

Observability 100: Using Elastic and OpenTelemetry to Observe Kubernetes

Using OpenTelemetry to Observe Kubernetes

We have our application stack running on Kubernetes. Now let's observe it using Elastic!

Install the OpenTelemetry Operator

With the advent of the OpenTelemetry Operator and related Helm chart, you can now easily deploy an entire observability signal collection package for Kubernetes, inclusive of: * application traces, metrics, and logs * infrastructure traces (nginx), metrics and logs * application and infrastructure metrics

1. button label="Elastic"
2. Click Add Data in bottom-left pane
3. Click Kubernetes
4. Click OpenTelemetry (Full Observability)
5. Click Copy to clipboard below Add the OpenTelemetry repository to Helm
6. button label="Terminal"
7. Paste and run helm chart command
8. button label="Elastic"
9. Click Copy to clipboard below Install the OpenTelemetry Operator
10. button label="Terminal"
11. Paste and run k8s commands to install OTel operator

Checking the Install

First, list out the available namespaces:

```
kubectl get namespaces
```

And get a list of pods running in the opentelemetry-operator-system namespace:

```
kubectl -n opentelemetry-operator-system get pods
```

And let's look at the logs from the daemonset collector to see if it is exporting to Elasticsearch without error:

```
kubectl -n opentelemetry-operator-system logs opentelemetry-kube-stack-gateway-collector-<xxxxxxxxx-xxxxx>
```

Checking Observability

Let's confirm what signals are coming into Elastic.

First, let's check for logs. Navigate to the button label="Elastic" tab and click on Observability > Discover.

Next, let's check for infrastructure metrics. Navigate to the button label="Elastic" tab and click on Infrastructure > Hosts.

Finally, let's check for application traces. Navigate to the button label="Elastic" tab and click on Applications > Service Inventory. Note that there is not yet any APM data flowing in. Let's figure out what's up.

Debugging APM

Let's describe one of our application pods... Specifically, the monkey pod:

```
kubectl -n trading describe pod monkey
```

Look at the environment variables section; note that there are not yet any OTel environment variables loaded into the pod.

It turns out that after you apply the OTel Operator to your Kubernetes cluster, you need to restart all of your application services:

```
kubectl -n trading rollout restart deployment
```

Now let's wait for our monkey pod to restart:

```
kubectl -n trading get pods
```

And once it has restarted, let's describe it again:

```
kubectl -n trading describe pod monkey
```

And now we can see OTel ENV vars being injected into the monkey pod. Let's check if we have APM data flowing in. Navigate to the button label="Elastic" tab and click on Applications > Service Inventory. Ok cool, this is starting to look good. Click on the trader app and look at the POST /trade/request transaction. Scroll down to the bottom (trace samples) and look at the waterfall graph. Notice the broken trace. It looks like perhaps one of our applications is not being instrumented. Click on the POST span and look at attributes.service.target.name. Note that this POST is intended to target the router service, yet we don't see the router service in our Service Map.

Let's look at our router pod and see if we can figure out what's up.

```
kubectl -n trading describe pod router
```

Huh. no OTel ENVs, even though the pod was restarted. Let's have a look at that deployment yaml. Click on the button label="Code" button and examine the deployment yaml. Look at the deployment yaml for the trader service and compare it to the router service. Notice anything missing?

In order for the Operator to attach the correct APM agent, you need to apply an appropriate annotation to each pod. Note that the router pod is missing an annotation. Let's add it. In the Code editor, modify the router yaml to add the following annotation:

```
spec:
  template:
    metadata:
      annotations:
        instrumentation.opentelemetry.io/inject-nodejs: "opentelemetry-operator-system/elastic-instrumentation"
    ...
```

And then reapply the yaml:

```
kubectl apply -f k8s
```

Note that router was reconfigured:

```
deployment.apps/router configured
```

Wait for the router pod to restart:

```
kubectl -n trading get pods
```

And once it has restarted, let's describe it again:

```
kubectl -n trading describe pod router
```

And now it looks like our OTel ENVs are getting injected as expected. Let's check Elasticsearch. Navigate to the button label="Elastic" tab and click on Applications > Service Inventory. Note that we can now see a full distributed trace, as expected!
