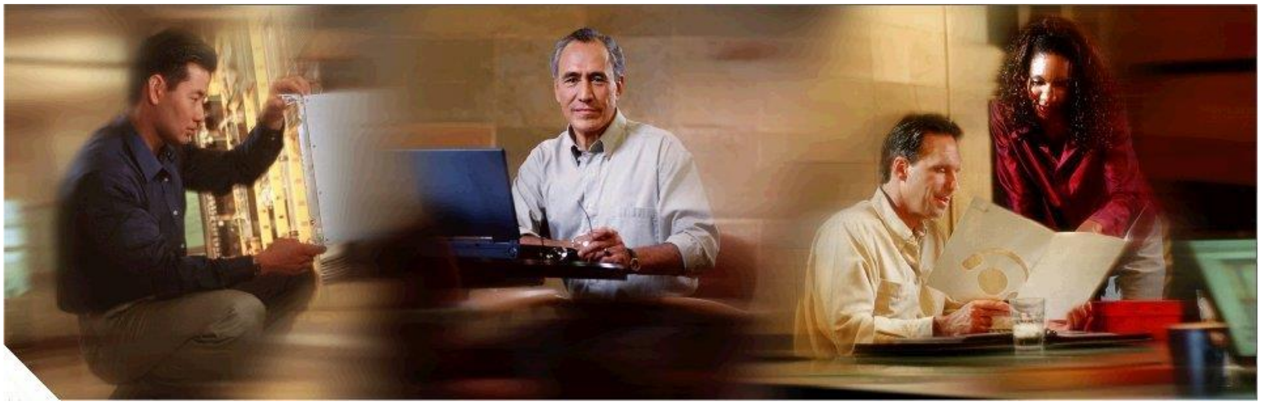
Cisco Advanced Web Security Reporting Distributed Deployment Guide



Terminologies

Terminology	Definition
AWSR	Advanced Web Security Reporting
WSA	Web Security Appliance
CWS	Cloud Web Security
Node	Any instance of AWSR

Table of Contents

Table of Contents

1 Introduction

The Cisco Advanced Web Security Reporting (AWSR) application provides filters and dashboards that are designed to give insight into very large volumes of data from multiple Web Security Appliances, Cloud Web Security (CWS) gateways, and Cisco Umbrella. The Cisco Advanced Web Security Reporting application includes a data collection and display application, and a related server that forwards log data collected from Web Security Appliances (WSAs), CWS services, and an Umbrella host.

1.1 AWSR Components and Pipeline

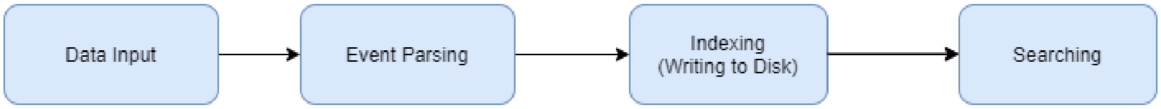


Fig 1. AWSR Data Pipeline

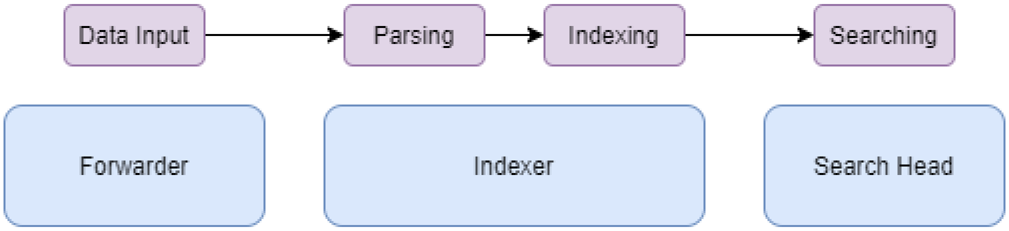


Fig 2. AWSR Components

Forwarder

Forwarder is an AWSR instance which consumes the data and forward it to the Indexers for processing. It requires minimal resources as it has limited impact on the performance, as compared to indexer and search head.

Indexer

Indexer is the cardinal AWSR instance which will parse, index and store the data coming from the forwarder. This AWSR instance transforms the incoming data into events and stores it in indexers for performing search operations efficiently. The Indexers also search the data, in response to requests from the Search Head. Dashboard and report requests (including request from Search Head) are processed in the indexer.

Search Head

Search head is the instance which provides an interface to view the data stored in indexer to the users. It is used for interacting and visualizing log data on the pre-built reports of AWSR and to build custom reports using Custom Filter.

1.2 Distributed Deployment

In single-instance deployments, one instance of AWSR handles all aspects of processing data, from input through indexing to search. A single-instance deployment can be useful and might serve the needs of department-sized environments.

To support larger environments, however, where data originates on many WSAs and where many users need to search the data, you can scale your deployment by distributing AWSR instances across multiple machines. When you do this, you configure the instances so that each instance performs a specialized task. For example, one or more instances might index the data, while another instance manages searches across the data (Refer Fig 2 & 3).

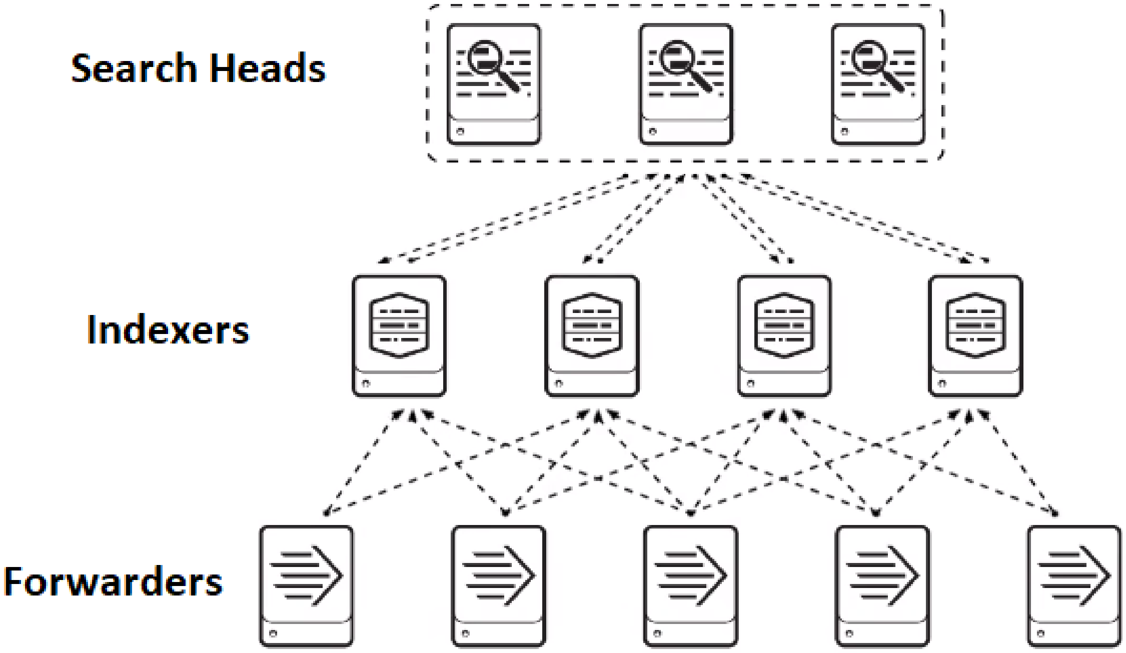


Fig 3. Distributed Deployment

Types of Distributed Deployment

Departmental

A single instance that combines indexing and search management functions.

Small enterprise

One search head with two or three indexers.

Medium enterprise

A small search head cluster, with several indexers.

Large enterprise

A large search head cluster, with large numbers of indexers.

2 System Requirements

Guest Operating System can be any one of following:

- Red Hat Linux (64-bit)
- Windows (64-bit) - Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Server 2016, Windows 8, Windows 8.1, Windows 10

Platform Requirements: Reference hardware can be commodity-grade, and must have the following minimum specifications:

- Intel x86 64-bit chip architecture with two CPUs, 12 cores per CPU, 2.0 Ghz or higher 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.

Please refer to the following table for VM resource requirements for each of Indexers and Search Heads.

Resource	Size
RAM	16 GBs
Hard Disk	100 GBs
2 CPU	12 Core

3 Procedure for Distributed Deployment

3.1 Procedure of Setting-up with 1 Indexer and 1 Search Head

3.1.1 Precondition:

1) Need to have two VMs with AWSR installed. One of the VMs will be the Indexer node and second will be the Search Head node with the License Master.

   For AWSR installation, please refer to the page 11 of the following document -

   https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_7/Advanced_Web_Security_Reporting_7_5.pdf

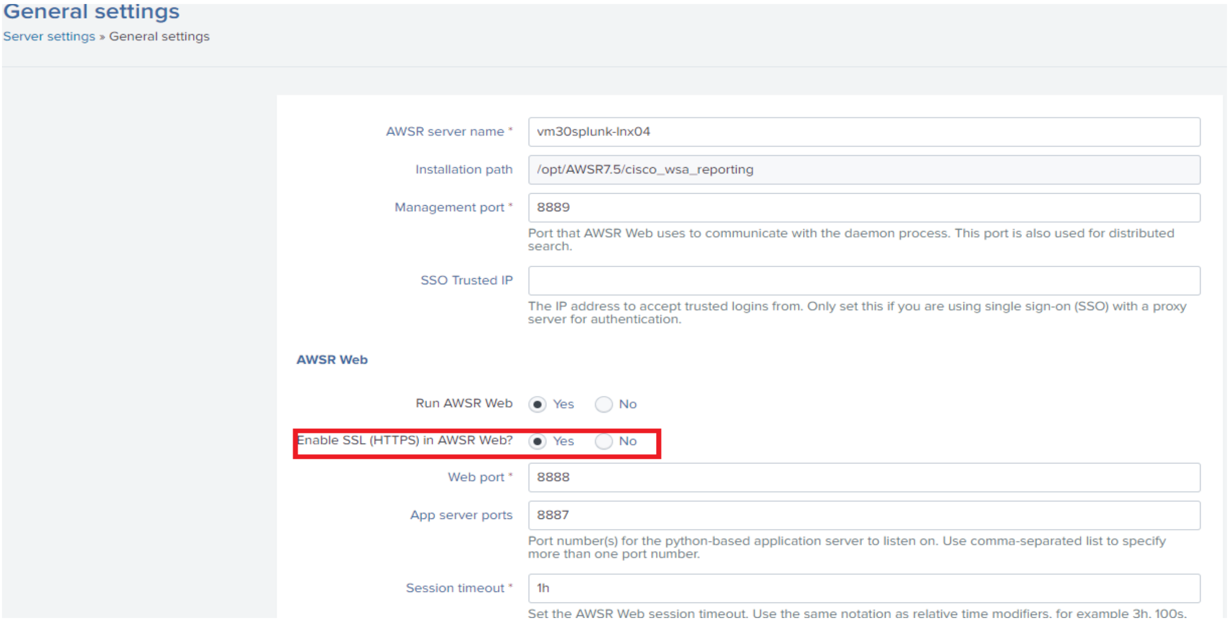
2) If there is an existing standalone setup, this AWSR node can become the Indexer of the Distributed Deployment. Backup entire folder of the current standalone AWSR and continue to follow the steps below.

Note:

i. The Indexer will act as both Indexer and Forwarder.

ii. Before backing up hot buckets, AWSR service should be stopped in order to prevent the loss of data in between the process of backing up. Once the AWSR services are stopped, the logs given as input afterwards, are at risk.

3) On all the nodes (Indexer and Search Head), enable HTTPS as it is required for License Master.
   a) Navigate to Settings → Systems → Server Settings
   b) Click on General Settings
   c) Select the “Yes” radio button in “Enable SSL (HTTPS) in AWSR Web”



General settings

Server settings » General settings

AWSR server name * vm30splunk-lnx04

Installation path /opt/AWSR7.5/cisco_wsa_reporting

Management port * 8889

Port that AWSR Web uses to communicate with the daemon process. This port is also used for distributed search.

SSO Trusted IP

The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.

AWSR Web

Run AWSR Web ● Yes ○ No

Enable SSL (HTTPS) in AWSR Web? ● Yes ○ No

Web port * 8888

App server ports 8887

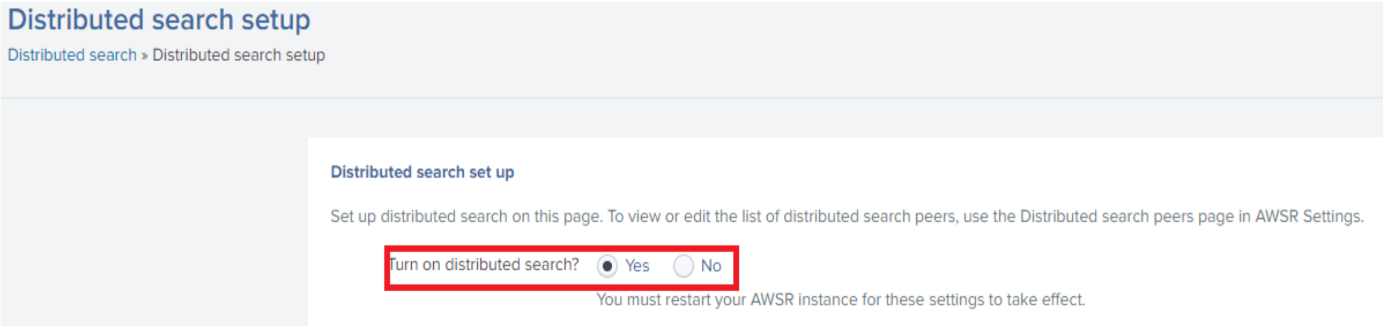
Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number.

Session timeout * 1h

Set the AWSR Web session timeout. Use the same notation as relative time modifiers. for example 3h. 100s.

3.1.2 Setup Procedure

1) On Search Head node, enable Distributed Search
   a. Navigate to Settings → Distributed Environment → Distributed Search
   b. Click on Distributed Search Setup.
   c. Select the “Yes” radio button in “Turn on Distributed Search?”



Distributed search setup

Distributed search » Distributed search setup

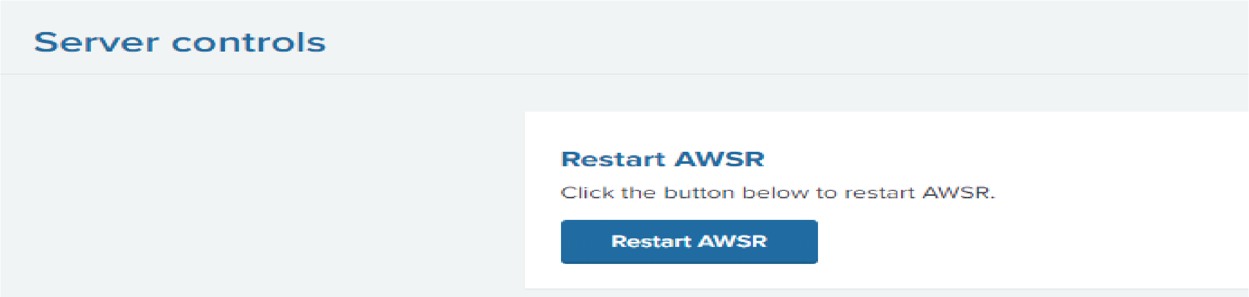
Distributed search set up

Set up distributed search on this page. To view or edit the list of distributed search peers, use the Distributed search peers page in AWSR Settings.

Turn on distributed search? ● Yes ○ No

You must restart your AWSR instance for these settings to take effect.

2) Restart the Search Head node.
   a. Settings → System → Server Controls → Restart AWSR

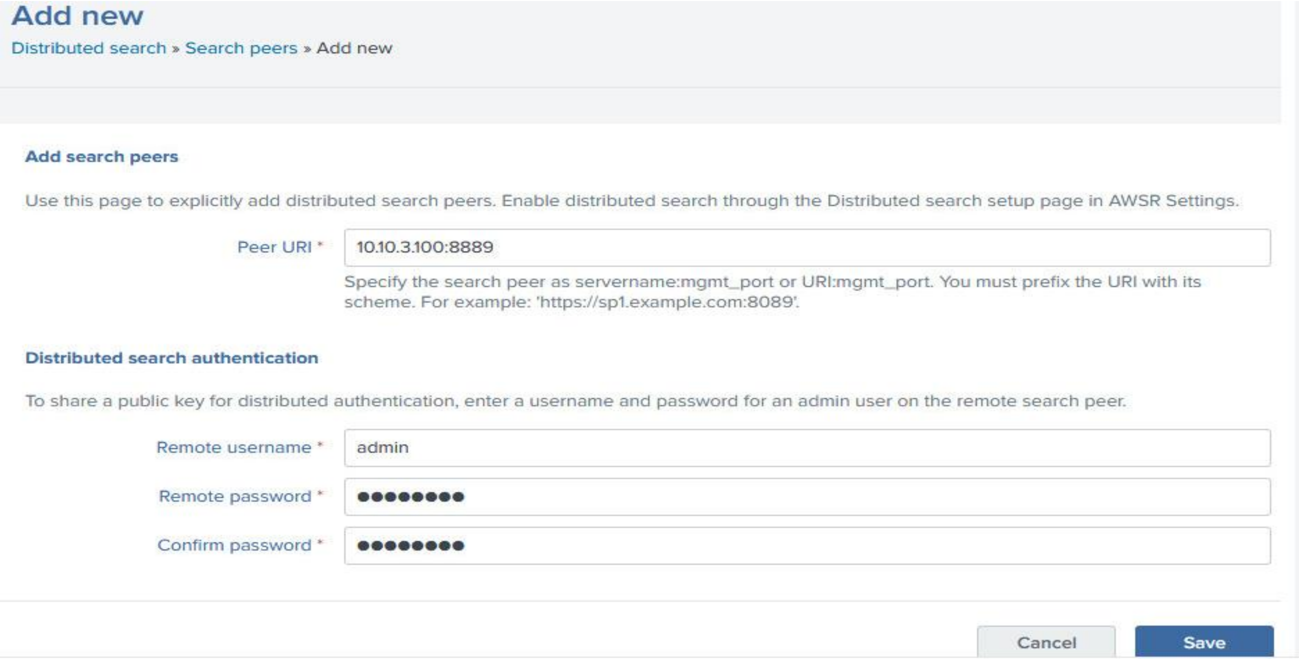


Server controls

Restart AWSR

Click the button below to restart AWSR.

3) In Search Head node, add Indexer.
   a. Navigate to Settings → Distributed Search → Search peers → Add new
   b. Add Indexer as:
      i. https://ipaddress:management_port or
      ii. https://servername:management_port or
      iii. https://URI:management_port
   c. Enter admin user and password configured at step 2



Add new

Distributed search » Search peers » Add new

Add search peers

Use this page to explicitly add distributed search peers. Enable distributed search through the Distributed search setup page in AWSR Settings.

Peer URI * 10.10.3.100:8889

Specify the search peer as servername:mgmt_port or URI:mgmt_port. You must prefix the URI with its scheme. For example: 'https://sp1.example.com:8089'.

Distributed search authentication

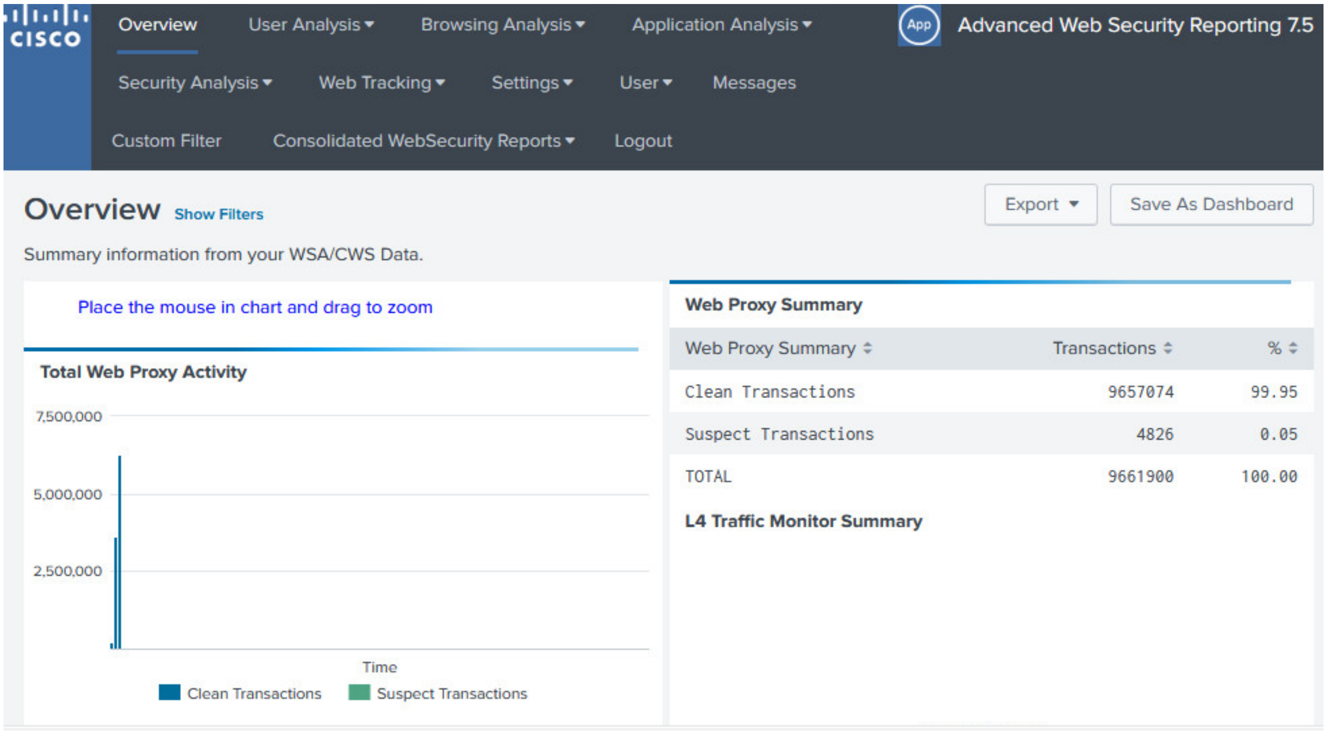
To share a public key for distributed authentication, enter a username and password for an admin user on the remote search peer.

Remote username * admin

Remote password * ●●●●●●●●

Confirm password * ●●●●●●●●

4) If the Indexer was previously a standalone AWSR, data can be verified in the Search head on pre-built reports and dashboards to ensure that both Search head node and the Indexer nodes are properly configured.
   Please refer to the following screenshots of Overview Page of AWSR.



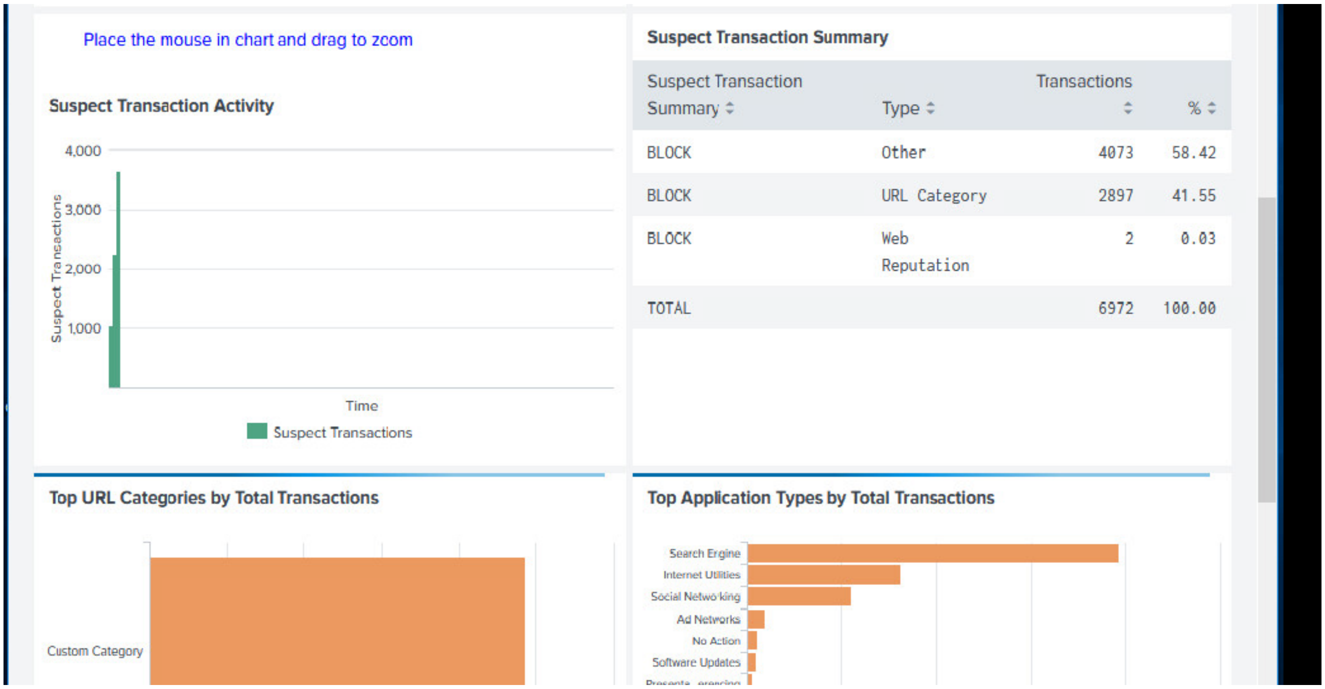
Overview

Summary information from your WSA/CWS Data.

Web Proxy Summary

Web Proxy Summary ⇕	Transactions ⇕	% ⇕
Clean Transactions	9657074	99.95
Suspect Transactions	4826	0.05
TOTAL	9661900	100.00

L4 Traffic Monitor Summary



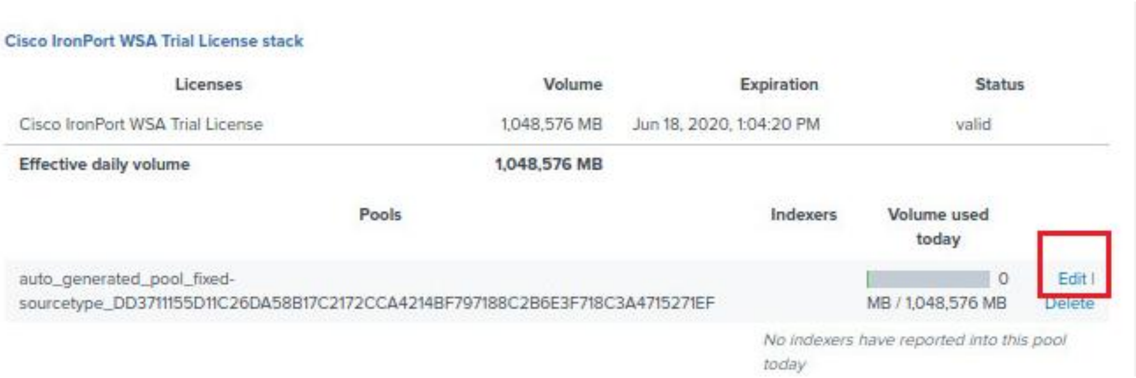
Suspect Transaction Summary

Suspect Transaction Summary ⇕	Type ⇕	Transactions ⇕	% ⇕
BLOCK	Other	4073	58.42
BLOCK	URL Category	2897	41.55
BLOCK	Web Reputation	2	0.03
TOTAL		6972	100.00

If the Indexer is a fresh installation of AWSR, please refer to section 4 to configure the WSA Log data.

3.1.3 Procedure of Licensing

1) Designate the search head as the License Master and make sure default settings is applied on Search Head node to accept all peers.
   a) Navigate to Settings → System → Licensing
   b) Under current default pool select Edit

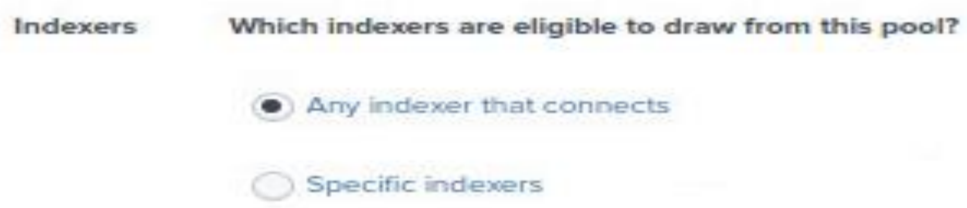


Cisco IronPort WSA Trial License stack

Licenses	Volume	Expiration	Status
Cisco IronPort WSA Trial License	1,048,576 MB	Jun 18, 2020, 1:04:20 PM	valid
Effective daily volume	**1,048,576 MB**		

Pools	Indexers	Volume used today	
auto_generated_pool_fixed-sourcetype_DD3711155D11C26DA58B17C2172CCA4214BF797188C2B6E3F718C3A4715271EF		0 MB / 1,048,576 MB *No indexers have reported into this pool today*	Edit | Delete

   c) Under Indexers mark – "Any Indexer that connects"

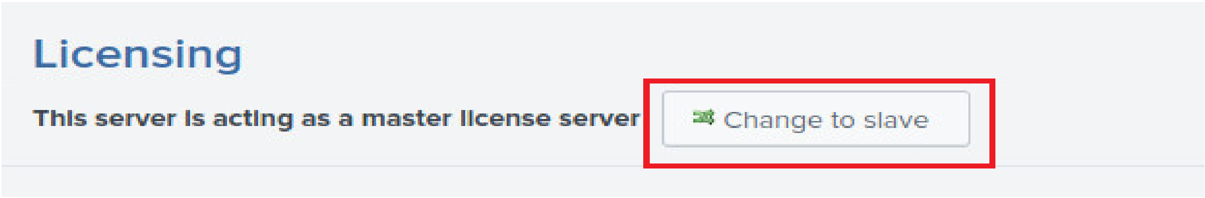


Indexers Which indexers are eligible to draw from this pool?

● Any indexer that connects

○ Specific indexers

2) In Indexer node, switch Indexer to slave
   a) Navigate to Settings → System → Licensing
   b) Select "Change to slave"



Licensing

This server is acting as a master license server

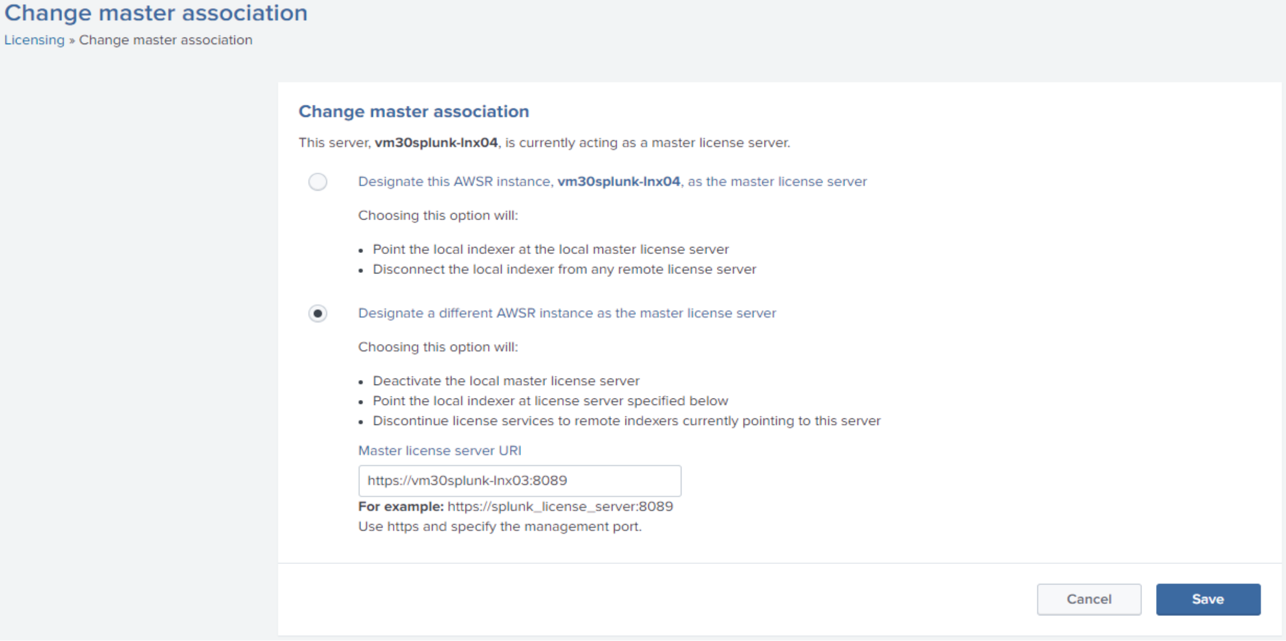
c) Under "Change master association" step, select: “Designate a different AWSR instance as the master license server” option.

i) Enter details into the box in the correct format –

(1) https://ipaddress:management_port or

(2) https://servername:management_port or

(3) https://URI:management_port



Change master association

Licensing » Change master association

Change master association

This server, **vm30splunk-lnx04**, is currently acting as a master license server.

○ Designate this AWSR instance, **vm30splunk-lnx04**, as the master license server

Choosing this option will:

- Point the local indexer at the local master license server
- Disconnect the local indexer from any remote license server

● Designate a different AWSR instance as the master license server

Choosing this option will:

- Deactivate the local master license server
- Point the local indexer at license server specified below
- Discontinue license services to remote indexers currently pointing to this server

Master license server URI: https://vm30splunk-lnx03:8089

For example: https://splunk_license_server:8089

Use https and specify the management port.

d) Click on Save

3) Verify license details on the Indexer node

a) Navigate to Settings → System → Licensing

3.2 Procedure of Setting-up with 2 Indexers and 1 Search Head

3.2.1 Precondition:

1) Need to have three VMs with AWSR installed. Two of the VMs will be the Indexer nodes and the third will be the Search Head node with the License Master.

For AWSR installation, please refer to the page 11 of the following document -

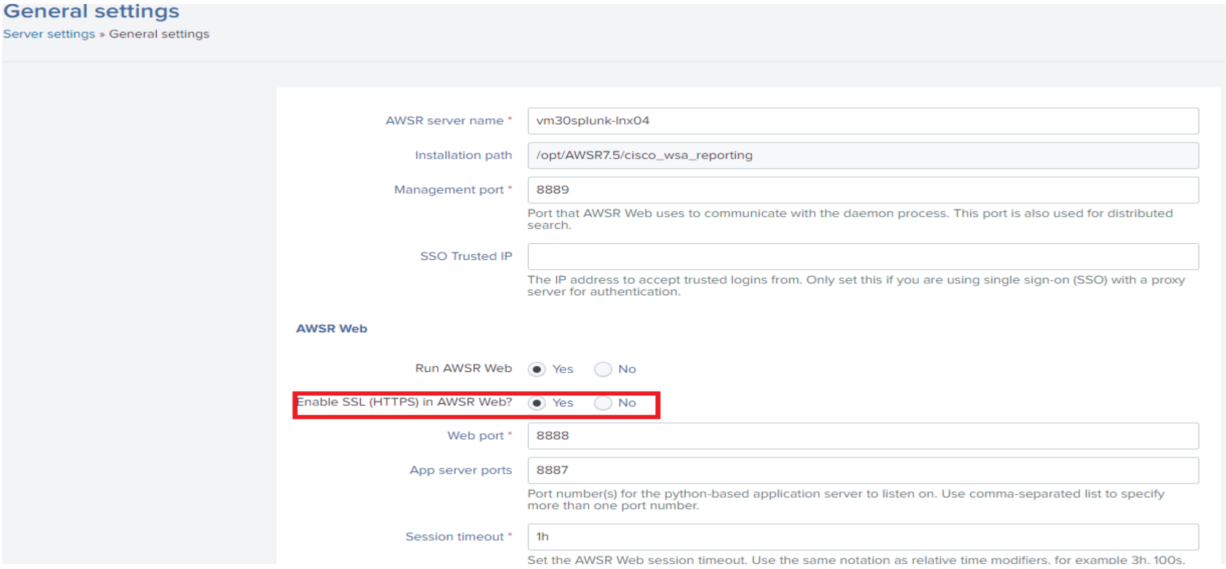
https://www.cisco.com/c/dam/en/us/td/docs/security/wsa/Advanced_Reporting/WSA_Advanced_Reporting_7/Advanced_Web_Security_Reporting_7_5.pdf

2) If there is an existing standalone setup, this AWSR node can become one of the Indexers of the Distributed Deployment. Backup entire folder of the current standalone AWSR and continue to follow the steps below.

Note:

i) Before backing up hot buckets, AWSR service should be stopped in order to prevent the loss of data in between the process of backing up. Once the AWSR services are stopped, the logs given as input afterwards, are at risk.

3) On all the nodes (Indexers and Search Head), enable HTTPS as it is required for License Master.
   a. Navigate to Settings → Systems → Server Settings
   b. Click on General Settings
   c. Select the "Yes" radio button in "Enable SSL (HTTPS) in AWSR Web"



General settings

Server settings » General settings

AWSR server name * vm30splunk-lnx04

Installation path /opt/AWSR7.5/cisco_wsa_reporting

Management port * 8889

Port that AWSR Web uses to communicate with the daemon process. This port is also used for distributed search.

SSO Trusted IP

The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.

AWSR Web

Run AWSR Web ● Yes ○ No

Enable SSL (HTTPS) in AWSR Web? ● Yes ○ No

Web port * 8888

App server ports 8887

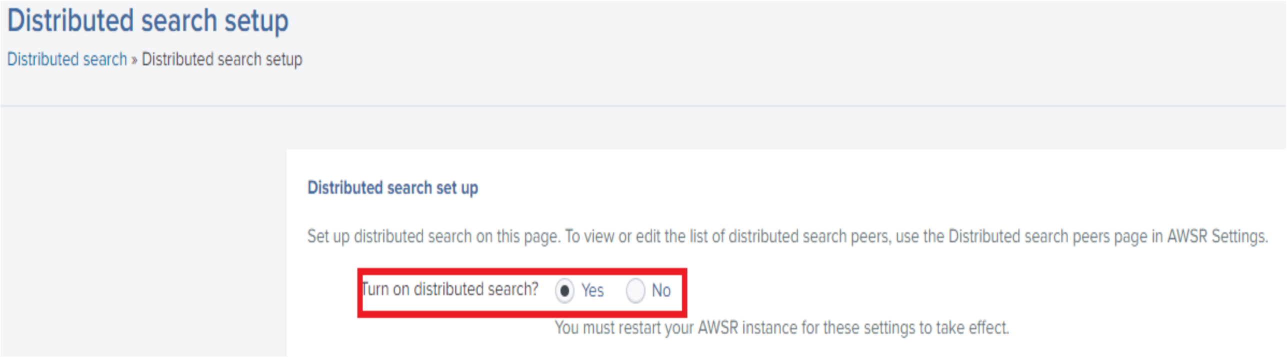
Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number.

Session timeout * 1h

Set the AWSR Web session timeout. Use the same notation as relative time modifiers. for example 3h. 100s.

3.2.2 Setup Procedure

1) On Search Head node, enable Distributed Search
   a. Navigate to Settings → Distributed Environment → Distributed Search
   b. Click on Distributed Search Setup.
   c. Select the "Yes" radio button in "Turn on Distributed Search?"



Distributed search setup

Distributed search » Distributed search setup

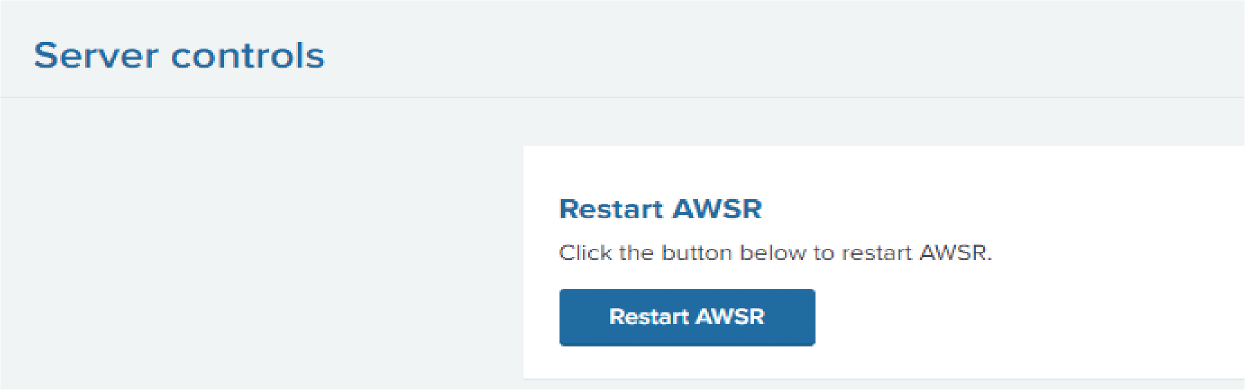
Distributed search set up

Set up distributed search on this page. To view or edit the list of distributed search peers, use the Distributed search peers page in AWSR Settings.

Turn on distributed search? ● Yes ○ No

You must restart your AWSR instance for these settings to take effect.

2) Restart the Search Head node.
   a. Settings → System → Server Controls → Restart AWSR

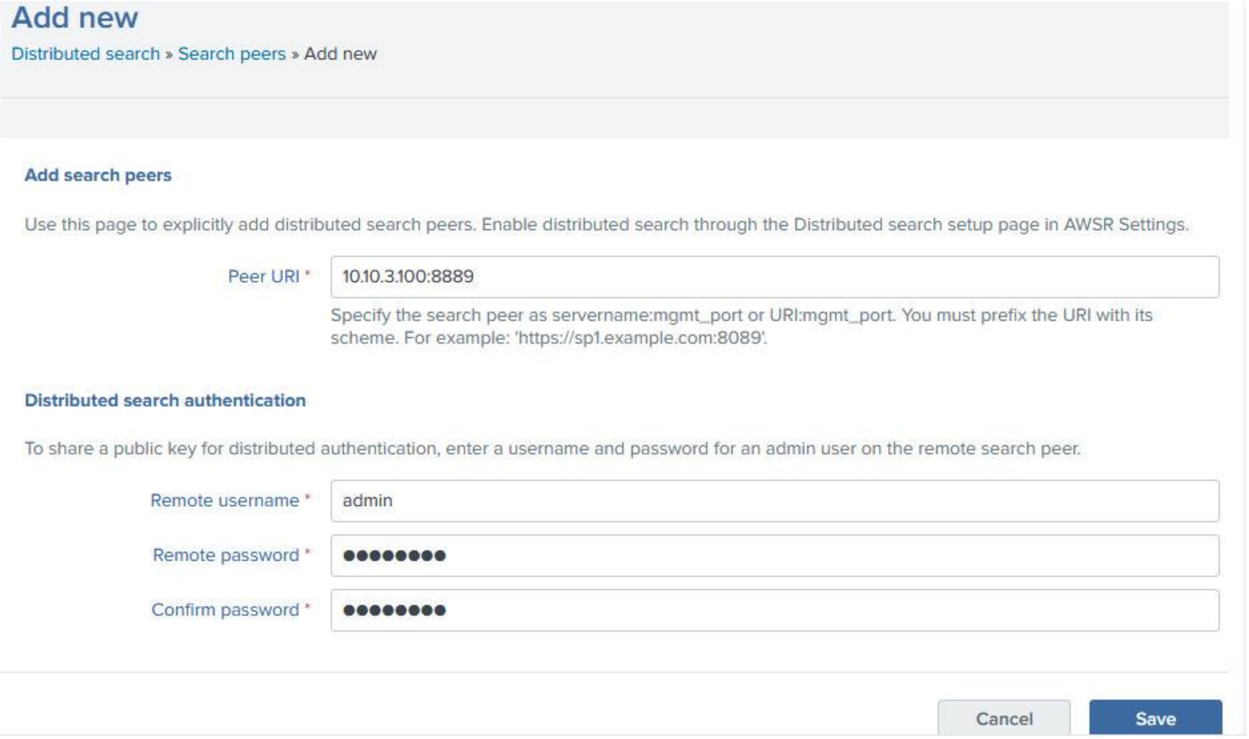


Server controls

Restart AWSR

Click the button below to restart AWSR.

3) In Search Head node, add Indexers.
   a. Navigate to Settings → Distributed Search → Search peers → Add new
   b. Add an Indexer as:
      i. https://ipaddress:management_port or
      ii. https://servername:management_port or
      iii. https://URI:management_port
   c. Enter admin user and password configured at step 2
   d. Repeat the process for the second indexer



Add new

Distributed search » Search peers » Add new

Add search peers

Use this page to explicitly add distributed search peers. Enable distributed search through the Distributed search setup page in AWSR Settings.

Peer URI *: 10.10.3.100:8889

Specify the search peer as servername:mgmt_port or URI:mgmt_port. You must prefix the URI with its scheme. For example: 'https://sp1.example.com:8089'.

Distributed search authentication

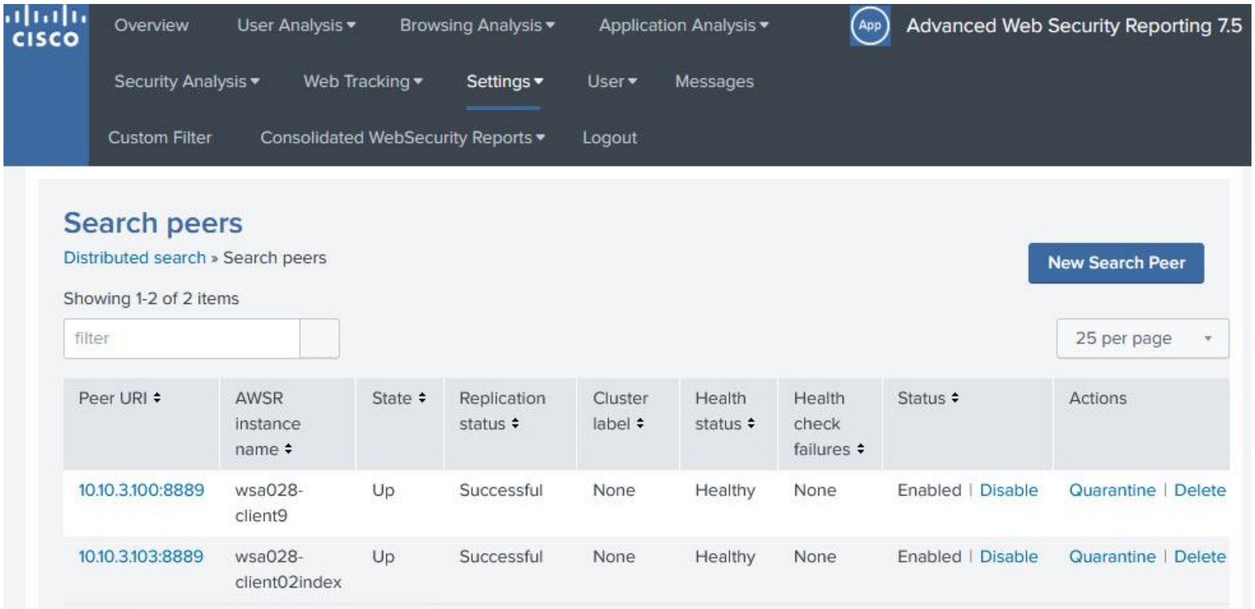
To share a public key for distributed authentication, enter a username and password for an admin user on the remote search peer.

Remote username *: admin

Remote password *: ●●●●●●●●

Confirm password *: ●●●●●●●●

The Search Peers page should look similar to the following screenshot –



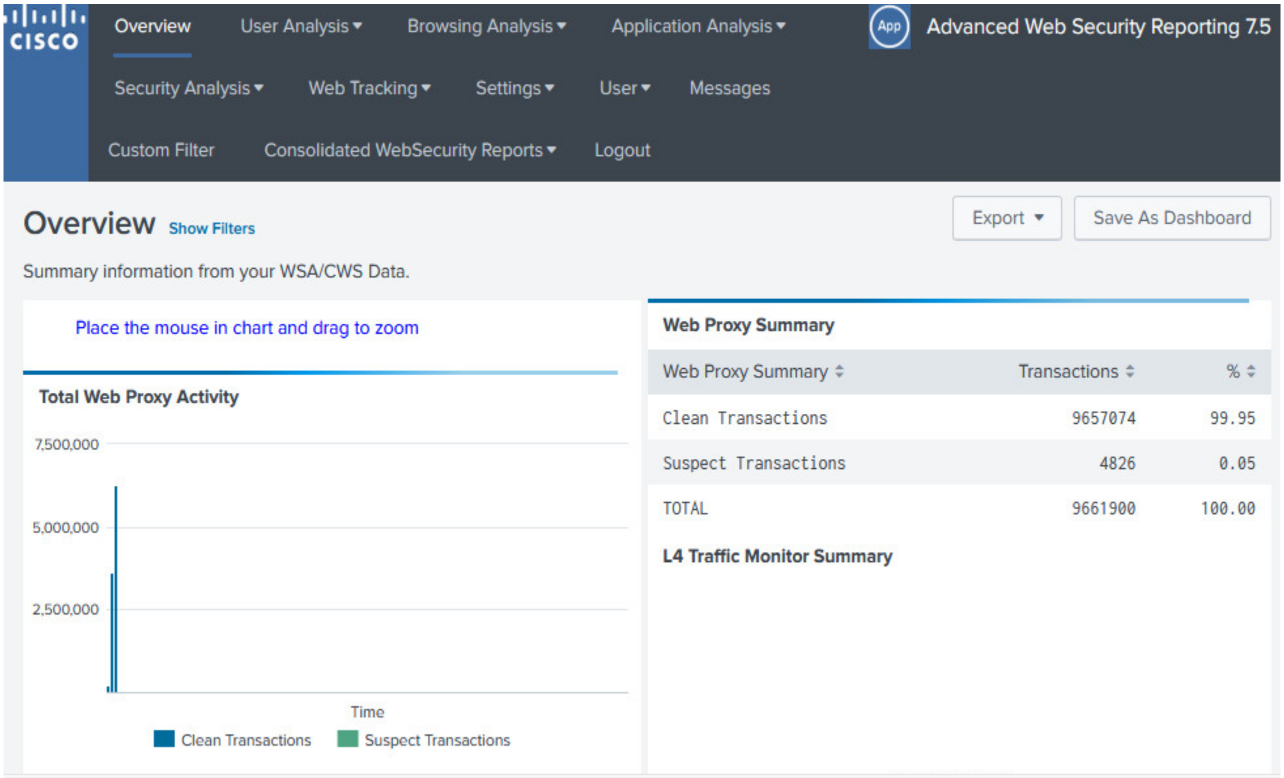
Search peers

Distributed search » Search peers

Showing 1-2 of 2 items

Peer URI	AWSR instance name	State	Replication status	Cluster label	Health status	Health check failures	Status	Actions
10.10.3.100:8889	wsa028-client9	Up	Successful	None	Healthy	None	Enabled | Disable	Quarantine | Delete
10.10.3.103:8889	wsa028-client02index	Up	Successful	None	Healthy	None	Enabled | Disable	Quarantine | Delete

4) If one of the Indexer was previously a standalone AWSR, data can be verified in the Search head on pre-built reports and dashboards to ensure that both Search head node and the Indexer nodes are properly configured.
Please refer to the following screenshots of Overview Page of AWSR.



Overview

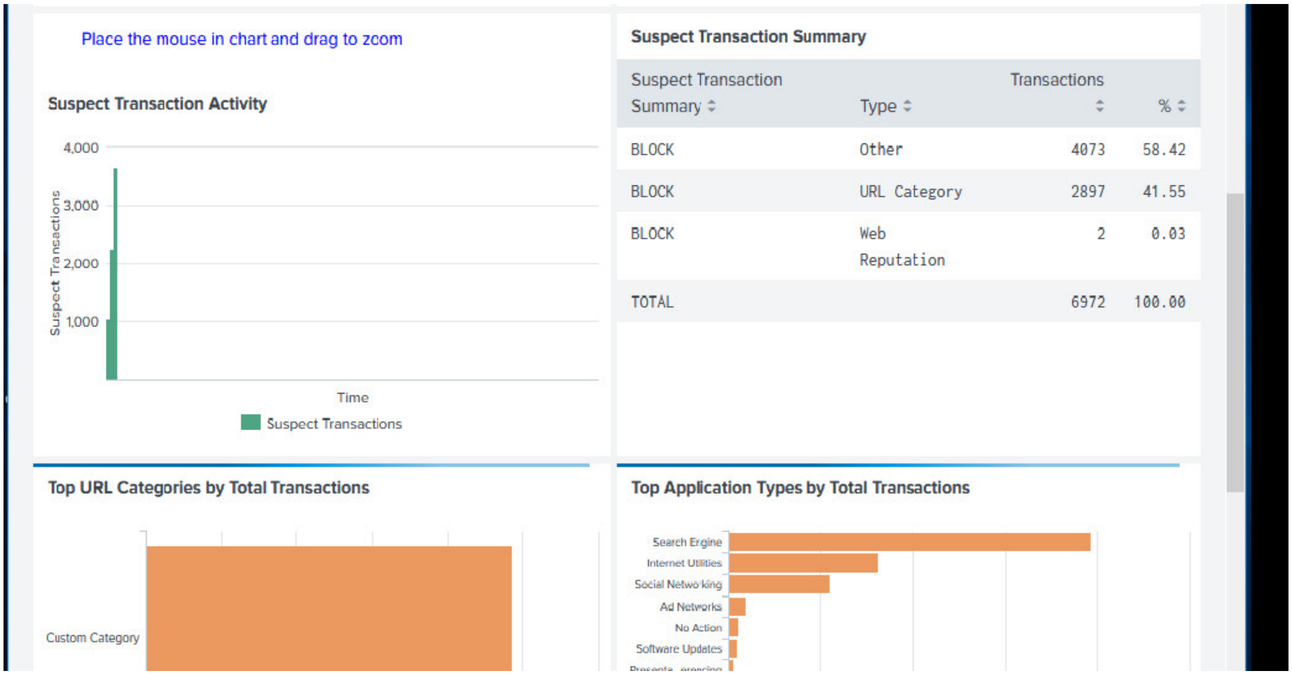
Summary information from your WSA/CWS Data.

Total Web Proxy Activity

Web Proxy Summary

Web Proxy Summary	Transactions	%
Clean Transactions	9657074	99.95
Suspect Transactions	4826	0.05
TOTAL	9661900	100.00

L4 Traffic Monitor Summary



Suspect Transaction Activity

Suspect Transaction Summary

Suspect Transaction Summary	Type	Transactions	%
BLOCK	Other	4073	58.42
BLOCK	URL Category	2897	41.55
BLOCK	Web Reputation	2	0.03
TOTAL		6972	100.00

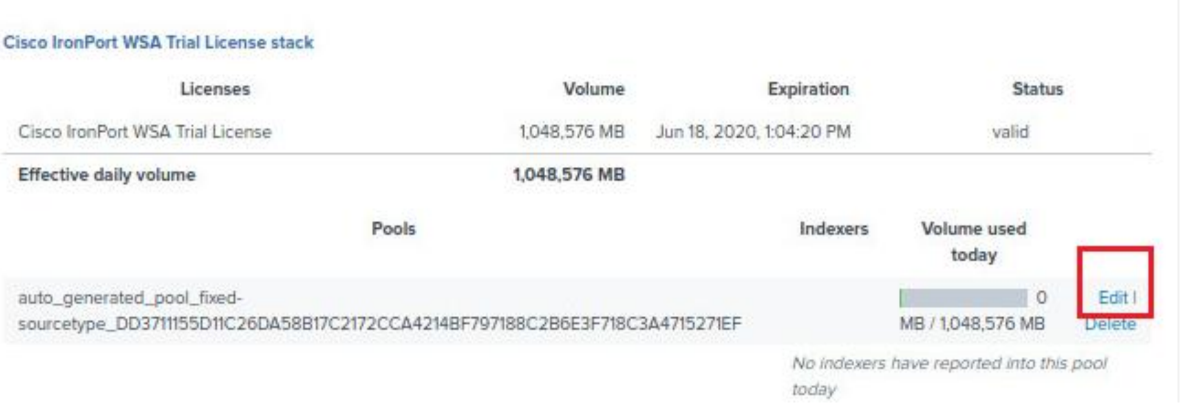
Top URL Categories by Total Transactions

Top Application Types by Total Transactions

If both Indexers are a fresh installation of AWSR, please refer to section 4 to configure the WSA Log data.

3.2.3 Procedure For Licensing

1) Designate the Search Head as the License Master and make sure default settings is applied on Search Head node to accept all peers.
   a. Navigate to Settings → System → Licensing
   b. Under current default pool select Edit



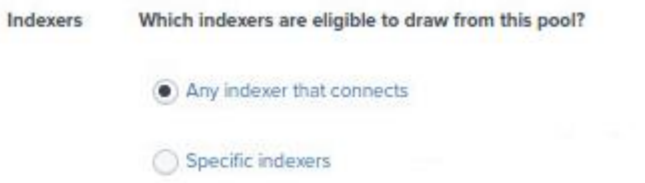
Cisco IronPort WSA Trial License stack

Licenses	Volume	Expiration	Status
Cisco IronPort WSA Trial License	1,048,576 MB	Jun 18, 2020, 1:04:20 PM	valid
Effective daily volume	**1,048,576 MB**		

Pools	Indexers	Volume used today	
auto_generated_pool_fixed-sourcetype_DD3711155D11C26DA58B17C2172CCA4214BF797188C2B6E3F718C3A4715271EF		0 MB / 1,048,576 MB	Edit | Delete

No indexers have reported into this pool today

   c. Under Indexers mark – “Any Indexer that connects”

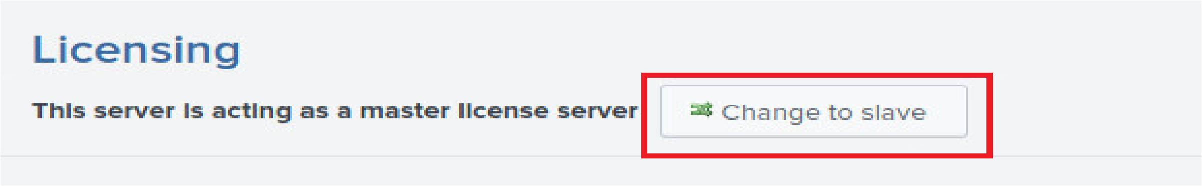


Indexers **Which indexers are eligible to draw from this pool?**

● Any indexer that connects

○ Specific indexers

2) Change both the Indexers as Slave. On both indexers,
   a. Navigate to Settings → System → Licensing
   b. Select "Change to slave"



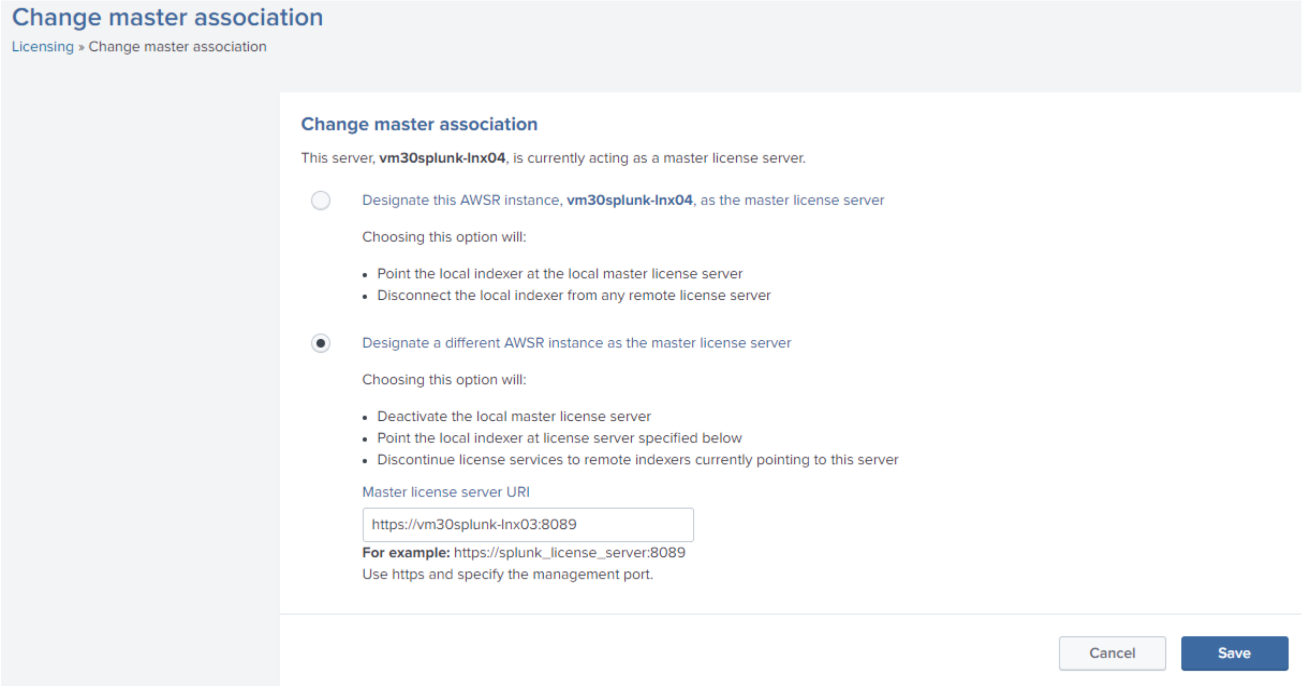
Licensing

This server is acting as a master license server

c. Under "Change master association" step, select: “Designate a different AWSR instance as the master license server” option.

Enter details into the box in the correct format –

1. https://ipaddress:management_port or
2. https://servername:management_port or
3. https://URI:management_port



Change master association

Licensing » Change master association

Change master association

This server, **vm30splunk-lnx04**, is currently acting as a master license server.

○ Designate this AWSR instance, **vm30splunk-lnx04**, as the master license server

Choosing this option will:

- Point the local indexer at the local master license server
- Disconnect the local indexer from any remote license server

● Designate a different AWSR instance as the master license server

Choosing this option will:

- Deactivate the local master license server
- Point the local indexer at license server specified below
- Discontinue license services to remote indexers currently pointing to this server

Master license server URI

https://vm30splunk-lnx03:8089

For example: https://splunk_license_server:8089

Use https and specify the management port.

d. Click on Save

e. Verify license details for Indexer node

   a. Navigate to Settings → System → Licensing

4 Configure Data Inputs for Web Security Appliance Logs In Indexers

Step 1 In the Indexers:
Navigate to Settings → Data → Data inputs → Files & directories.

Step 2 Click “New Local File and Directory”.

Step 3 In both the procedures -
Enter the full path to the FTP directory to which Web Security appliance logs will be sent. This path, and the FTP path provided on the Web Security appliance's Log Subscription page must match. Configure the indexers such that the load is balanced with one Indexer indexing logs from one WSA. For example, if there are 3 WSAs, logs from WSA1 coming to dir1 should be configured in Indexer1 and similarly from WSA2 coming to dir2 should be configured in Indexer2 and so on.

Step 4 Click Next.

Step 5 Click “Select”**.**

Step 6 Select the Source Type.

wsa_accesslogs **-** These are used for all reports except layer 4 traffic monitor & Advanced Malware Protection reports.

wsa_trafmonlogs - These are used for layer 4 traffic monitor reports.

wsa_amplogs - These are used for Advanced Malware Protection reports**.**

Step 7 Choose Advanced Web Security Reporting 7.5 from the App Context drop-down list.

Step 8 Click Constant value and enter the Web Security appliance host name in the Host field value field.

Step 9 Choose Main as the destination Index.

Step 10 Click Review and review the values you provided.

Step 11 Click Submit

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.