후원사

다이아몬드

Microsoft

플래티넘

KOSS | Korea Software Service

(주)한국소프트웨어서비스

골드

go deploy

STK

TRAINOCATE

실버

OPEN SG Solution Group

브론즈

한빛미디어

Microsoft 365 Copilot

답답한 쿠버네티스 장애 추적, 로그 창 닫고 눈으로 확인하기 (feat. eBPF)

MCT 박민진

MCT 박민진

Modernization Solutions Architect
@MegazoneCloud

Training & Speaking

Delivering **DevOps**(Azure, GitHub) and AI(GitHub Copilot)
@Hyundai AutoEver, Hanwha Vision, KT, MS's US partner Corp etc.

DDD Seoul 2024 / .NET Conf 2024

I ♥ Open Source

Contributing **Azure OpenAI SDK Proxy** etc.

Aya(Rust **eBPF**) based K8s Selective LLM Observability Tool Co-Developer
(Active in CNCF ecosystem community)

MCT 박민진

Modernization Solutions Architect
@MegazoneCloud

Minjin Park • 나
Modernization Solutions Architect | Microsoft Certified Trainer | @Microsof...

Since transitioning from an instructor to a Solutions Architect in February, I've been fully focused on adapting to my new role, which left me little time for side projects since early April.

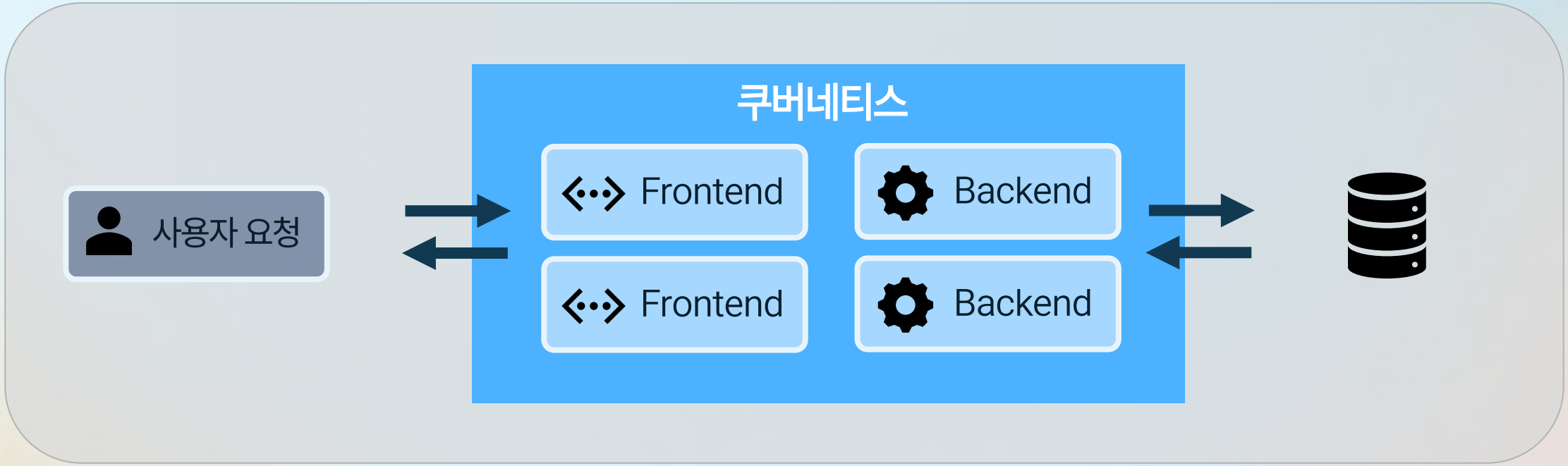
However, I'm incredibly honored to receive a shout-out for the eBPF-based LLM observability open source project that I've been working on since last year! Although my contributions were modest, I'm truly grateful to the team for giving me the wonderful opportunity to be a part of this amazing journey as a core developer.

#ebpf #llm #ai #observability #kubernetes #opensource #techcommunity

Bill Mulligan • 1촌
Community @ Isovalent at Cisco | Cilium and ebpf.io Maintainer
2주 •

Lightweight eBPF-based observability agent for AI/LLM workloads - monitors token usage, latency, and sensitive file access in Kubernetes without code changes

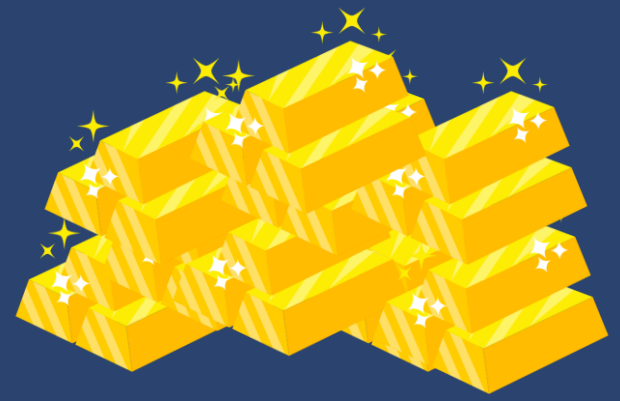
AI나 서비스, 응답이 왜 이렇게 늦죠?

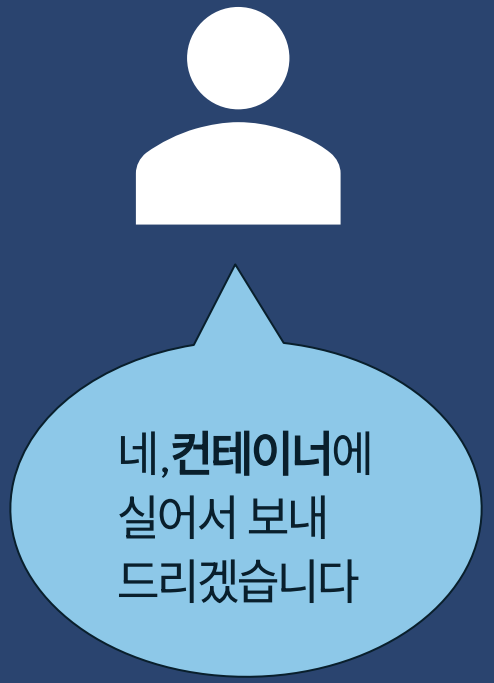


요청 뒤에는 많은 로직들이 작동하고 있습니다.

많은 현대 서비스 운영의 중심, 쿠버네티스

컨테이너란?





컨테이너란?

컨테이너란?

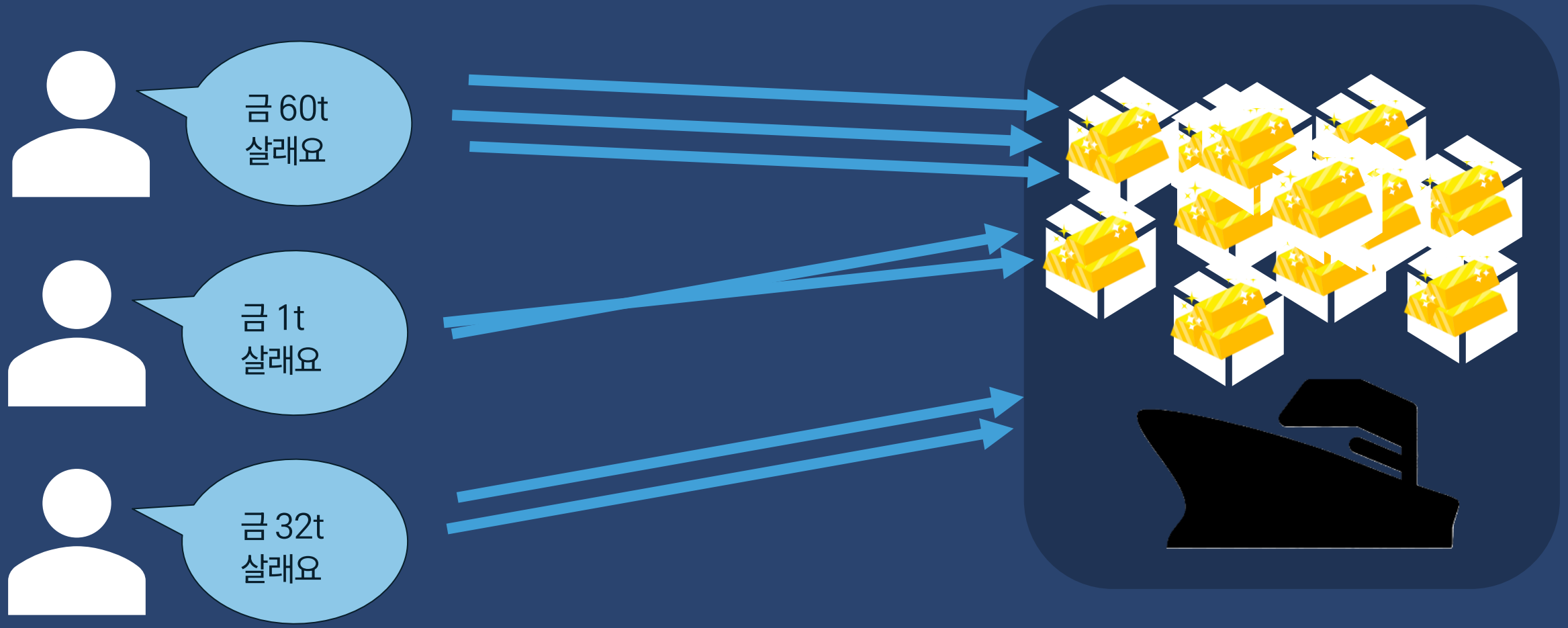
컨테이너란?

보내야 할 게 많네?
컨테이너를
추가해야 겠다

컨테이너란?

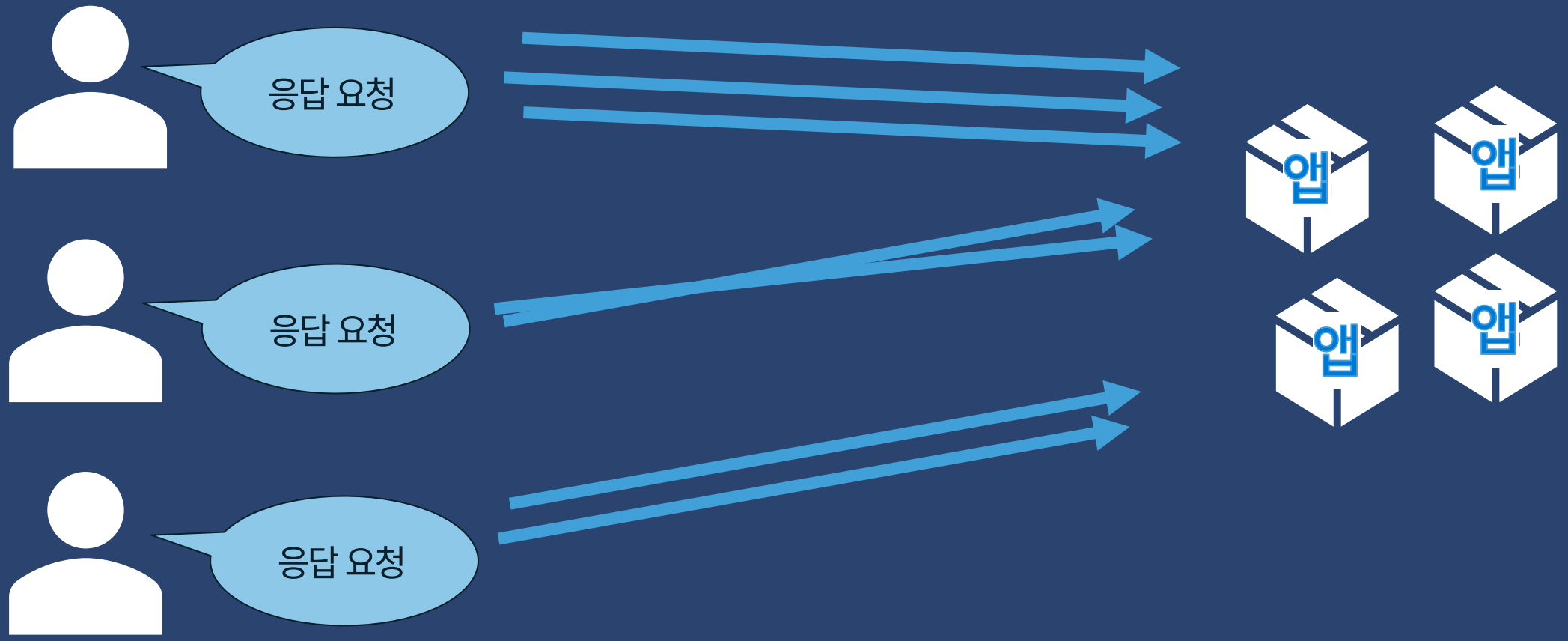
컨테이너란?

컨테이너란?

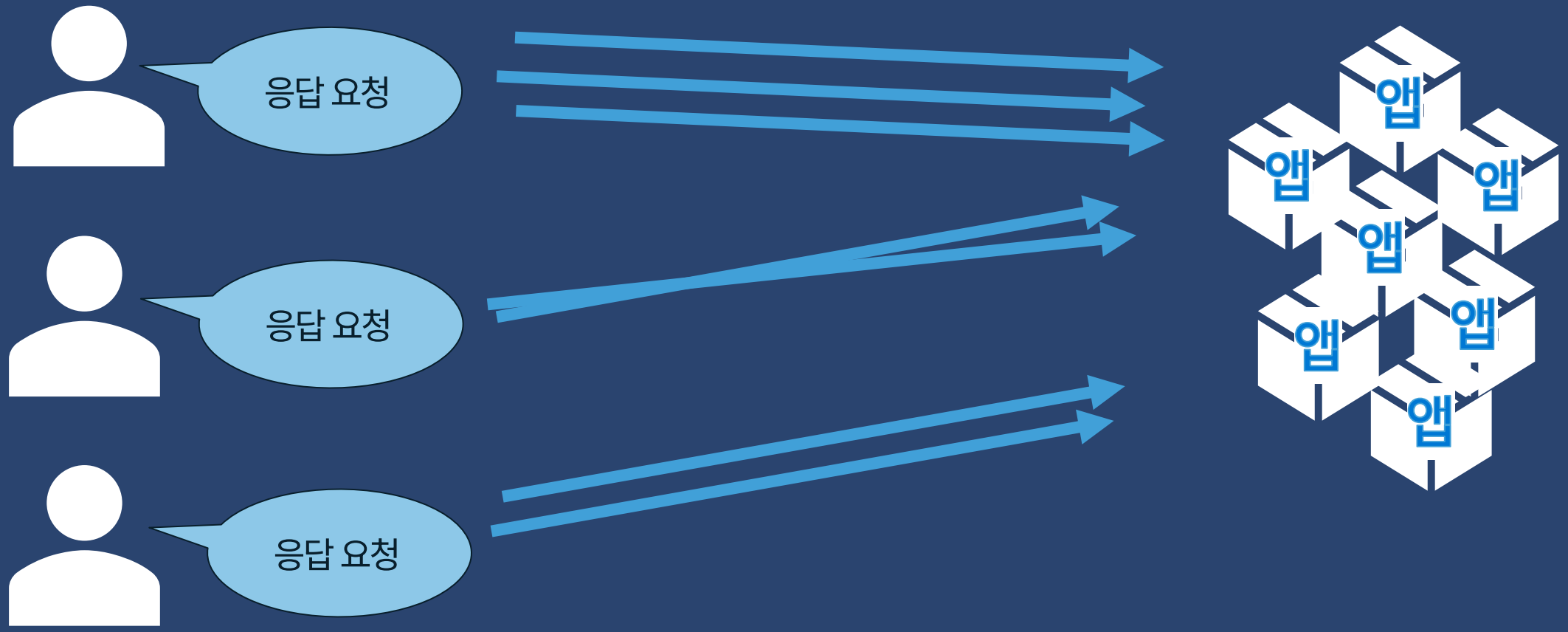


컨테이너란?

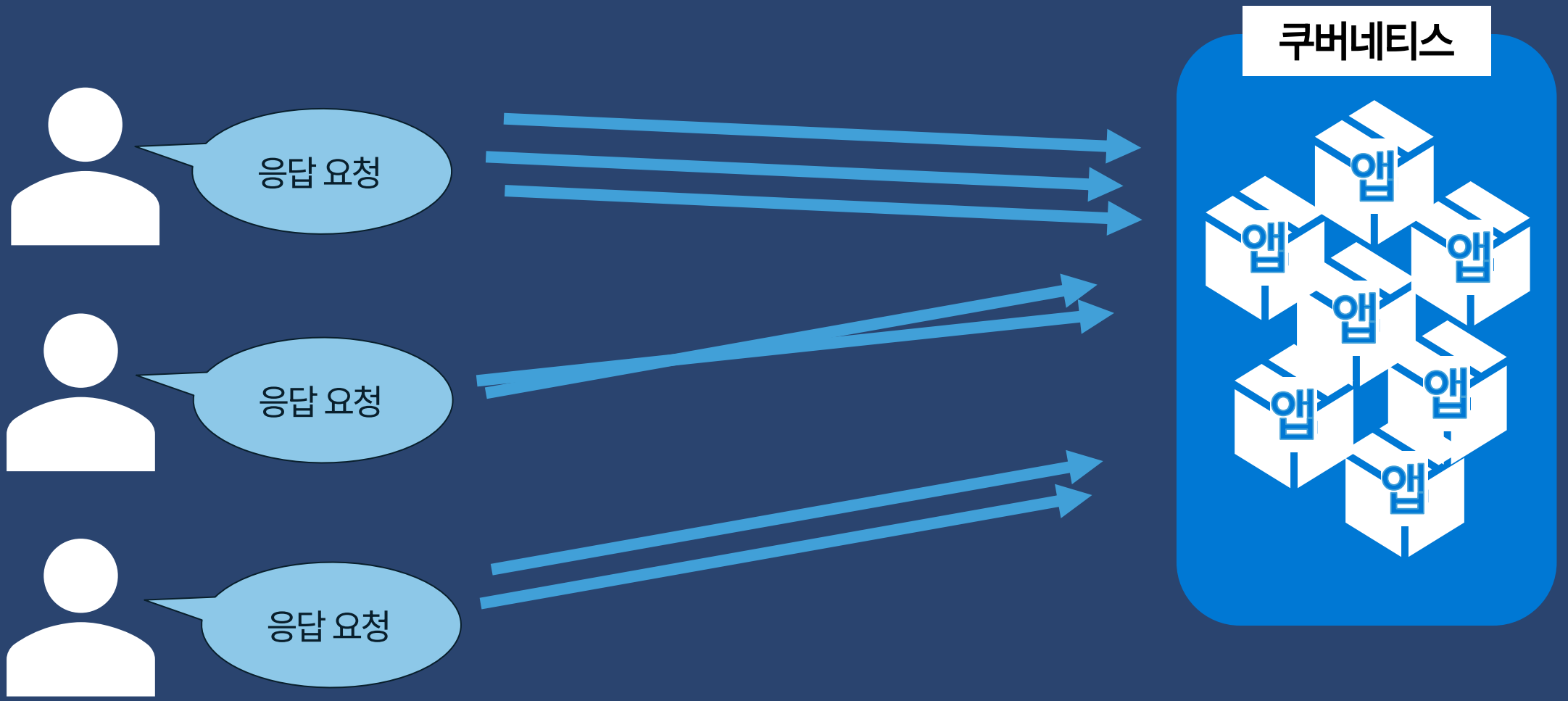
컨테이너란?



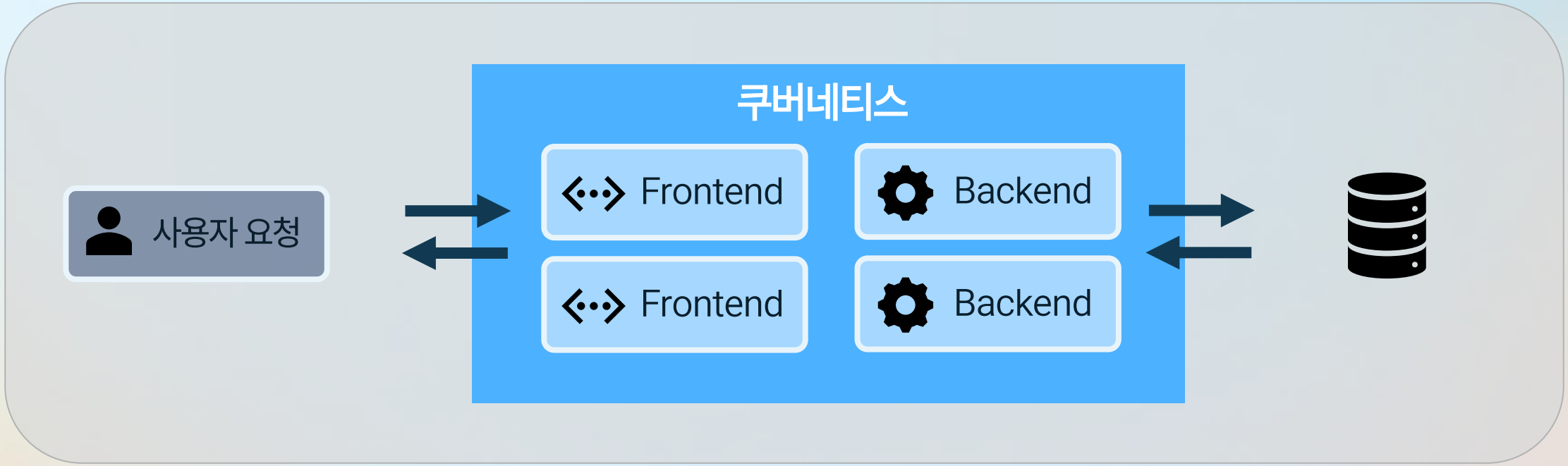
컨테이너란?



컨테이너란?

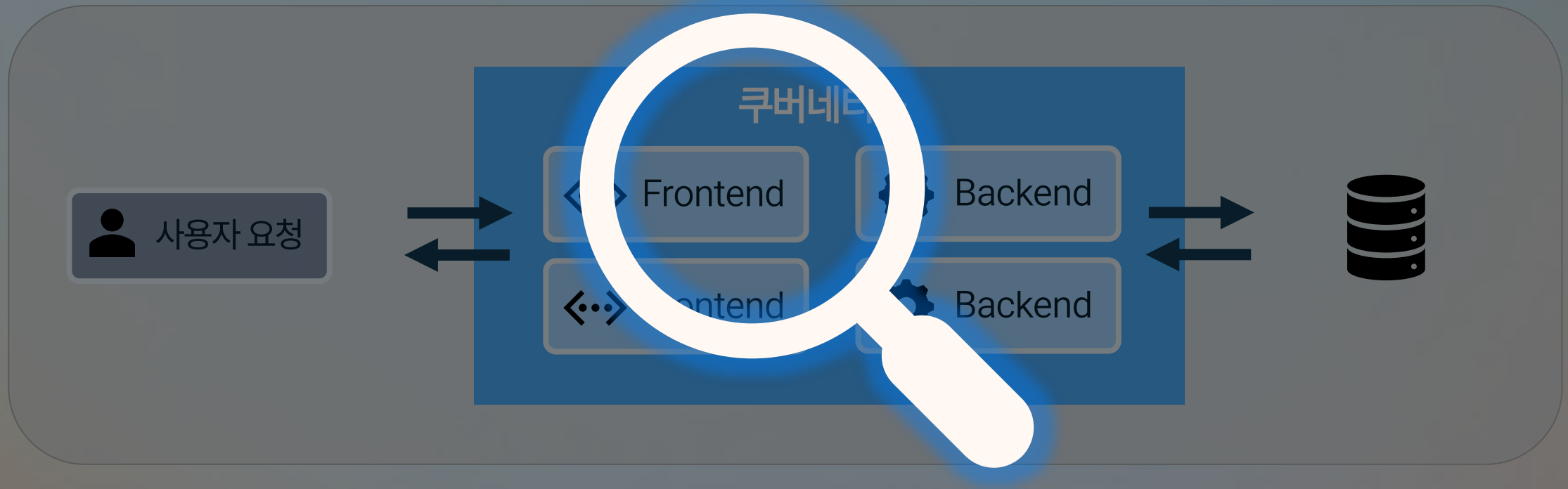


AI나 서비스, 응답이 왜 이렇게 늦죠?

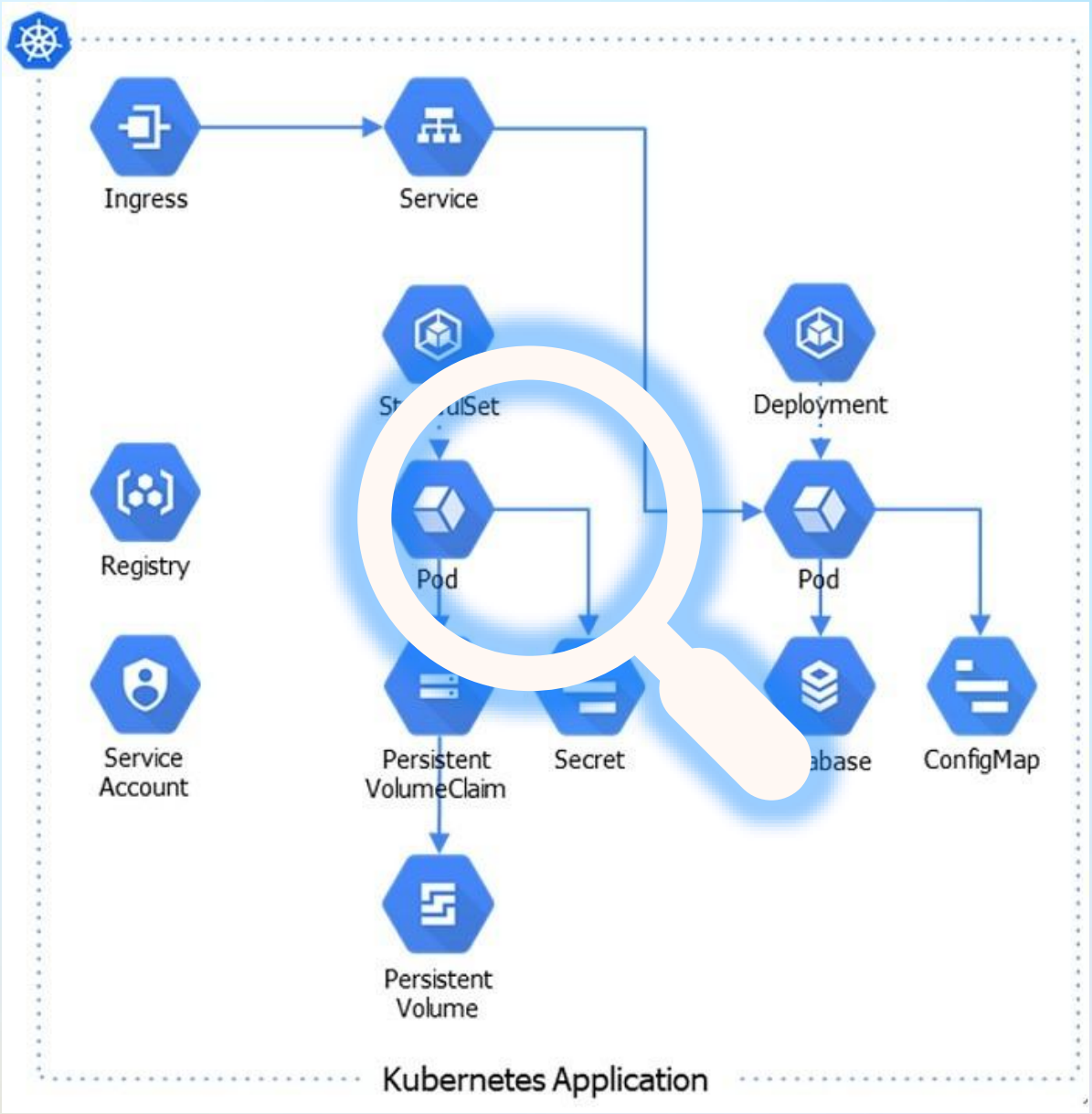


요청 뒤에는 많은 로직들이 작동하고 있습니다.

AI나 서비스, 응답이 왜 이렇게 늦죠?



요청 뒤에는 많은 로직들이 작동하고 있습니다.


Ingress
Service
Deployment
Registry
Pod
Pod
Service Account
Persistent VolumeClaim
Secret
ConfigMap
Persistent Volume
Kubernetes Application

default / nginx

Overview Revisions **Logs** YAML Events

Pods 3/3 Tail

```
5nsxc  127.0.0.1 - - [22/Jul/2025:08:55:13 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc  2025/07/22 08:55:13 [error] 35#35: *157 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2  2025/07/22 08:55:15 [error] 37#37: *280 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2  127.0.0.1 - - [22/Jul/2025:08:55:15 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc  127.0.0.1 - - [22/Jul/2025:08:55:16 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc  2025/07/22 08:55:16 [error] 35#35: *158 op                r/share/nginx/html/api" failed (2: No such file or
5nsxc  127.0.0.1 - - [22/Jul/2025:08:55:16 +00      "GET /ap      TTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc  2025/07/22 08:55:16 [error] 35#35: *15       open() "/usr      hare/nginx/html/api" failed (2: No such file or
5nsxc  127.0.0.1 - - [22/Jul/2025:08:55:16 +0      0] "GET /api      TP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc  2025/07/22 08:55:16 [error] 35#35: *16       open() "/usr      hare/nginx/html/api" failed (2: No such file or
4xvr2  127.0.0.1 - - [22/Jul/2025:08:55:17 +00      "GET /      TTP/1.1" 404 153 "-" "curl/8.7.1" "-"
4xvr2  2025/07/22 08:55:17 [error] 38#38: *284 open()       /usr      e/nginx/html/api" failed (2: No such file or
5nsxc  2025/07/22 08:55:17 [error] 35#35: *161 open() "/usr/s      nginx/html/api" failed (2: No such file or
5nsxc  127.0.0.1 - - [22/Jul/2025:08:55:17 +0000] "GET /api HTT      .1" 404 153 "-" "curl/8.7.1" "-"
5nsxc  2025/07/22 08:55:18 [error] 35#35: *162 open() "/usr/share/nginx/html/api" failed (2: No such file or
5nsxc  127.0.0.1 - - [22/Jul/2025:08:55:18 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
4xvr2  2025/07/22 08:55:19 [error] 38#38: *287 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2  127.0.0.1 - - [22/Jul/2025:08:55:19 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
4xvr2  2025/07/22 08:55:20 [error] 38#38: *291 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2  127.0.0.1 - - [22/Jul/2025:08:55:20 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc  2025/07/22 08:55:21 [error] 35#35: *165 open() "/usr/share/nginx/html/api" failed (2: No such file or
```

default / nginx

Overview Revisions Logs YAML Events Pods 3/3 Tail

- 초당 수천 줄씩 올라가는 방대한 텍스트
- DNS 실패, 연결 유실 등 네트워크 상황 누락
- 과거의 기록일 뿐, 실시간 파악 불가

쿠버네티스 모니터링 툴을 써도 여전히 답답한 이유?

Grafana

Prometheus

Jaeger


Home › Dashboards › node resource uses
Add
Last 1 hour
Namespqce
kube-system
Pod
All
Cluster Metrics
node status
master
Good
worker1
Good
node cpu 사용률
master
worker1
node memory 사용률
worker1
master
node network평균 송/수신 트래픽
master-tranmit
worker1-tranmit
master-receive
worker1-receive
kube-system Metrics
API Server 응답 시간(5분/SLA 99%)
1 min
All CPU 사용률
coredns-5d78c9869d-qfs6f
coredns-5d78c9869d-t9qnx
etcd-master
kube-apiserver-master
kube-controller-manager-master
kube-proxy-8qrg5
kube-proxy-bvj9f
kube-scheduler-master
weave-net-8dphk
weave-net-qwqnj
All 메모리 사용량
Pod 상태
Failed
0
Pending
0
Running
10
Succeeded
0
Unknown
0


※ 근본적인 한계
대부분 메트릭(숫자) + 텍스트 위주.
CPU가 몇 %인지는 알 수 있지만,
어떤 앱(Pod)에서 네트워크 패킷이
막혔는지는 보여주지 못함.
Failed
Pending
Running
Succeeded
Unknown
0
0
10
0
0

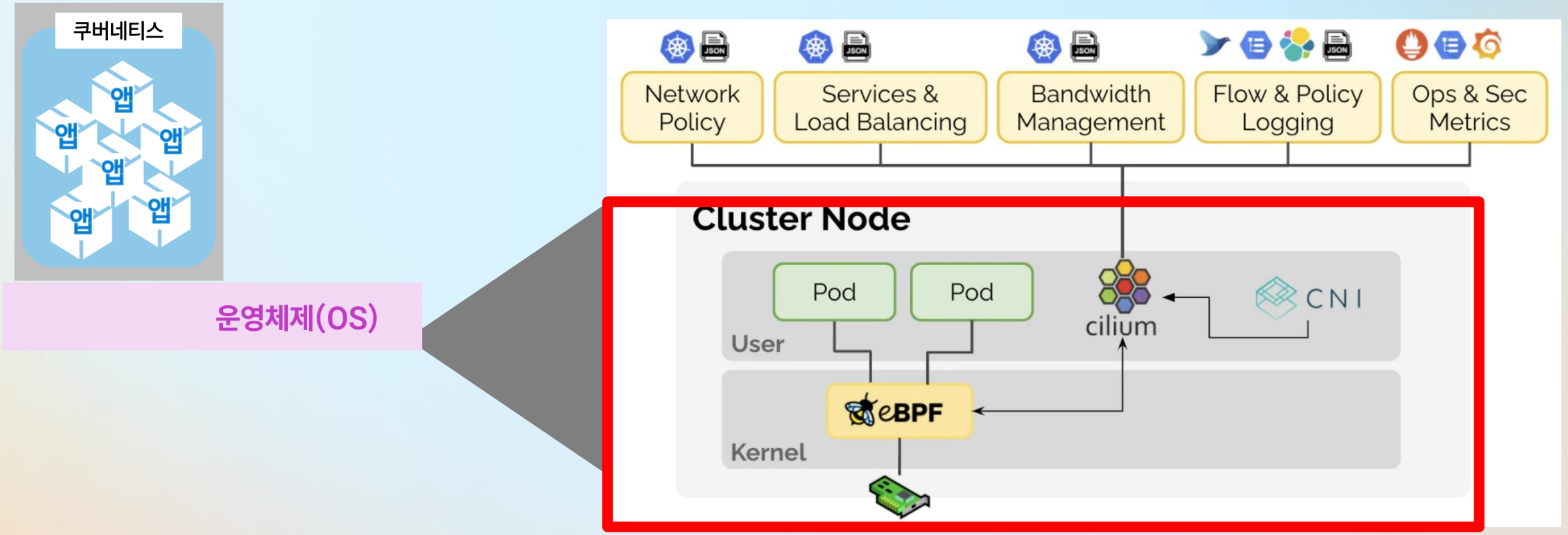
운영체제(OS) 심장에 심는 투명 CCTV

운영체제(OS) 심장에 심는 투명 CCTV

운영체제(OS)

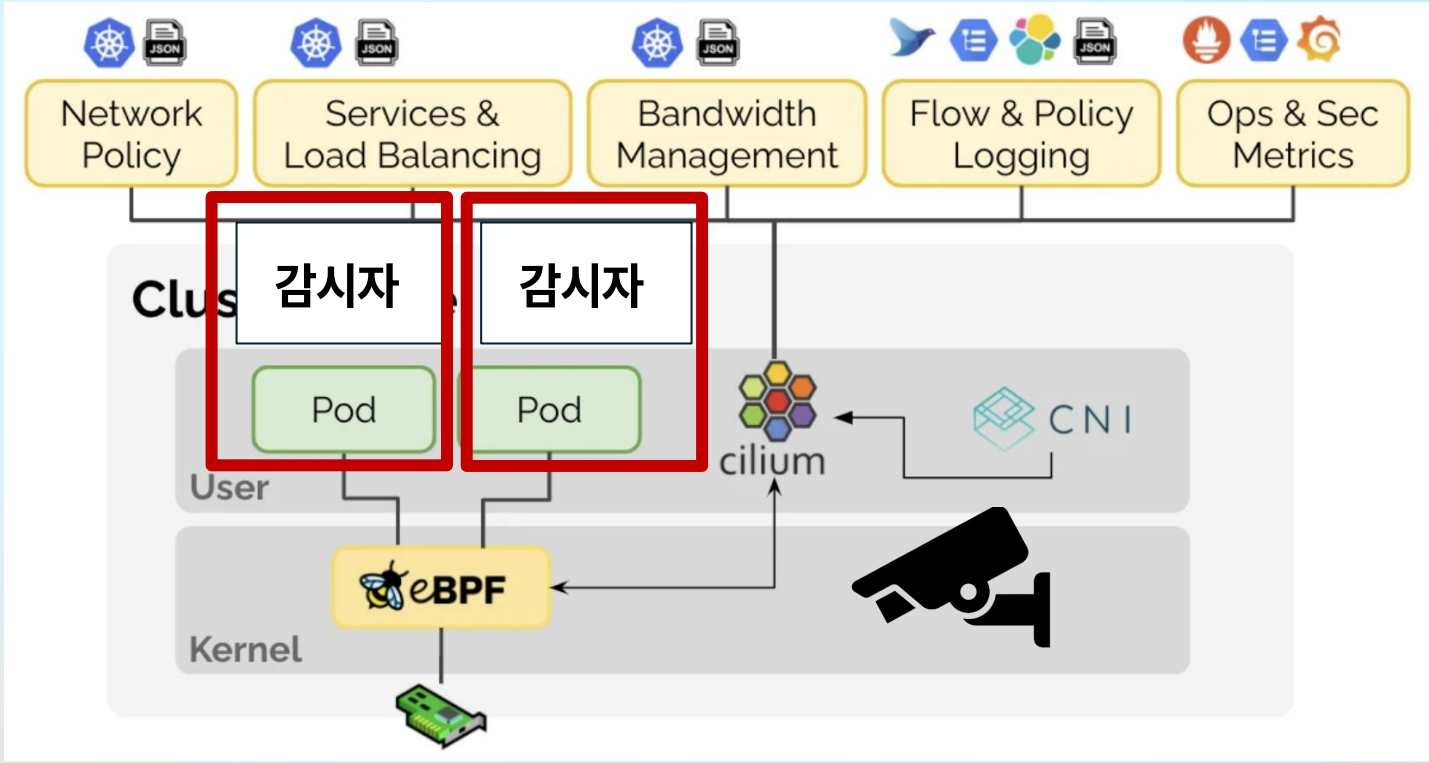
eBPF: 서비스들이 올라가 있는 OS의 깊은 곳(커널 모드)에서 정보를 가져오는 것

운영체제(OS) 심장에 심는 투명 CCTV



eBPF: 서비스들이 올라가 있는 OS의 깊은 곳(커널 모드)에서 정보를 가져오는 것

운영체제(OS) 심장에 심는 투명 CCTV



eBPF: 커널 모드에서 정보를 가져오는 것

운영체제(OS) 심장에 심는 투명 CCTV

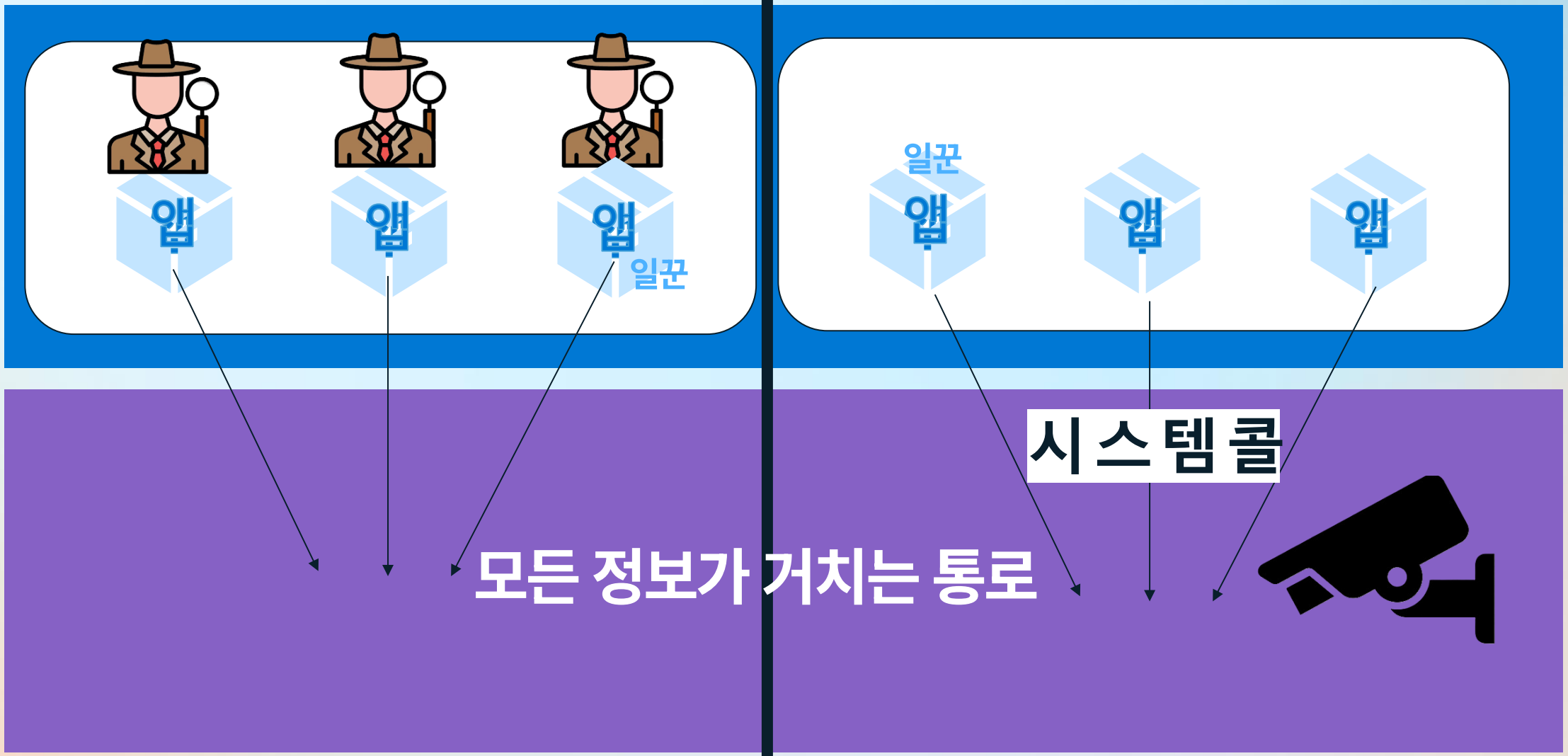
왜 eBPF?

기존 방식(사이드카)

eBPF 방식(데몬셋)

유저 모드

커널 모드



어떻게 빠르고 안전하게 작동할까?

1

Verifier

가장 중요한 **안전 검사관,** 커널 패닉을 유발할 위험 요소가 1%라도 있으면 진입을 원천 차단. 무중단 환경에서도 완벽한 런타임 안정성 보장.

2

Event Hook

복잡한 네트워크 스택을 층층이 다 거칠 때까지 기다리지 않음.

커널의 핵심 길목에서 지나가는 데이터를 **직접 낚아채어(Bypass)** 실시간 포착.

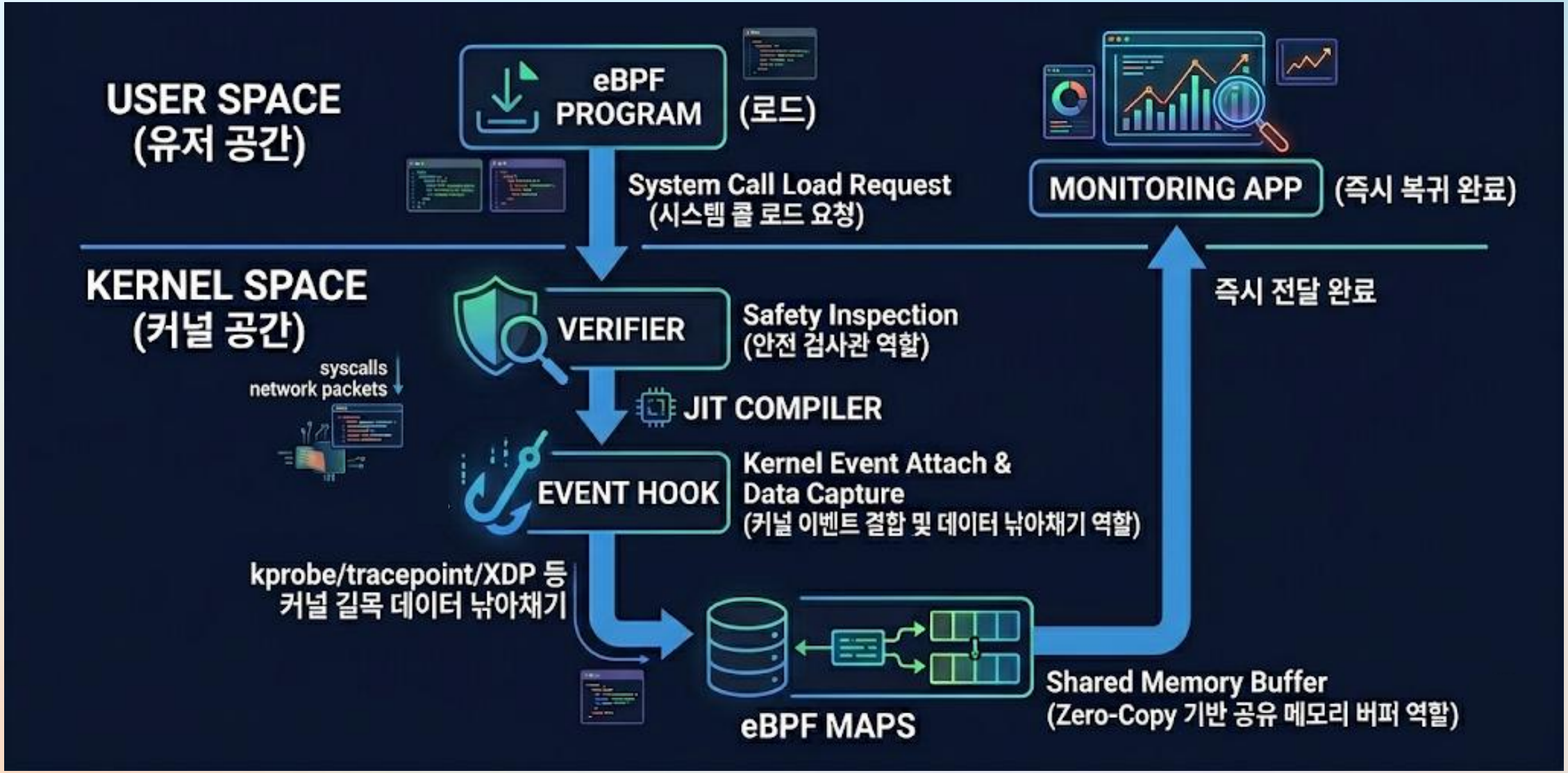
3

eBPF Maps

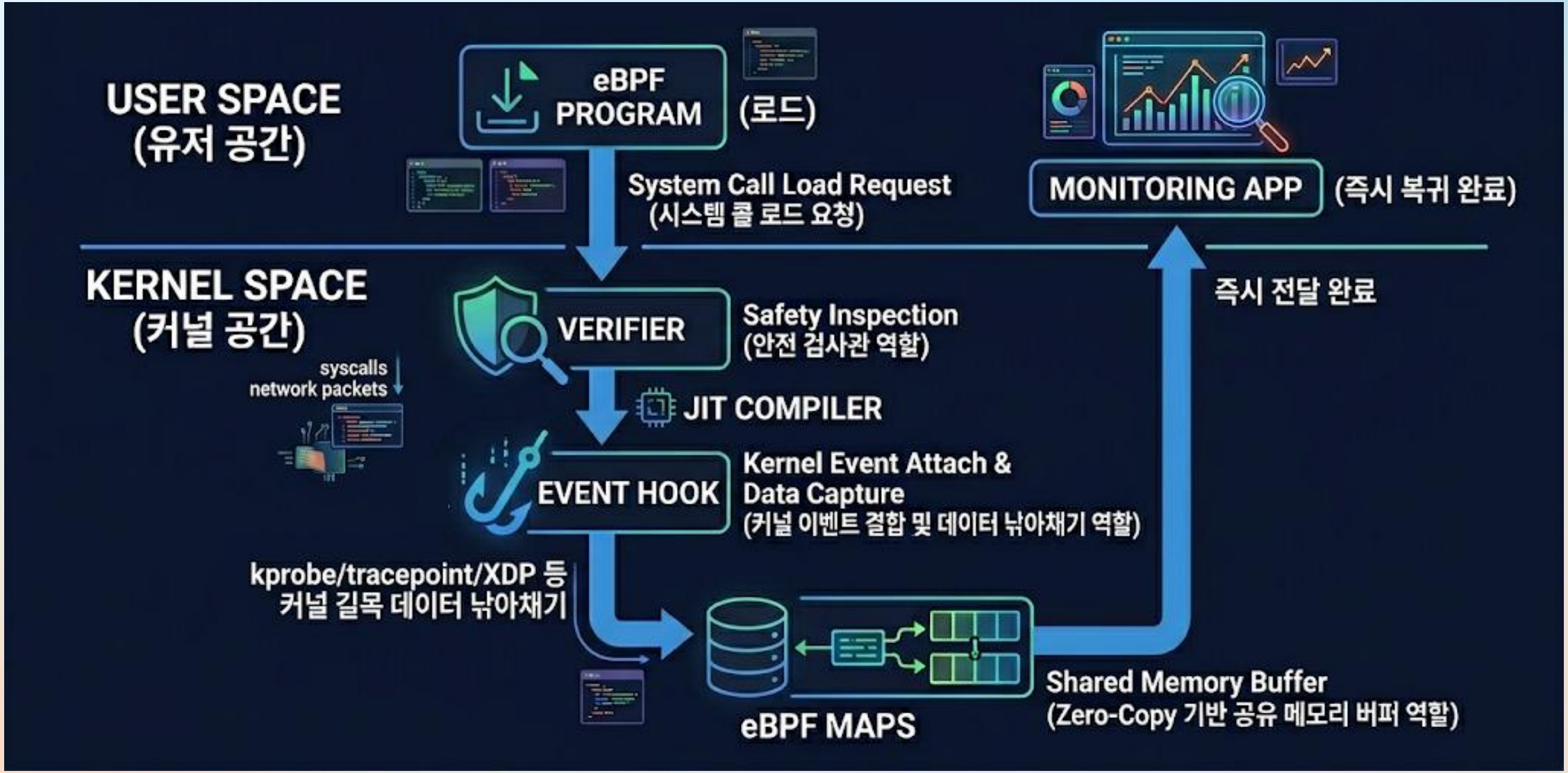
검사를 통과해 안전하게 모은 데이터는 무거운 복사(Context Switch) 과정 없이,

고속 우체통을 통해 Zero-Copy 형태로 유저 공간에 즉시 쏘아 올려짐.

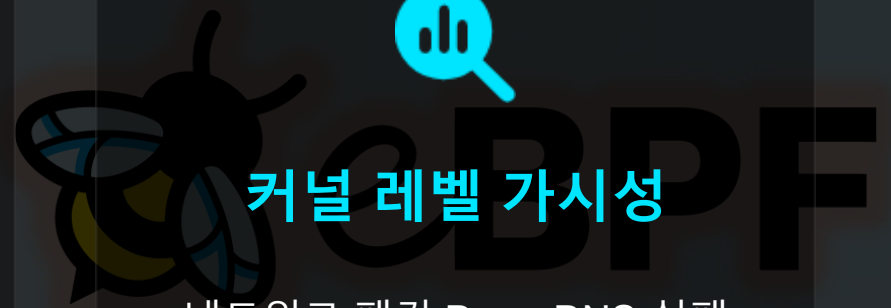
어떻게 빠르고 안전하게 작동할까?



어떻게 빠르고 안전하게 작동할까?



운영체제(OS) 심장에 심는 투명 CCTV



왜 eBPF?

코드 수정 X

"로그 좀 남겨주세요" 부탁할 필요 없이, 기존 소스 코드 0줄 수정으로 모든 흐름 관찰.

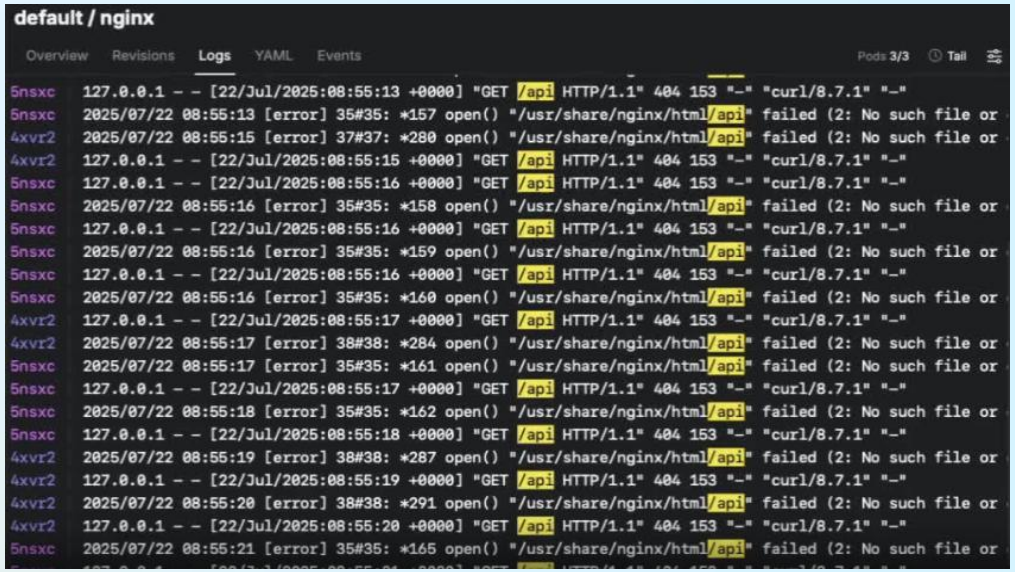
커널 레벨 가시성

네트워크 패킷 Drop, DNS 실패 등 기존 모니터링 툴이 놓치는 사각지대를 바닥에서 포착.

서비스 지연 Zero

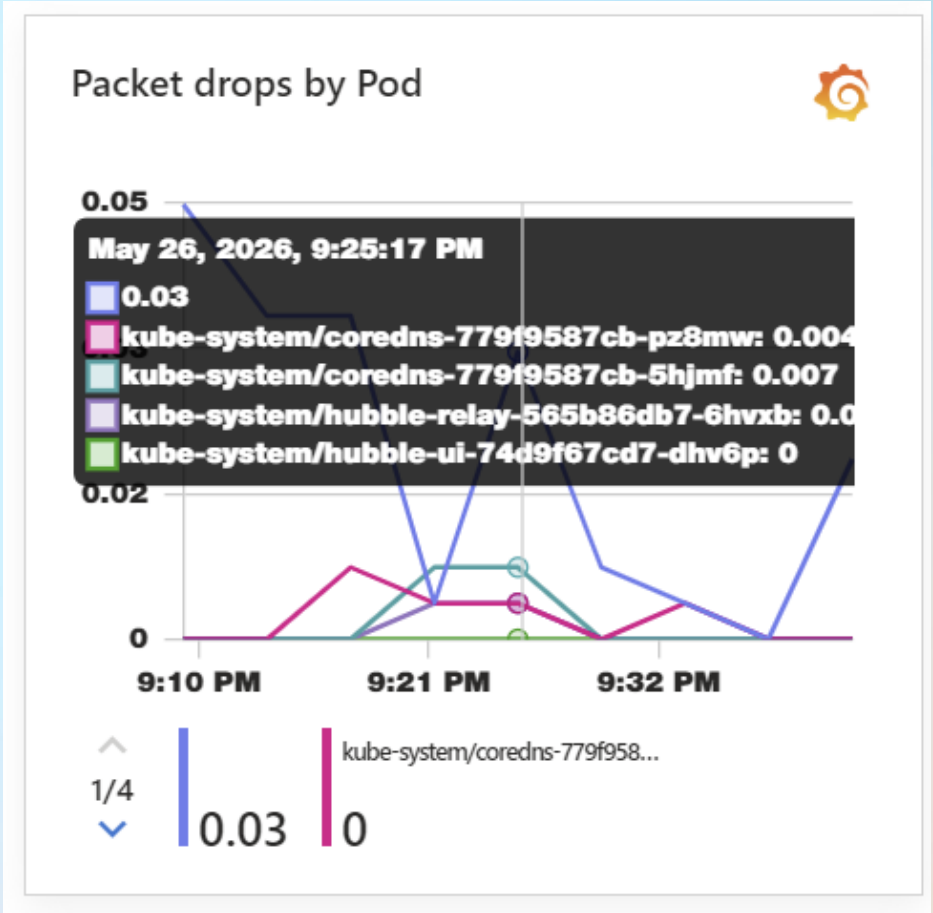
무거운 Agent 박스를 띄우지 않아 시스템 리소스를 낭비하지 않고 네이티브 속도로 동작합니다.

기존 방식

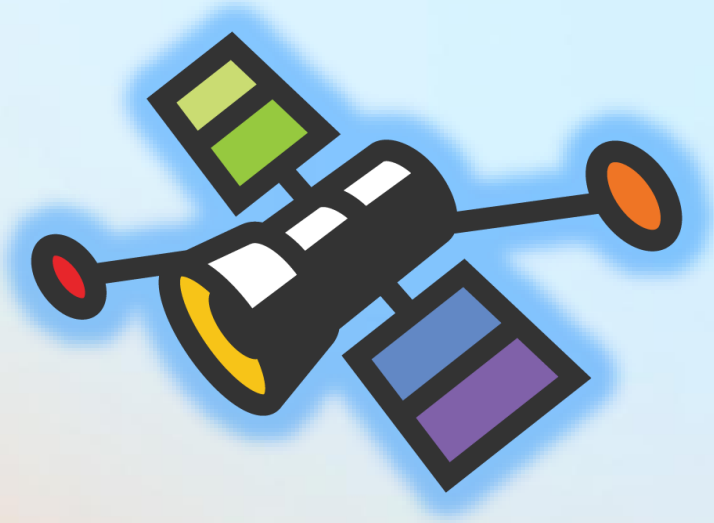

default / nginx
Overview
Revisions
Logs
YAML
Events
Pods 3/3
Tail
5nsxc 127.0.0.1 - - [22/Jul/2025:08:55:13 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc 2025/07/22 08:55:13 [error] 35#35: *157 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2 2025/07/22 08:55:15 [error] 37#37: *280 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2 127.0.0.1 - - [22/Jul/2025:08:55:15 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc 127.0.0.1 - - [22/Jul/2025:08:55:16 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc 2025/07/22 08:55:16 [error] 35#35: *158 open() "/usr/share/nginx/html/api" failed (2: No such file or
5nsxc 127.0.0.1 - - [22/Jul/2025:08:55:16 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc 2025/07/22 08:55:16 [error] 35#35: *159 open() "/usr/share/nginx/html/api" failed (2: No such file or
5nsxc 127.0.0.1 - - [22/Jul/2025:08:55:16 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc 2025/07/22 08:55:16 [error] 35#35: *160 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2 127.0.0.1 - - [22/Jul/2025:08:55:17 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
4xvr2 2025/07/22 08:55:17 [error] 38#38: *284 open() "/usr/share/nginx/html/api" failed (2: No such file or
5nsxc 2025/07/22 08:55:17 [error] 35#35: *161 open() "/usr/share/nginx/html/api" failed (2: No such file or
5nsxc 127.0.0.1 - - [22/Jul/2025:08:55:17 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc 2025/07/22 08:55:18 [error] 35#35: *162 open() "/usr/share/nginx/html/api" failed (2: No such file or
5nsxc 127.0.0.1 - - [22/Jul/2025:08:55:18 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
4xvr2 2025/07/22 08:55:19 [error] 38#38: *287 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2 127.0.0.1 - - [22/Jul/2025:08:55:19 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
4xvr2 2025/07/22 08:55:20 [error] 38#38: *291 open() "/usr/share/nginx/html/api" failed (2: No such file or
4xvr2 127.0.0.1 - - [22/Jul/2025:08:55:20 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/8.7.1" "-"
5nsxc 2025/07/22 08:55:21 [error] 35#35: *165 open() "/usr/share/nginx/html/api" failed (2: No such file or


master
Good
worker1
Good
1 min
Failed
Pending
Running
Succeeded
Unknown
0
0
10
0
0

eBPF 방식


Packet drops by Pod
0.05
May 26, 2026, 9:25:17 PM
0.03
kube-system/coredns-77919587cb-pz8mw: 0.004
kube-system/coredns-77919587cb-5hjmf: 0.007
kube-system/hubble-relay-565b86db7-6hvxb: 0.0
kube-system/hubble-ui-74d9f67cd7-dhv6p: 0
0.02
0
9:10 PM
9:21 PM
9:32 PM
1/4
0.03
kube-system/coredns-779f958...
0

운영체제(OS) 심장에 심는 투명 CCTV



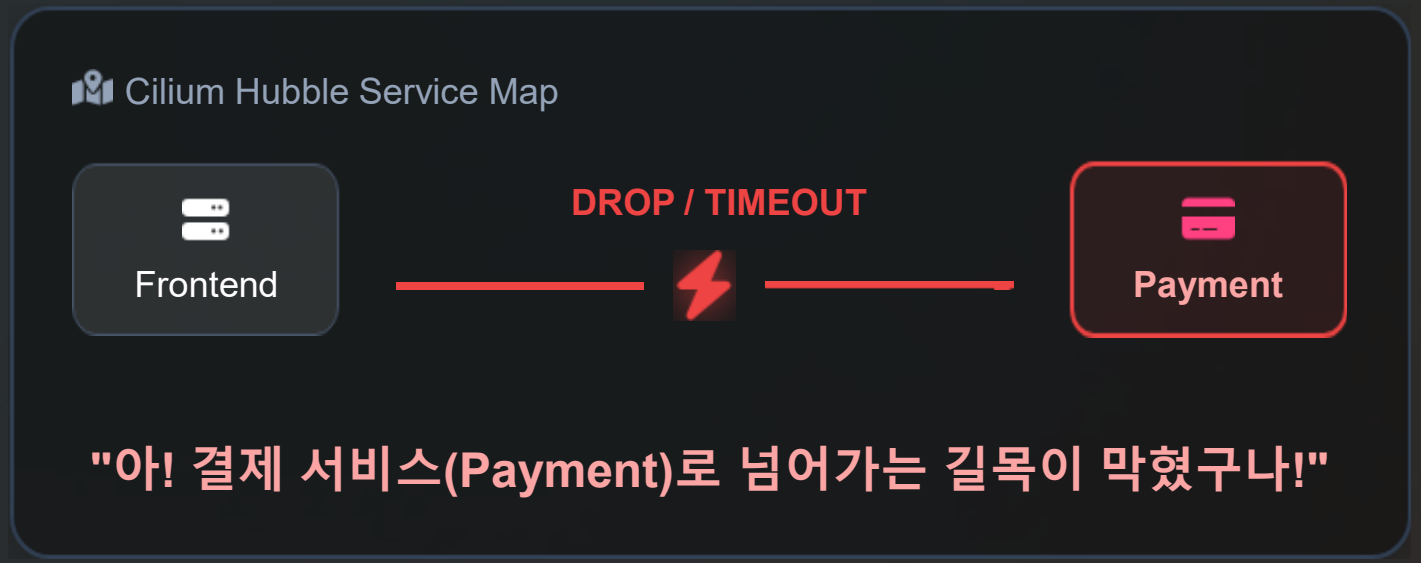
Hubble

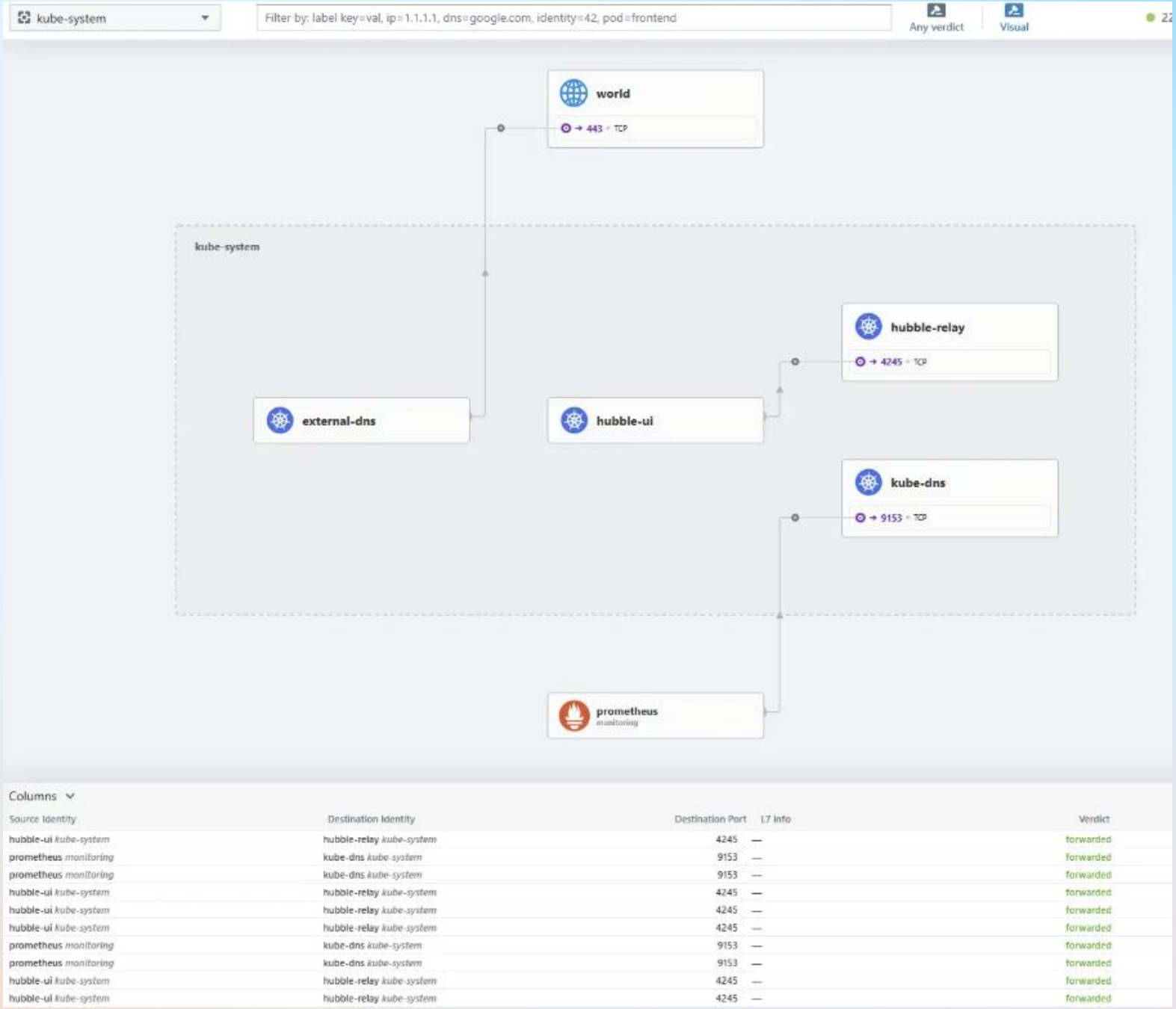
로그 변환 지도

초당 수천 줄의 텍스트 대신 지도로 확인하기. 3시간 걸릴 추적이 1초 만에 끝납니다.

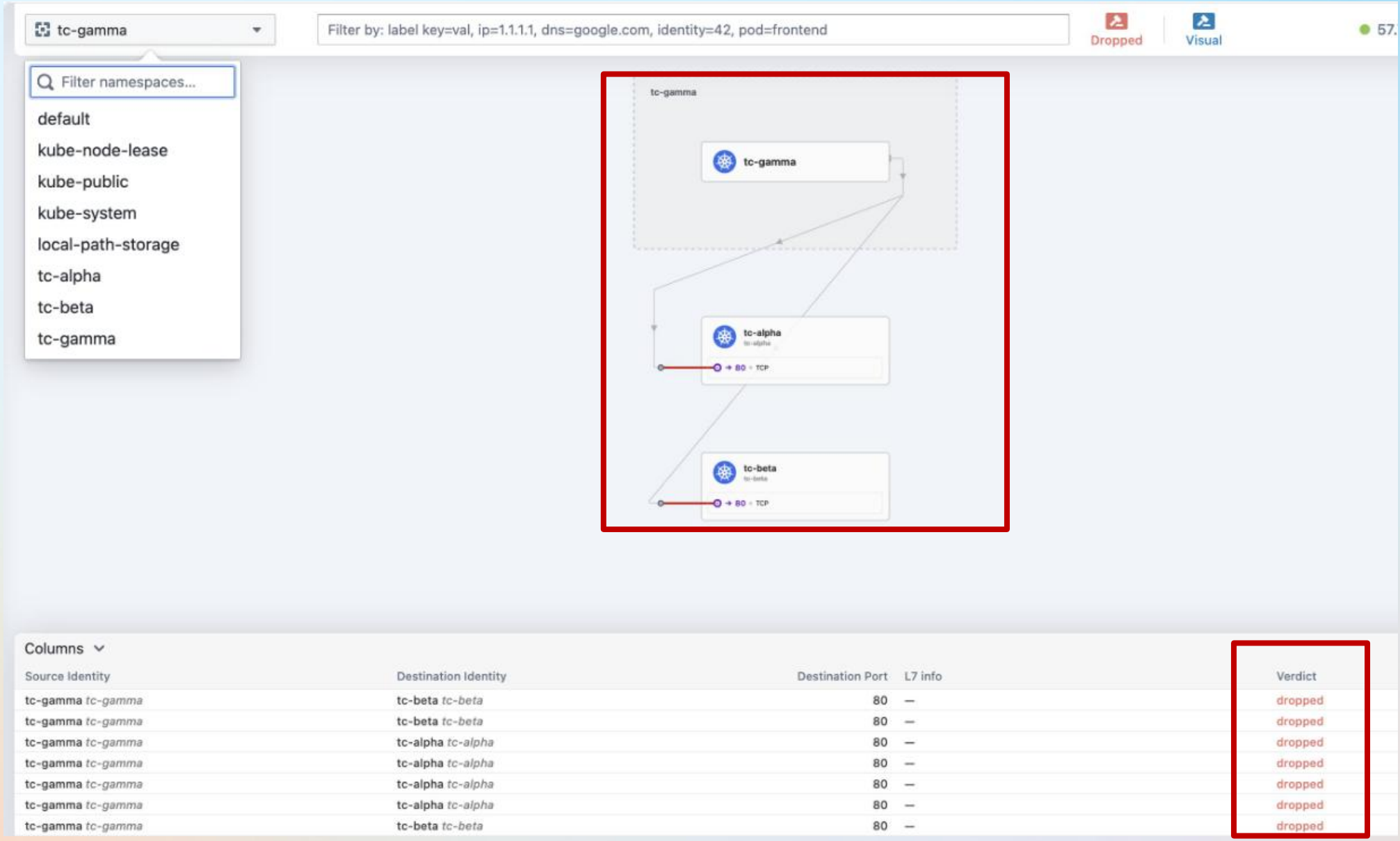
kubectl logs

[INFO] Request incoming...
[INFO] Parsing headers...
[WARN] Latency detected...
[ERROR] 504 Gateway Timeout
[INFO] Retrying connection...
[ERROR] Connection refused...
... (수만 줄의 텍스트)



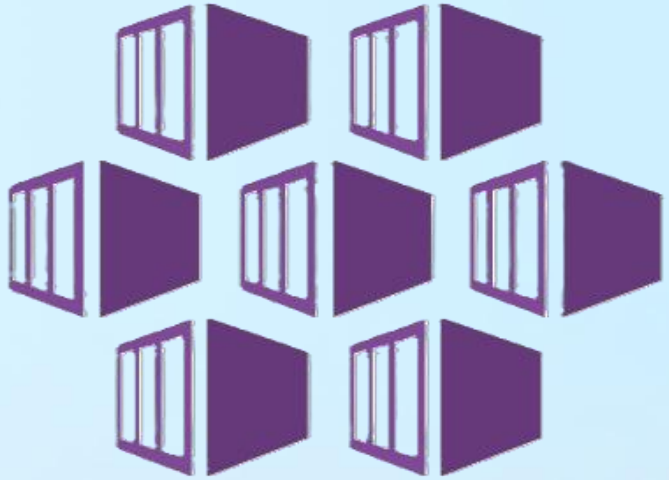

kube-system
Filter by: label key=val, ip=1.1.1.1, dns=google.com, identity=42, pod=frontend
Any verdict
Visual
world
443 TCP
kube-system
hubble-relay
4245 TCP
external-dns
hubble-ui
kube-dns
9153 TCP
prometheus
monitoring
Columns
Source Identity
Destination Identity
Destination Port
L7 info
Verdict
hubble-ui kube-system
hubble-relay kube-system
4245
forwarded
prometheus monitoring
kube-dns kube-system
9153
forwarded

연결이 잘 되는 경우



연결에 문제가 있는 경우(보안 정책에 의해 차단)

운영체제(OS) 심장에 심는 투명 CCTV

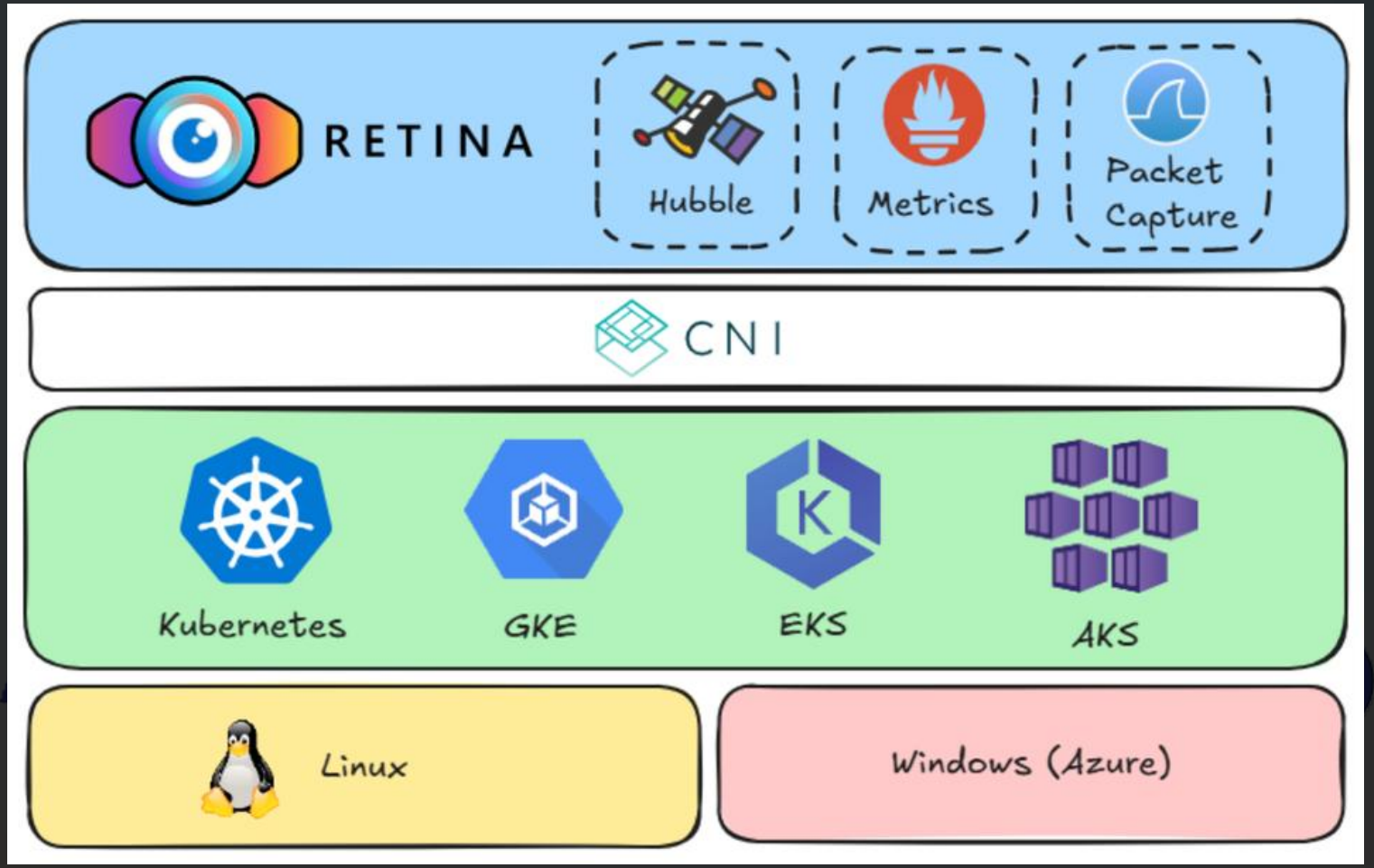


Azure Kubernetes Service (AKS)

에선?

운영체제(OS) 심장에 심는 투명 CCTV

eBPF

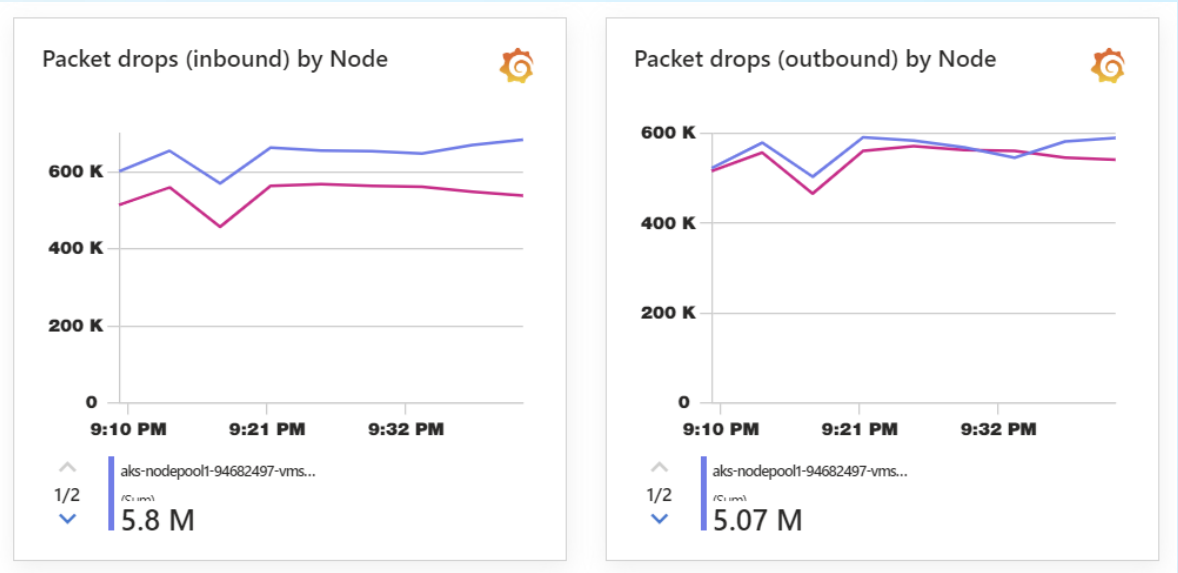


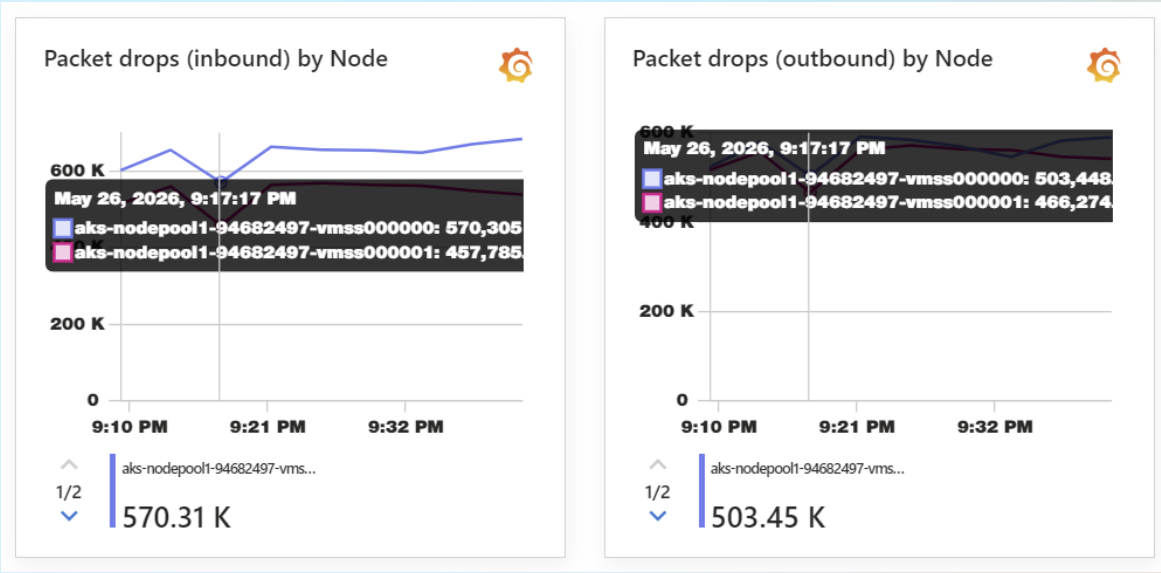
운영체제(OS) 심장에 심는 투명 CCTV


```
minjin [ ~ ]$ az aks update -g myRG -n MyCluster --enable-acns
# ProvisioningControlPlane ..
```

운영체제(OS) 심장에 심는 투명 CCTV

eBPF



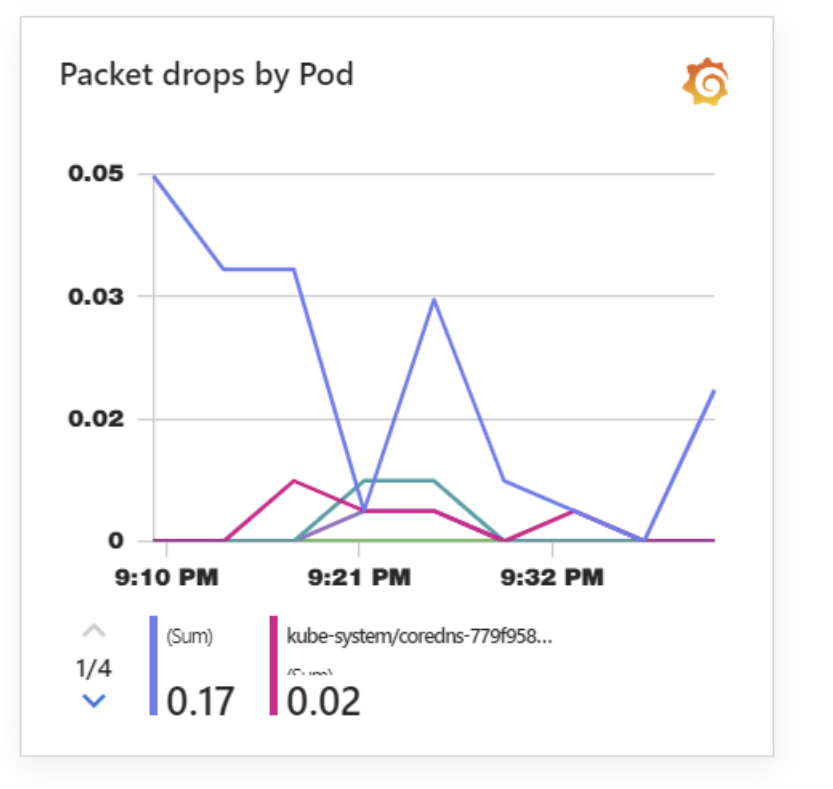


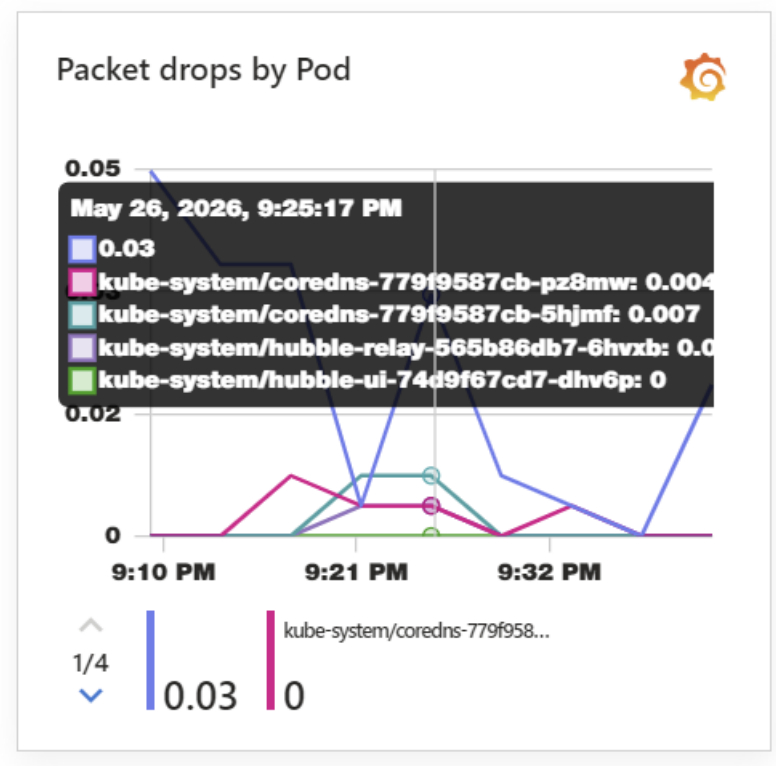
장애 유발 위치를 정확히 지목


Home › Dashboards › node resource uses
Add
Last 1 hour
Namespqce
kube-system
Pod
All
Cluster Metrics
node status
master
Good
worker1
Good
node cpu 사용률
2
1.5
1
0.5
0
23:20 23:25 23:30 23:35 23:40 23:45 23:50 23:55 00:00 00:05 00:10 00:15
master worker1
node memory 사용률
2500000000
2000000000
1500000000
1000000000
23:20 23:25 23:30 23:35 23:40 23:45 23:50 23:55 00:00 00:05 00:10 00:15
worker1 master
node network평균 송/수신 트래픽
20000
10000
0
-10000
-20000
23:20 23:25 23:30 23:35 23:40 23:45 23:50 23:55 00:00 00:05 00:10 00:15
master-tranmit worker1-tranmit master-receive worker1-receive
kube-system Metrics
API Server 응답 시간(5분/SLA 99%)
1 min
All CPU 사용률
0.15
0.1
0.05
0
23:20 23:25 23:30 23:35 23:40 23:45 23:50 23:55 00:00 00:05 00:10 00:15
coredns-5d78c9869d-qfs6f coredns-5d78c9869d-t9qnx etcd-master kube-apiserver-master kube-controller-manager-master kube-proxy-8qrg5 kube-proxy-bvj9f kube-scheduler-master
weave-net-8dphk weave-net-qwqnj
All 메모리 사용량
1250000000
1000000000
750000000
500000000
250000000
0
23:20 23:25 23:30 23:35 23:40 23:45 23:50 23:55 00:00 00:05 00:10 00:15
coredns-5d78c9869d-qfs6f coredns-5d78c9869d-t9qnx etcd-master kube-apiserver-master kube-controller-manager-master kube-proxy-8qrg5 kube-proxy-bvj9f kube-scheduler-master
weave-net-8dphk weave-net-qwqnj
Pod 상태
Failed
0
Pending
0
Running
10
Succeeded
0
Unknown
0

운영체제(OS) 심장에 심는 투명 CCTV

eBPF





장애 유발 위치를 정확히 지목

Cilium Hubble	Microsoft Retina
권장 환경 (CNI) 네트워크 엔진(CNI)을 통째로 교체 및 새로 설계 가능한 조직	**권장 환경 (CNI)** 기존 Azure CNI 서비스 가동을 유지하며 안전하게 도입하려는 조직
핵심 강점 네트워크 정책 제어 및 심층 패킷 레벨 관찰 (가장 정밀한 분석)	**핵심 강점** Azure Monitor 중심의 매끄러운 모니터링 연동 (Azure 생태계 통합)

요약 및 톺아보기

1. eBPF

추가 개발 없이, 운영체제 바닥에서 통신을 관찰하는 기술

2. Cilium Hubble

까만 텍스트 로그를 비전문가도 쉽게 이해할 수 있는 '네트워크 지도'로 바꿔주는 도구

3. Microsoft Retina

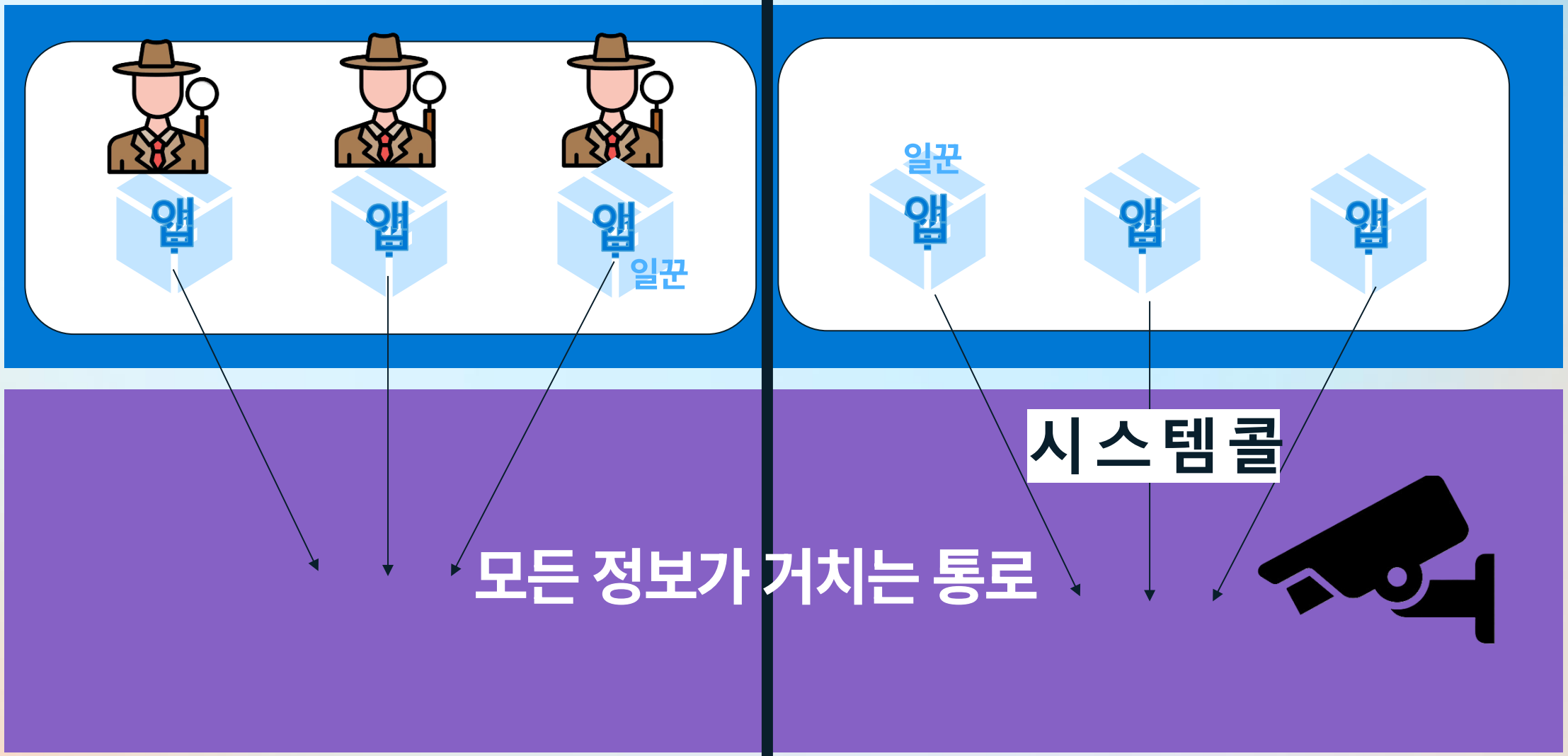
기존 Azure CNI를 건드리지 않고 가시성만 안전하게 추가하는 마이크로소프트 솔루션

기존 방식(사이드카)

eBPF 방식(데몬셋)

유저 모드

커널 모드




billy