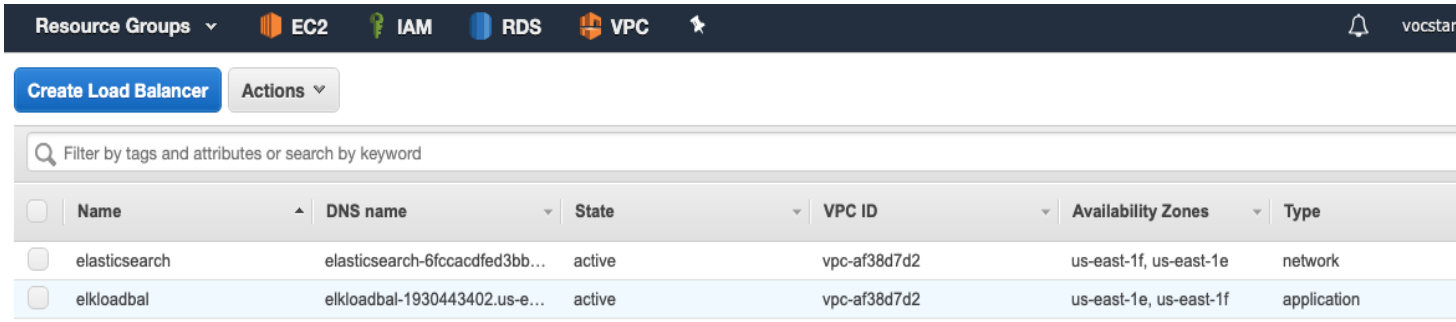
Jerome Thompson – ES Stack

1. Definition:

Elasticsearch is an open source, full-text search and analysis engine, based on the Apache Lucene search engine.
Logstash is a log aggregator that collects data from various input sources, executes different transformations and enhancements and then ships the data to various supported output destinations.
Kibana is a visualization layer that works on top of Elasticsearch, providing users with the ability to analyze and visualize the data.
Beats are lightweight agents that are installed on edge hosts to collect different types of data for forwarding into the stack.

2. AWS Service Setup

At the heart of our AWS setup are two load balancer



Name	DNS name	State	VPC ID	Availability Zones	Type
elasticsearch	elasticsearch-6fccacdfed3bb…	active	vpc-af38d7d2	us-east-1f, us-east-1e	network
elkloadbal	elkloadbal-1930443402.us-e…	active	vpc-af38d7d2	us-east-1e, us-east-1f	application

There is network (elasticsearch) and application (kibana) that were used. Both achieved the same end result; thus, it was a matter of exploring the options that were available.

Below is a screenshot of the elasticsearch load balancer settings:

Jerome Thompson – ES Stack

Name	elasticsearch
ARN	arn:aws:elasticloadbalancing:us-east-1:765128034604:loadbalancer/net/elasticsearch/6fccacdfed3bb83b
DNS name	elasticsearch-6fccacdfed3bb83b.elb.us-east-1.amazonaws.com (A Record)
State	active
Type	network
Scheme	internet-facing
IP address type	ipv4
VPC	vpc-af38d7d2
Availability Zones	subnet-842ebb8a - us-east-1f IPv4 address: Assigned by AWS subnet-08c02639 - us-east-1e IPv4 address: Assigned by AWS Edit subnets
Hosted zone	Z26RNL4JYFTOTI
Creation time	July 18, 2020 at 4:07:06 PM UTC-4

Attributes

Deletion protection	Disabled
Cross-Zone Load Balancing	Disabled
Access logs	Disabled

The following snippet is of the elasticsearch listener and target group

Listener ID	Security policy	SSL Certificate	ALPN policies	Default action
TCP : 9200 arn...cc3e6d5fa8578f4f	N/A	N/A	N/A	Forward to estarget
TCP : 9300 arn...a13393714e4710f9	N/A	N/A	N/A	Forward to elasticsearch93

Below is a screenshot of the kibana load balancer settings:

Jerome Thompson – ES Stack

Name	elkloadbal
ARN	arn:aws:elasticloadbalancing:us-east-1:765128034604:loadbalancer/app/elkloadbal/56d01e7fc64091e6
DNS name	elkloadbal-1930443402.us-east-1.elb.amazonaws.com (A Record)
State	active
Type	application
Scheme	internet-facing
IP address type	ipv4 Edit IP address type
VPC	vpc-af38d7d2
Availability Zones	subnet-08c02639 - us-east-1e IPv4 address: Assigned by AWS subnet-842ebb8a - us-east-1f IPv4 address: Assigned by AWS Edit subnets
Hosted zone	Z35SXDOTRQ7X7K
Creation time	July 15, 2020 at 3:05:55 AM UTC-4

Security

Security groups	sg-03d261985cd0b395d, **es-load-balancer-wizard-1** • load-balancer-wizard-1 created on 2020-07-15T02:58:03.314-04:00

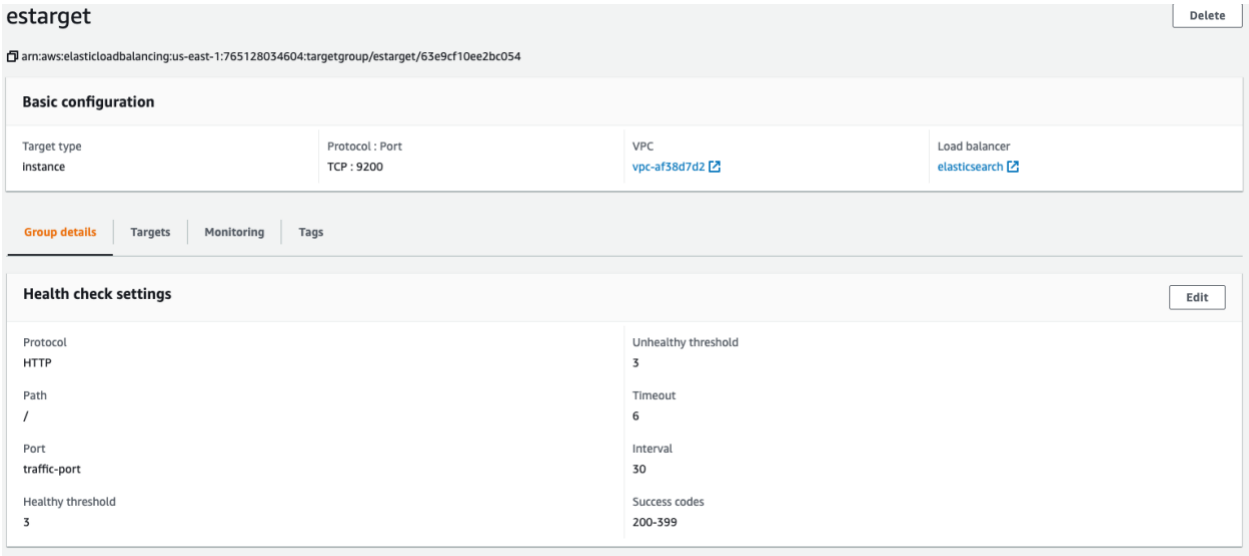
Below is a shot of the kibana listeners / target group

Listener ID	Security policy	SSL Certificate	Rules
HTTP : 5601 arn...2e034d0f4baddb64	N/A	N/A	Default: forwarding to kibanatrggrp View/edit rules

As follows we note the target groups (there are four but we are only using 2 of them)

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
elasticsearch93	arn:aws:elasticload...	9300	TCP	Instance	elasticsearch	vpc-af38d7d2
estarget	arn:aws:elasticload...	9200	TCP	Instance	elasticsearch	vpc-af38d7d2
estrggrp	arn:aws:elasticload...	9200	HTTP	Instance		vpc-af38d7d2
kibanatrggrp	arn:aws:elasticload...	5601	HTTP	Instance	elkloadbal	vpc-af38d7d2

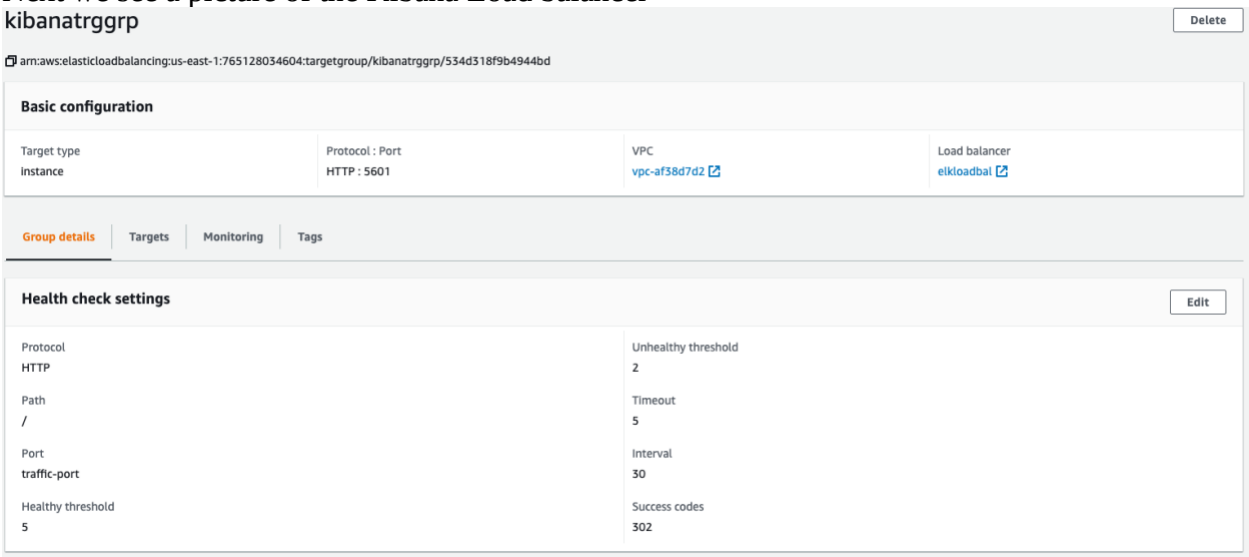
We are making use of the elasticsearch group that monitors traffic for port 9200



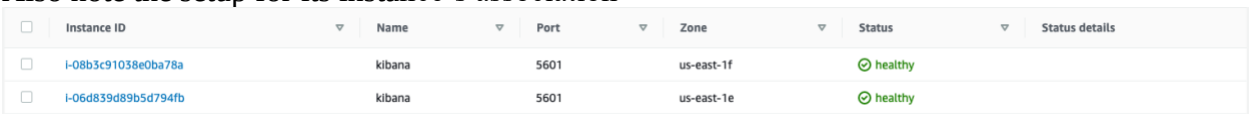
Along with the instance tied to that node (note that we are using one node).
Based on "The simple answer is that **Elasticsearch** is designed specifically to not **need a load balancer**." (How to Connect to Multiple Elasticsearch Client Nodes Without a Load Balancer, November 2017). So only went with one node and keep the option of the load balancer so that I could use the name when doing elasticsearch setups.

Instance ID	Name	Port	Zone	Status	Status details
i-0f62f5f221599de82	elasticsearch	9200	us-east-1f	healthy	

Next we see a picture of the Kibana Load balancer



Also note the setup for its instance's association



Instance ID	Name	Port	Zone	Status	Status details
i-08b3c91038e0ba78a	kibana	5601	us-east-1f	healthy	
i-06d839d89b5d794fb	kibana	5601	us-east-1e	healthy	

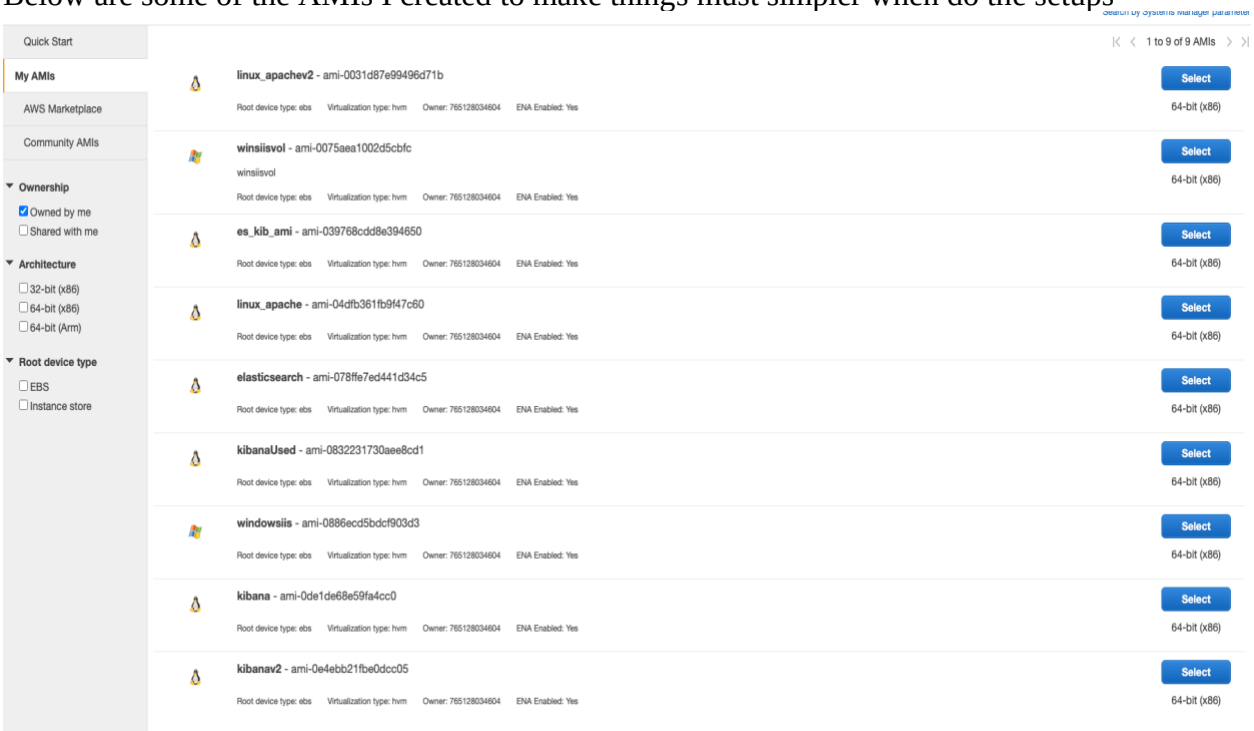
Next we take a look at the launch configurations, which uses AMIs to define what OS and specs should be spun up when auto scaling

Create launch configuration | Create Auto Scaling group | Copy to launch template | Actions

Filter: Filter launch configurations...

Name	AMI ID	Instance Type	Spot Price	Creation Time
kibana_launch...	ami-0e4ebb21fbe0dcc05	t2.micro		July 18, 2020 at 8:14:42 PM UT...
kib_launch_conf	ami-0e4ebb21fbe0dcc05	t2.micro		July 18, 2020 at 7:47:42 PM UT...
es_launch_conf1	ami-078ffe7ed441d34c5	t2.small		July 18, 2020 at 5:11:32 PM UT...

Below are some of the AMIs I created to make things must simpler when do the setups



I create a lot of AMIs for different purposes

The last key service for the auto scaling group, this what governs how the instances are scaled per target group. Notice that elasticsearch remains at one will the kibana starts at 2 and can grow to 4.

Create Auto Scaling group | Actions

Filter: Filter Auto Scaling groups...

Name	Launch Configuration /	Instances	Desired	Min	Max	Availability Zones	Default Cooldown	Health Check Gr
KIB Auto Scali...	kibana_launch_conf	2	2	2	4	us-east-1e, us-east-1f	300	300
ES Auto Scalin...	es_launch_conf1	1	1	1	1	us-east-1f	300	300

The scaling policy is note below for kibana, when the CPU > 85 scaling occurs

Scale Group Size

Policy type:	Target Tracking scaling
Execute policy when:	As required to maintain Average CPU Utilization at 85
Take the action:	Add or remove instances as required
Instances need:	300 seconds to warm up after scaling
Disable scale-in:	No

Below we take of instances that are in play

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
	i-0b2febb397425c8a8	t2.small	us-east-1e	stopped		None		-	-
linux_hhtpd	i-03e56a22f288ebfda	t2.micro	us-east-1a	running	2/2 checks passed	None	ec2-34-207-201-161.co...	34.207.201.161	-
winsiis	i-02d45d2ec2fc19ee5	t2.micro	us-east-1e	running	2/2 checks passed	None	ec2-34-229-161-82.co...	34.229.161.82	-
kibana	i-08b3c91038e0ba78a	t2.micro	us-east-1f	running	2/2 checks passed	None	ec2-34-239-156-10.co...	34.239.156.10	-
elasticsearch	i-0f62f5f221599de82	t2.small	us-east-1f	running	2/2 checks passed	None	ec2-3-236-52-168.com...	3.236.52.168	-
kibana	i-06d839d89b5d794fb	t2.micro	us-east-1e	running	2/2 checks passed	None	ec2-18-208-119-107.co...	18.208.119.107	-

3. Server Setup

1. Linux Apache setup

Below are the aws settings

linux_hhtpd	i-03e56a22f288ebfda	t2.micro	us-east-1a	running	2/2 checks passed	None	ec2-34-207-201-161.co...	34.207.201.161

Instance ID	i-03e56a22f288ebfda
Instance state	running
Instance type	t2.micro
Finding	You may not have permission to access AWS Compute Optimizer.
Private DNS	ip-172-31-34-218.ec2.internal
Private IPs	172.31.34.218
Secondary private IPs	
VPC ID	vpc-af38d7d2
Subnet ID	subnet-1497484b
Network interfaces	eth0
IAM role	-
Key pair name	elk_key
Owner	765128034604
Launch time	July 18, 2020 at 8:51:25 PM UTC-4 (54 hours)
Termination protection	False
Lifecycle	normal
Monitoring	basic
Alarm status	None
Kernel ID	-
RAM disk ID	-
Placement group	-
Partition number	-
Virtualization	hvm
Reservation	r-02a940a6be166f298
AMI launch index	0
Tenancy	default

Public DNS (IPv4)	ec2-34-207-201-161.compute-1.amazonaws.com
IPv4 Public IP	34.207.201.161
IPv6 IPs	-
Elastic IPs	
Availability zone	us-east-1a
Security groups	es_kib_sg. view inbound rules. view outbound rules
Scheduled events	No scheduled events
AMI ID	linux_apache (ami-04dfb361fb9f47c60)
Platform details	Linux/UNIX
Usage operation	RunInstances
Source/dest. check	True
T2/T3 Unlimited	Disabled
EBS-optimized	False
Root device type	ebs
Root device	/dev/xvda
Block devices	/dev/xvda
Elastic Graphics ID	-
Elastic Inference accelerator ID	-
Capacity Reservation	-
Capacity Reservation Settings	Open
Outpost Arn	-

Below was used to yum install filebeat

```
[root@ip-172-31-34-218 ~]# cat /etc/yum.repos.d/elastic-beats.repo
[elastic-6.x]
name=Elastic repository for 6.x packages
baseurl=https://artifacts.elastic.co/packages/oss-6.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
[root@ip-172-31-34-218 ~]#
```

```
- type: log

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /var/log/messages
    - /var/log/httpd/*
    - /var/log/filebeat/*
    #- c:\programdata\elasticsearch\logs\*
```

Above shows the path that will be used filebeat to eed elasticsearch

```
#============================== Dashboards =====================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here, or by using the `-setup` CLI flag or the `setup` command.
setup.dashboards.enabled: true

# The URL from where to download the dashboards archive. By default this URL
# has a value which is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:
```

Above shows that dashboards have been sent to kibana server

```
#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/pa
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "elkloadbal-1930443402.us-east-1.elb.amazonaws.com:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:
```

Above shows the kibana settings

```
#------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["elasticsearch-6fccacdfed3bb83b.elb.us-east-1.amazonaws.com:9200"]

  # Enabled ilm (beta) to use index lifecycle management instead daily indices.
  #ilm.enabled: false

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"
```

Above shows the elasticsearch settings

```
#================================ Logging ======================================

# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug
logging.level: debug
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
  permissions: 0644
```

Above shows the logging option chosen

```
vim /etc/filebeat/modules.d/
filebeat modules enable apache2
systemctl restart filebeat
```

Above shows the apache2 being enabled

Below shows the filebeat options for starting and enabling:
systemctl start filebeat
systemctl enable filebeat

Jerome Thompson – ES Stack

2. Windows 98 IIS Server setup

1. Filebeat

Can be used to install filebeat
https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-installation.html

```
filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

- type: log

  # Change to true to enable this input configuration.
  enabled: false

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    #- C:\inetpub\logs\LogFiles\W3SVC1
    #- /var/log/*.log
    #- c:\programdata\elasticsearch\logs\*
```

Above shows the input for filebeat

```
# ================================= Dashboards =================================
# These settings control loading the sample dashboards to the Kibana index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here or by using the `setup` command.
setup.dashboards.enabled: true

# The URL from where to download the dashboards archive. By default this URL
# has a value which is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:
```

Above shows the option for sending dashboards to kibana has been enabled

```
# ================================= Kibana =================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify and additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "elkloadbal-1930443402.us-east-1.elb.amazonaws.com:5601"

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:
```

Above shows the kibana host setup settings

```
# ---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["elasticsearch-6fccacdfed3bb83b.elb.us-east-1.amazonaws.com:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"
```

Above shows the elasticsearch settings setup

```
# ================================== Logging ===================================

# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug
#logging.level: debug
logging.level: debug
logging.to_files: true
logging.files:
  path: C:\Program Files\filebeat-7\Logs
  name: filebeat
  keepfiles: 7
  permissions: 0644
# At debug level, you can selectively enable logging only for some components.
```

Above shows the logging settings

Above shows the what is displayed in kibana for filebeat

2. Winlogbeat

Can be used to install winlogbeat
https://www.elastic.co/guide/en/beats/winlogbeat/current/winlogbeat-installation.html

```
#======================== Winlogbeat specific options ==========================

# event_logs specifies a list of event logs to monitor as well as any
# accompanying options. The YAML data type of event_logs is a list of
# dictionaries.
#
# The supported keys are name (required), tags, fields, fields_under_root,
# forwarded, ignore_older, level, event_id, provider, and include_xml. Please
# visit the documentation for the complete details of each option.
# https://go.es.io/WinlogbeatConfig
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: Security
  - name: System
  - name: ForwardedEvents
    tags: [forwarded]
#===================== Elasticsearch template setting ==========================
```

Above shows the events that will be sent to kibana

```
#============================== Dashboards =====================================
# These settings control loading the sample dashboards to the Kibana:q
 #index. Loading
# the dashboards is disabled by default and can be enabled either by setting the
# options here, or by using the `-setup` CLI flag or the `setup` command.
setup.dashboards.enabled: true

# The URL from where to download the dashboards archive. By default this URL
# has a value which is computed based on the Beat name and version. For released
# versions, this URL points to the dashboard archive on the artifacts.elastic.co
# website.
#setup.dashboards.url:
```

Above shows the dashboard is being sent to kibana

```
#================================ Outputs ======================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["elasticsearch-6fccacdfed3bb83b.elb.us-east-1.amazonaws.com:9200"]

  # Enabled ilm (beta) to use index lifecycle management instead daily indices.
  #ilm.enabled: false

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"
```

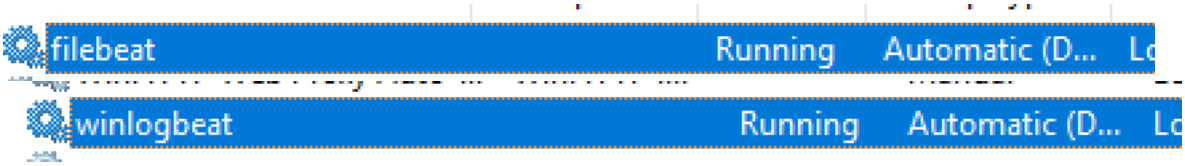
Above shows the elasticsearch settings for winlogbeat

```
#================================ Logging ===================================

# Sets log level. The default log level is info.
# Available log levels are: error, warning, info, debug
#logging.level: debug
logging.level: debug
logging.to_files: true
logging.files:
  path: C:\Program Files\winlogbeat-7\Logs
  name: winlogbeat
  keepfiles: 7
  permissions: 0644

# At debug level, you can selectively enable logging only for some components
```

Above shows the logging for winlogbeat



Above shows the services have been started

[Above shows the kibana display for winlogbeat](#)

3. Elasticsearch server setup

Used the same repo noted in setup of filebeat on Linux Apache server to yum install elasticsearch.

I followed the posted guide for elasticsearch install (tried a couple things that didn't work out such as index renaming).

```
# ---------------------------------- Paths ----------------------------------
#
# Path to directory where to store the data (separate multiple locations by comma):
#
path.data: /var/lib/elasticsearch
#
# Path to log files:
#
path.logs: /var/log/elasticsearch
#
# ---------------------------------- Memory ---------------------------------
```

Above shows the paths for elasticsearch settings

```
#
# ---------------------------------- Network ---------------------------------
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
#network.host: 192.168.0.1
network.host: 0.0.0.0
network.bind_host: 0.0.0.0
network.publish_host: 0.0.0.0
transport.host: localhost
transport.tcp.port: 9300
#
# Set a custom port for HTTP:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
```

Above shows the network config for elasticsearch

```
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
cluster.name: elasticsearch
discovery.type: single-node
discovery.seed_providers: ec2
discovery.ec2.endpoint: ec2.us-east-1.amazonaws.com
discovery.ec2.tag.Name: "elasticsearch"
http.cors.enabled: true
http.cors.allow-origin: "*"
```

Above shows the discovery option for elasticsearch as it regards the ec2 instances

```
[root@ip-172-31-69-138 ~]# tail -f /var/log/elasticsearch/elasticsearch.log
[2020-07-21T04:07:30,247][INFO ][o.e.c.m.MetadataMappingService] [ip-172-31-69-138.ec2.internal] [winlogbeat-7.8.0-2020.07.21/s3whThUhTCSQS-CpXo_A]
A] update_mapping [_doc]
[2020-07-21T04:07:39,309][INFO ][o.e.c.m.MetadataMappingService] [ip-172-31-69-138.ec2.internal] [winlogbeat-7.8.0-2020.07.21/s3whThUhTCSQS-CpXo_A]
A] update_mapping [_doc]
[2020-07-21T04:08:02,416][INFO ][o.e.c.m.MetadataMappingService] [ip-172-31-69-138.ec2.internal] [winlogbeat-7.8.0-2020.07.21/s3whThUhTCSQS-CpXo_A]
A] update_mapping [_doc]
```

Above shows the elasticsearch logs after being started

Below can used to start and enable elasticsearch:
systemctl enable elasticsearch
systemctl start elasticsearch

Below depics hwo to delete an index for the command line:
/usr/share/elasticsearch/bin/elasticsearch-plugin install discovery-ec2
curl -XDELETE 'http://http://ec2-54-160-96-119.compute-1.amazonaws.com/:9200/.kibana_1' --header "content-type: application/JSON"

4. Kibana server setup

Used the same repo noted in setup of filebeat on Linux apache server to yum install kibana-oss

```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names
# The default is 'localhost', which usually means remote machines will not be able to con
# To allow connections from remote users, set this parameter to a non-loopback address.
#server.host: "localhost"
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePat
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""
```

Above shows Part 1of the kibana server settings local port and server ip settings

```
# The Kibana server's name.  This is used for display purposes.
#server.name: "your-hostname"
server.name: "kibana"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://elasticsearch-6fccacdfed3bb83b.elb.us-east-1.amazonaws.com:9200"]

# When this setting's value is true Kibana uses the hostname specified in the server.host
# setting. When the value of this setting is false, Kibana uses the hostname of the host
# that connects to this Kibana instance.
#elasticsearch.preserveHost: true
elasticsearch.preserveHost: false

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"
```

Above shows Part2 of kibana settings with additionally server info

```
elasticsearch.requestTimeout: 60000

# List of Kibana client-side headers to send to Elasticsearch. To send
# headers, set this value to [] (an empty list).
#elasticsearch.requestHeadersWhitelist: [ authorization ]

# Header names and values that are sent to Elasticsearch. Any custom he
# by client-side headers, regardless of the elasticsearch.requestHeader
#elasticsearch.customHeaders: {}

# Time in milliseconds for Elasticsearch to wait for responses from sha
#elasticsearch.shardTimeout: 30000

# Time in milliseconds to wait for Elasticsearch at Kibana startup befo
#elasticsearch.startupTimeout: 5000

# Logs queries sent to Elasticsearch. Requires logging.verbose set to t
#elasticsearch.logQueries: false
elasticsearch.logQueries: true

# Specifies the path where Kibana creates the process ID file.
#pid.file: /var/run/kibana.pid

# Enables you specify a file where Kibana stores log output.
#logging.dest: stdout
logging.dest: /var/log/kibana/kibana.log
```

Above shows the Part 3 of elasticsearch settings

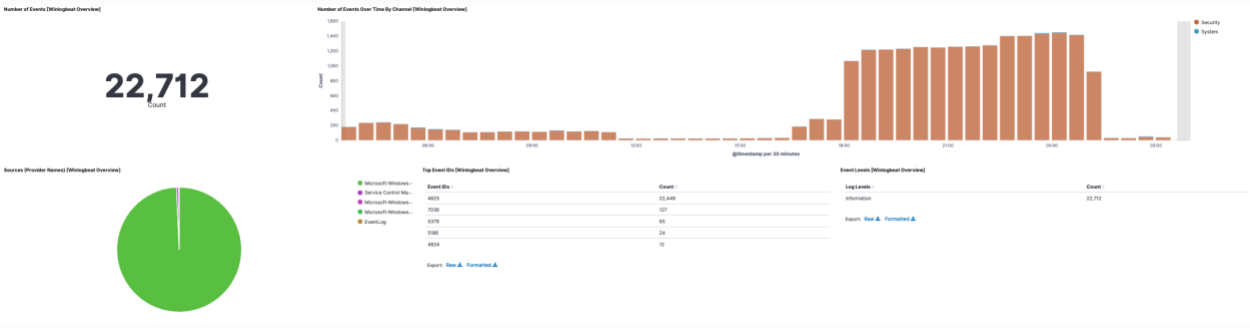
Below can be used to stop and start server:
systemctl enable kibana
systemctl start kibana

4. Reports and Dashboards
    1. Dashboards

Access and error logs ECS

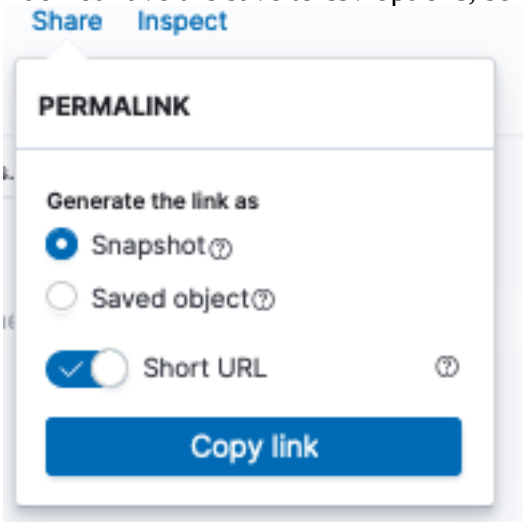
Jerome Thompson – ES Stack

[Winlogbeat] Overview



2. Reports

I do not have the save to csv options, so I have hyper-linked reports below



windows_iis_filebeat7_iss_error
is used to display windows iis error related entries
windows_winlogbeat_admin_activity
is used to display admin related windows events

5. Conclusion

This was an amazing project that showed how to harness the power of the ES Slack through creation of servers that did various pieces of the stack along with ones that feed logs to elasticsearch.

6. Reference

How to Connect to Multiple Elasticsearch Client Nodes Without a Load Balancer, ObjectRocket, November 11 2017, https://www.objectrocket.com/blog/elasticsearch/elasticsearch-and-load-balancers,