Question 1 of 6

Which non-default user has accessed the cluster?

support-eng

Question 2 of 6

For a pod called 'nginx' within the default namespace and core API group, what requestURI would indicate a 'kubectl exec' command to the pod?

/api/v1/namespaces/default/pods/nginx/exec

Question 3 of 6 The Pod Name may be differnent, get it from your kibnana search result

The user from the first question 'exec'd into a pod. What pod did they exec into?

wordpress-mysql-6c479567b-kmbpq

auditID: 60f91867-463e-4c56-8463-992139a32620 requestReceivedTimestamp: Mar 15, 2021 @ 14:33:19.289503000 objectRef.apiVersion: v1 objectRef.resource: pods
objectRef.subresource: exec objectRef.namespace: default objectRef.name: wordpress-mysql-6c479567b-kmbpq level: Metadata kind: Event verb: create userAgent: kubectl/v1.20.2
(linux/amd64) kubernetes/faecb19 requestURI: /api/v1/namespaces/default/pods/wordpress-mysql-6c479567b-kmbpq/exec?command=tar&command=cf&command=-
&command=5ecr3tDump.sql&container=mysql&stderr=true&stdout=true stageTimestamp: Mar 15, 2021 @ 14:33:19.289503000 sourceIPs: 172.31.16.176 apiVersion: audit.k8s.io/v1
@timestamp: Mar 15, 2021 @ 14:33:19.289503000 stage: RequestReceived user.groups: system:authenticated user.username: support-eng _id: fCHQNnqBOWRBEn_OZEC9 _type: _doc

Question 4 of 6

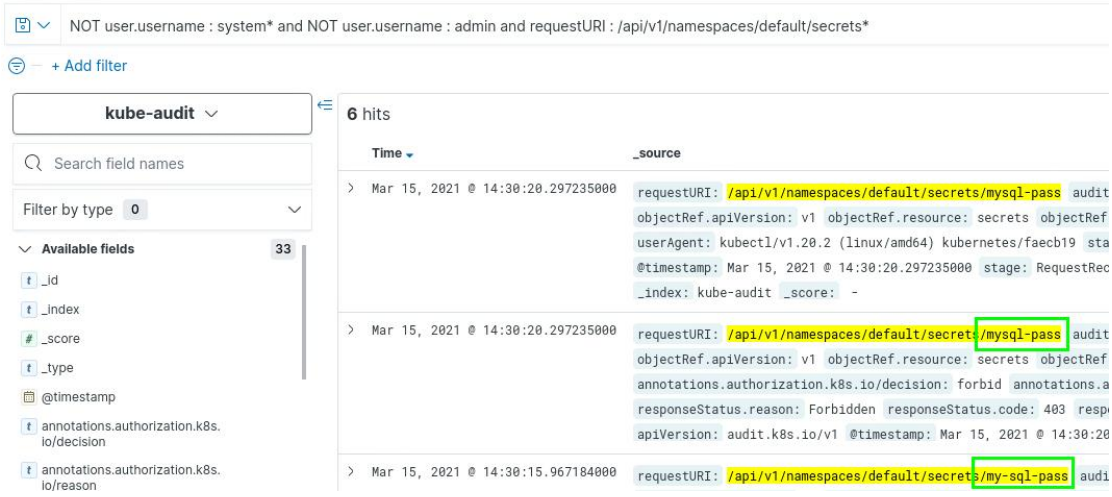
What 'kubectl get' query would result in a GET request to the following path? '/api/v1/namespaces/prod/secrets/creds'. Answer with the full command.

kubectl get secret creds -n prod

Question 5 of 6

The user attempted to read a specific secret in the default namespace. What is the name of this secret?

mysql-pass my-sql-pass also works



Question 6 of 6

What file was copied from the pod to a local machine?

5ecr3tDump.sql

auditID: 60f91867-463e-4c56-8463-992139a32620 requestReceivedTimestamp: Mar 15, 2021 @ 14:33:19.289503000 objectRef.apiVersion: v1 objectRef.resource: pods objectRef.subresource: exec objectRef.namespace: default objectRef.name: wordpress-mysql-6c479567b-kmbpq level: Metadata kind: Event verb: create userAgent: kubectl/v1.20.2 (linux/amd64) kubernetes/faecb19 requestURI: /api/v1/namespaces/default/pods/wordpress-mysql-6c479567b-kmbpq/exec?command=tar&command=cf&command=-&command=5ecr3tDump.sql&container=mysql&stderr=true&stdout=true stageTimestamp: Mar 15, 2021 @ 14:33:19.289503000 sourceIPs: 172.31.16.176 apiVersion: audit @timestamp: Mar 15, 2021 @ 14:33:19.289503000 stage: RequestReceived user.groups: system:authenticated user.username: support-eng _id: fCHQNngBOWRBEn_OZEC9