splunk-connect-for-syslog Documentation

Release latest

May 24, 2022

CONTENTS

# Introduction

When using Splunk Connect for Syslog to onboard a data source, the syslog-ng “app-parser” performs the operations that are traditionally performed at index-time by the corresponding Technical Add-on installed there. These index-time operations include linebreaking, source/sourcetype setting and timestamping. For this reason, if a data source is exclusively onboarded using SC4S then you will not need to install its corresponding Add-On on the indexers. You must, however, install the Add-on on the search head(s) for the user communities interested in this data source.

SC4S is designed to process “syslog” referring to IETF RFC standards 5424, legacy BSD syslog, RFC3164 (Not a standard document), and many “almost” syslog formats.

# SC4S Documentation link The rest of the documentation is moved to [SC4S new documents](https://splunk.github.io/splunk-connect-for-syslog/main/)

Owner: rjha-splunk[^1].