



Amazon Elasticsearch Service

Fully managed, reliable, and scalable Elasticsearch service.

Easy and Scalable Log Analytics

Inside a VPC

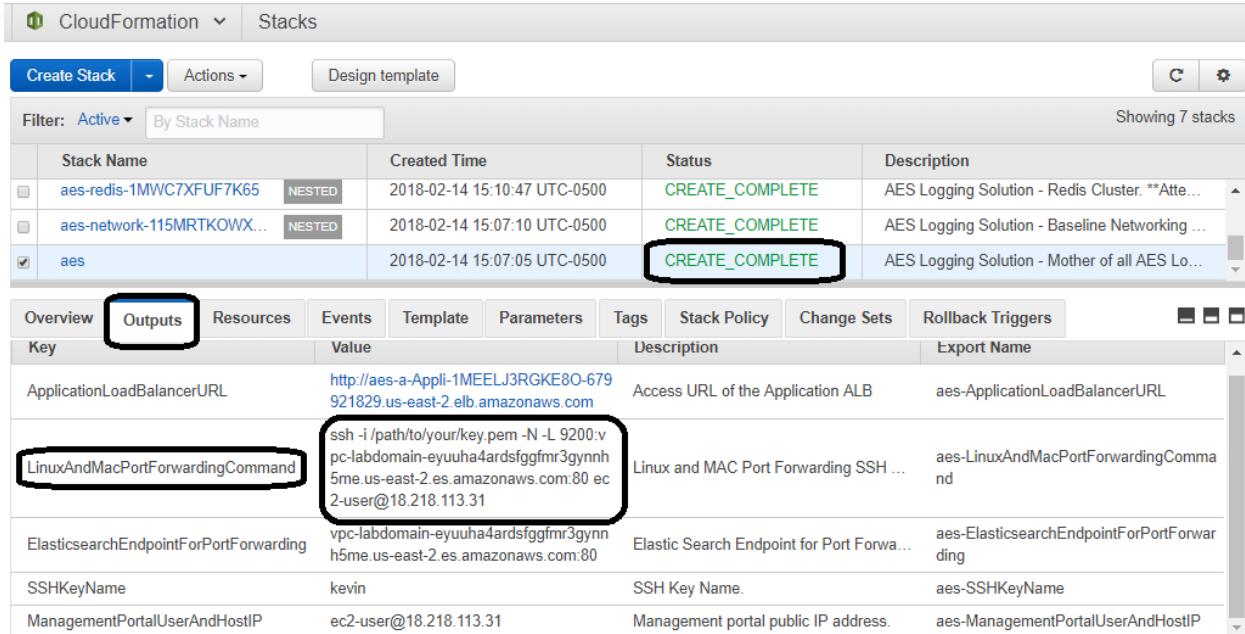
Mac / Linux Proxy Instructions

Set up an SSH tunnel to forward your local traffic to Amazon ES [Mac and Linux]

In order to load Kibana on your laptop's browser, you need to send the traffic to your Amazon ES domain. Since the domain is in your VPC, and your Amazon ES cluster is in a private subnet, you must pass the traffic through the linux management portal.

You need the public IP address of the Linux management portal instance. Navigate to the CloudFormation, AWS console. Click the parent stack to view the details.

Then click the **Outputs** tab.



The screenshot shows the AWS CloudFormation console. The 'Stacks' section lists three stacks: 'aes-redis-1MWC7XFUF7K65', 'aes-network-115MRTKOWX...', and 'aes'. The 'aes' stack is selected, and its status is 'CREATE_COMPLETE'. The 'Outputs' tab is active, showing a list of outputs. The 'LinuxAndMacPortForwardingCommand' output is highlighted, showing the SSH command: `ssh -i /path/to/your/key.pem -N -L 9200:vpc-labdomain-eyuuha4ardsfggfm3gynnh5me.us-east-2.es.amazonaws.com:80 ec2-user@18.218.113.31`.

| Stack Name | Created Time | Status | Description |
|---------------------------|------------------------------|-----------------|---|
| aes-redis-1MWC7XFUF7K65 | 2018-02-14 15:10:47 UTC-0500 | CREATE_COMPLETE | AES Logging Solution - Redis Cluster. **Atte... |
| aes-network-115MRTKOWX... | 2018-02-14 15:07:10 UTC-0500 | CREATE_COMPLETE | AES Logging Solution - Baseline Networking ... |
| aes | 2018-02-14 15:07:05 UTC-0500 | CREATE_COMPLETE | AES Logging Solution - Mother of all AES Lo... |

| Key | Value | Description | Export Name |
|--|---|---|---|
| ApplicationLoadBalancerURL | http://aes-a-Appli-1MEELJ3RGKE8O-679921829.us-east-2.elb.amazonaws.com | Access URL of the Application ALB | aes-ApplicationLoadBalancerURL |
| LinuxAndMacPortForwardingCommand | <code>ssh -i /path/to/your/key.pem -N -L 9200:vpc-labdomain-eyuuha4ardsfggfm3gynnh5me.us-east-2.es.amazonaws.com:80 ec2-user@18.218.113.31</code> | Linux and MAC Port Forwarding SSH ... | aes-LinuxAndMacPortForwardingComma nd |
| ElasticsearchEndpointForPortForwarding | <code>vpc-labdomain-eyuuha4ardsfggfm3gynnh5me.us-east-2.es.amazonaws.com:80</code> | Elastic Search Endpoint for Port Forwa... | aes-ElasticsearchEndpointForPortForwa ding |
| SSHKeyName | kevin | SSH Key Name. | aes-SSHKeyName |
| ManagementPortalUserAndHostIP | <code>ec2-user@18.218.113.31</code> | Management portal public IP address. | aes-ManagementPortalUserAndHostIP |


Find the **LinuxAndMacPortForwardingCommand**

Open the Terminal app and use the command found in the value to set up SSH tunnel forwarding. For example, mine value looks like so:

```
ssh -i /path/to/your/key.pem -N -L 9200:vpc-labdomain-eyuuha4ardsfggfm3gynnh5me.us-east-2.es.amazonaws.com:80 ec2-user@18.218.113.31
```

Be sure to use the location of your pem file (created in prior instructions for the lab) as the replacement for the italic, underlined value (/path/to/your/key.pem).

Open your browser and hit `http://localhost:9200/_plugin/kibana`. You will see a splash screen, followed by

kibana

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Management / Kibana

Index Patterns Saved Objects Advanced Settings

Warning

No default index pattern.
You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

Index name or pattern

logstash-*

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

Time Filter field name ⓘ [refresh fields](#)

@timestamp

☐ Expand index pattern when searching [DEPRECATED]

With this option selected, searches against any time-based index pattern that contains a wildcard will automatically be expanded to query only the indices that contain data within the currently selected time range.

Searching against the index pattern *logstash-** will actually query Elasticsearch for the specific matching indices (e.g. *logstash-2015.12.21*) that fall within the current time range.

With recent changes to Elasticsearch, this option should no longer be necessary and will likely be removed in future versions of Kibana.

☐ Use event times to create index names [DEPRECATED]

Create

Kibana is now in place and with your browser and a proxy.