Updates to CEF and Syslog Data Connector

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

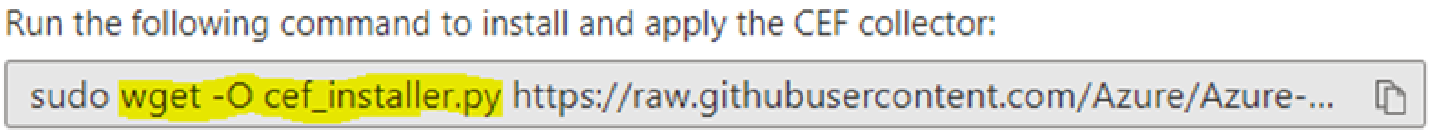
Contents

Here is an update on the progress of the CEF connector over the past few weeks.

The fixes below were implemented and already provide a response to the customers' needs.

Changing CEF scripts installation commands-

We changed the installation commands for the cef_installer.py and cef_troubleshoot.py script to contain "wget -O {script name}" instead of just "wget" (see the screenshot below).



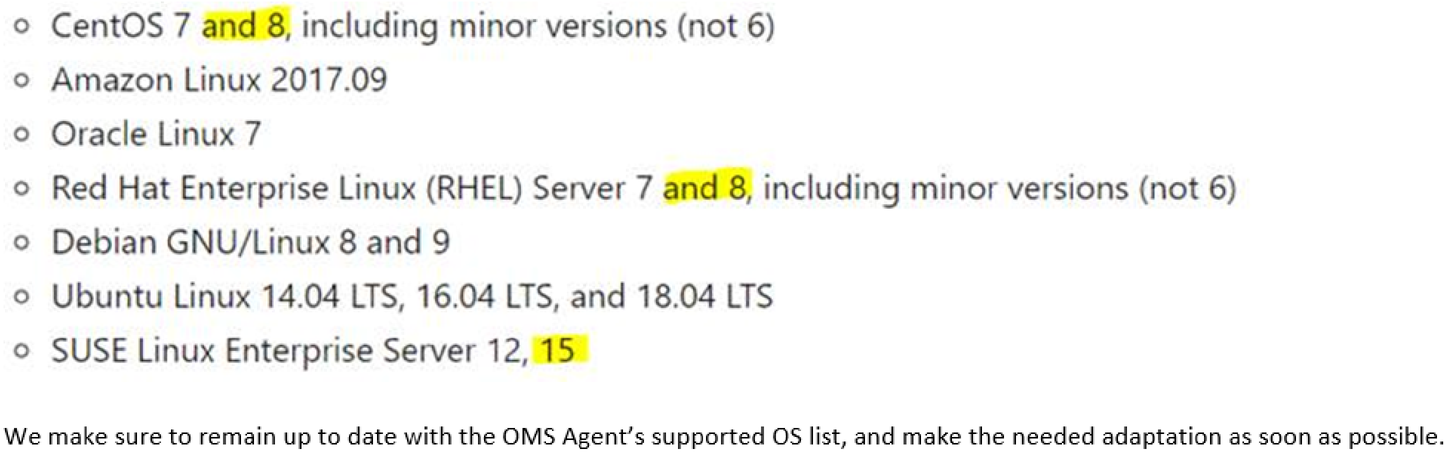
Run the following command to install and apply the CEF collector:

```
sudo wget -O cef_installer.py https://raw.githubusercontent.com/Azure/Azure-...
```

While this change might seem small, it is actually very crucial to our customers. This new command will override any old scripts in the users directory, making sure scripts don't pile up there and that only the newest script will be run instead of being rotated as previously done (see below).

Supporting new OS

It's been long coming: the support of new operating systems. Newest on the list: • CentOS 8 • RedHat 8 • SUSE Linux 15



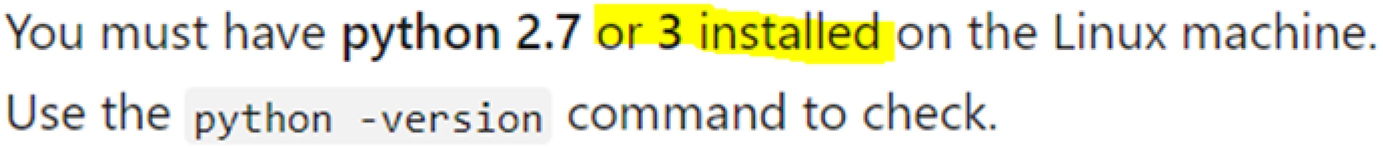
- CentOS 7 and 8, including minor versions (not 6)
- Amazon Linux 2017.09
- Oracle Linux 7
- Red Hat Enterprise Linux (RHEL) Server 7 and 8, including minor versions (not 6)
- Debian GNU/Linux 8 and 9
- Ubuntu Linux 14.04 LTS, 16.04 LTS, and 18.04 LTS
- SUSE Linux Enterprise Server 12, 15

We make sure to remain up to date with the OMS Agent’s supported OS list, and make the needed adaptation as soon as possible.

We make sure to remain up to date with the OMS Agent’s supported OS list, and make the needed adaptation as soon as possible.

Supporting Python 3

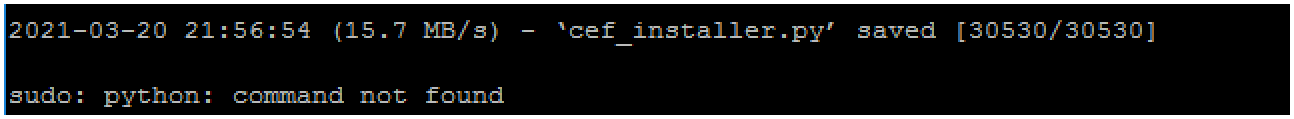
Probably even more anticipated then the previous bullet, we are happy to announce that we finished all the required checks and made all the needed changes in order to support Python 3! (in addition to the already supported python 2.7) Customers will now have the option to use whatever Python version they prefer (or whatever comes by default with their machine).



You must have **python 2.7** or 3 installed on the Linux machine. Use the `python -version` command to check.

Python: command not found

For Customers facing the error as shown below -



```
2021-03-20 21:56:54 (15.7 MB/s) - ‘cef_installer.py’ saved [30530/30530]

sudo: python: command not found
```

Simply replace python with python3 in the install script.

So the updated command should look similar to -

```
 sudo wget -O cef_troubleshoot.py https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/CEF/cef_troubleshoot.py&&sudo python3 cef_troubleshoot.py
```

Alert from auto-sync with the portal-

While mostly affecting customers who are using their machines to forward both CEF and Syslog messages, it’s good that everyone will be aware of this. Whenever a machine is auto-synced with the portal, any changes made to its syslog configuration will be overwritten by the configuration stated in the portal. We have created a check that detects such a sync and entered it to the troubleshooting script for customers to be aware of. Of course, we suggested a command for them to run to disable this auto-sync if they wish so.