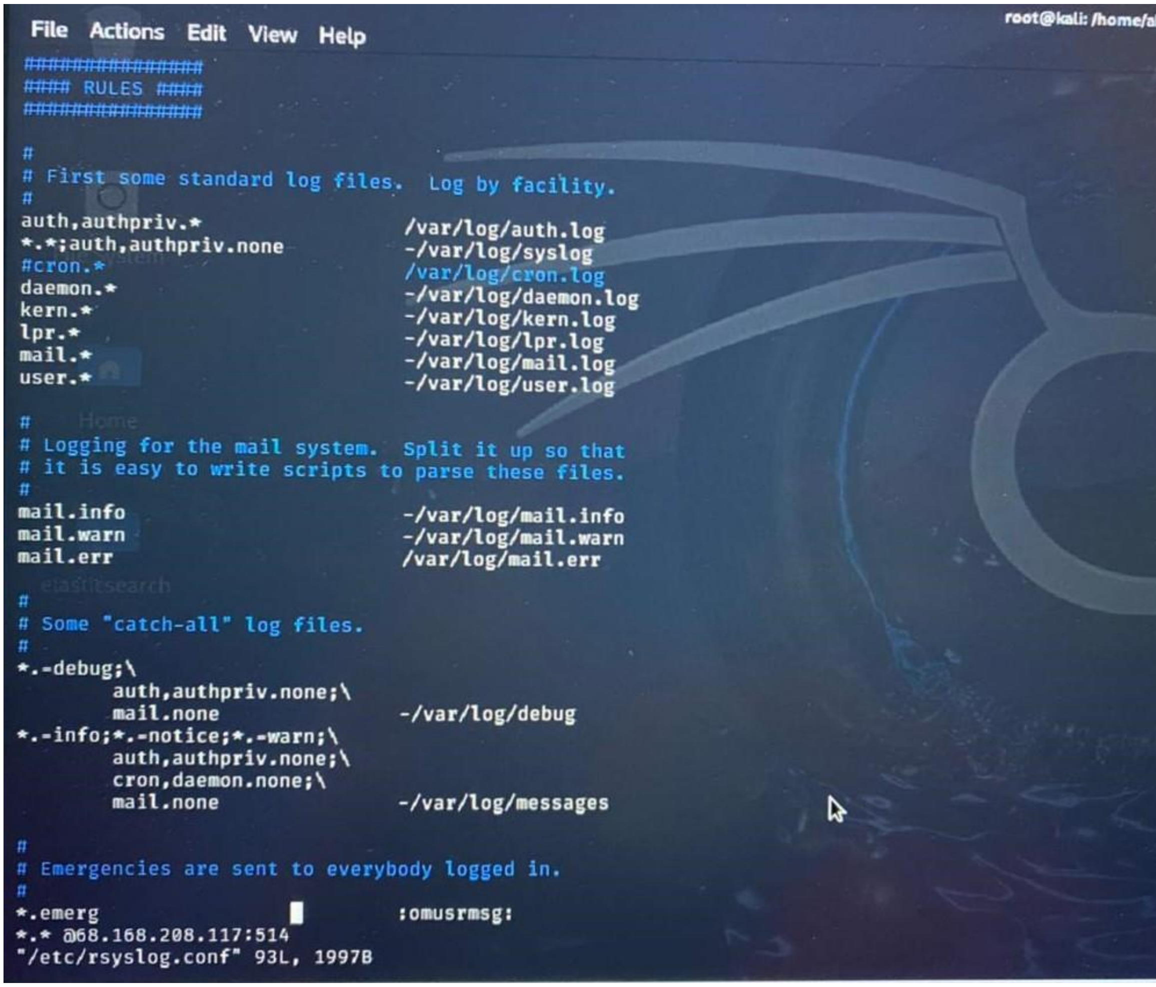
Data security

Assignment 3

First : integrating linux syslog with qradar

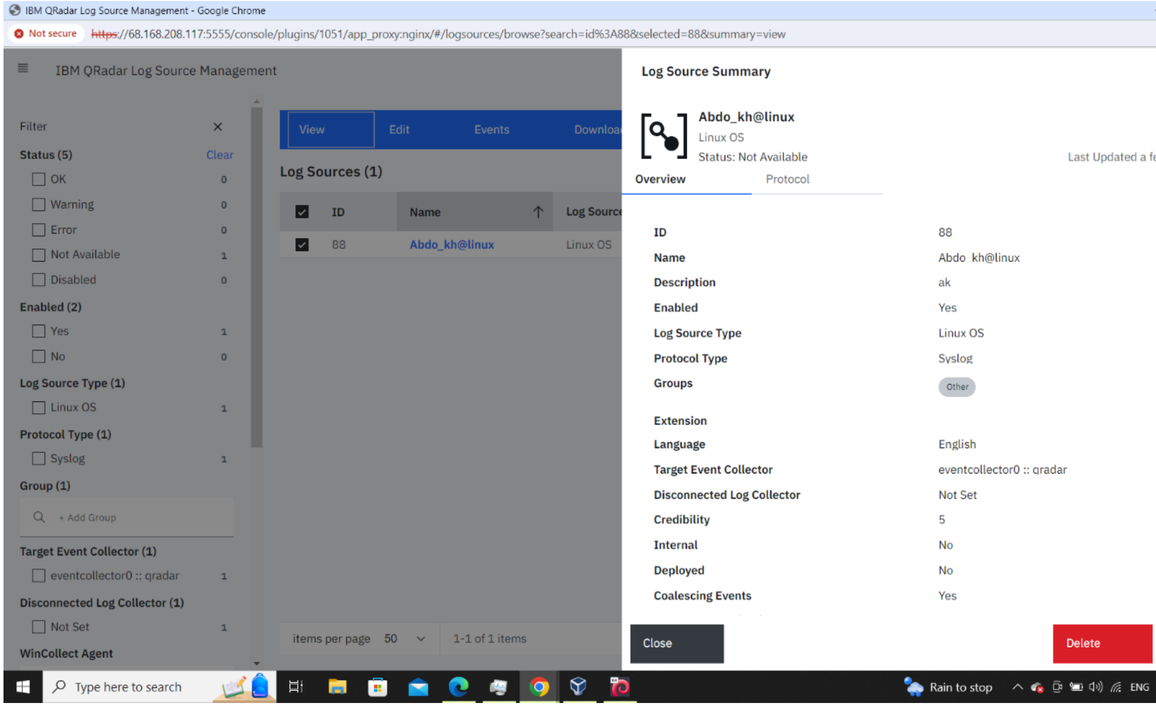
Steps:

- **Adding qradar ip address to syslog.conf files for logs forwarding**



```
#################
#### RULES ####
#################

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info                       -/var/log/mail.info
mail.warn                       -/var/log/mail.warn
mail.err                        /var/log/mail.err

#
# Some "catch-all" log files.
#
*.=debug;\
        auth,authpriv.none;\
        mail.none               -/var/log/debug
*.=info;*.=notice;*.=warn;\
        auth,authpriv.none;\
        cron,daemon.none;\
        mail.none               -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:
*.* @68.168.208.117:514
"/etc/rsyslog.conf" 93L, 1997B
```

- **After that I opened qradar web page and logged in , then I checked the log sources in the admin panel and I found the logs being transmitted successfully**



IBM QRadar Log Source Management - Google Chrome

Not secure https://68.168.208.117:5555/console/plugins/1051/app_proxy:nginx/#/logsources/browse?search=id%3A88&selected=88&summary=view

Log Sources (1)

ID	Name	Log Sourc
88	Abdo_kh@linux	Linux OS

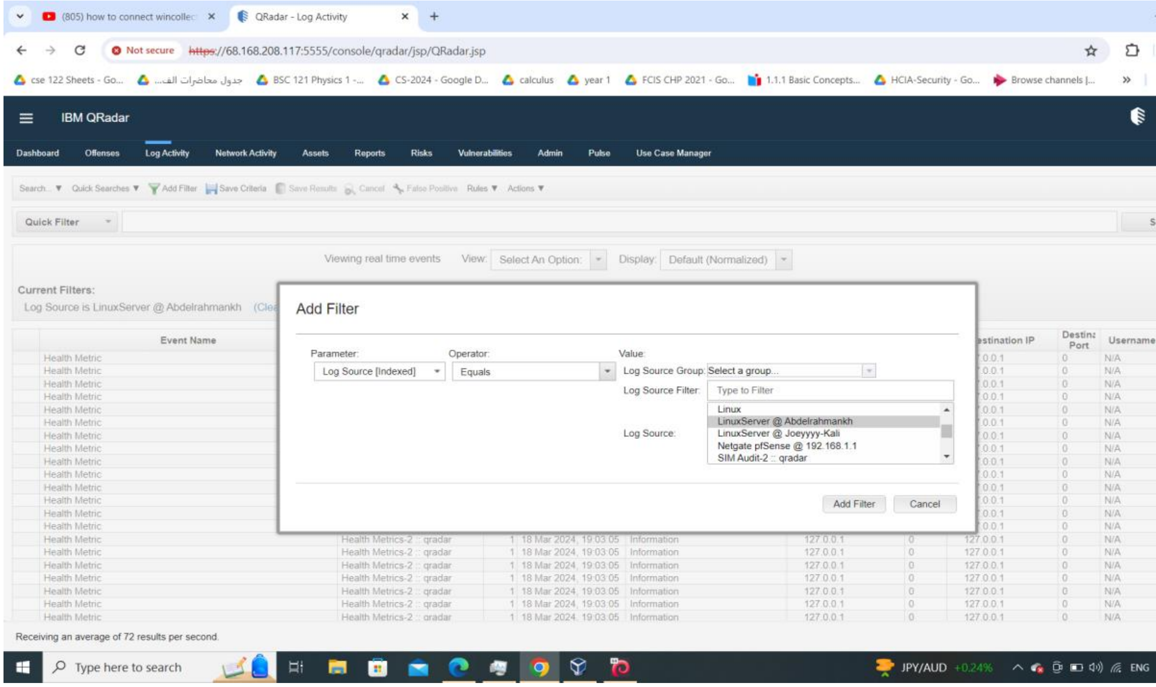
Filter: Status (5) — OK 0, Warning 0, Error 0, Not Available 1, Disabled 0; Enabled (2) — Yes 1, No 0; Log Source Type (1) — Linux OS 1; Protocol Type (1) — Syslog 1; Group (1); Target Event Collector (1) — eventcollector0 :: qradar 1; Disconnected Log Collector (1) — Not Set 1; WinCollect Agent

Log Source Summary

Abdo_kh@linux
Linux OS
Status: Not Available

ID	88
Name	Abdo_kh@linux
Description	ak
Enabled	Yes
Log Source Type	Linux OS
Protocol Type	Syslog
Groups	Other
Extension	
Language	English
Target Event Collector	eventcollector0 :: qradar
Disconnected Log Collector	Not Set
Credibility	5
Internal	No
Deployed	No
Coalescing Events	Yes

- **Then I changed my host name and applied filter to view only my Logs**



QRadar - Log Activity

Not secure https://68.168.208.117:5555/console/qradar/jsp/QRadar.jsp

IBM QRadar

Viewing real time events View: Select An Option: Display: Default (Normalized)

Current Filters:
Log Source is LinuxServer @ Abdelrahmankh

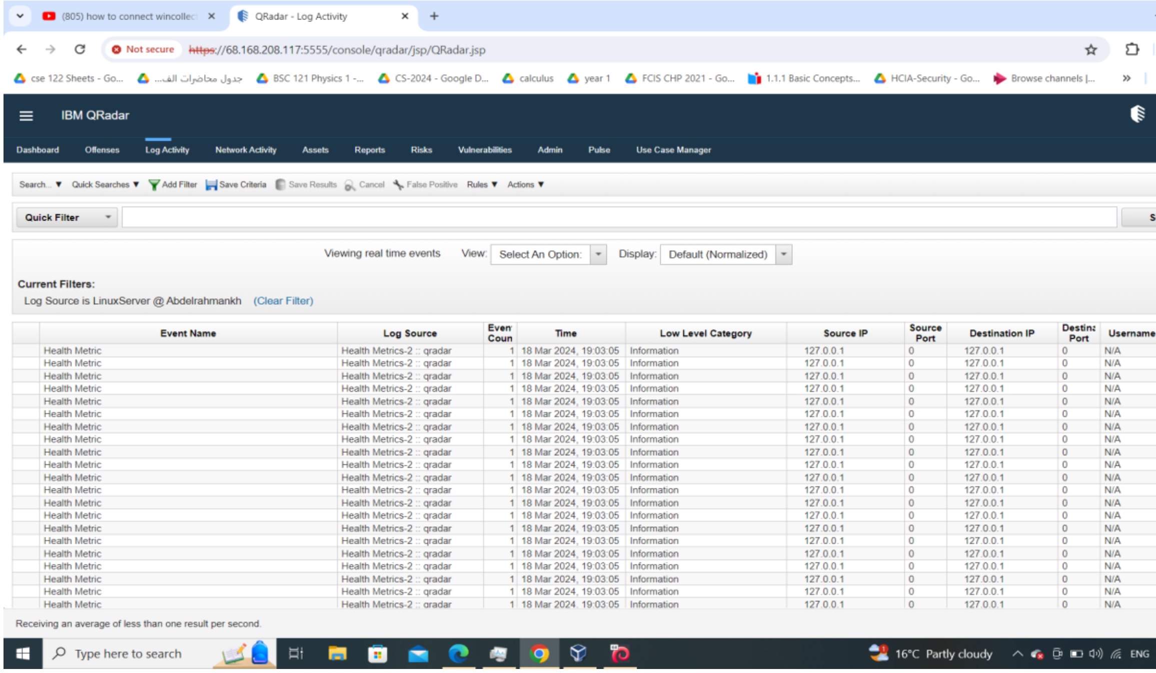
Add Filter

Parameter: Log Source [Indexed]
Operator: Equals
Value:
Log Source Group: Select a group...
Log Source Filter: Type to Filter
Log Source:
Linux
LinuxServer @ Abdelrahmankh
LinuxServer @ Joeyyyy-Kali
Netgate pfSense @ 192.168.1.1
SIM Audit-2 :: qradar

Add Filter Cancel

```
Health Metric   Health Metrics-2 :: qradar   1   18 Mar 2024, 19:03:05   Information   127.0.0.1   0   127.0.0.1   0   N/A
```

Receiving an average of 72 results per second.



Viewing real time events View: Select An Option: Display: Default (Normalized)

Current Filters:

Log Source is LinuxServer @ Abdelrahmankh (Clear Filter)

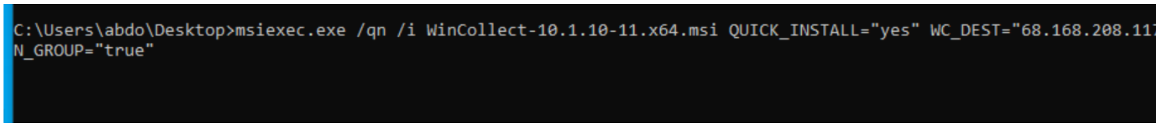
Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: qradar	1	18 Mar 2024, 19:03:05	Information	127.0.0.1	0	127.0.0.1	0	N/A

Receiving an average of less than one result per second.

Second : Integrating windows with qradar using wincollect agent

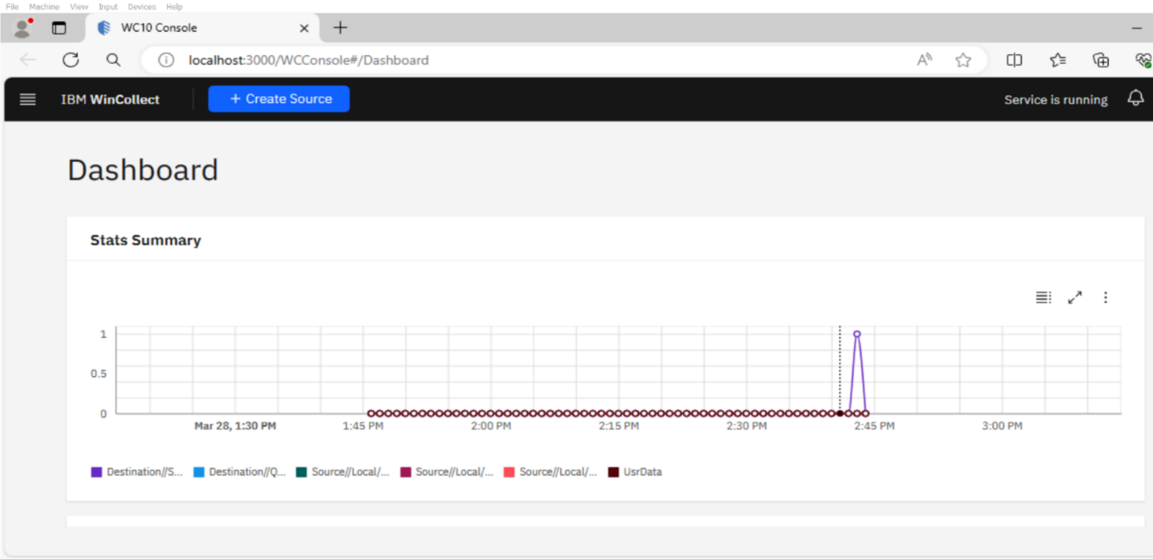
Steps:

- I could not install the agent by the normal way so I installed it using cmd

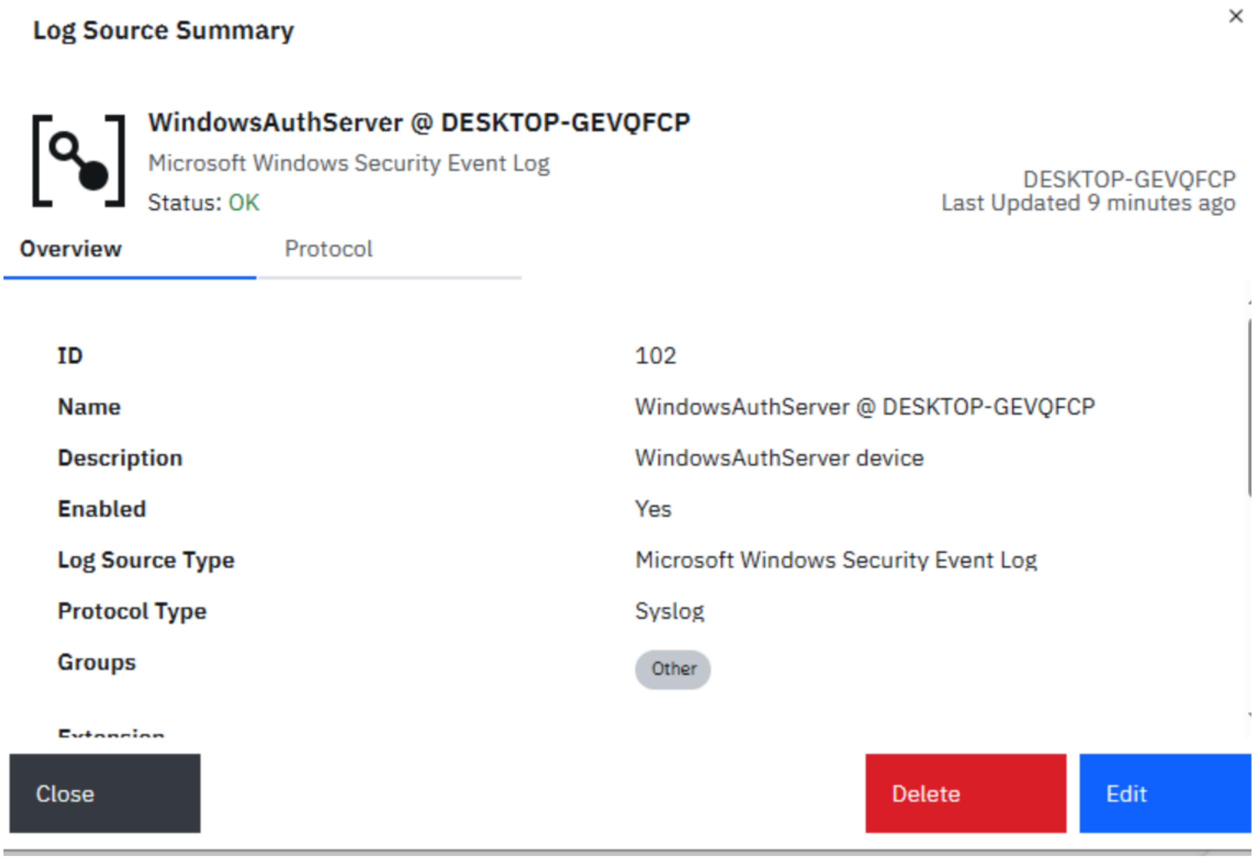


```
C:\Users\abdo\Desktop>msiexec.exe /qn /i WinCollect-10.1.10-11.x64.msi QUICK_INSTALL="yes" WC_DEST="68.168.208.11
N_GROUP="true"
```

- After that I ran the wincollect agent



- **After that I checked if the qradar is getting my logs successfully, and I have seen my hostname in the log sources under admin panel**



Log Source Summary

WindowsAuthServer @ DESKTOP-GEVQFCP

Microsoft Windows Security Event Log

Status: OK

DESKTOP-GEVQFCP
Last Updated 9 minutes ago

ID	102
Name	WindowsAuthServer @ DESKTOP-GEVQFCP
Description	WindowsAuthServer device
Enabled	Yes
Log Source Type	Microsoft Windows Security Event Log
Protocol Type	Syslog
Groups	Other
Extension	