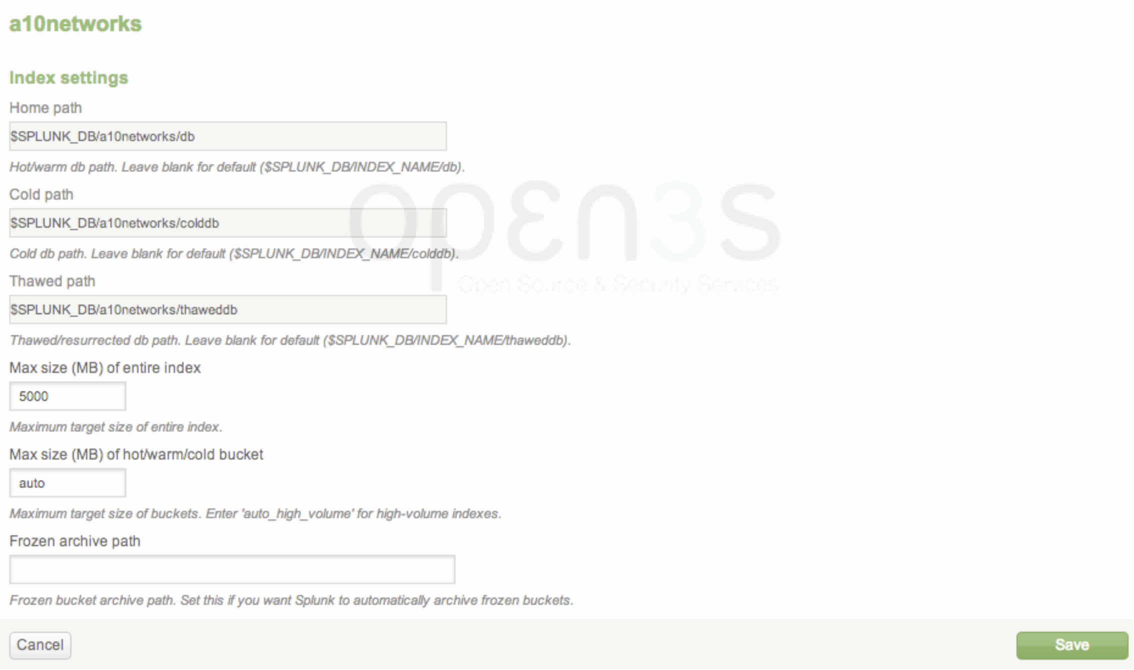
Installing and Configuring
Splunk for A10 Networks app

Disclaimer
All trademarks and registered trademarks displayed on this app as well as all logos shown are the property of their respective owners.

Splunk for A10 Networks app provides visibility into the ADC logs, allowing to detect and analyze Web traffic, trends, and Web threats.

Splunk server configurations

First of all, let's prepare the Splunk server to receive the A10 Networks ADC's logs. We will need to create a new index named *a10networks*. To do this, go to *Manager > Indexes*, and click on the *New* button:



a10networks

Index settings

Home path
$SPLUNK_DB/a10networks/db
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold path
$SPLUNK_DB/a10networks/colddb
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed path
$SPLUNK_DB/a10networks/thaweddb
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

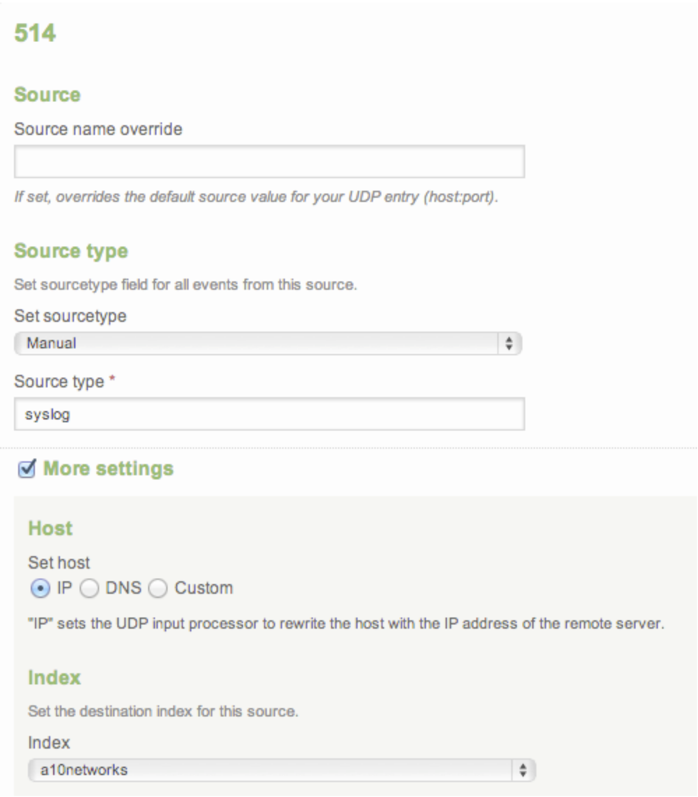
Max size (MB) of entire index
5000
Maximum target size of entire index.

Max size (MB) of hot/warm/cold bucket
auto
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen archive path

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

The A10 Network ADC will send the logs via syslog, so we need to set up a new data input associated to our new index (a10networks). Go to *Manager > Data inputs > UDP* and click on the *New* button:



514

Source

Source name override

If set, overrides the default source value for your UDP entry (host:port).

Source type

Set sourcetype field for all events from this source.

Set sourcetype: Manual

Source type *: syslog

☑ More settings

Host

Set host

● IP ○ DNS ○ Custom

"IP" sets the UDP input processor to rewrite the host with the IP address of the remote server.

Index

Set the destination index for this source.

Index: a10networks

As you can see, the index *a10networks* is forced to the new data input. The Splunk app expects the logs to arrive in udp/514 port. In case of conflict with other data input that is already using this port, you have to edit the props.conf file located on *<SPLUNK_HOME>/etc/apps/SplunkForA10Networks/default* directory, and specify the new port.

Now we are ready to Splunk the ADC's logs.

A10 Networks ADC configurations

The Splunk app uses 2 types of logs:

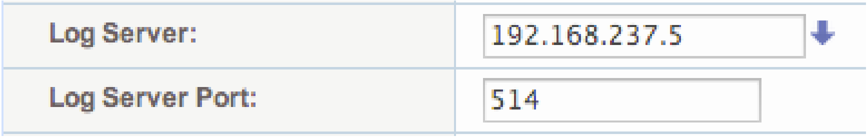
- **Web Access logs**: The logs are generated by an aFleX code that logs the Web Access traffic in W3C format.
- **WAF logs**: The logs are in CEF format and are generated by the WAF module itself.

Each type of log will be source typed by the application automatically for you, so you do not have to change anything.

Configure Web Access logs

This section assumes that you already have a Virtual Service configured.

In order to send the logs we need to configure the ADC to send the logs to a syslog server (Splunk). Access the ACOS Web GUI and go to *Config Mode* > *System* > *Settings* > *Log*. Leave the default settings and specify the IP of the Splunk server:



Log Server: 192.168.237.5

Log Server Port: 514

Next, we need to add the aFleX code. Go to *Config Mode* > *SLB* > *aFleX* and click on the *Add* button. You can copy&paste the following text, or go to the Splunk app folder and copy it from there, the file is located in *<SPLUNK_HOME>/etc/apps/SplunkForA10Networks/appserver/static/logging_ w3c.aflex*:

```
# This aFleX logs client/server Web traffic in W3C format

when HTTP_REQUEST {
# Set strings for the "client side"
set time_client_request [TIME::clock seconds]
set clicks_client_request [TIME::clock milliseconds]
set date_time_request [clock format $time_client_request -format {%Y-%m-%d
%H:%M:%S} ]
set c_ip [IP::client_addr]
set cs_uri_stem [HTTP::host][HTTP::uri]
set cs_method [HTTP::method]
set s_ip [IP::local_addr]
set s_port [TCP::local_port]
set host [HTTP::host]
if {[HTTP::query] equals ""} {
set cs_uri_query [HTTP::query]
} else { set cs_uri_query "null"
}
if {[HTTP::header exists Content-Length]} {
set cs_bytes [HTTP::header Content-Length]
} else { set cs_bytes "0"
}
if {[HTTP::header exists Referer]} {
set cs_referer [HTTP::header "Referer"]
} else { set cs_referer "null"
}
set cs_useragent [string map {" " "+"} [HTTP::header "User-Agent"]]
}


when HTTP_RESPONSE {
# Set strings for the "server side"
set clicks_server_response [TIME::clock milliseconds]
set n_ip [IP::server_addr]
set n_port [TCP::server_port]
set sc_status [HTTP::status]
if {[HTTP::header exists Content-Length]} {
set sc_bytes [HTTP::header Content-Length]
} else { set sc_bytes "0"
}

# Correct TCL Bug with floating point values
set time_taken [expr $clicks_server_response - $clicks_client_request ]
if {$time_taken < 10} {
set final_time_taken [string range "0.00$time_taken" 0 4]
} elseif { $time_taken < 100 } {
set final_time_taken [string range "0.0$time_taken" 0 4]
} elseif { $time_taken < 1000} {
set final_time_taken [string range "0.$time_taken" 0 4]
} else {
set final_time_taken "[string index $time_taken 0].[string range $time_taken 1 3
]"
}

# Format strings for logging
set log_str "$date_time_request $c_ip $s_ip $s_port $cs_method $cs_uri_stem
$cs_uri_query $n_ip $n_port $sc_status $sc_bytes $cs_bytes
$final_time_taken $cs_useragent $cs_referer"

# write to syslog with Debug level
log local0.7 $log_str
}
```

Finally, we have to add the aFleX to a Virtual Service. Go to *Config Mode > SLB > Service > Virtual Service*, and edit your LB Service. In the *aFleX* section select your recent added code.

Now Splunk should be receiving the Web Access logs and the SLB Dashboards should work correctly.

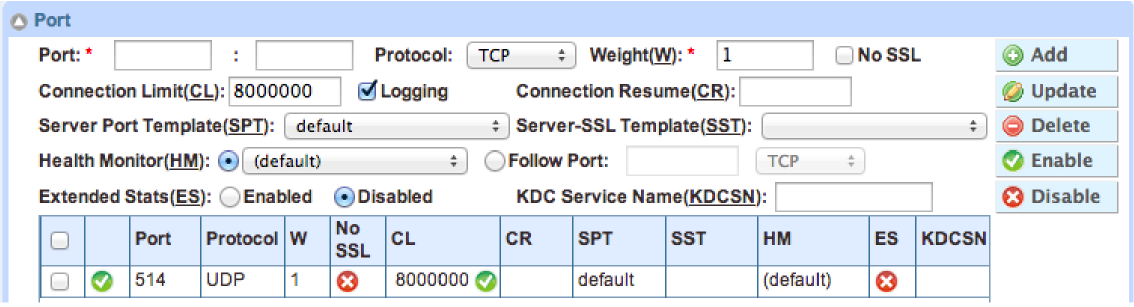
Configure Web Application Firewall (WAF) logs

In this section we will cover how to set up the ADC to send the WAF logs. Either if you have the WAF module active, or you are willing to do so, we will cover the process of setting up the module, and the activation of logging.

NOTE: The WAF module is a new feature that comes in the ACOS v2.7.1 code, so if you have an earlier versión, an upgrade of firmware is required.

First, we need to configure the Splunk server in the ADC. Go to *Config Mode > SLB > Service > Server* and click on the *Add* button:

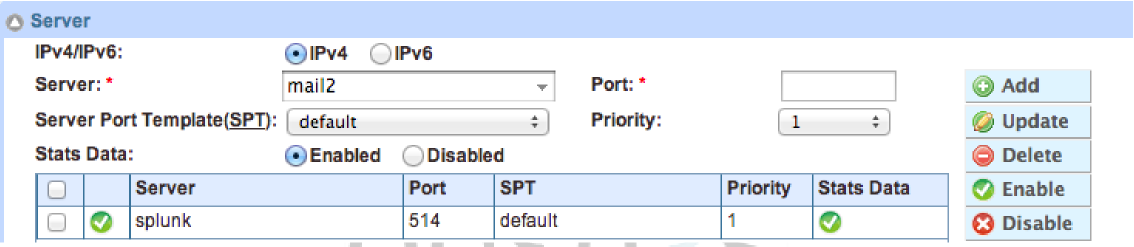
Specify the IP of the Splunk server and the syslog port (udp/514). You can just leave the defaults settings for the rest of settings:



Port: * : Protocol: TCP Weight(W): * 1 □ No SSL
Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):
Server Port Template(SPT): default Server-SSL Template(SST):
Health Monitor(HM): ● (default) ○ Follow Port: TCP
Extended Stats(ES): ○ Enabled ● Disabled KDC Service Name(KDCSN):

□		Port	Protocol	W	No SSL	CL	CR	SPT	SST	HM	ES	KDCSN
□	✓	514	UDP	1	☒	8000000 ✓		default		(default)	☒	

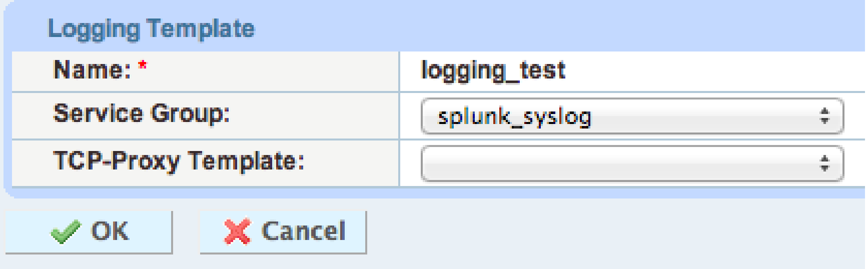
Then set up a service group for the syslog port: *Config Mode > SLB > Service > Service Group*. Leave the defaults settings and specify the recent Splunk server node created:



IPv4/IPv6: ● IPv4 ○ IPv6
Server: * mail2 Port: *
Server Port Template(SPT): default Priority: 1
Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	splunk	514	default	1	✓

Now we need to set up a logging template, go to *Config Mode > SLB > Template > Application > Logging*, and click on the *Add* button:



Name: *	logging_test
Service Group:	splunk_syslog
TCP-Proxy Template:	

As you can see, just add the new Service Group and click *OK*.

Finally, we will create a WAF test sensor in learning mode. If you already have WAF templates created, just add the new Logging Template.

Go to *Config Mode > Security > WAF > Template > WAF* and click on the *Add* button to create a new WAF template. As we want to use the learning mode, we select the *Learning* check box, and then specify the Logging Template. The remaining options can be left as default.

Now we are ready to go, we can check if everything is working as expected by going to the Splunk app. Enjoy!

Feedback is welcome:

- Website: www.open3s.com
- Email: info@open3s.com

open3s
Open Source & Security Services