Introducing Istio Service Mesh for Microservices

5,6,7 장

윤평호 2019-04-16

목차

Chaos Testing

카오스 엔지니어링

1. (실 서비스에) 장애를 주입하여
2. (출시 전) 테스트에서 드러나지 않는 아키텍처상의 문제를 직접 드러내는

> 프로덕션 서비스의 각종 장애 조건을 견딜 수 있는 시스템 신뢰성을 확보하기 위해 분산 시스템을 실험하고 배우는 분야

- https://www.slideshare.net/Channy/chaos-engineering-in-action-for-kubernates
- https://www.slideshare.net/AmazonWebServices/chaos-engineering-and-scalability-at-audiblecom-arc308-aws-reinvent-2018
- https://www.slideshare.net/AmazonWebServices/globalizing-player-accounts-at-riot-games-while-maintaining-availability-arc314-aws-reinvent-2018

장애 주입(Failure Injection)

작게 시작해서 점진적으로 신뢰성 구축

- 애플리케이션 부하 테스트
- 호스트 서버 이슈
- 데이터베이스 문제
- 자원 부족(CPU, memory, disk, …)
- 네트워크 부족(종속성, 지연, …)
- 서비스 부족

Q. Istio 에서 할 수 있는 것은?

- HTTP(S) 관련 장애 주입

HTTP error 장애 주입

istiofiles/virtual-service-recommendation-503.yml *

```
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: recommendation
spec:
  hosts:
  - recommendation
  http:
  - fault:
      abort:
        httpStatus: 503
        percent: 50
    route:
    - destination:
        host: recommendation
        subset: app-recommendation
```

참고: * 책과 다릅니다. RouteRule --> VirtualService(v0.7)

HTTP status code, fault.abort

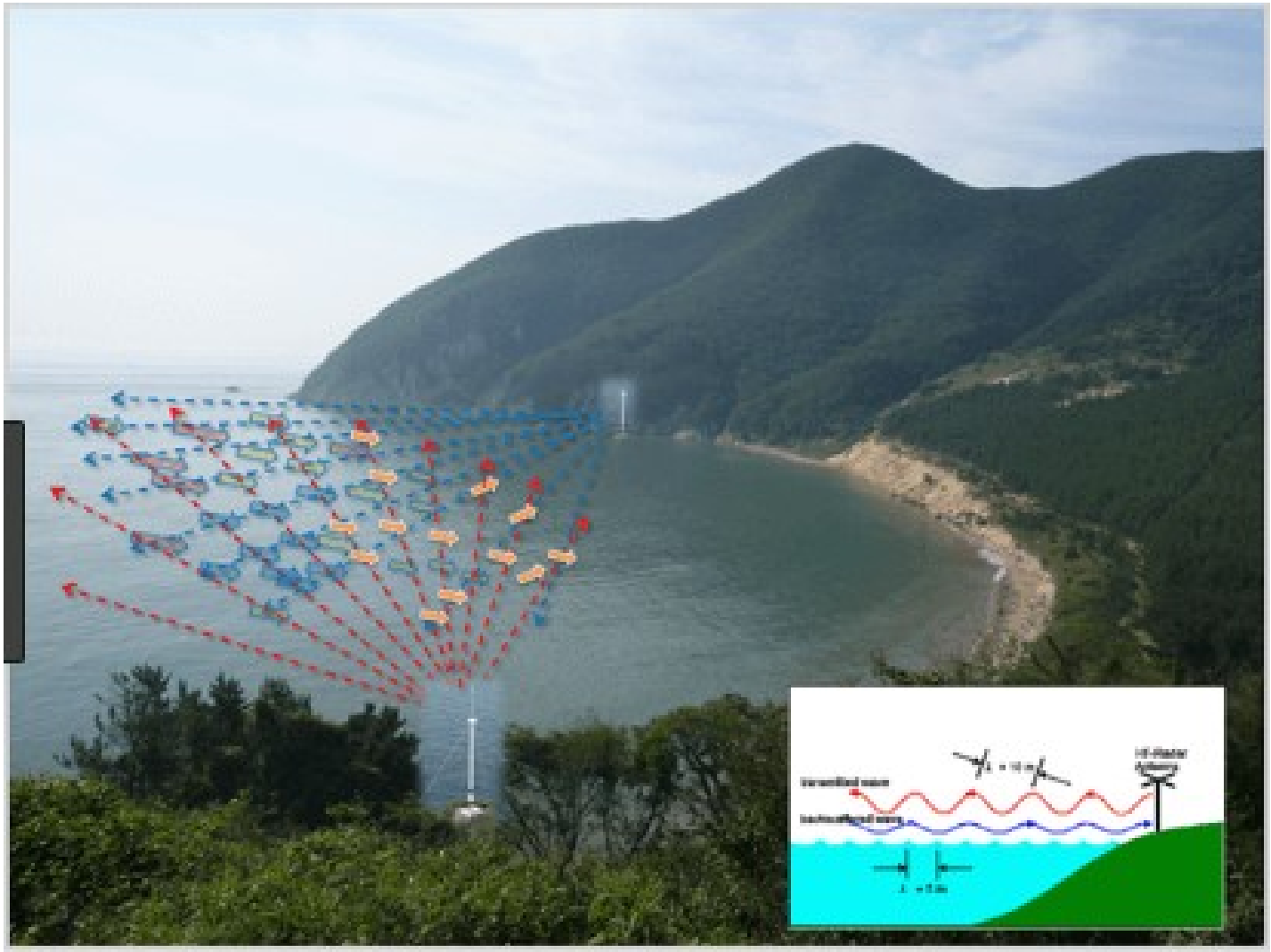
HTTP delay 장애 주입

istiofiles/virtual-service-recommendation-delay.yml

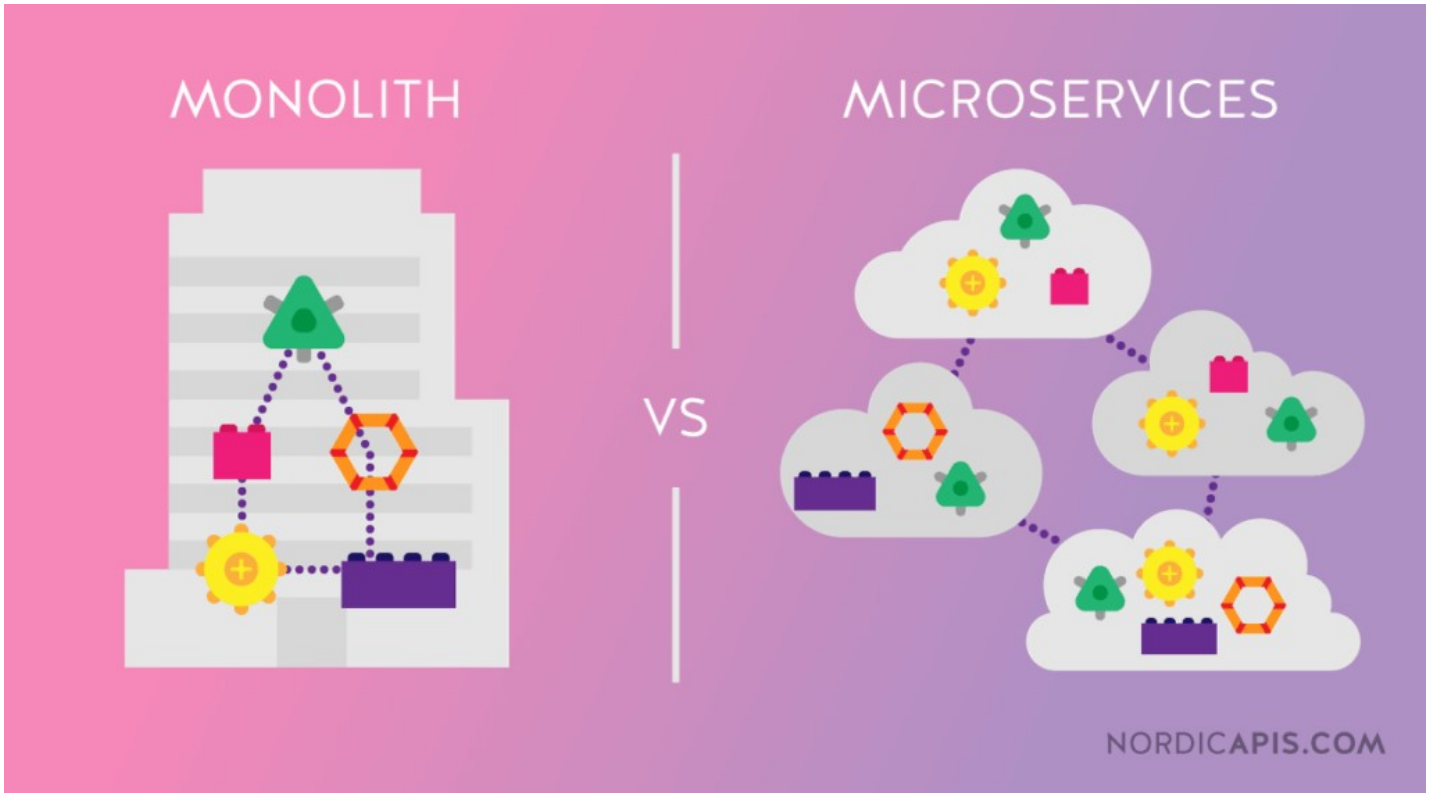
```yaml
apiVersion: networking.istio.io/v1alpha3
kind: VirtualService
metadata:
  name: recommendation
spec:
  hosts:
  - recommendation
  http:
  - fault:
      delay:
        fixedDelay: 7.000s
        percent: 50
    route:
    - destination:
        host: recommendation
        subset: app-recommendation
```

참고: fault.delay

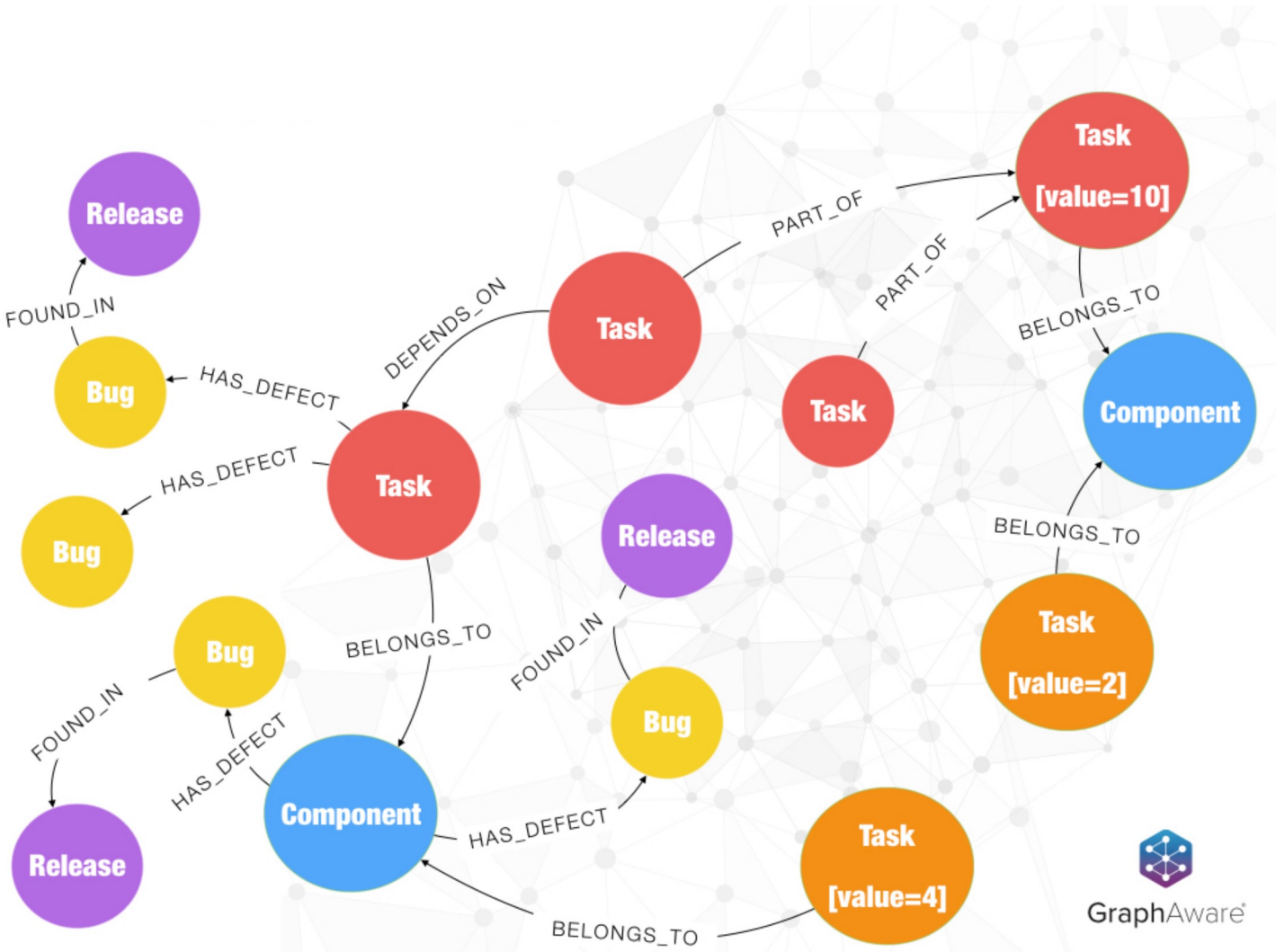
Observability



Monolith vs Micro service architecture

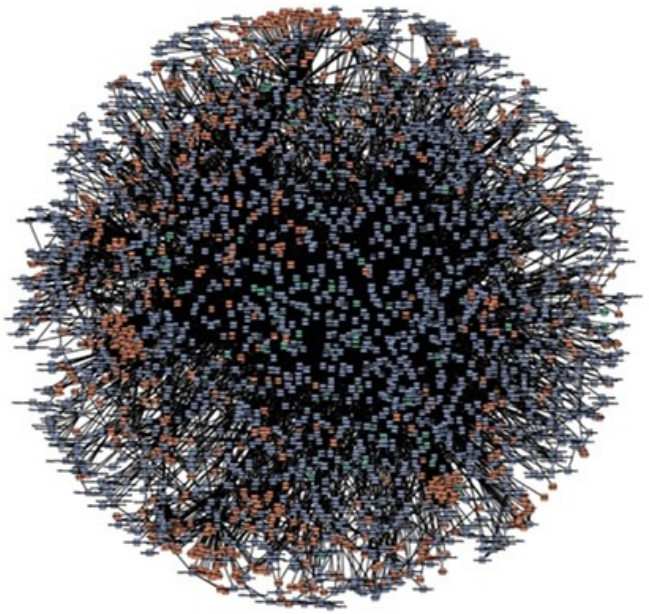


MSA 의 구성 요소 간에 관계



Traffic Pattern! 이것들이 모이면...

MSA 의 미래?!



amazon.com

NETFLIX

Q. Istio 에서 할 수 있는 것은?

- 경로에 따른 서비스 간에 관계성(종족성)
- 서비스 흐름 정상 모니터링
- 로드밸런싱, 풀링, 서킷 브레이크, 배포
- ...

Span, Trace

from Jaeger

Span

- "작업명칭, 시작시간, 소요시간을 가진 작업의 논리 단위. 중첩 가능하고 인과 관계를 모델링 할 수 있음. i.e. RPC call"

Trace

- "시스템을 통한 데이터/실행 경로로 span의 방향성있는 비순환 그래프 형식으로 표현"

https://istio.io/docs/reference/config/policy-and-telemetry/templates/tracespan/

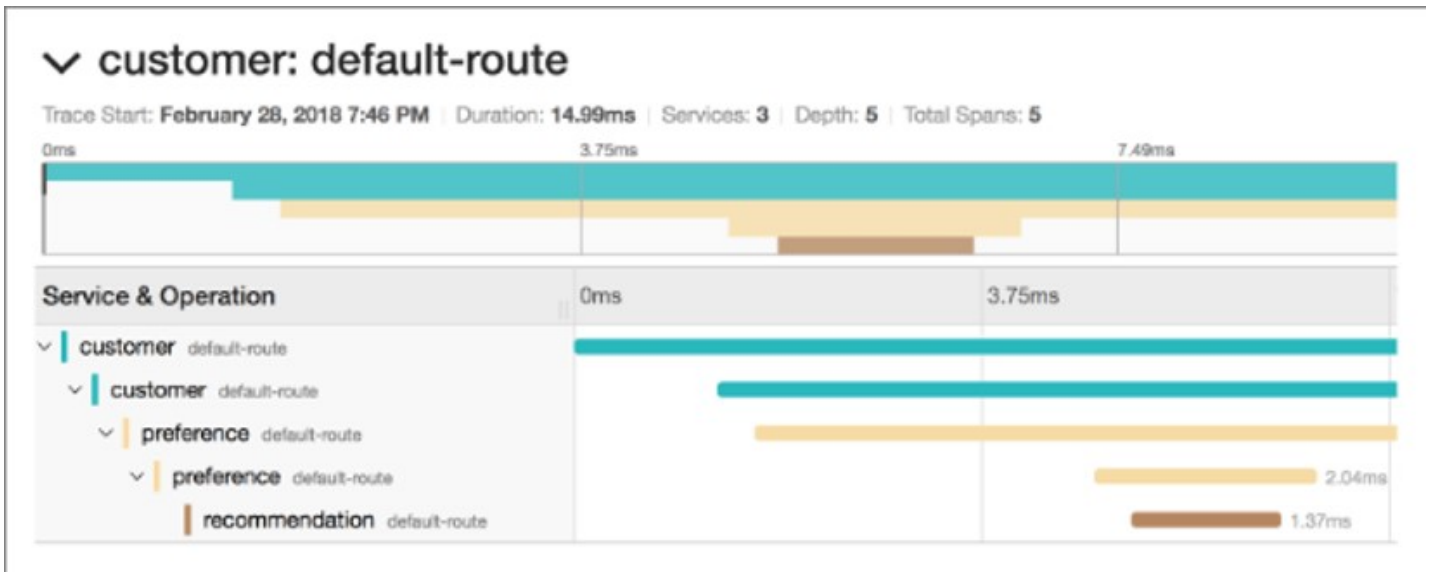
서비스 추적을 위해 필요한 HTTP 헤더(전파해야함)

```
...
public class HttpHeaderForwarderHandlerInterceptor extends HandlerInterceptorAdapter {

  private static final Set<String> FORWARDED_HEADER_NAMES = ImmutableSet.of(
    "x-request-id",
    "x-b3-traceid",
    "x-b3-spanid",
    "x-b3-parentspanid",
    "x-b3-sampled",
    "x-b3-flags",
    "x-ot-span-context",
    "user-agent"
  );

  @Override
  public boolean preHandle( ... ) {
  Map<String, List<String>> headerMap = Collections.list(request.getHeaderNames())
    .stream()
    .map(String::toLowerCase)
    .filter(FORWARDED_HEADER_NAMES::contains)
    .collect(Collectors.toMap(
      Function.identity(),
      h -> Collections.list(request.getHeaders(h))
    ));
  HEADERS_THREAD_LOCAL.set(headerMap);
  return super.preHandle(request, response, handler);
  }
```

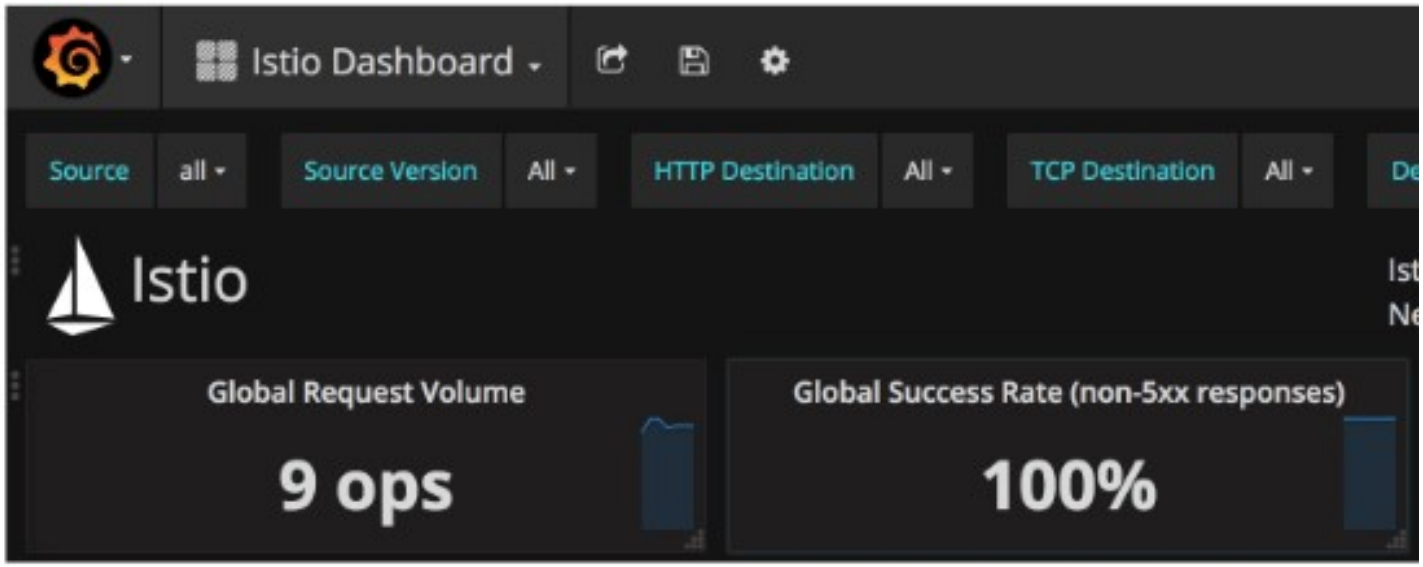
HTTP Tracing: https://zipkin.io/pages/instrumenting.html

Metrics

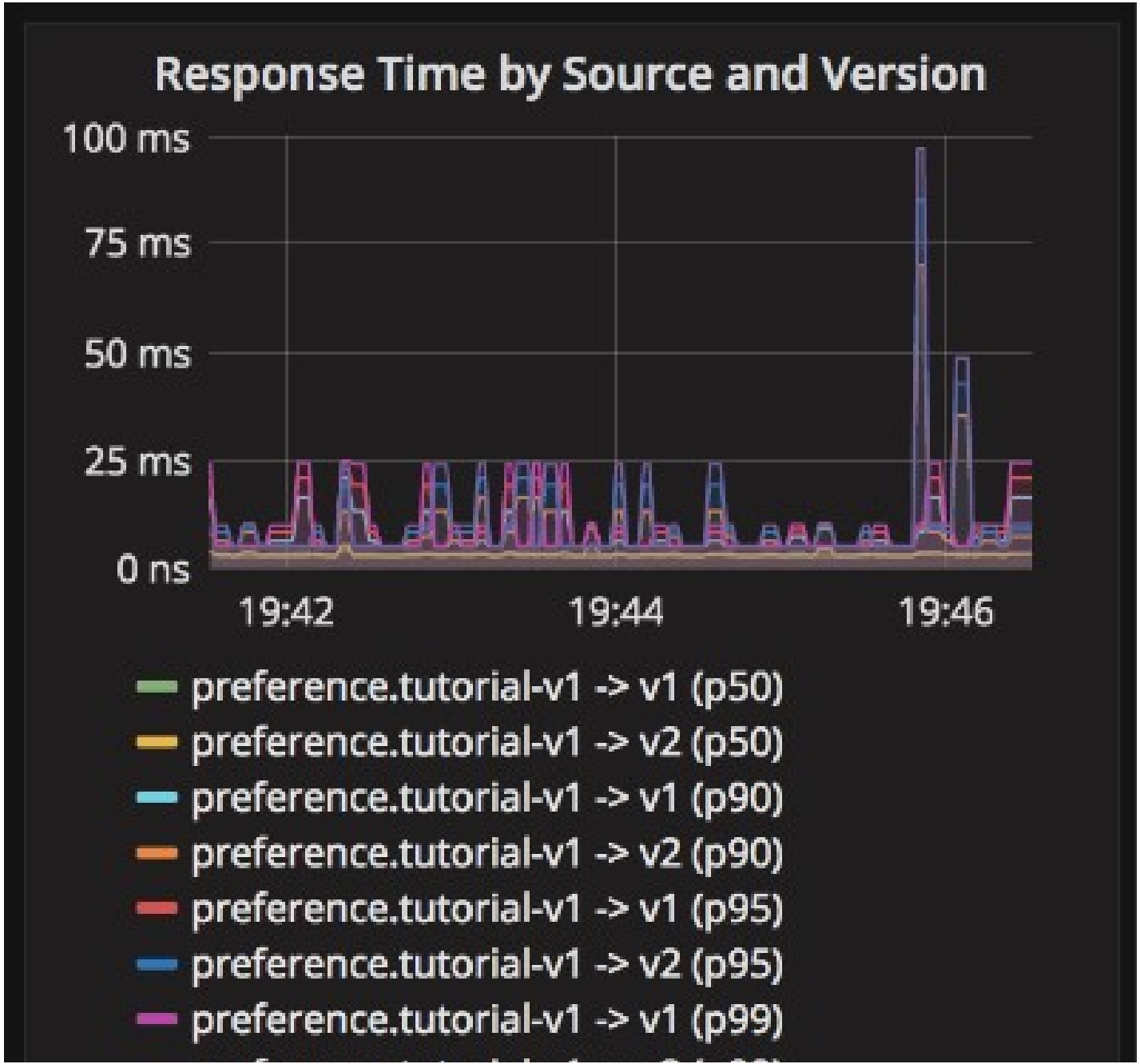
Istio는 기본적으로 텔레메트리 데이터를 수집합니다.



Metrics



http://grafana-istio-system.192.168.99.101.nip.io/dashboard/db/istio-dashboard?var-source=All


Response Time by Source and Version
100 ms
75 ms
50 ms
25 ms
0 ns
19:42
19:44
19:46
preference.tutorial-v1 -> v1 (p50)
preference.tutorial-v1 -> v2 (p50)
preference.tutorial-v1 -> v1 (p90)
preference.tutorial-v1 -> v2 (p90)
preference.tutorial-v1 -> v1 (p95)
preference.tutorial-v1 -> v2 (p95)
preference.tutorial-v1 -> v1 (p99)

Security(ACL)

https://istio.io/docs/tasks/policy-enforcement/denial-and-list/

블랙 리스트

Mixer selector를 이용하여 조건별로(특정 호출 경로) 명시적으로 거부

istiofiles/acl-blacklist.yml (customer -> preference 일 때에 거부(403 Forbidden))

```
apiVersion: "config.istio.io/v1alpha2"
kind: denier
metadata:
  name: denycustomerhandler
spec:
  status:
    code: 7
    message: Not allowed
---
apiVersion: "config.istio.io/v1alpha2"
kind: checknothing
metadata:
  name: denycustomerrequests
spec:
---
apiVersion: "config.istio.io/v1alpha2"
kind: rule
metadata:
  name: denycustomer
spec:
  match: destination.labels["app"] == "preference" && source.labels["app"]=="customer"
  actions:
```

denier:

- https://istio.io/docs/reference/config/policy-and-telemetry/adapters/denier/
- https://istio.io/blog/2017/adapter-model/
- https://github.com/istio/istio/wiki/Mixer-Compiled-In-Adapter-Dev-Guide

checknothing:

- https://istio.io/docs/reference/config/policy-and-telemetry/templates/checknothing/

rule:

- https://istio.io/docs/reference/config/policy-and-telemetry/istio.policy.v1beta1/#Rule
- https://istio.io/docs/reference/config/policy-and-telemetry/istio.policy.v1beta1/#Action
- https://istio.io/docs/reference/config/policy-and-telemetry/istio.policy.v1beta1/#Handler

화이트 리스트

승인된 호출 경로를 제외하고는 모든 규칙을 거부

istiofiles/acl-whitelist.yml(recommendation -> preferences)

```
apiVersion: "config.istio.io/v1alpha2"
kind: listchecker
metadata:
  name: preferencewhitelist
spec:
  overrides: ["recommendation"]
  blacklist: false
---
apiVersion: "config.istio.io/v1alpha2"
kind: listentry
metadata:
  name: preferencesource
spec:
  value: source.labels["app"]
---
apiVersion: "config.istio.io/v1alpha2"
kind: rule
metadata:
  name: checkfromcustomer
spec:
  match: destination.labels["app"] == "preference"
  actions:
  - handler: preferencewhitelist.listchecker
```

listentry:

- https://istio.io/docs/reference/config/policy-and-telemetry/templates/listentry/

listchecker:

- https://istio.io/docs/reference/config/policy-and-telemetry/adapters/list/

rule:

- https://istio.io/docs/reference/config/policy-and-telemetry/istio.policy.v1beta1/#Rule
- https://istio.io/docs/reference/config/policy-and-telemetry/istio.policy.v1beta1/#Action
- https://istio.io/docs/reference/config/policy-and-telemetry/istio.policy.v1beta1/#Handler

IP CIDR

```
apiVersion: config.istio.io/v1alpha2
kind: listchecker
metadata:
  name: whitelistip
spec:
  # providerUrl: ordinarily black and white lists are maintained
  # externally and fetched asynchronously using the providerUrl.
  overrides: ["10.57.0.0/16"]  # overrides provide a static list
  blacklist: false
  entryType: IP_ADDRESSES
```

남은 것들

Traffic flow

- https://bit.ly/2Pcuqyg
- Debugging Envoy and Pilot
- https://www.youtube.com/watch?v=I9ZskIT-jxg
- https://mt165.co.uk/speech/life-of-a-packet-istio-cloud-native/

핸즈온 (Katakoda)

fault injection

- https://learn.openshift.com/servicemesh/6-fault-injection
- https://www.katacoda.com/courses/istio/increasing-reliability

monitoring

- https://learn.openshift.com/servicemesh/3-monitoring-tracing
- https://www.katacoda.com/courses/istio/observing-microservices

access control

- https://learn.openshift.com/servicemesh/5-advanced-routerules

katacoda tip

https://wsend.net/

install

```
wget https://wsend.net/wsend
chmod +x wsend
```

usage

```
user@system:~$ wsend README.md
https://wsend.net/73efe0fd8bb12baac9d023708a9db634/README.md
```