CEF- Bugs and Fixes

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

Common issues - and fixes too!

Symptom	Problem	Solution	Add
Empty computer field in workspace	Missing field mapping line in /opt/microsoft/omsagent/plugin/filtere_syslog_security.rb	Run the cef_troubleshoot script and follow the instructions	App A
slow data stream, occasional agent malfunctions	Outdated Rsyslog regex	Run the cef_troubleshoot script and follow the instructions	App B
Data delays, data loss, server-level malfunctions	Full disk on the machine	Delete logs periodicaly (crontab), use logrotate, change daemon configuration (Doicumentation was add to both cef installation and troubleshoot scripts)	App C
Continues message to create exception in Firewall on RH machines	Fault detection of Firewalld exception rule	Redownload the troubleshoot script to the new version with the updated check.	App D
User sends Cisco ASA logs and many fields remain empty	Bug in OMS agent “/opt/microsoft/omsagent/plugin/security_lib” configuration file	Run the cef_troubleshoot script and follow the instructions	App E
User runs old cef scripts version although	There are older versions of the script in the same directory	Delete old script versions in the directory from which the user is running, Also-	Cha the dov com fror

Symptom	Problem	Solution	Add
redownloads the new one		the script download command was updated so it will run over any other scripts in the directory	"wg "wg
Everything seems to work but data doesn't flow to WS	Might have enabled SELinux on the machine	Run the troubleshoot script and follow the instructions on how to disable SElinux	App F
Changes to syslog configuration is being overwritten	Auto sync with the portal	Run the portal disable sync commnd (when in TS just run the script	App G

Appendixes:

A-

```
Warning: Current content of the omsagent syslog filter mapping configuration doesn't map the Computer field from your hostname.
To enable the Computer field mapping, please run:
"sed -i -e "/'Severity' => tags\[tags.size - 1\]/ a \ \t  'Host' => record['host']" -e "s/'Severity' => tags\[tags.size - 1\]/&,/" /opt/microsoft/omsagent/plugin/filter_syslog_security.rb && sudo /opt/microsoft/omsagent/bin/service_control restart 758faa33-c1de-4bb2-ae8d-57a7444d92a4"
```

B-

```
Error: found an outdated rsyslog daemon configuration file: /etc/rsyslog.d/security-config-omsagent.conf
The updated file should contain the following configuration: 'if $rawmsg contains "CEF:" or $rawmsg contains "ASA-" then @@127.0.0.1:25226'
Notice: Please run the following command to update the configuration and restart the rsyslog daemon:
"echo 'if $rawmsg contains "CEF:" or $rawmsg contains "ASA-" then @@127.0.0.1:25226' > /etc/rsyslog.d/security-config-omsagent.conf && service rsyslog restart"
```

C-

```
Warning: please make sure your logging daemon configuration does not store unnecessary logs. This may cause a full disk on your machine, which will disrupt the
function of the oms agent installed. For more information:
https://www.rsyslog.com/doc/master/configuration/actions.html
```

D-

```
Checking if firewalld is installed.
systemctl status firewalld
Warning: you have a firewall running on your linux machine this can prevent communication between the syslog daemon and the omsagent.
Checking if firewall has exception for omsagent port [25226]
Warning: no exception found for omsagent in the firewall
You can add exception for the agent port[25226] by using the following commands:
Add exception:
sudo firewall-cmd --direct --permanent --add-rule ipv4 filter INPUT 0 -p tcp --dport 25226  -j ACCEPT
Reload the firewall:
sudo firewall-cmd --reload
Validate the exception was added in the configuration:
sudo firewall-cmd --direct --get-rules ipv4 filter INPUT
You can disable your firewall by using this command - not recommended:
sudo systemctl stop firewalld
```

E-

```
Warning: Current content of the omsagent security configuration doesn't support Cisco ASA parsing.
To enable Cisco ASA firewall events parsing run the following:
"sed -i "s|return '%ASA' if ident.include?('%ASA')|return ident if ident.include?('%ASA')|g" /opt/microsoft/omsagent/plugin/security_lib.rb && sudo /opt/micr
osoft/omsagent/bin/service_control restart 758faa33-c1de-4bb2-ae8d-57a7444d92a4"
```

F-

```
Checking if security enhanced linux is enabled
getenforce
Security enhanced linux is in Enforcing mode.
This is not supported by the OMS Agent and can harm the communication with it.
For more information: https://docs.microsoft.com/azure/azure-monitor/platform/agent-linux
To set SELinux to Permissive mode use elevated privileges to perform the following:
Run the following command to temporarily change SELinux to permissive mode: "setenforce 0"
Please restart the syslog daemon running on your machine
In order to make changes permanent please visit: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/changing-selinux
-states-and-modes_using-selinux#changing-selinux-modes_changing-selinux-states-and-modes
For more information on SELinux: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/using_selinux/index
```

G-

```
sudo su omsagent -c 'python
/opt/microsoft/omsconfig/Scripts/OMS_MetaConfigHelper.py --disable'
```

References

Recording Session on CEF TSG (11/04/2020) : Click Here

Presentation Slides on CEF TSG (11/04/2020) : CEF presentation-slides.pptx