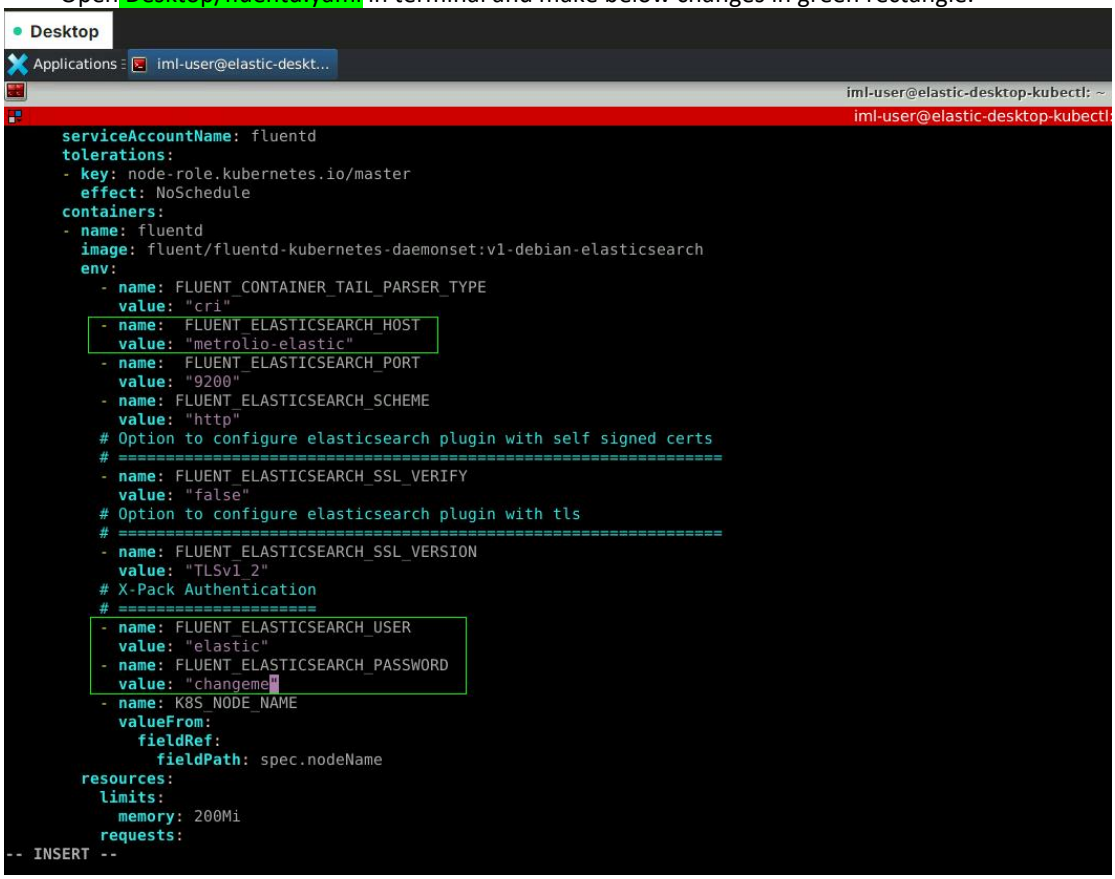
Question 1 of 5

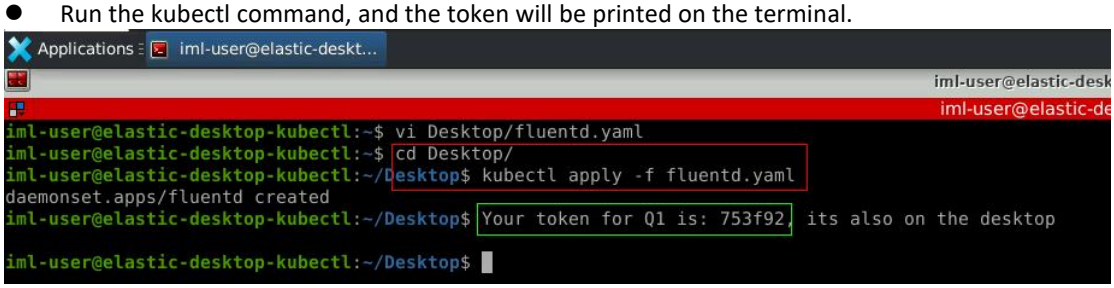
What is the token from deploying fluentd?

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.



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



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-kubectl:~$ 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-kubectl:~$
```

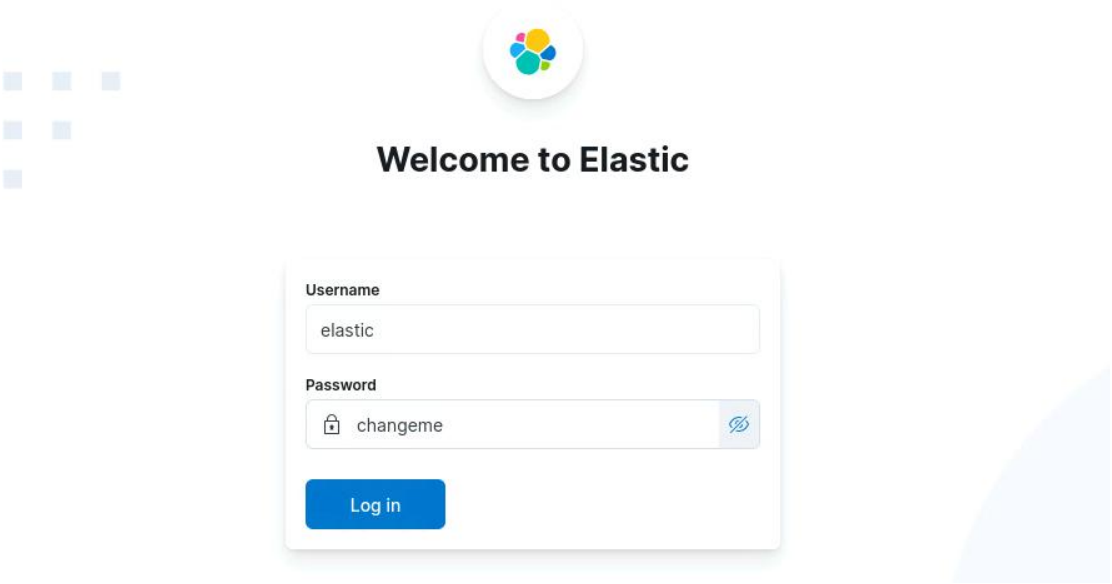
Question 3 of 5

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

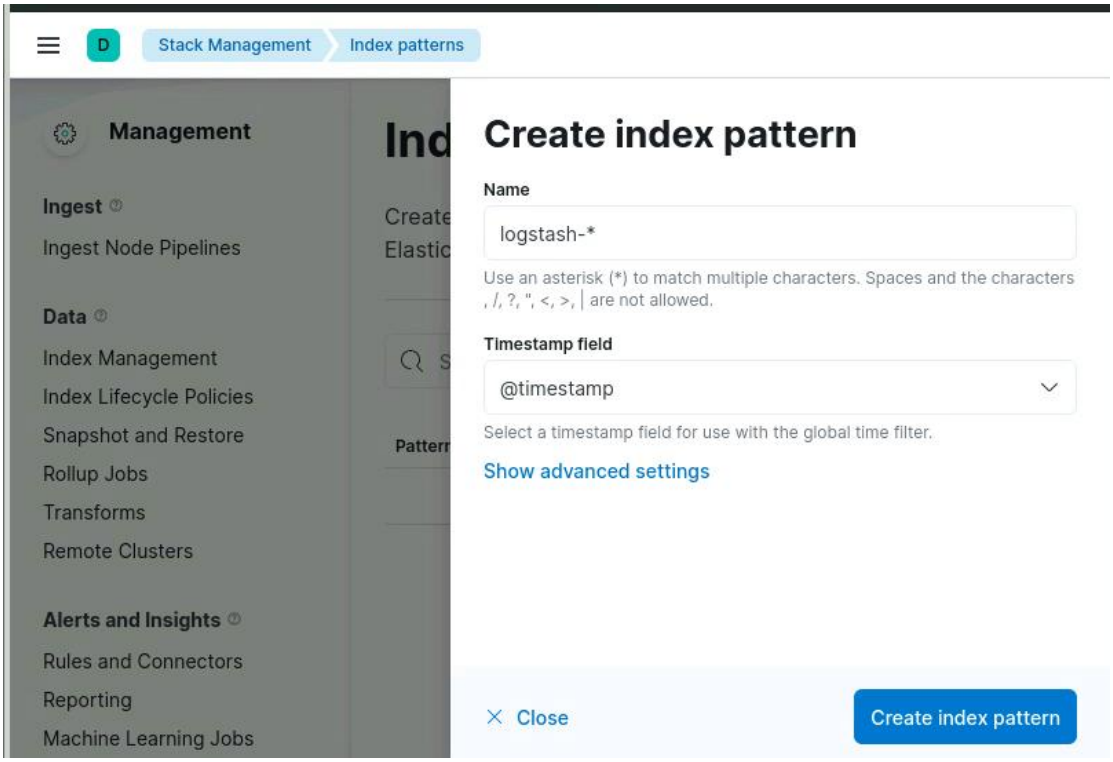
ab5d7f

Steps for question 3

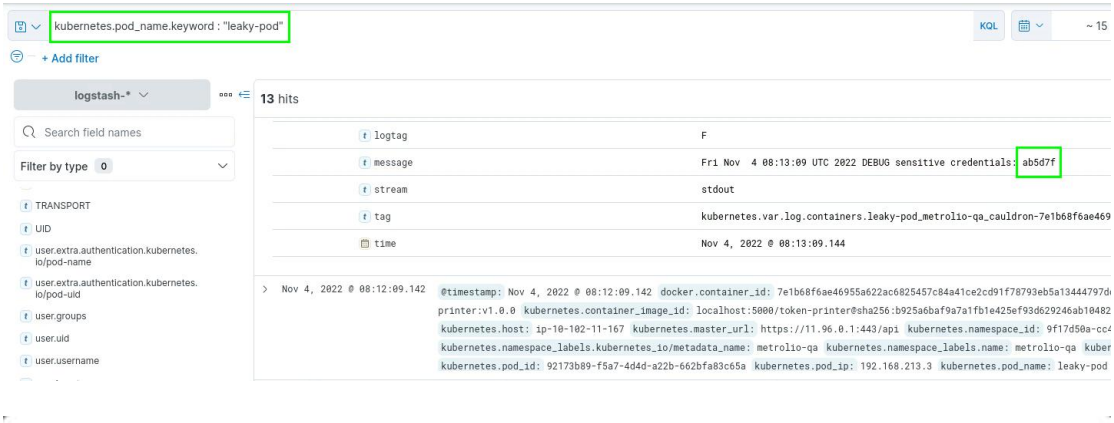
- Log in to Elasticsearch



- Create Index Pattern



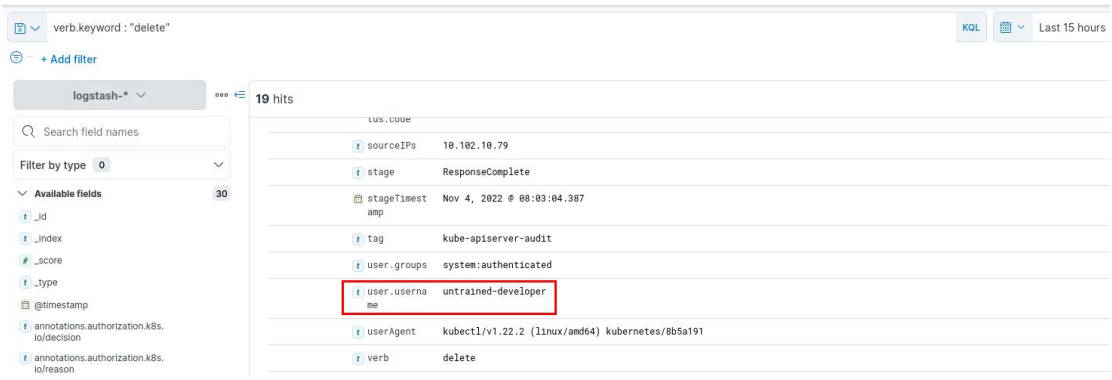
- Query and look for the token in message field



Question 4 of 5

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

untrained-developer



Question 5 of 5

What 'metrolio-' namespace has been deployed to the cluster and is not in the following list: ['metrolio-qa', 'metrolio-ops']?

metrolio-security