Understanding best practices for Splunk Connect for Syslog

As a Splunk admin, you need to easily ingest syslog data, at scale, while removing the requirement of up-front design work and “syslog-fu”. You need a turnkey, scalable, and repeatable approach for syslog data ingestion. Therefore, you download the Splunk Connect for Syslog Add-on, which enables you to achieve the following:

- Transport syslog data into Splunk at extremely high scale (> 5 TB/day from a single instance to multiple indexers)
- Properly categorize (sourcetype) for the most common data sources, with little to no custom configuration
- Provide enhanced data enrichment beyond the standard Splunk metadata of timestamp, host, source, and sourcetype
- Provide for additional custom-designed “filters” for additional sourcetypes beyond those supported out of the box

Now, you want some recommendations so you can be sure you have implemented the add-on the best way possible in your environment.

How to use Splunk software for this use case

As you use the Splunk Connect for Syslog add-on, you may find some or all of the following best practices helpful:

- Filtering syslog data to dev null
- Adding compliance data to syslog data in stream
- Routing syslog data to custom indexes

Next steps

Implementing these best practices will help you customize your deployment and use syslog data more efficiently and effectively. In addition, Splunk Connect for Syslog is fully Splunk supported and is released as open source. Join the community to provide feedback, enhancement ideas, communication, and log path (filter) creation Formal request for feature (especially log path/filters) inclusion, bug tracking, and more can be conducted via the GitHub repo.

Finally, the content in this guide comes from a previously published blog, one of the thousands of Splunk resources available to help users succeed. These additional Splunk resources might help you understand and implement this use case:

- .Conf Talk: Splunk Connect for Syslog: Extending the platform
- Docs: Welcome to Splunk Connect for Syslog

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.