

## 56Kubernetes 系列（五十三）Kubernetes 流量查看器：Kubeshark

### Kubernetes 系列（五十三）Kubernetes 流量查看器：Kubeshark

Kubeshark 是一个类似 TCPDump 的工具，可以监听 Kubernetes 中流量信息并提供界面展示。

#### 安装

Kubeshark 基于 GO 语言开发，大家在各自的系统上下载二进制程序，配置到环境变量中，即可在命令行中启动。参考：  
<https://github.com/kubeshark/kubeshark/releases/tag/37.0>


#### 运行

下面以 windows 为例运行：

```
PS C:\Users\yueyong> kubeshark tap -n ops-common
Kubeshark will store up to 200MB of traffic, old traffic will be cleared once the limit is reached.
Tapping pods in namespaces "ops-common"
+xxxx-server-c78cf95fc-bmj2h
+xxxx-server-c78cf95fc-tmz8t
+xxxx-client-778fddbcc5-2wdzx
+xxxx-common-6b9966c8cc-5pdvh
.....
Waiting for Kubeshark Agent to start...
Kubeshark is available at http://localhost:8899
```

- 上面命令默认使用用户目录kube 文件夹下的 config 文件来连接 k8s（你可以通过 --help 查看具体的参数进行调整）。
- tap 就是进行监控的命令，它会在 k8s 中创建一个名为 **kubeshark** 的命名空间，然后自动创建一个 api web 服务以及用于监控的 daemonset 应用，类似下图：

Pods(kubeshark) [4]													
NAME↑	PF	READY	RESTARTS	STATUS	CPU	MEM	%CPU/R	%CPU/L	%MEM/R	%MEM/L	IP	NODE	AGE
kubeshark-api-server	●	2/2	0	Running	0	0	0	0	0	0	0 192.168.192.141	k8s-prod-xxl-0	28m
kubeshark-tapper-daemon-set-4165s	●	1/1	2	Running	0	0	0	0	0	0	0 172.28.1.115	k8s-prod-xxl-0	27m
kubeshark-tapper-daemon-set-twls2	●	1/1	2	Running	86	59	172	11	118	5	5 172.28.1.116	master	27m
kubeshark-tapper-daemon-set-vm8g7	●	1/1	1	Running	0	0	0	0	0	0	0 172.28.1.116	k8s-prod-xxl-0	27m

云原生拓展

云原生拓展

- -n 用于指定采集的目标命名空间，可以指定全部，具体参数 --help 查看
- 最终完成运行，它自动转发web 页面到本地端口，打开监控页面，如下：



streaming paused

Service Catalog

Service Map

Traffic Stats

src.ip == "192.168.186.185"

Apply



HTTP	200	POST	/metrics/job/spr	192.168.186.185:47564	10.102.29.2009091
HTTP	200	POST	/metrics/job/s	192.168.186.185:47566	192.168.219.2269091
HTTP	200	POST	/metrics/job/spr	192.168.186.185:47566	10.102.29.2009091
HTTP	200	POST	/metrics/job/spr	192.168.186.185:47568	10.102.29.2009091
HTTP	200	POST	/metrics/job/s	192.168.186.185:47568	192.168.219.2269091
HTTP	200	POST	/metrics/job/s	192.168.186.185:47570	192.168.219.2269091
HTTP	200	POST	/metrics/job/spr	192.168.186.185:47570	10.102.29.2009091

Displaying 154 results out of 2684 total  
First traffic entry time 12/14/2022, 9:01:21.355 AM

## Redis Serialization Protocol

3KB 29 B 0ms

HMSET auth:client:auth:sessions:1 ops-common 192.168.186.185:53316 192.168.56.2436379

REQUEST | RESPONSE

## Details

Command HMSET

Key auth:client:auth:sessions:11cfeb9-e411-4dfe-9ed1-1c3be48842b9

Keyword

Type Array

## Value

☒ Line numbers

```
1 [lastAccessedTime, @sr @java.lang.Long; @value @java.lang.Number;  
2 loadFactorI thresholdxp7@ w@ @ @t ,fPq54KeQM1Wiq175kmo4QQZulqHptvqbUuk  
3 L @additionalParameters @java.util.Map;L
```

云原生拓展

## Service Catalog

auth:commo...

Search...

auth:server



http://auth:common.ops-common (1.0)

Download OpenAPI specification: Download

Kubeshark observed 1083 entries (0 failed), at 5.789 hits/s, average response time is 0.002 seconds

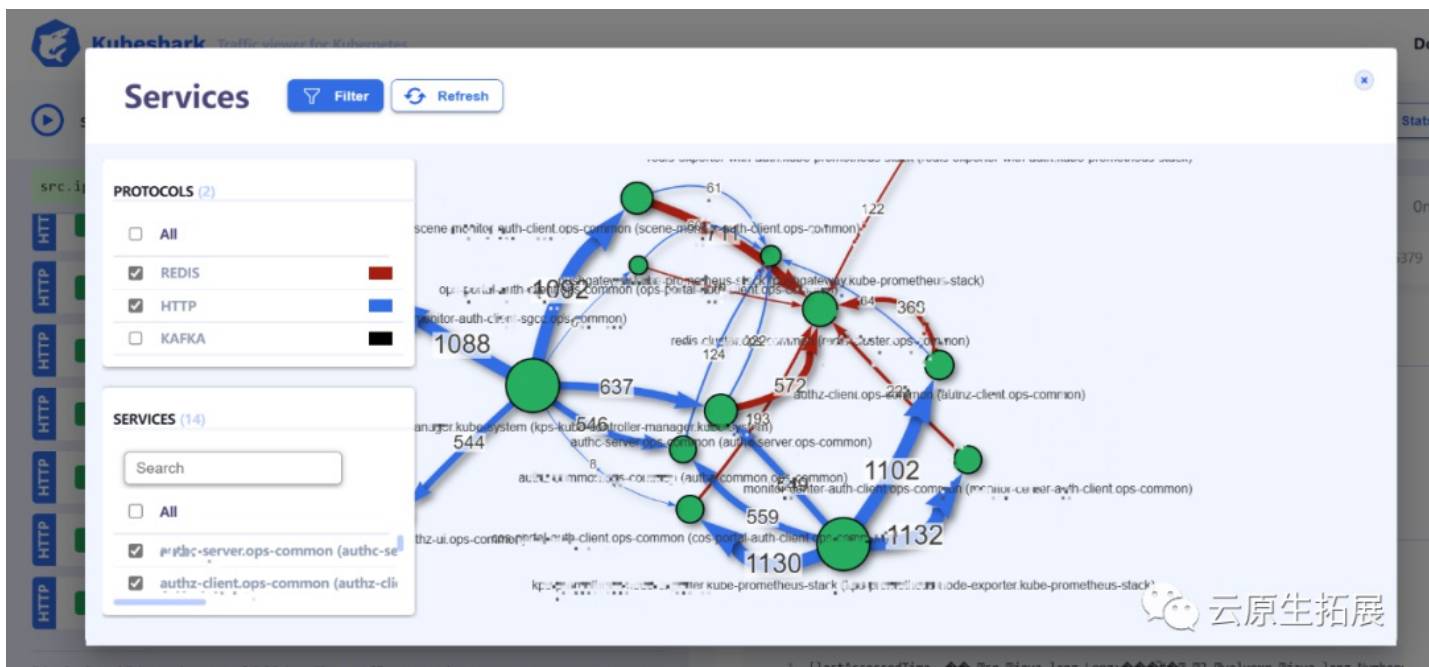
authorize-server

/authorize-server/actuator/health/liveness

GET

/authorize-server/actuator/he...

云原生拓展



终端运行 Ctrl + C 即可退出采集，同时自动删除 k8s 中创建的命名空间以及采集程序。

更多扩展功能，可以自己尝试。

欢迎关注我的公众号“云原生拓展”，原创技术文章第一时间推送。