

Question 1 of 5

What is the token from deploying fluentd?

753f92 The token might be changed, get the token from your terminal output

- Open **Desktop/fluentd.yaml** in terminal and make below changes in green rectangle.

```
Desktop
Applications: iml-user@elastic-desk...
iml-user@elastic-desktop-kubectl: ~
iml-user@elastic-desktop-kubectl: ~

serviceAccountName: fluentd
tolerations:
- key: node-role.kubernetes.io/master
  effect: NoSchedule
containers:
- name: fluentd
  image: fluent/fluentd-kubernetes-daemonset:v1-debian-elasticsearch
  env:
    - name: FLUENT_CONTAINER_TAIL_PARSER_TYPE
      value: "cri"
    - name: FLUENT_ELASTICSEARCH_HOST
      value: "metrol-io-elastic"
    - name: FLUENT_ELASTICSEARCH_PORT
      value: "9200"
    - name: FLUENT_ELASTICSEARCH_SCHEME
      value: "http"
    # Option to configure elasticsearch plugin with self signed certs
    # =====
    - name: FLUENT_ELASTICSEARCH_SSL_VERIFY
      value: "false"
    # Option to configure elasticsearch plugin with tls
    # =====
    - name: FLUENT_ELASTICSEARCH_SSL_VERSION
      value: "TLSv1.2"
    # X-Pack Authentication
    # =====
    - name: FLUENT_ELASTICSEARCH_USER
      value: "elastic"
    - name: FLUENT_ELASTICSEARCH_PASSWORD
      value: "changeme"
    - name: K8S_NODE_NAME
      valueFrom:
        fieldRef:
          fieldPath: spec.nodeName
resources:
  limits:
    memory: 200Mi
  requests:
-- INSERT --
```

- Run the kubectl command, and the token will be printed on the terminal.

```
Applications: iml-user@elastic-desk...
iml-user@elastic-desktop-kubectl: ~
iml-user@elastic-desktop-kubectl: ~

iml-user@elastic-desktop-kubectl:~$ vi Desktop/fluentd.yaml
iml-user@elastic-desktop-kubectl:~$ cd Desktop/
iml-user@elastic-desktop-kubectl:~/Desktop$ kubectl apply -f fluentd.yaml
daemonset.apps/fluentd created
iml-user@elastic-desktop-kubectl:~/Desktop$ Your token for Q1 is: 753f92, its also on the desktop
iml-user@elastic-desktop-kubectl:~/Desktop$
```

Question 2 of 5

Name one other Daemonset deployed in the kube-system namespace?

calico-node or kube-proxy, both answer should work

```
iml-user@elastic-desktop-kubect1:~$ kubectl get ds -n kube-system
```

NAME	DESIRED	CURRENT	READY	UP-TO-DATE	AVAILABLE	NODE SELECTOR	AGE
calico-node	2	2	2	2	2	kubernetes.io/os=linux	25m
fluentd	2	2	2	2	2	<none>	5m26s
kube-proxy	2	2	2	2	2	kubernetes.io/os=linux	25m

```
iml-user@elastic-desktop-kubect1:~$
```

Question 3 of 5

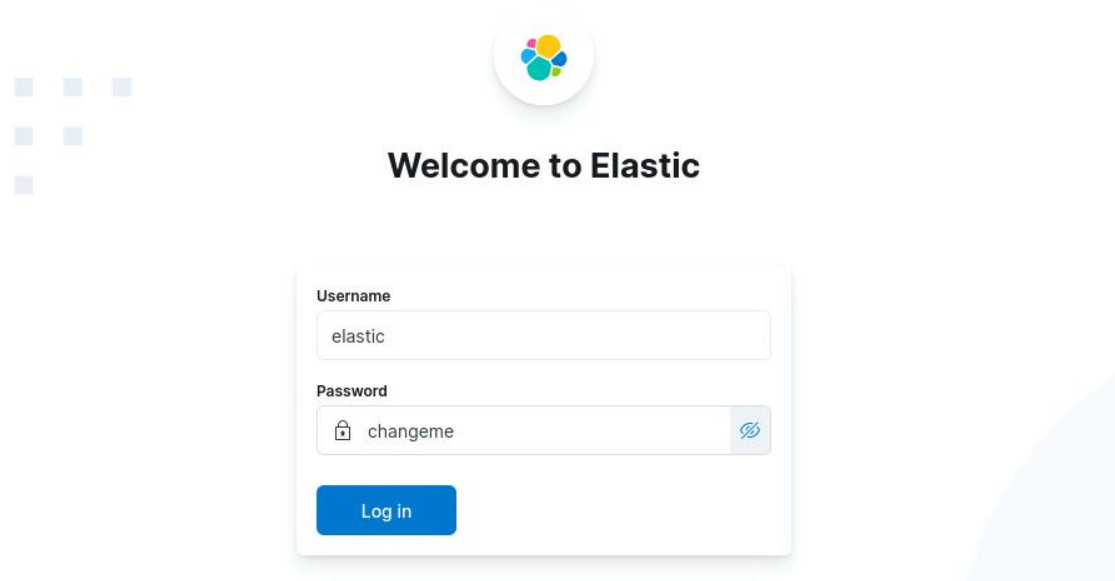
What is the token from the pod called "leaky-pod"?

ab5d7f

Steps for question 3

- Log in to Elasticsearch

metrol-io-elastic:5601/login?next=%2Fapp%2Fdiscover#/



- Create Index Pattern

Stack Management

Index patterns

Management

Ingest

Ingest Node Pipelines

Data

Index Management

Index Lifecycle Policies

Snapshot and Restore

Rollup Jobs

Transforms

Remote Clusters

Alerts and Insights

Rules and Connectors

Reporting

Machine Learning Jobs

Create index pattern

Name

logstash-*

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

Timestamp field

@timestamp

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

Show advanced settings

Close

Create index pattern

- Query and look for the token in message field

kubernetes.pod_name.keyword : "leaky-pod"

KQL

~ 15

+ Add filter

logstash-*

Search field names

Filter by type 0

TRANSPORT

UID

user.extra.authentication.kubernetes.io/pod-name

user.extra.authentication.kubernetes.io/pod-uid

user.groups

user.uid

user.username

13 hits

logtag	F
message	Fri Nov 4 08:13:09 UTC 2022 DEBUG sensitive credentials: ab5d7f
stream	stdout
tag	kubernetes.var.log.containers.leaky-pod_metrolio-qa_cauldron-7e1b68fae469
time	Nov 4, 2022 @ 08:13:09.144

Nov 4, 2022 @ 08:12:09.142

@timestamp: Nov 4, 2022 @ 08:12:09.142

docker.container_id: 7e1b68fae46955a622ac6825457c84a41ce2cd91f78793eb5a13444797d

printer:v1.0.0 kubernetes.container_image_id: localhost:5000/token-printer@sha256:b925a6baf9a7a1fb1e425ef93d629246ab10482

kubernetes.host: ip-10-102-11-167 kubernetes.master_url: https://11.96.0.1:443/api kubernetes.namespace_id: 9f17d50a-cc4

kubernetes.namespace_labels.kubernetes.io/metadata_name: metrolio-qa kubernetes.namespace_labels.name: metrolio-qa kuber

kubernetes.pod_id: 92173b89-f5a7-4d4d-a22b-662bfa83c65a kubernetes.pod_ip: 192.168.213.3 kubernetes.pod_name: leaky-pod

Question 4 of 5

From the audit event logs, which user.username keeps deleting the critical-system pod using kubectl?

untrained-developer

