Aruba Networks Add-on for Splunk Documentation

Release 0.1.0

Diogo Silva

Jan 10, 2022

Contents:

1 Introduction 1

2 Release Notes 3

3 Requirements 5

4 Installation 7

5 Sourcetypes 9

6 Troubleshooting 15

7 Support 17

8 Indices and tables 19

CHAPTER 1

Introduction

CHAPTER 2

Release Notes

2.1 v0.1.3 - August 2020

- Added missing extractions to aruba:wms
- Removed unused REGEX
- Added missing sourcetype renaming for FW Visibility
- Added missing sourcetype aruba:fw_visibility and rename old sourcetype for compatibility
- Added missing extractions for aurba:httpd
- Added url related fields to aruba:httpd
- Added mssing extractions for aruba:aaa

2.2 v0.1.2 - July 2020

- Minor fixes

2.3 v0.1.1 - October 2019

- Added missing extractions for CIM compliance
- Updated aruba_actions.csv

2.4 v0.1.0 - September 2019

- Public release to splunkbase

2.4.1 Major features

- Sourcetype renaming depending on log type
- Field extractions
- Event description enrichment
- Event types and tags assignment for CIM compliancy

CHAPTER 3

Requirements

- Splunk 7.0 or newer
- ArubaOS 7.2 or newer

CHAPTER 4

Installation

4.1 Install the Aruba Networks Add-on for Splunk

- Get the Aruba Networks Add-on for Splunk by downloading it from Splunkbase or browsing to it using the app browser within Splunk Web.
- Determine where and how to install this add-on in your deployment, using the tables on this page.
- Perform any prerequisite steps before installing, if required and specified in the tables below.
- Complete your installation.

4.1.1 Distributed deployments

Reference the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, all supported add-ons can be safely installed to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in Splunk Add-ons for more information.

This table provides a reference for installing this specific add-on to a distributed deployment of Splunk Enterprise.

Splunk platform component	Supported	Required	Comments
Search Heads	Yes	Yes	Install this add-on to all search heads.
Indexers	Yes	Optional	Required for the parsing operations (sourcetype renaming) if the data is not coming from a heavy forwarder.
Heavy Forwarders	Yes	Optional	Required for the parsing operations (sourcetype renaming).
Universal Forwarders	Yes	Optional	

Distributed deployment compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality.
Indexer Clusters	Yes	
Deployment Server	Yes	Supported for deploying via Deployment server

4.1.2 Installation walkthroughs

The Splunk Add-Ons manual includes an Installing add-ons guide that helps you successfully install any add-on to your Splunk platform. For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud

CHAPTER 5

Sourcetypes

5.1 aruba:aaa

Description: AAA logging security, system, user

5.2 aruba:ads

Description: Logging for Anomaly Detection system

5.3 aruba:approc

Description: Logging for AP processes system

5.4 aruba:authmgr

Description: Logging for user authentication security security, network, system, user, wireless security, system, user

5.5 aruba:certmgr

Description: Logging for Certificate Manager security, system

5.6 aruba:cfgm

Description: Logging for Configuration Manager system

5.7 aruba:crypto

Description: Logging for VPN (IKE/IPSEC) security, network, system, user

aruba:cts — Description: Logging for transport service system

5.8 aruba:dbsync

Description: Logging for Database Synchronization system

5.9 aruba:dhcpd

Description: Logging for DHCP packets network

5.10 aruba:dhcpdwrap

Description: Logging for DHCP network

aruba:esi — Description: Logging for External Services Interface system, network, user

5.11 aruba:fpapps

Description: Logging for Layer 2,3 control network, system

5.12 aruba:httpd

Description: Logging for Apache system, security

5.13 aruba:l2tp

Description: Logging for L2TP security

5.14 aruba:ldap

Description: Directory access protocols security, network, system, user, wireless

5.15 aruba:licensemgr

Description: Logging for license manager system

5.16 aruba:lldp

Link Layer Discovery Protocol https://community.arubanetworks.com/t5/Controller-Based-WLANs/LLDP-on-Aruba-Controller/ta-p/180578

5.17 aruba:localdb

Description: Logging for local database security, network, system, user, wireless

5.18 aruba:meshd

Description: Logging for Mesh daemon security, system, wireless

5.19 aruba:mobileip

Description: Logging for Mobile IP security, network, system, user

5.20 aruba:nanny

Description: Logging for process management system

aruba:ntp — Description: Network Time Protocol network, system

5.21 aruba:packetfilter

Description: Logging for packet filtering of messaging and control frames system

5.22 aruba:phonehome

Description: Logging for PhoneHome network, system

aruba:pim — Description: Logging for Protocol Independent Multicast system, network, user

aruba:ppp — Description: Logging for PPP security, network, system, user

5.23 aruba:pppoed

Description: Logging for PPPoE security, network, system, user

5.24 aruba:pptp

Description: Logging for PPTP security, network, system

5.25 aruba:processes

Description: Logging for run-time processes system

5.26 aruba:profmgr

Description: Logging for Profile Manager system

5.27 aruba:publisher

Description: Logging for publish subscribe service system

aruba:rfd — Description: Logging for RF Management daemon (AP) system

aruba:rfm — Description: Logging for RF Troubleshooting Manager system

5.28 aruba:sapd

Description: Logging for Access Point Manager (AP) system

5.29 aruba:sapm

Description: Logging for Access Point Manager (Controller) system, wireless

5.30 aruba:snmp

Description: SNMP logging security, system

aruba:stm — Description: Logging for Station Management security, network, system, user, wireless

5.31 aruba:syslogdwrap

Description: Logging for System Logging daemon system

5.32 aruba:traffic

Description: Logging for traffic system

5.33 aruba:voip

Description: Voice over IP issues security, network, system, user, wireless

5.34 aruba:vrrpd

Description: Logging for VRRP system

aruba:wms — Description: Logging for Wireless Management (Master switch only) security, network, system, wireless

CHAPTER 6

Troubleshooting

Vendor Docs https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c05316684

Syslog Messages https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c05321932

CHAPTER 7

Support

7.1 Bugs & Support Issues

You can file bug reports on our GitHub issue tracker and they will be addressed as soon as possible. **Support is a volunteer effort** and there is no guaranteed response time.

CHAPTER 8

Indices and tables

- genindex
- modindex
- search