NETWAYS WEB SERVICES

Observing Cluster-Traffic - Cilium

Erstellt von: Justin Lamp

Erstellt am: 16 October 2023 16:07:39

Version: 1

Inhaltsverzeichnis

Observing Cluster-Traffic - Cilium

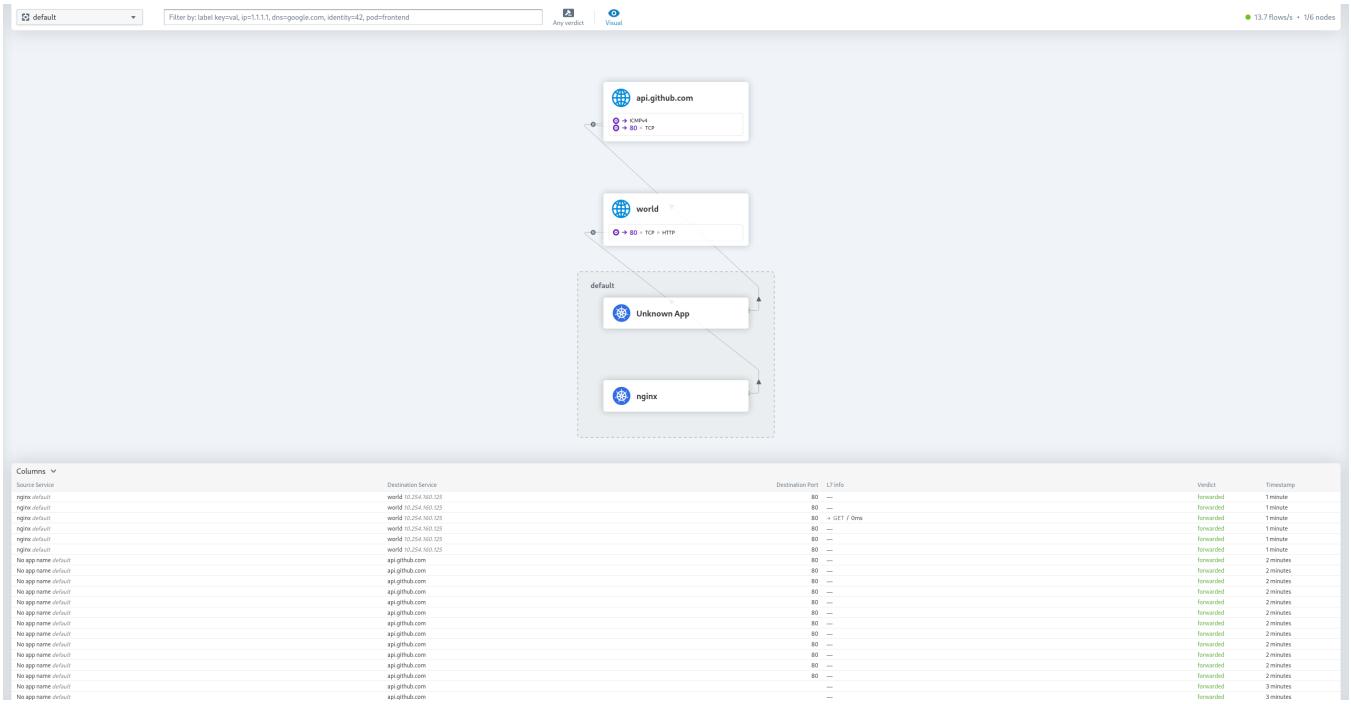
Cilium has an extension called Hubble. Similar to the well known telescope it specializes in observability. With it's hubble-ui component you are able to graphically visualize all traffic flowing in your cluster. But you are not constrained to the web-ui and can also use the hubble cli, which is even more powerful and can help you debug issues faster.

Webui

To gain access to the webui, you'll need to port-forward traffic to the web-ui service into the cluster. It works as follows:

```
$ kubectl get svc -n kube-system hubble-ui
$ kubectl port-forward -n kube-system svc/hubble-ui 8080:80
```

After initiation the port-foward, the hubble ui will be accessable locally on port `8080`: http://127.0.0.1:8080.



On the top left, you'll see a drop-down list with all the namespace that are defined. Choosing one, will initiate a session and observe all the traffic flowing in that namespace. To drill down on a specific pod, you can either click on a pod that already popped up or set a filter in the top bar manually.

CLI

To gain access to the hubble cli, you'll either need to install the hubble locally or execute everything in the cilium container.

Installation

```
HUBBLE_VERSION=$(curl -s https://raw.githubusercontent.com/cilium/hubble/master/stable.txt)
HUBBLE_ARCH=amd64
if [ "$(uname -m)" = "aarch64" ]; then HUBBLE_ARCH=arm64; fi
curl -L --fail --remote-name-all https://github.com/cilium/hubble/releases/download/$HUBBLE_VERSION/hubble-linux-${HUBBLE_ARCH}.tar.gz{,.sha256sum}
```

```
sha256sum --check hubble-linux-${HUBBLE_ARCH}.tar.gz.sha256sum
sudo tar xzvfC hubble-linux-${HUBBLE_ARCH}.tar.gz /usr/local/bin
rm hubble-linux-${HUBBLE_ARCH}.tar.gz{,.sha256sum}
```

For hubble to work locally it needs access to the API as well.

```
$ kubectl port-forward -n kube-system svc/hubble-relay 4245:80 &
Forwarding from 0.0.0.0:4245 -> 4245
Forwarding from [::]:4245 -> 4245
```

Remote exec

```
$ alias hubble='kubectl exec -in kube-system ds/cilium -c cilium-agent -- hubble'
$ hubble status
Healthcheck (via unix:///var/run/cilium/hubble.sock): Ok
Current/Max Flows: 4,095/4,095 (100.00%)
Flows/s: 4.07
```

Observing

To observe any traffic (much like tcpdump) you can just run observe in --follow mode. It will show any traffic that runs through your cluster.

```
$ hubble observe --follow
Sep  4 07:28:18.255: 10.100.2.60:48428 (host) -> 10.100.2.77:4240 (health) to-endpoint FORWARDED (TCP Flags: ACK, PSH)
Sep  4 07:28:18.256: 10.100.2.60:48428 (host) <- 10.100.2.77:4240 (health) to-stack FORWARDED (TCP Flags: ACK, PSH)
Sep  4 07:28:23.290: 10.100.5.13:55176 (remote-node) <- 10.100.2.77:4240 (health) to-overlay FORWARDED (TCP Flags: ACK)
Sep  4 07:28:23.292: 10.100.5.13:55176 (remote-node) -> 10.100.2.77:4240 (health) to-endpoint FORWARDED (TCP Flags: ACK)
Sep  4 07:28:23.613: 10.100.2.60:37112 (host) -> kube-system/coredns-69bc699795-trnxn:8181 (ID:17050) to-endpoint FORWARDED (TCP Flags: SYN)
Sep  4 07:28:23.613: 10.100.2.60:37112 (host) <- kube-system/coredns-69bc699795-trnxn:8181 (ID:17050) to-stack FORWARDED (TCP Flags: SYN, ACK)
Sep  4 07:28:23.613: 10.100.2.60:37112 (host) -> kube-system/coredns-69bc699795-trnxn:8181 (ID:17050) to-endpoint FORWARDED (TCP Flags: ACK)
Sep  4 07:28:23.613: 10.100.2.60:34644 (host) -> kube-system/coredns-69bc699795-trnxn:8080 (ID:17050) to-endpoint FORWARDED (TCP Flags: SYN)
```

Hubble can also filter based on many different identies, like pod labels, namespaces and dns lookups.

```
$ hubble observe --follow \
  --pod default/nginx-5f8f49fff4-m8m9h \
  --not --label k8s-app=kube-dns
Sep  4 08:23:29.510: default/nginx-5f8f49fff4-m8m9h:53700 (ID:37906) -> 142.250.184.238:80 (world) to-stack FORWARDED (TCP Flags: SYN)
Sep  4 08:23:29.519: default/nginx-5f8f49fff4-m8m9h:53700 (ID:37906) -> 142.250.184.238:80 (world) to-stack FORWARDED (TCP Flags: ACK)
Sep  4 08:23:29.519: default/nginx-5f8f49fff4-m8m9h:53700 (ID:37906) -> 142.250.184.238:80 (world) to-stack FORWARDED (TCP Flags: ACK, PSH)
Sep  4 08:23:29.542: default/nginx-5f8f49fff4-m8m9h:53700 (ID:37906) -> 142.250.184.238:80 (world) to-stack
```

```
FORWARDED (TCP Flags: ACK, FIN)
Sep  4 08:23:29.548: default/nginx-5f8f49fff4-m8m9h:53700 (ID:37906) -> 142.250.184.238:80 (world) to-stack
FORWARDED (TCP Flags: ACK)
```

That for example will monitor all traffic of the nginx pod found in the `default` namespace except DNS lookups.

Another common use case would be to filter based on destination port. This can be done with the `--to-port` Flag. If you need more info, the output can be formatted as json:

```
$ hubble observe --follow --pod nginx-5f8f49fff4-m8m9h --to-port 80 -o json | jq
{
 "flow": {
  "time": "2023-09-04T08:25:35.610232081Z",
  "uuid": "c488a8f9-1301-4490-84f1-7ed96afd36f3",
  "verdict": "FORWARDED",
  "ethernet": {
   "source": "d6:5b:64:ee:1c:86",
   "destination": "e2:1e:63:4a:0b:cf"
  },
  "IP": {
   "source": "10.100.3.241",
   "destination": "142.250.184.238",
   "ipVersion": "IPv4"
  },
  "l4": {
   "TCP": {
    "source_port": 33610,
    "destination_port": 80,
    "flags": {
     "SYN": true
    }
   }
  },
  "source": {
   "ID": 740,
   "identity": 37906,
   "namespace": "default",
   "labels": [
    "k8s:app=nginx",
    "k8s:io.cilium.k8s.namespace.labels.kubernetes.io/metadata.name=default",
    "k8s:io.cilium.k8s.policy.cluster=default",
    "k8s:io.cilium.k8s.policy.serviceaccount=default",
    "k8s:io.kubernetes.pod.namespace=default"
   ],
   "pod_name": "nginx-5f8f49fff4-m8m9h",
   "workloads": [
    {
     "name": "nginx",
     "kind": "Deployment"
    }
   ]
  },
  "destination": {
   "identity": 2,
   "labels": [
    "reserved:world"
```

```
      ]
    },
    "Type": "L3_L4",
    "node_name": "cl-cilium-15-jibbo4pnpgn7-node-1",
    "event_type": {
      "type": 4,
      "sub_type": 3
    },
    "traffic_direction": "EGRESS",
    "trace_observation_point": "TO_STACK",
    "is_reply": false,
    "Summary": "TCP Flags: SYN"
  },
  "node_name": "cl-cilium-15-jibbo4pnpgn7-node-1",
  "time": "2023-09-04T08:25:35.610232081Z"
}
```