Elasticsearch & ArcSight Integration

Build Guide

V3 – 07/10/2018

Contents

Description

This guide shows how to install Elasticsearch 6.3 and configure it to consume ArcSight enriched events from SmartConnectors & Event Broker or Kafka.

Prerequisites

- Minimal installation of CentOS / RHEL 7.4.1708 or later
- An ArcSight environment with at least a single SmartConnector and/or Event Broker
    - SmartConnectors should be configured to send to the IP/hostname of the system which will be operating Logstash as CEF Syslog TCP to port 5000.

- Internet access to download Elasticsearch & root access to install Elasticsearch
- These procedures are designed for lab environments by disabling the firewall; this is ***NOT*** recommended for production environments.

CentOS/RHEL preparation

• Once the OS is installed

- yum & nano
  - yum install epel* -y && yum install net-tools wget git nano htop java-1.8* -y
  - yum update -y && systemctl disable firewalld && systemctl stop firewalld && reboot now
    - *System reboots*
  - nano /etc/yum.repos.d/elasticsearch.repo
    - *Paste this into elasticsearch.repo and save.*

```
[elasticsearch-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

  - nano /etc/yum.repos.d/kibana.repo
    - *Paste this into kibana.repo and save.*

```
[kibana-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
```

gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md

- nano /etc/yum.repos.d/logstash.repo
  - *Paste this into logstash.repo and save.*

[logstash-6.x]
name=Elasticsearch repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md

- rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
- yum install elasticsearch logstash kibana -y

Modify Elasticsearch, Kibana, and Logstash Configuration Files & Install X-Pack

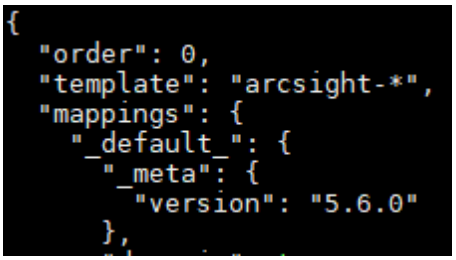
- nano /etc/elasticsearch/elasticsearch.yml
  - *Uncomment and modify for your environment:*
    - network.host: 10.0.100.10 (Accessible IP address of Elasticsearch)
    - network.port: 9200 (Default port)
  - *Optional modifications:*
    - cluster.name: (Cosmetic)
    - node.name: (Cosmetic)

- nano /etc/elasticsearch/jvm.options
    - *Modify for your environment, recommend 50% of physical RAM:*
        - Example for a system with 24GB of RAM:
        - -Xms12g
        - -Xmx12g
- service elasticsearch start (Once started, wait approximately 3 minutes before continuing)
- *Wait approximately 3 minutes before continuing*
- systemctl enable elasticsearch
- nano /etc/kibana/kibana.yml
    - *Uncomment and modify for your environment:*
        - server.port: 5601 (Default port)
        - server.host: "10.0.100.10" (Accessible IP address of Kibana)
        - elasticsearch.url: "http://10.0.100.10:9200" (IP & Port of elastic)
    - *Optional modifications:*
        - server.name: "ElasticSight"
- service kibana start
- systemctl enable kibana

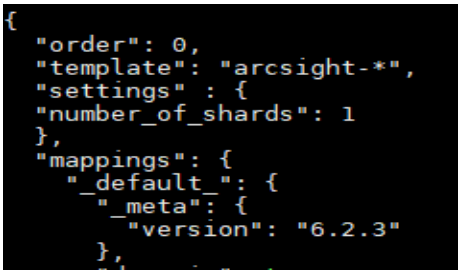
Optional configuration:

- nano /usr/share/logstash/x-pack/modules/arcsight/configuration/elasticsearch/arcsight.json
    - *Add the following and update the version to match this installation. This change is to lower the indexing shard count to "1", which is ideal for single node deployments; as well as to ensure standardization across the Elasticsearch installation.*

      Original:



Modified:



Logstash Configuration Options

Please read this section before continuing:

This next section provides two pathways to initiate Logstash; the first is to start Logstash as an application, which will require a restart after a reboot. The second is to configure Logstash as a service. The configuration for Logstash as a service is described once, with various configuration samples to select from. Please select your desired path and configuration then replace hostnames with your values. (IP addresses are acceptable as well.)

Logstash Application Consuming from Event Broker "eb-cef" Topic Only

- bash /usr/share/logstash/bin/logstash --modules arcsight --setup -M "arcsight.var.input.eventbroker.bootstrap_servers=*EventBroker.Hostname.TLD*:39092" -M "arcsight.var.input.eventbroker.topics=eb-cef" -M "arcsight.var.elasticsearch.hosts= *Elastic.Hostname.TLD*:9200" -M "arcsight.var.kibana.host= *Kibana.Hostname.TLD*:5601" &

Logstash Application Consuming from Event Broker "eb-cef" & "eb-other" Topics Only

- bash /usr/share/logstash/bin/logstash --modules arcsight --setup -M "arcsight.var.input.eventbroker.bootstrap_servers=*EventBroker.Hostname.TLD*:39092" -M "arcsight.var.input.eventbroker.topics=eb-cef, eb-other" -M

"arcsight.var.elasticsearch.hosts=*Elastic.Hostname.TLD*:9200" -M "arcsight.var.kibana.host=*Kibana.Hostname.TLD*:5601" &

Logstash Application Consuming from SmartConnectors Only

- bash /usr/share/logstash/bin/logstash --modules arcsight --setup -M "arcsight.var.inputs=smartconnector" -M "arcsight.var.input.smartconnector.port=*5000*" -M "arcsight.var.elasticsearch.hosts= *Elastic.Hostname.TLD*:9200" -M "arcsight.var.kibana.host= *Kibana.Hostname.TLD*:5601" &

Logstash Application Consuming from SmartConnectors & Multiple Kafka Topics

- bash /usr/share/logstash/bin/logstash --modules arcsight --setup -M "arcsight.var.inputs=*smartconnector,eventbroker*" -M "arcsight.var.input.smartconnector.port=*5000*" -M "arcsight.var.input.eventbroker.bootstrap_servers=*Kafka.Hostname.TLD*:9092" -M "arcsight.var.input.eventbroker.topics=*eb-cef,CEF*" -M "arcsight.var.elasticsearch.hosts= *Elastic.Hostname.TLD*:9200" -M "arcsight.var.kibana.host= *Kibana.Hostname.TLD*:5601" &

Logstash Service Consuming from Event Broker "eb-cef" Topic Only

- nano /etc/logstash/logstash.yml
- *Locate the "Module Settings" section, uncomment and complete for your environment.*

  Original:

```
# ------------ Module Settings ---------------
# Define modules here.  Modules definitions must be defined as an array.
# The simple way to see this is to prepend each `name` with a `-`, and keep
# all associated variables under the `name` they are associated with, and
# above the next, like this:
#
# modules:
#   - name: MODULE_NAME
#     var.PLUGINTYPE1.PLUGINNAME1.KEY1: VALUE
#     var.PLUGINTYPE1.PLUGINNAME1.KEY2: VALUE
#     var.PLUGINTYPE2.PLUGINNAME1.KEY1: VALUE
#     var.PLUGINTYPE3.PLUGINNAME3.KEY1: VALUE
#
# Module variable names must be in the format of
#
# var.PLUGIN_TYPE.PLUGIN_NAME.KEY
#
```

- *Replace the configuration with your hostname or IP address to reflect your environment.*

  Modified:

```
# ------------ Module Settings ---------------
# Define modules here.  Modules definitions must be defined as an array.
# The simple way to see this is to prepend each `name` with a `-`, and keep
# all associated variables under the `name` they are associated with, and
# above the next, like this:
#
modules:
   - name: arcsight
     var.inputs: eventbroker
     var.input.eventbroker.bootstrap_servers: EventBroker.Hostname.TLD:9092
     var.input.eventbroker.topics: eb-cef
     var.elasticsearch.hosts: Elastic.Hostname.TLD:9200
     var.kibana.host: Kibana.Hostname.TLD:5601
#
# Module variable names must be in the format of
#
# var.PLUGIN_TYPE.PLUGIN_NAME.KEY
#
```

- service logstash start
- systemctl enable logstash

Event Broker “eb-cef” Topic Only Sample

modules:

- name: arcsight

var.inputs: eventbroker

var.input.eventbroker.bootstrap_servers: EventBroker.Hostname.TLD:9092

```
    var.input.eventbroker.topics: eb-cef
    var.elasticsearch.hosts: Elastic.Hostname.TLD:9200
    var.kibana.host: Kibana.Hostname.TLD:5601
```

Event Broker “eb-cef” & “eb-other” Topics Only Sample

```
modules:
  - name: arcsight
    var.inputs: eventbroker
    var.input.eventbroker.bootstrap_servers: EventBroker.Hostname.TLD:9092
    var.input.eventbroker.topics: eb-cef,eb-other
    var.elasticsearch.hosts: Elastic.Hostname.TLD:9200
    var.kibana.host: Kibana.Hostname.TLD:5601
```

SmartConnectors Only Sample

```
modules:
 - name: arcsight
   var.inputs: smartconnector
    var.input.smartconnector.port: 5000
    var.elasticsearch.hosts: Elastic.Hostname.TLD:9200
    var.kibana.host: Kibana.Hostname.TLD:5601
```

SmartConnectors & Multiple Kafka Topics Sample

```
modules:
  - name: arcsight
    var.inputs: smartconnector,eventbroker
    var.input.eventbroker.bootstrap_servers: Kafka.Hostname.TLD:9092
    var.input.eventbroker.topics: eb-cef,CEF
    var.input.smartconnector.port: 5000
```

var.elasticsearch.hosts: Elastic.Hostname.TLD:9200

var.kibana.host: Kibana.Hostname.TLD:5601

Log Into Elasticsearch via the Kibana Interface

- Open a browser to your Kibana IP address or hostname on port 5601.
    - e.g. http://Elastic.Host.TLD:5601
- You will be automatically logged in.
- Click on “Timelion” to ensure events are being ingested.