Release Notes for Web Security Advanced Reporting (Release 4.5)

Published: June 22, 2015
Revised: December 11, 2015

Contents

What's New in Release 4.5

Feature	Description
Advanced Malware Protection (AMP)	Added AMP-related reporting; specifically reports for Advanced Malware Protection, File Analysis and AMP Verdict Updates. **Note** This feature supports only WSA; CWS AMP log reporting is not available in this release.

Cisco Systems, Inc.
www.cisco.com

System Requirements

AsyncOS Version Compatibility

Web Security Advanced Reporting Application	AsyncOS for Web Security	
4.5	8.5	

Note Scheduled report PDFs cannot be generated.

Requirements for Web Security Advanced Reporting

Operating System Requirements

- Red Hat Linux (64-bit)
- Windows (64-bit)

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 two CPUs, six cores per CPU, 2.5-3 Ghz per core (minimum)
- 16 GB RAM
- Four 300-GB SAS hard disks at 10,000 rpm each, in RAID1+0 (800 IOPS or better)
- Standard 1-Gb Ethernet NIC, optional second NIC for a management network

Note Web Security Advanced Reporting Enterprise is often constrained by disk I/O first, so always consider disk infrastructure 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 Enterprise 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 three parts of the core functionality of a typical Web Security Advanced Reporting Enterprise deployment:
  - a search instance
  - an indexer
  - a monitor for data sources
- If the estimated requirements for indexed data volume exceed 100 K/Users (estimate: 100 GB/day,) the Enterprise infrastructure should be adjusted.

- By adding another Enterprise 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 Enterprise 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 you engage Professional Services.

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

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

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

Daily Volume	77 GB/day	140 GB/day	180 GB/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 @70 GB/day	33
Predefined Report Loading time	< 20 seconds

Total Users	Daily Indexing Volume						
	< 2 GB/day	2 to 250 GB/day	250 to 500 GB/day	500 to 750 GB/day	750GB to 1 TB/day	1 to 2 TB/day	2 to 3 TB/Day
< 4	1 combined instance	1 Search instance 1 Indexer	1 Search instance 2 Indexers	1 Search instance 3 Indexers	1 Search instance 4 Indexers	1 Search instance 8 Indexers	1 Search instance 12 Indexers
up to eight	1 combined instance	1 Search instance 1 Indexer	1 Search instance 2 Indexers	1 Search instance 4 Indexers	1 Search instance 5 Indexers	1 Search instance 10 Indexers	1 Search instance 15 Indexers

Total Users	Daily Indexing Volume						
up to 16	1 Search instance 1 Indexer	1 Search instance 1 Indexer	1 Search instance 3 Indexers	1 Search instance 4 Indexers	2 Search instance 6 Indexers	2 Search instance 12 Indexers	2 Search instance 18 Indexers
up to 24	1 Search instance 1 Indexer	1 Search instance 2 Indexers	1 Search instance 3 Indexers	1 Search instance 4 Indexers	2 Search instance 6 Indexers	2 Search instance 12 Indexers	2 Search instance 18 Indexers
up to 48		1 Search instance 2 Indexers	1 Search instance 3 Indexers	1 Search instance 4 Indexers	3 Search instance 8 Indexers	3 Search instance 16 Indexers	3 Search instance 24 Indexers

Install and Upgrade Instructions

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

Licensing

This release provides “hybrid reporting”; that is, support for both WSA and CWS log reports. To use hybrid reporting, you must upgrade your licenses; however, you can continue to use WSA-only reporting with your existing license. Refer to the “Licensing and Migration” section of the *Cisco Web Security Advanced Reporting Installation, Setup, and User Guid*e for more information.

Note To migrate from WSA-only to hybrid reporting, you must open a Cisco Technical Assistance Center (TAC) case to remove your existing license and install a new hybrid-reporting license that contains the complete list of reporting source types (that is, the `ciscocws` source type is included). This is not necessary if you are a new user of Web Security Advanced Reporting version 4.0.

Open Issues

- Application name and type is missing in CWS log extraction and so related reports will not work for CWS or aggregate data sources.
- Time shown in the time-spent column is not in user-readable format.
- Application name and application type are missing in the CWS logs. (CSCut57068)

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.

- *Web Security Advanced Reporting Installation, Setup, and User Guide*

- User Guide for your supported release of AsyncOS for Web Security Appliances

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

Support Site: Visit 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.