

Question 1 of 6

Which non-default user has accessed the cluster?

support-eng

NOT user.username : system* and NOT user.username : admin

Mar 15, 2021 @ 14:00:00.0 → Mar 15, 2021 @ 15:00:00.0

98 hits

Time	_source
Mar 15, 2021 @ 14:33:19.289503000	<pre>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: ku (linux/amd64) kubernetes/faeb19 requestURI: /api/v1/namespaces/default/pods/wordpress-mysql-6c479567b-kmbpq/exec?command=tar&command=cf&command= &command=Secr3tDump.sql&container=mysql&stderr=true&stdout=true stageTimestamp: Mar 15, 2021 @ 14:33:19.289503000 sourceIPs: 172.31.16.176 apiVersion: audit.k8s.1 @timestamp: Mar 15, 2021 @ 14:33:19.289503000 stage: RequestReceived user.groups: system:authenticated user.username: support-eng _id: fCHQNgBOWRBEEn_OZEC9 _type: _doc</pre>

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 different, 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/faeb19 requestURI: /api/v1/namespaces/default/pods/wordpress-mysql-6c479567b-kmbpq/exec?command=tar&command=cf&command=
&command=Secr3tDump.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: fCHQNgBOWRBEEn_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

NOT user.username : system* and NOT user.username : admin and requestURI : /api/v1/namespaces/default/secrets*

+ Add filter

kube-audit

Search field names

Filter by type 0

Available fields 33

- _id
- _index
- _score
- _type
- @timestamp
- annotations.authorization.k8s.io/decision
- annotations.authorization.k8s.io/reason

6 hits

Time	_source
> Mar 15, 2021 @ 14:30:20.297235000	requestURI: /api/v1/namespaces/default/secrets/mysql-pass audit objectRef.apiVersion: v1 objectRef.resource: secrets objectRef userAgent: kubectl/v1.20.2 (linux/amd64) kubernetes/faecb19 sta @timestamp: Mar 15, 2021 @ 14:30:20.297235000 stage: RequestRec _index: kube-audit _score: -
> Mar 15, 2021 @ 14:30:20.297235000	requestURI: /api/v1/namespaces/default/secrets/my-sql-pass audit objectRef.apiVersion: v1 objectRef.resource: secrets objectRef annotations.authorization.k8s.io/decision: forbid annotations.a responseStatus.reason: Forbidden responseStatus.code: 403 resp apiVersion: audit.k8s.io/v1 @timestamp: Mar 15, 2021 @ 14:30:20
> Mar 15, 2021 @ 14:30:15.967184000	requestURI: /api/v1/namespaces/default/secrets/my-sql-pass audi

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  
(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: fCHQNngBOWRBE_n_OZEC9
```