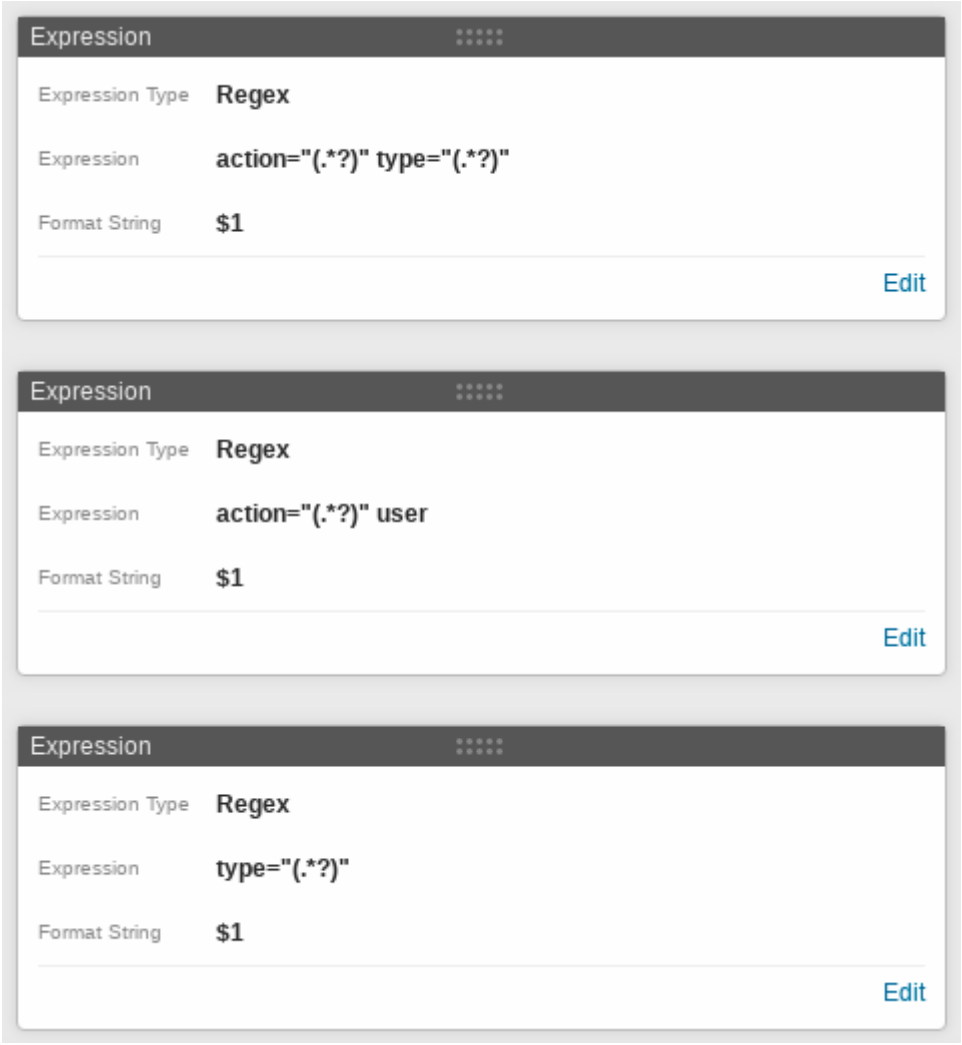
In case of « Unknown » logs events, you may want to check the properties of the DSM in the DSM Editor

Select the WALLIX Bastion DSM then copy and paste the unknown log in the « Workspace » :



Check that Event ID and Event Category are properly recognize, if not it means that the regex inside Properties are not properly set for it.

Click on Event ID and expand it, you should see 3 regex :



The regex allows Qradar to recognize the ID in the log, make sure you have them.

It will also be the same with the regex for Event Category :