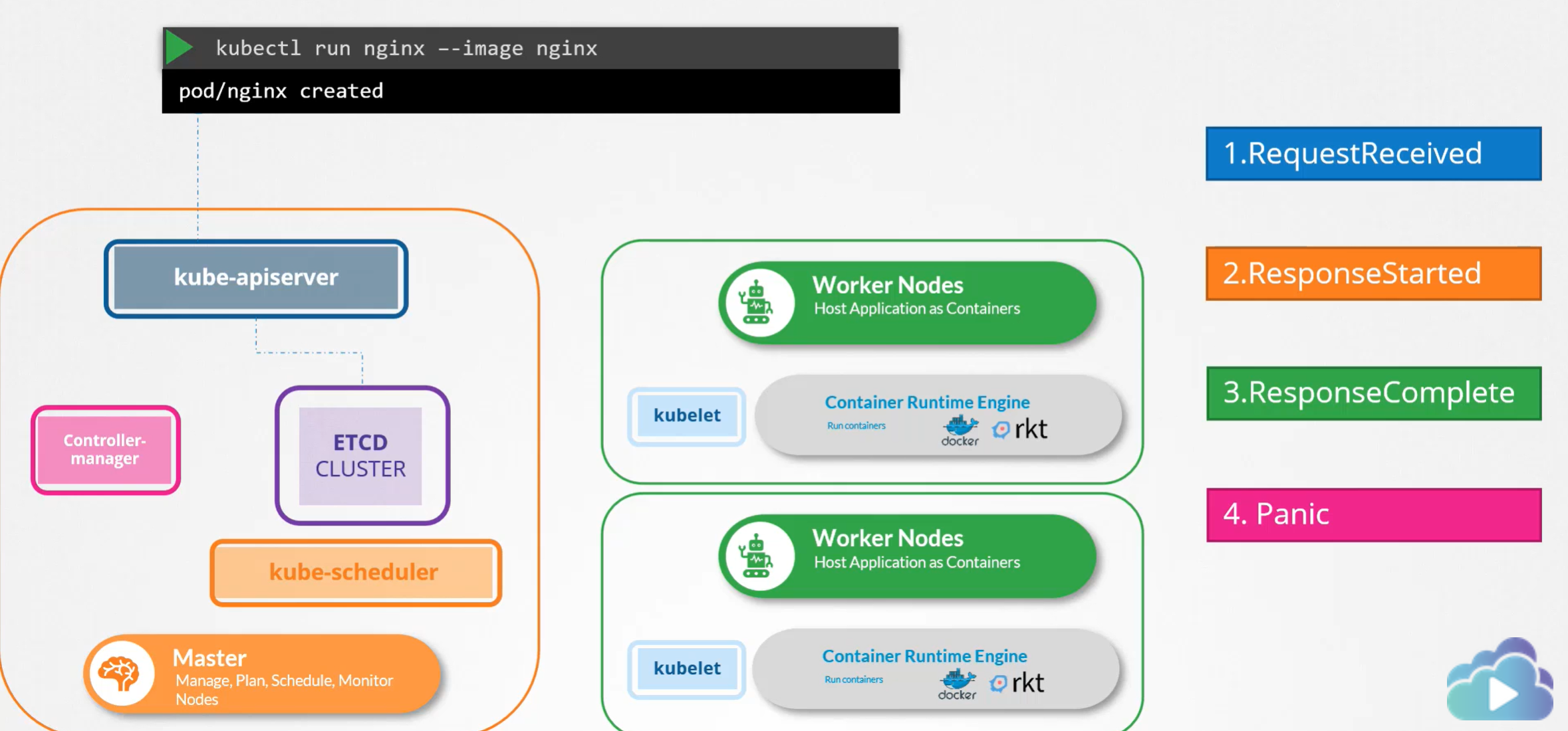
# K8S Audit log

1. Request go through kubernetes

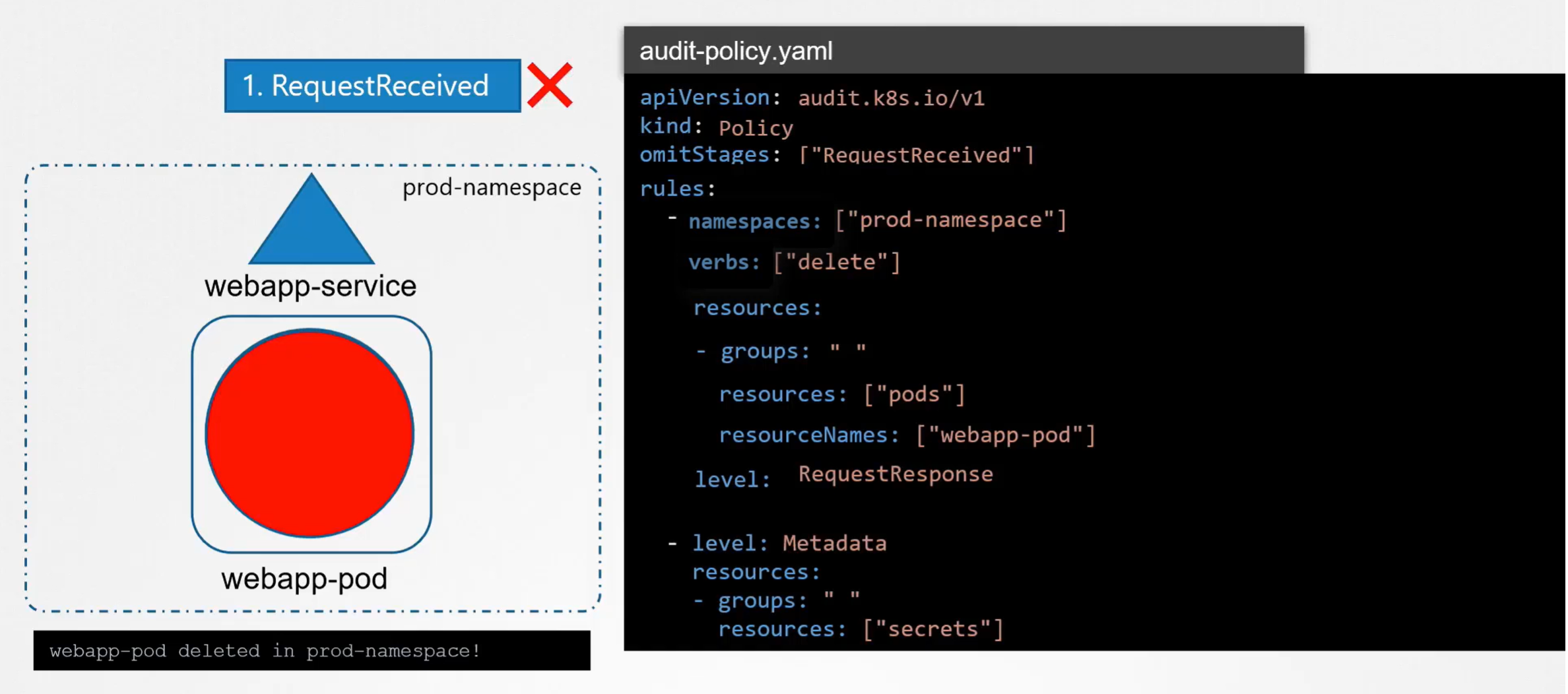
All requests made to the kubernetes cluster has to go through the kube-apiserver

* RequestReceived Stage: Events are generated irrespective of whether the request is valid or not
* ResponseStarted: After request is authenticated, validated, and authorized. This is applicable for requests that can take some time to complete. E.g. watch kubectl get xxxx to continuously observe the states of objects.
* ResponseComplete: Request has been completed and a response body is sent back.
* Panic: In case of an invalid request or an error.

These stage can all be recorded by api-server.



1. Audit Policy



\***omitStages**: stages event will not be recorded

\***namespace**(optional): It is all object cross all namespaces if not specified

\***verbs**(optional): operations, create, delete,update will be logged by default if not declare

\***level**:

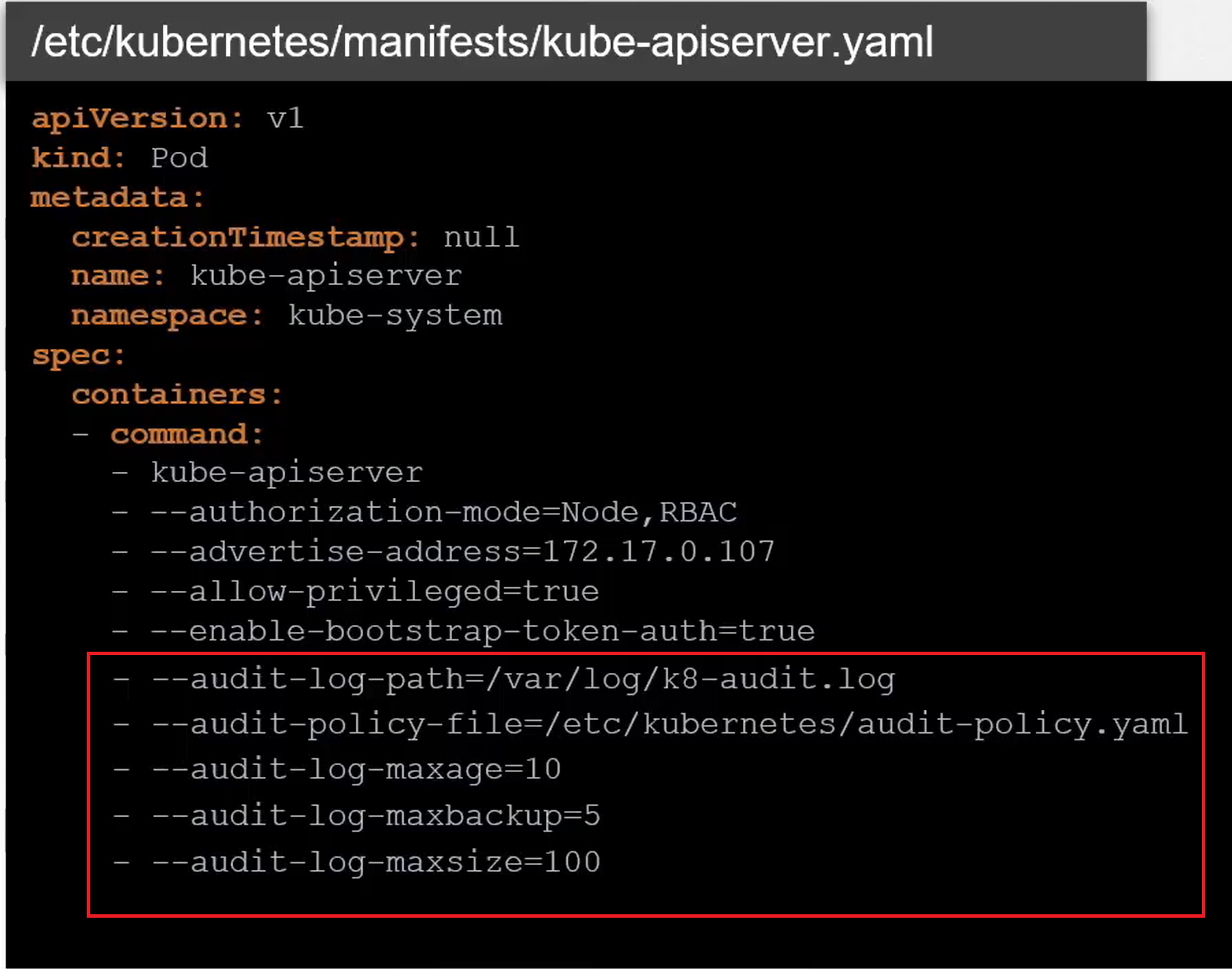
* None: Events will not be logged for this specific rule
* Metadata: timestamp, username, resources, verbs, will be logged
* Request: including metadata, more verbose
* RequestResponse: Request an Response body

1. Enable Auditing

\*audit-log-maxage: Maximum days to keep the audit records

\*audit-log-maxbackup: Preserving space, can set maximum number of these audit files

\*audit-log-maxsize:Maximum size in megabytes the audit file can grow to before being rotated



1. Audit log when delete pods

