Release Notes for Cisco Web Security Appliance Advanced Reporting (Releases 2.0 and Later)

Published: May 03, 2013
Revised: November 20, 2014

Contents

New Features

What's New in Release 3.0

Feature	Description
Support for additional AsyncOS versions	Some versions of AsyncOS 8.0.x for Cisco Web Security Appliances are supported, excluding reporting for Advanced Malware Protection (AMP) features. See AsyncOS and Splunk Version Compatibility, page 2.
Support for Splunk 6.1.4	Users of Cisco Web Security Appliance Advanced Reporting version 3.0 can use the application with Splunk 6.1.4

Cisco Systems, Inc.
www.cisco.com

Feature	Description
Improved performance	Faster report generation.
Web Tracking query improvement	Web Tracking queries now default to the currently selected fields instead of to a predefined set of default values.

What's New in Release 2.0

Feature	Description
New Reports	Top Destinations for SOCKS. Top User for SOCKS.
SOCKS and L4TM Tracking	Search capabilities for SOCKS and Layer 4 Traffic Monitor.

System Requirements

AsyncOS and Splunk Version Compatibility

Note Scheduled report PDFs cannot be generated when using Splunk 6.2.

Cisco Web Security Appliance Advanced Reporting Application	AsyncOS for Web Security	Splunk
3.0	8.0.6 (excluding AMP data)	6.1.4
	8.0	5.0.10
2.0	7.7	5.x

Requirements for Splunk Instances

Find the system requirements for Splunk releases on their web site: http://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements.

Select the Splunk version from the drop-down list.

Requirements for Cisco Web Security Appliance Advanced Reporting

Operating System Requirements:

- Red Hat Linux
- Windows

Platform Requirements: Reference hardware can be commodity-grade, and must have the following minimum specifications to be eligible for Cisco support.

- Intel x86-64-bit chip architecture with (2) CPU's, 4 cores per CPU, 2.5-3Ghz per core
- 16GB RAM
- (4) 300GB SAS hard disks at 10,000 rpm each in RAID10 (800 IOPS or better)
- Standard 1Gb Ethernet NIC, optional 2nd NIC for a management network

Note Splunk is often constrained by disk I/O first, so always consider that first when selecting the storage hardware.

The file system will be assumed to be running on local disk volumes formatted as NTFS or EXT2/3. A separate OS volume should be created per industry best practices. The Splunk installation should reside on its own logical volume whenever possible.

Sizing & Scaling Recommendations

- The base configuration is a single-tier architecture with one server offering all 3 parts of the core functionality of a typical Splunk deployment:
  - a search head
  - an indexer
  - a monitor for data sources
- If the estimated requirements for indexed data volume exceed 100k/Users (estimate: 100GB/day,) the Splunk infrastructure should be adjusted.
- By adding another Splunk instance and adjusting the configuration, the new infrastructure would offer an increase in aggregate indexing and search performance (once the data is load-balanced), and an increase in storage and retention capacity.
- A dedicated forwarder server would also be added to the Splunk infrastructure and configured to monitor the WSA log files and forward the log data across multiple indexers using load balancing.
- To facilitate the implementation and configuration of an environment that exceeds 100k users, it is recommended that Cisco engage Splunk professional services on behalf of the Cisco Web Security Appliance customer.

Based upon log volume estimates against a Cisco Web Security Appliance with 10k users, the amount of data collected is 10GB/day uncompressed. Once indexed, the data compresses to an estimated 2.5GB/day indexed storage used. The Splunk instance would retain approximately 200 days of indexed data based upon a volume size of 500GB.

Cisco Web Security Appliance Users	Estimated Log Volume (2,500 transactions/user/day)	Estimated Indexed Volume	Estimated retention (500GB volume)
10K	10GB/day	2.5GB	200 days
50K	50GB/day	13GB	40 days
100K	100GB/day	25GB	20 days

Note Guidelines based upon estimated log volumes and mid-capacity drives in an array.

Daily Volume	77 GB/day	140 GB/day	180GB/day
Total Transactions	172 Million	325 Million	417 Million
Predefined Report Load time	<5 seconds	<10 seconds	<15 seconds

Total Volume	2.3 TB
Business days retention @70GB/day	33
Predefined Report Loading time	<20 seconds

Install and Upgrade Instructions

For essential instructions, including scripts to be run, see the *Cisco Web Security Appliance Advanced Reporting Installation, Setup, and User Guide,* available from the location shown in Related Documentation, page 4.

Related Documentation

The following documentation is available from http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html.

- *Cisco Web Security Appliance Advanced Reporting Installation, Setup, and User Guide*
- User Guide for your supported release of AsyncOS for Cisco Web Security Appliances

Previous documentation for this product used "Splunk Application for Cisco Web Security Appliance" as the product name.

Support

Cisco Support Community

Cisco Support Community is an online forum for Cisco customers, partners, and employees. It provides a place to discuss general web security issues as well as technical information about specific Cisco products. You can post topics to the forum to ask questions and share information with other Cisco and Cisco IronPort users.

Access the Cisco Support Community for web security and associated management at the following URL:

https://supportforums.cisco.com/community/netpro/security/web

Customer Support

International: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.