SECRET VISONS

Utility for HP ArcSight Common Event Format (CEF) data inputs

Release Notes

Version 1.0.0

Yan Wen Digitally signed by Yan Wen Date: 2018.05.19 17:47:59 +10'00'

Publish Date: 19/05/2018

Legal Notices

License

The Utility for HP ArcSight CEF data inputs is open source add-on developed by Secret Visons under GNU General Public License v3.0. The users may use this software for both private and commercial usages free of charge. The developers may modify the software and redistribute the modification version of the application, but the developers should NOT remove the information of the original authors, NOR should the developers change the license conditions for commercial activities.

Warranty

The current version of Utility for HP ArcSight CEF data inputs is certified by Splunk and does NOT contain any malicious code which may impact the Splunk environment, including the Splunk application, the backbone infrastructure and the stored data. However, based on the GNU General Public License v3.0 agreement, Secret Visons do not hold any public liability of this product, nor should provide any warranty.

Support Information

Currently, Secret Visons provide the community support for the Utility for HP ArcSight CEF data inputs.

If you encountered any issue or have any question, please feel free to contact the support (support@secretvisons.com), or send the emails to the author (rockey@secretvisons.com), or you can raise the tickets via GitHub (https://github.com/SecretVisons/Splunk_ArcSight).

Revision History

Version	Date	Author	Summary
1.0	May 19, 2018	Yan (Rockey) Wen	Release notes for Util_ArcSightCEF_datainputs version 1.0.0.

Contents

Application Summary

Background

This is the optional accessory for the Technology Add-on for HP ArcSight CEF data inputs. The add-on is meant to be deployed on the on premise Splunk instances, hybrid cloud or public clouds (IaaS and PaaS) Splunk instances, including Splunk heavy forwarders, Splunk indexer nodes (if there are CEF data streams directly reaching the indexer nodes), or used in all-in-one instances (primarily in develop environments).

This Splunk add-on was originally a part of the Technology Add-on for HP ArcSight CEF data inputs (https://splunkbase.splunk.com/app/3694). Considering the growth of the managed cloud (SaaS) Splunk instances, such as Splunk Cloud, the built-in index time functions like log source renaming and sourcetype renaming might not be compatible with those cloud configurations.

To reduce the efforts deploying the Technology Add-on for HP ArcSight CEF data inputs in various environments, those features were removed from the Technology Add-on for HP ArcSight CEF data inputs and form this Splunk add-on.

Change History

Content Details

The following table lists the changes have been made in the current release (version 1.0.0):

File path	File Name	Summary
Util_ArcSightCEF_datainputs/	README	Brief summary of the Utility for HP ArcSight CEF data inputs
	app.manifest	Application manifest file for Utility for HP ArcSight CEF data inputs.
	LICENSE	License agreement document
Util_ArcSightCEF_datainputs/default	app.conf	Contains the base information about this Splunk add-on.
	props.conf	Used for Field extractions and transformations.
	transforms.conf	REGEX configurations for the field transformation.
Util_ArcSightCEF_datainputs/docs	CHANGES.LOG	Document the changes over the develop versions.
	REFERENCES	Reference information relevant to the Splunk add-on.
Util_ArcSightCEF_datainputs/metadata	default.meta	Default metadata files.
Util_ArcSightCEF_datainputs/static	appIcon.png	Splunk app Logo.
	appIcon_2x.png	Splunk app Logo.
	appLogo.png	Splunk app Logo.
	appLogo_2x.png	Splunk app Logo.

Support Matrix

The following table lists the support details between different versions of the Utility for HP ArcSight CEF data inputs:

App Version	Splunk Enterprise (on premise or public clouds)	Splunk Cloud
1.0.0	6.5.x, 6.6.x, 7.0.x, 7.1.x	No[*]

* Notes that this add-on is designed to be deployed onto the on premise Splunk instances or the Splunk instances in the hybrid/public clouds (IaaS and PaaS). This add-on should NOT be deployed on the managed clouds such as Splunk Cloud

Known issues

There is no known issue or bug by the time the current version is released. However, this add-on will NOT work properly if you already have some other Splunk apps or add-ons which perform the index time source renaming, sourcetype renaming or field extractions.