

# Logstash to LA Connector

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

---

## Logstash basics

### Introduction

1. Download log stash: <https://www.elastic.co/downloads/logstash>  (Sentinel Supports only version 7.x.x)
2. Install Logstash :
  - Linux: <https://www.elastic.co/guide/en/logstash/current/installing-logstash.html#installing-logstash> 
  - Windows: <http://www.dissmeyer.com/2017/11/11/installing-logstash-on-windows/> 
3. Install the log analytics plug in: [https://github.com/yokawasa/logstash-output-azure\\_loganalytics](https://github.com/yokawasa/logstash-output-azure_loganalytics) 
4. Create a conf file in bin (logstash folder location in linux is /usr/share/logstash), here is an example:

File Plugin: [https://www.elastic.co/guide/en/logstash/current/plugins-inputs-file.html#plugins-inputs-file-start\\_position](https://www.elastic.co/guide/en/logstash/current/plugins-inputs-file.html#plugins-inputs-file-start_position) 

- a. Add the workspace configuration (workspace Id and Key)
- b. Point the Log file (json format)
- c. Add the correct columns
- d. Add the table name in LA
- e. Define TimeGenerated column

Here is an example for conf file: Logstash conf file example

1. You will find the logs in the tale under CustomLogs

Some helpful links:

Date Plugin: <https://www.elastic.co/guide/en/logstash/current/plugins-filters-date.html> 

Json Plugin: <https://www.elastic.co/guide/en/logstash/current/plugins-filters-json.html> 

Using LA Agent:

CrowdStrike_CL	
...	
Completed. Showing results from the last 24 hours.	
TABLE CHART Columns ▾	
Drag a column header and drop it here to group by that column	
TimeGenerated [UTC]	Computer
RawData	AuthenticationId_s
CommandLine_s	
2019-06-06T12:21:17.473	
...	
TenantId	802d39e1-9d70-404d-832c-2de5e2478eda
SourceSystem	RestAPI
TimeGenerated [UTC]	2019-06-06T12:21:17.473Z
_version_s	1
Message	{"AuthenticationId": "999", "CommandLine": "C:\\WINDOWS\\system32\\svchost.exe -k netsvcs -p -s wisvc", "ConfigBui
_timestamp_t [UTC]	2019-06-06T12:16:54.597Z
host_s	logstashtest2
Type	CrowdStrike_CL

Using Logstash connector with LA API:

CrowdStrike_CL	
...	
Completed. Showing results from the last 24 hours.	
TABLE CHART Columns ▾	
Drag a column header and drop it here to group by that column	
TimeGenerated [UTC]	Computer
RawData	AuthenticationId_s
CommandLine_s	
2019-06-06T03:01:27.401	976 C:\\WINDOWS\\system32\\svchost.exe -k net
...	
TenantId	802d39e1-9d70-404d-832c-2de5e2478eda
SourceSystem	RestAPI
TimeGenerated [UTC]	2019-06-06T03:01:27.401Z
AuthenticationId_s	976
CommandLine_s	C:\\WINDOWS\\system32\\svchost.exe -k netsvcs -p -s wisvc
ConfigBuild_s	1007.3.0008802.1
ConfigStateHash_s	4125532706
EffectiveTransmissionClass_s	3
Entitlements_s	15
ImageFileName_s	\\??\\C:\\WINDOWS\\system32\\svchost.exe

Suggested commands:

```
java -version
```

```
sudo apt install default-jre
```


```
sudo apt install default-jdk
```

Download Logstash : <https://www.elastic.co/downloads/logstash> 

Install:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch  | sudo apt-key add -
```

```
sudo apt-get install apt-transport-https
```

```
echo "deb https://artifacts.elastic.co/packages/7.x/apt  stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt-get update && sudo apt-get install logstash
```

Navigate /usr/share/logstash/bin -Run the following

```
./logstash-plugin install microsoft-logstash-output-azure-loganalytics
```

Create a conf file in bin --> /usr/share/logstash/bin/ (logstash folder location in linux is /usr/share/logstash)

```
Cat >test.conf
```

```
Vi test.conf
```

((Contents of conf file : <https://docs.microsoft.com/en-us/azure/sentinel/connect-logstash#sample-configuration>

```
input {
  tcp {
    port => "514"
    type => syslog #optional, will effect log type in table
  }
}
filter {
}
output {
  microsoft-logstash-output-azure-loganalytics {
    workspace_id => "7e31edf1-4929-449d-b5f4-274a447891d3" # <your workspace id>
    workspace_key => "Z9DDT9p00QsrZjbr71FfoQqpVWdUquwRdmrvINkMjOekpqjZt9z7Yyj+u5RLA9uuvqwiF+8CJY+hYOVH++Lo
    custom_log_table_name => "Testtable_CL"
  }
}
```

Press escape and ":wq!"

Run

```
./logstash -f test.conf
```

## Change the default TimeGenerated behaviour

In case we need to override the default TimeGenerated field in Log Analytics we can specify a new field for it.

In the following example we are:

1. Taking a test log in /var/log/test.log
2. Parsing the new timestamp value from the log string using a regex with grok and a Json string
3. Parsing the extracted timestamp string to be in the ISO 8601 format (YYYY-MM-DDThh:mm:ssZ)
4. Exporting this new field
5. Assigning the new field to the time\_generated\_field variable plus selecting what fields do we want to log

```
# take an input
input {
  file {
    path => "/var/log/test.log"
  }
}
filter {
  # extract the header timestamp and the Json section
  grok {
    match => {
      "message" => ["^(?<timestamp>.{24}):\\s(?<json_data>.*)$"]
    }
  }
  # parse the extracted header as a timestamp
  date {
    id => 'parse_metric_timestamp'
    match => [ 'timestamp', 'EEE MMM dd HH:mm:ss yyyy' ]
    timezone => 'Europe/Rome'
    target => 'custom_time_generated'
  }
  json {
    source => "json_data"
  }
}
# output to a file for debugging (optional)
output {
  file {
    path => "/tmp/test.txt"
    codec => line { format => "custom format: %{message} %{custom_time_generated} %{json_data}" }
  }
}
# output to the console output for debugging (optional)
output {
  stdout { codec => rubydebug }
}
# Log into Log Analytics
output {
  microsoft-logstash-output-azure-loganalytics {
    workspace_id => '[REDACTED]'
    workspace_key => '[REDACTED]'
    custom_log_table_name => 'RSyslogMetrics'
    time_generated_field => 'custom_time_generated'
    key_names => ['custom_time_generated', 'name', 'origin', 'sender', 'messages']
  }
}
```

*Example of /var/log/test.log*

*Mon Nov 07 20:45:08 2022: { "name": "\_custom\_time\_generated", "origin": "test\_microsoft", "sender": "test@microsoft"*



*Edgie Enabled*