How to Configure Logstash to send local data to Elastic Cloud

Both single files and active logs

Produced for CISA by Team Anomalous

Logstash Pre-Configuration

Download Logstash

Download Logstash from: https://www.elastic.co/downloads/logstash

Download the Pre-Configured Config Files Associated with this Document

Insert them into the config folder inside your downloaded Logstash folder and replace the existing files.

Configure Config Files

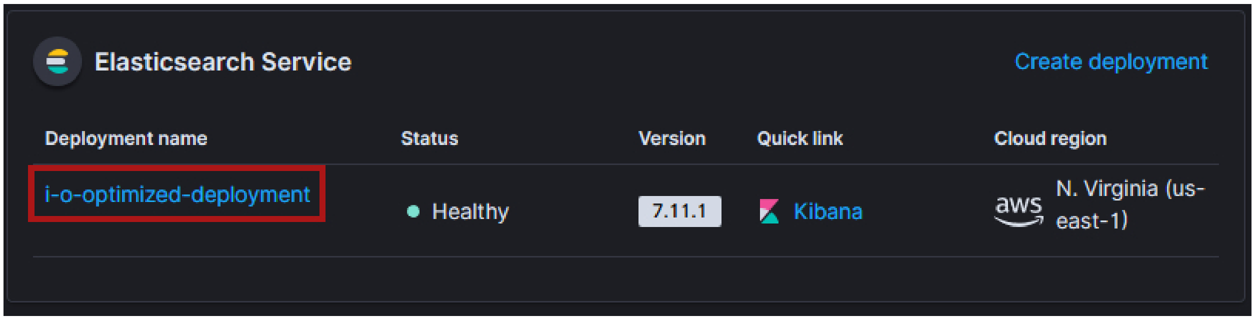
Open up both the logstash.conf as well as the logstash.yml and as you gather the information in the next section insert the information into the config files.

DO NOT USE BACKSLASH (\) AT ANY POINT IN YOUR CONFIG. LOGSTASH TREATS IT AS AN EXIT SYMBOL.

IF AT ANY POINT YOU HAVE TO RUN LOGSTASH AGAIN ON A DATASET DELETE THE DATASET YOU RAN IT ON ORIGINALLY AND EITHER RE-DOWNLOAD OR RE-EXTRACT THE FILE. LOGSTASH WILL IGNORE ANY FILE IT HAS EVEN PARTIALLY INTERACTED WITH.

Gather information from your Elastic Deployment

Select Deployment



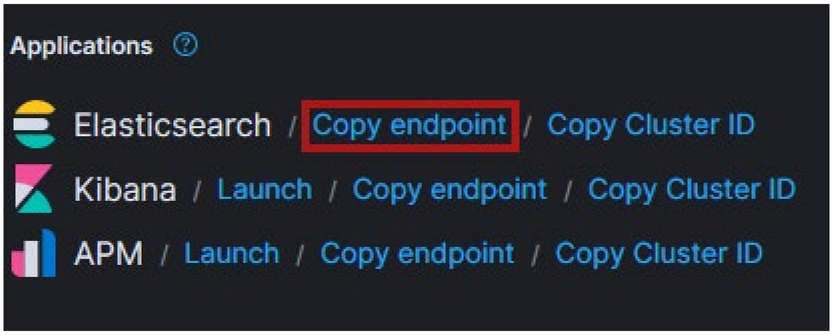
Elasticsearch Service

Create deployment

Deployment name	Status	Version	Quick link	Cloud region
i-o-optimized-deployment	● Healthy	7.11.1	Kibana	aws N. Virginia (us-east-1)

Click on your desired deployment to enter the home page.

Copy the Elastic Endpoint



Applications

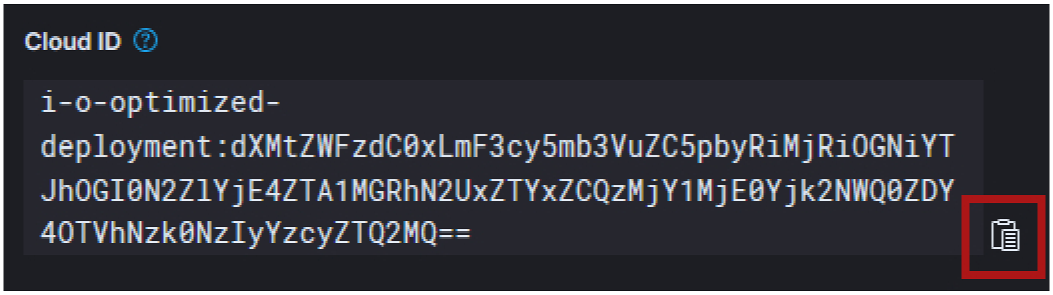
Elasticsearch / Copy endpoint / Copy Cluster ID

Kibana / Launch / Copy endpoint / Copy Cluster ID

APM / Launch / Copy endpoint / Copy Cluster ID

Copy the Elasticsearch endpoint and insert it into line 19: hosts, in the logstash.conf file.

Copy the Cloud ID

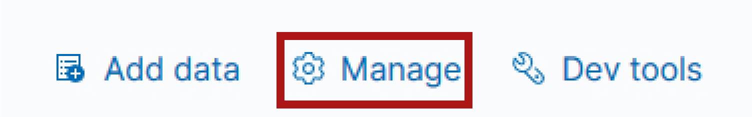


Cloud ID

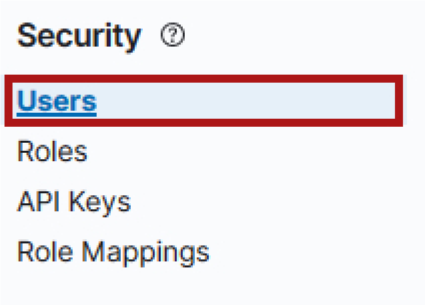
```
i-o-optimized-
deployment:dXMtZWFzdC0xLmF3cy5mb3VuZC5pbyRiMjRiOGNiYT
JhOGI0N2ZlYjE4ZTA1MGRhN2UxZTYxZCQzMjY1MjE0Yjk2NWQ0ZDY
4OTVhNzk0NzIyYzcyZTQ2MQ==
```

Copy the Cloud ID using the clipboard button and insert the entire ID including the name into line 150 of the logstash.yml file.

Go to Kibana and Open the Manage Toolbar

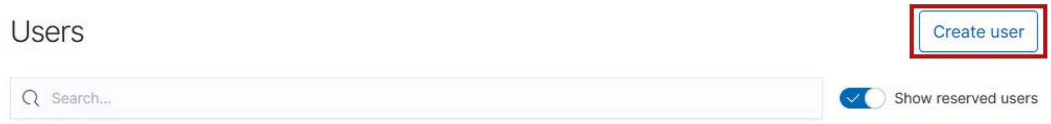


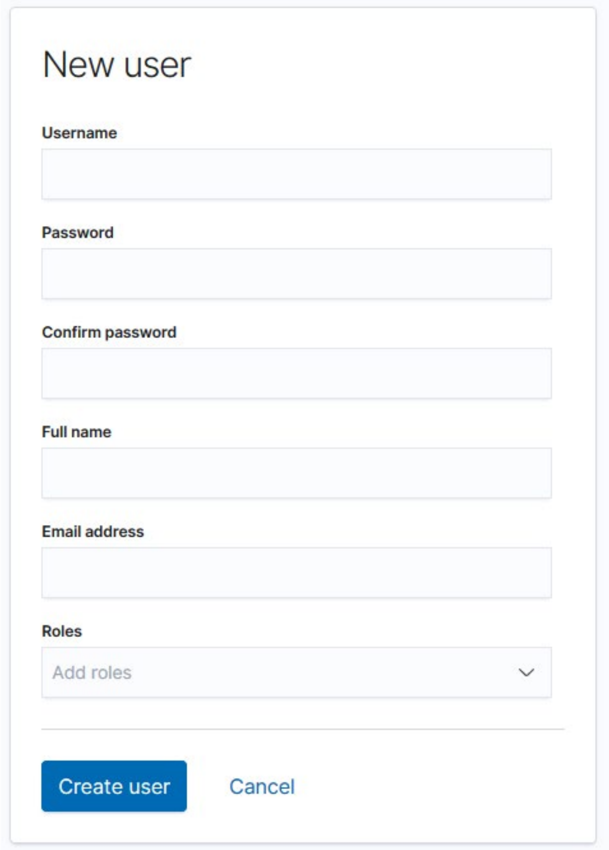
Open the Users Menu



On the left side menu, four sections down under the security subsection click on the Users tab.

Create a New User





Fill out the new user information with a new username and password combination. There is no need to fill in the full name or the email address boxes. Under role on the left side menu, four sections down under the security subsection click on the User. Give the user superuser role, if making it into a production model use the guides provided by Elastic for creating a permanent role for your Logstash user. Once finished, create the user.

Fill in the username and password under line 155 in the logstash.yml as well as lines 20 and 21 in the logstash.conf

Final Logstash Configuration and Execution

Path to File

On line 6 of the logstash.conf insert the path to your intended dataset.

Running Logstash

Open Command Prompt (Administrator is not necessary) and navigate to the logstash folder then to the bin folder within.

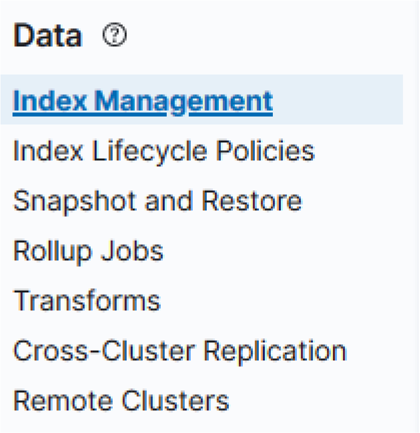
Then run this command to run Logstash: logstash -f ../config/logstash.conf

Logstash will then run and over approximately 2 minutes Logstash will print a lot of [INFO] messages as well as two [WARN] messages. Then Logstash will stay on the line “[INFO][logstash.agent   ] Successfully started Logstash API endpoint {:port=>9600}” until Logstash shuts down once it is finished.

LOGSTASH WILL DELETE YOUR FILE ONCE IT IS FINISHED PROCESSING

Configuring Elastic Cloud to be Able to Use Logstash Data

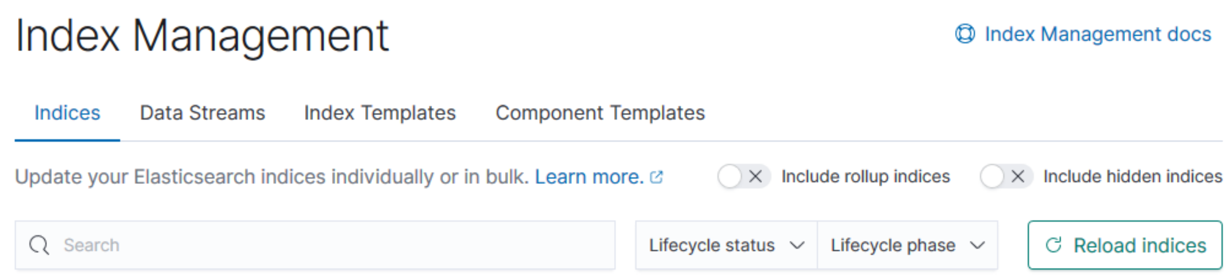
Confirming That Elastic Received Your Data



Data ⓘ

Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Cross-Cluster Replication
Remote Clusters

Navigate to Kibana and open the manage menu. In the second section Data, click on the Index Management tab.



Index Management — Index Management docs

Indices | Data Streams | Index Templates | Component Templates

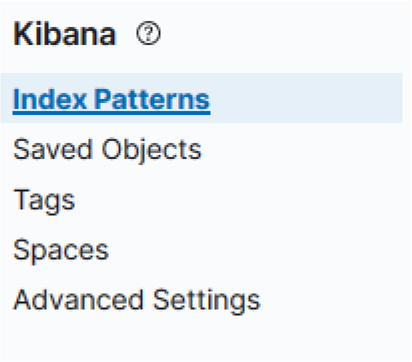
Update your Elasticsearch indices individually or in bulk. Learn more.

○ Include rollup indices ○ Include hidden indices

Search | Lifecycle status | Lifecycle phase | Reload indices

The Indices should be in the order of most recent at the top, so if you were successful you should see your logstashindex index at the top.

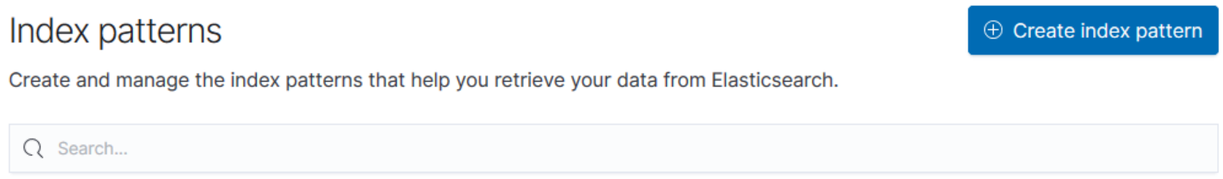
Putting the Data into Kibana



Kibana ⓘ

Index Patterns
Saved Objects
Tags
Spaces
Advanced Settings

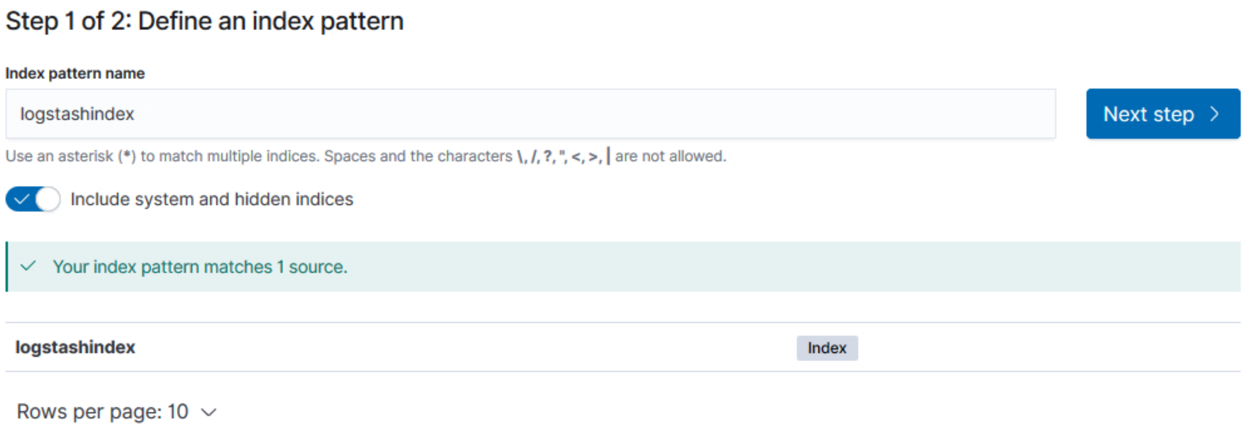
On the left-hand menu in Kibana in the fifth section Kibana, select the first tab Index Patterns.



Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

Click Create index pattern



Step 1 of 2: Define an index pattern

Index pattern name

logstashindex

Use an asterisk (*) to match multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.

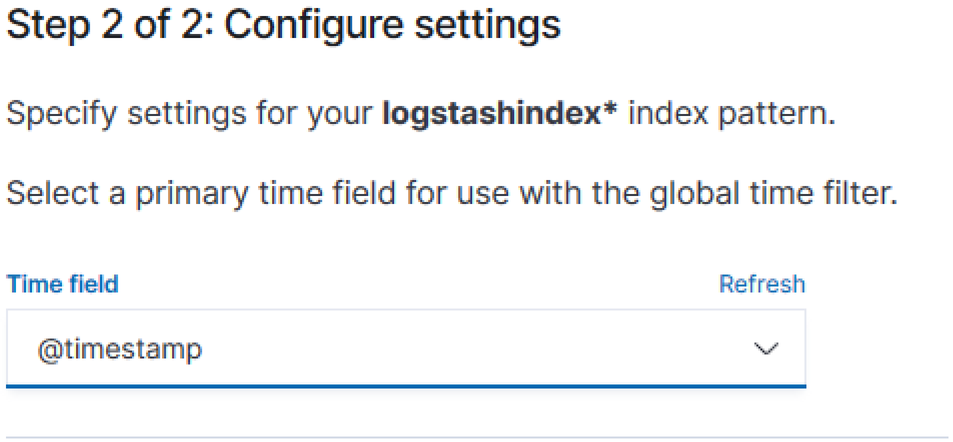
Include system and hidden indices

✓ Your index pattern matches 1 source.

logstashindex	Index

Rows per page: 10

Type in logstashindex into the name and your index from the last step should appear. Once you see that as the only index in the list below and the next step button is blue you can click the button.



Step 2 of 2: Configure settings

Specify settings for your **logstashindex*** index pattern.

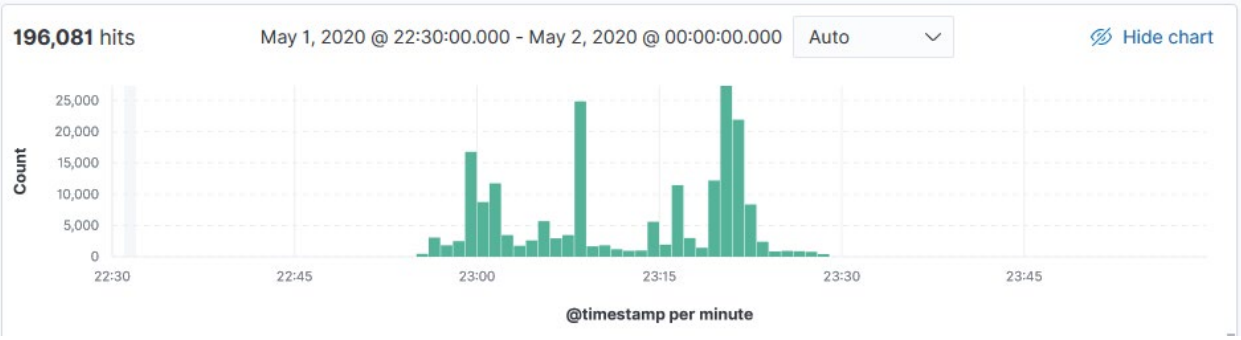
Select a primary time field for use with the global time filter.

Time field

@timestamp

Click on the Time Field drop-down and select @timestamp.

Displaying Your Data



Once you have finished your data should be available in any of the data select drop downs in Kibana.