Network Isolation for 1500 Microservices

Jack Kleeman

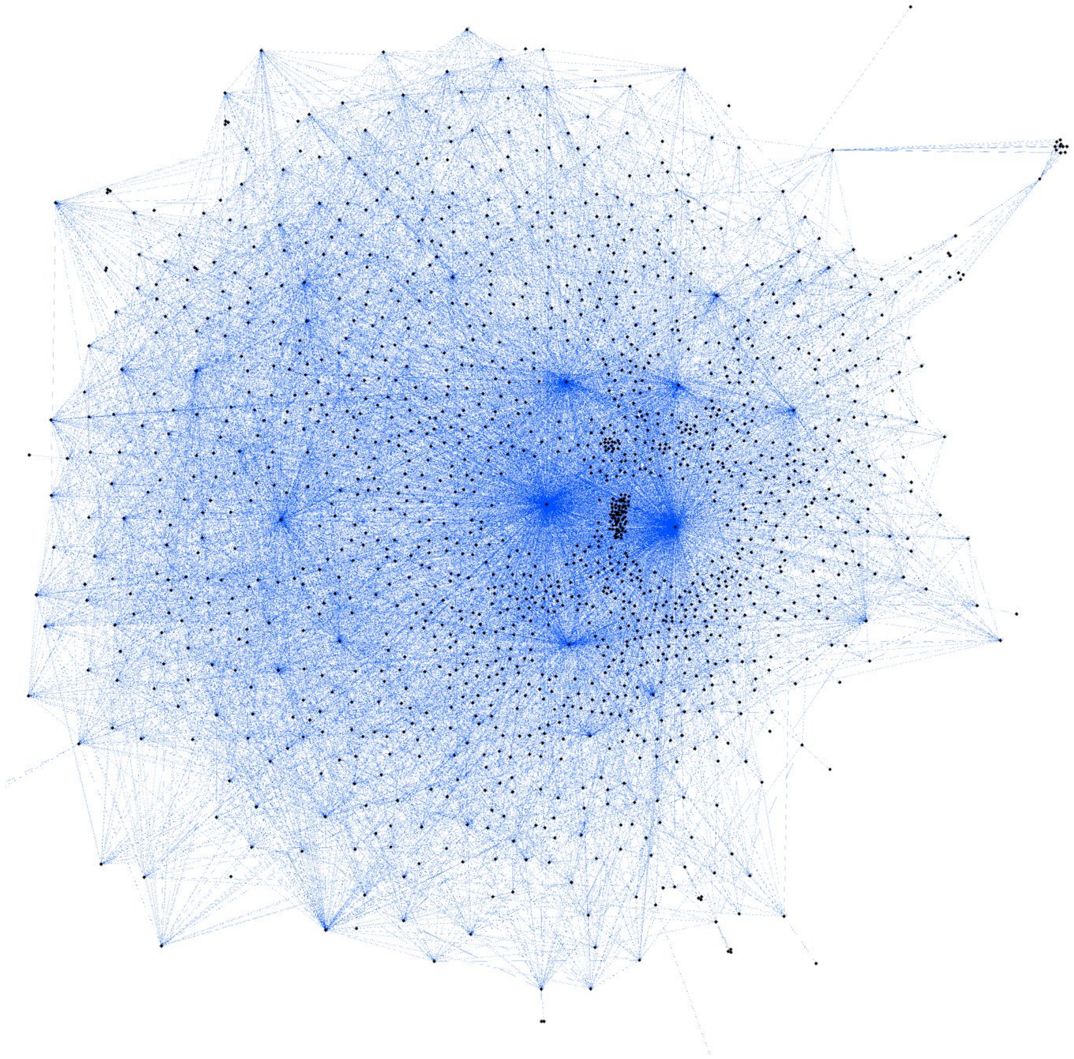
KubeCon | CloudNativeCon

Europe 2020

Virtual

```
$ k get ns default
NAME       STATUS   AGE
default    Active   3y249d


$ ls */main.go | wc -l
    1576
```



🤯

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: s-foo
spec:
  podSelector:
    matchLabels:
      routing-name: bank.com/service.foo
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            name: main
```

🤷‍♀️

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: s-ledger
spec:
  ingress:
  - from:
    - podSelector:
        matchExpressions:
        - key: bank.com/routing-name
          operator: In
          values:
          - service.a-client
          - service.client2
          - ...
```

🤔

```
$ rpcmap -generate ./service.client
Adding service.client/manifests/egress/service.ledger.rule
Adding service.client/manifests/egress/service.platform.config.rule

$ cat CODEOWNERS
…
*/manifests/egress/service.ledger.rule @bank/finance

$ k get pods -l bank.com/egress-s-ledger=true
NAME
s-client-558f9c649c-6h6qc
...
```

⭐

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: s-ledger
spec:
  podSelector:
    matchLabels:
      bank.com/network-policy: “true”
      bank.com/routing-name: service.ledger
  ingress:
  - from:
    - podSelector:
        matchLabels:
          bank.com/egress-s-ledger: “true”
```

Rolling out safely

```
apiVersion: projectcalico.org/v3
kind: NetworkPolicy
metadata:
  name: dry-run
spec:
  ingress:
  - action: Log
  - action: Allow
  order: 9001
  selector: bank.com/network-policy == 'true'
```

github.com/box/kube-iptables-tailer

```
Chain cali-tw-cali686c8ad42d5
pkts   target
49M    ACCEPT                          ctstate RELATED,ESTABLISHED
10243  MARK                            /* Start of policies */
10243  cali-pi-_aDS-SJx4CthxMnwe1uW
32     RETURN                          /* Return if policy accepted */
10211  cali-pi-_NaD31q6knMNjHx7iKSV
10211  RETURN                          /* Return if policy accepted */
0      cali-pi-_OGJkn7StS9uXFPWiw8v
0      RETURN                          /* Return if policy accepted */
0      DROP                            /* Drop if no policies passed packet
*/
```

http://tiny.cc/calico-accountant

```
$ find . -name "*.rule" | wc -l
  13376

$ find */main.go | wc -l
   1576

$ echo '13376/1576' | bc -l
8.487
```

🔒

🌍

```
$ k get ExternalService github-api
NAME         AGE   DNS NAME         HIJACK DNS
github-api   43d   api.github.com   true

$ ls service.github/manifests/egress/external
api.github.com:443.rule
```

http://tiny.cc/egress-operator

```
$ k get VirtualService s-istio-test
NAME           HOSTS                  AGE
s-istio-test   [service.istio-test]   22d
```

NEW

Blog of the talk

tiny.cc/network-isolation

My twitter

twitter.com/jackkleeman

Email me

kubecon@kleeman.dev

KubeCon | CloudNativeCon

Europe 2020

Virtual

KEEP CLOUD NATIVE CONNECTED