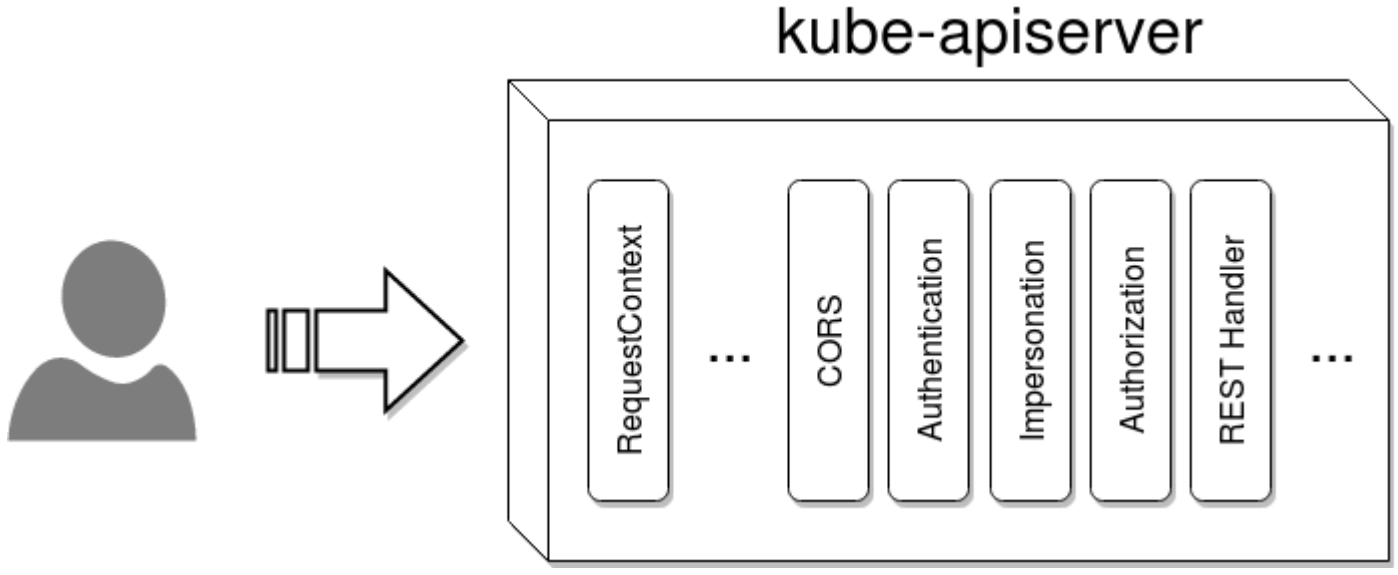
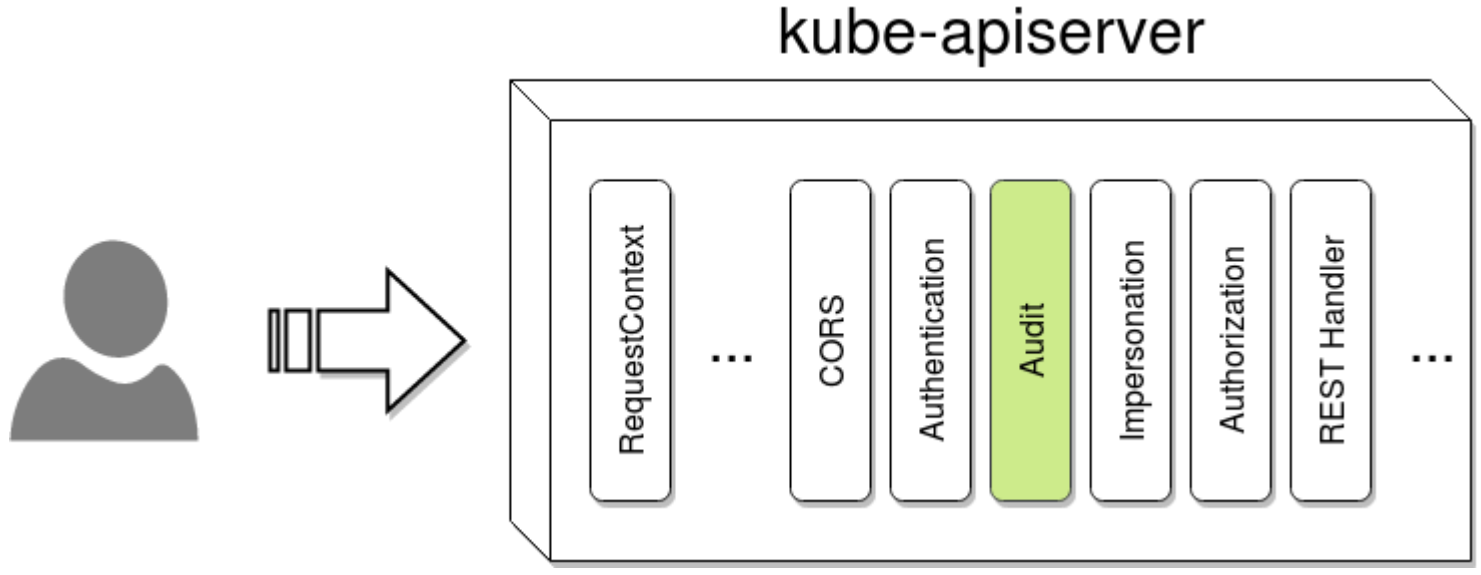
Audit in Kubernetes now, and the future

Maciej Szulik (@soltysh), Senior Software Engineer, Red Hat

Request flow



Request flow



Demo

```
kube-apiserver
...
    --audit-log-maxage
    --audit-log-maxbackup
    --audit-log-maxsize
    --audit-log-path
```

https://kubernetes.io/docs/admin/kube-apiserver/

Audit does not provide additional security to your system

Audit trails maintain a record of (...) activity (...).

(...) audit trails can assist in detecting security violations, performance problems, and flaws in applications.

http://csrc.nist.gov/publications/nistbul/itl97-03.txt

Cloud Auditing Data Federation

https://www.dmtf.org/standards/cadf

What happened?

When did it happen?

Who initiated it?

On what did it happen?

Where it was observed?

From where it was initiated?

To where was it going?

What happened?

```
method="GET"
```

When did it happen?

```
2016-09-07T13:03:57.400333046Z
```

Who initiated it?

```
user="admin"
groups="admins"
as="<self>"
asgroups="<lookup>"
```

On what did it happen?

```
namespace="default"
uri="/api/v1/namespaces/default/pods"
```

From where was it initiated?

```
ip="127.0.0.1"
```

Where it was observed?

To where was it going?

Pros

lightweight

simple format

Cons

HTTP-only

simple

noisy

log-file based

The Future

features/issues/22

community/pull/145

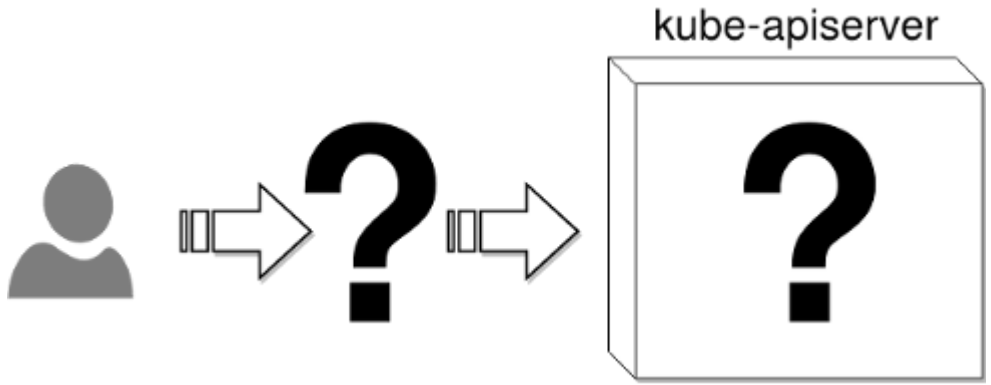
Architecture

In front of the apiserver

- keeps complexity out of the apiserver
- reuses existing solutions

Inside the apiserver

- deeper insight into the Kubernetes api
- knowledge of auth, authn, admission
- access to the storage level for differential output



Main concepts

Event

Holds all the data necessary for the output to produce a log entry.

Policy

Describe which layers of the apiserver will fill the Event object.

Rules

Describe filters which Events are interesting.

Output

Describe where the Event should be saved.

Maciej Szulik / @soltysh

Red Hat / OpenShift