Datadog Live Seoul 2024

데이터 안전 수송 작전 From Samsung To Datadog

Heesoo Kim, Sunghwan Kim
Advanced Solution Development Team
Samsung Electronics

Presenter Introduction

Heesoo Kim

Samsung Electronics

SRE, Architecture & Planning

Sunghwan Kim

Samsung Electronics

SRE, Firmware Development

DATADOG

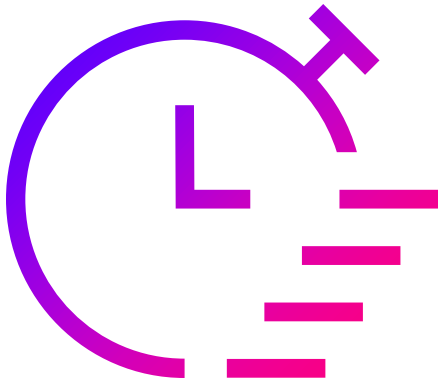
Agenda

Motivation

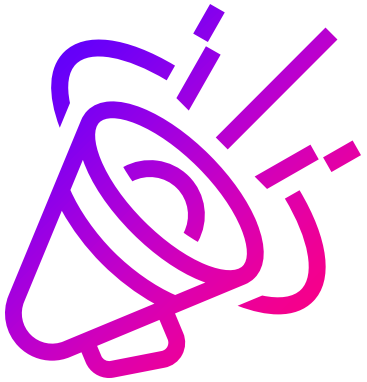
Pain Point

Datadog 도입 동기

Node / Backend Storage
불안정성

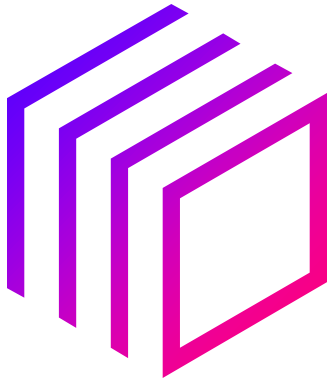


기존 Logging Stack
느린 검색 성능

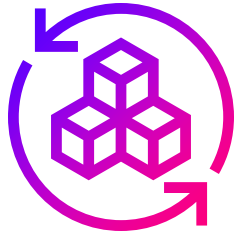


Notification 접근성 제약

Datadog 도입 동기



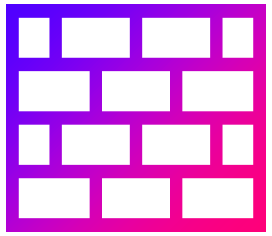
Event / Issue 발생 시 분석의 연계성



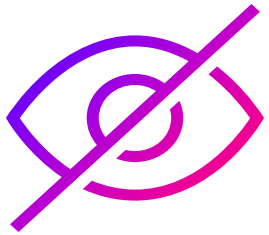
CI 통합 Observability 필요

Constraints / Requirements

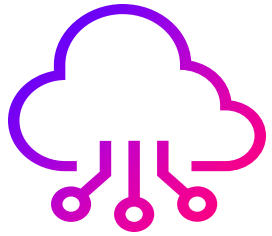
Constraints & Requirements



Air-Gapped Environment



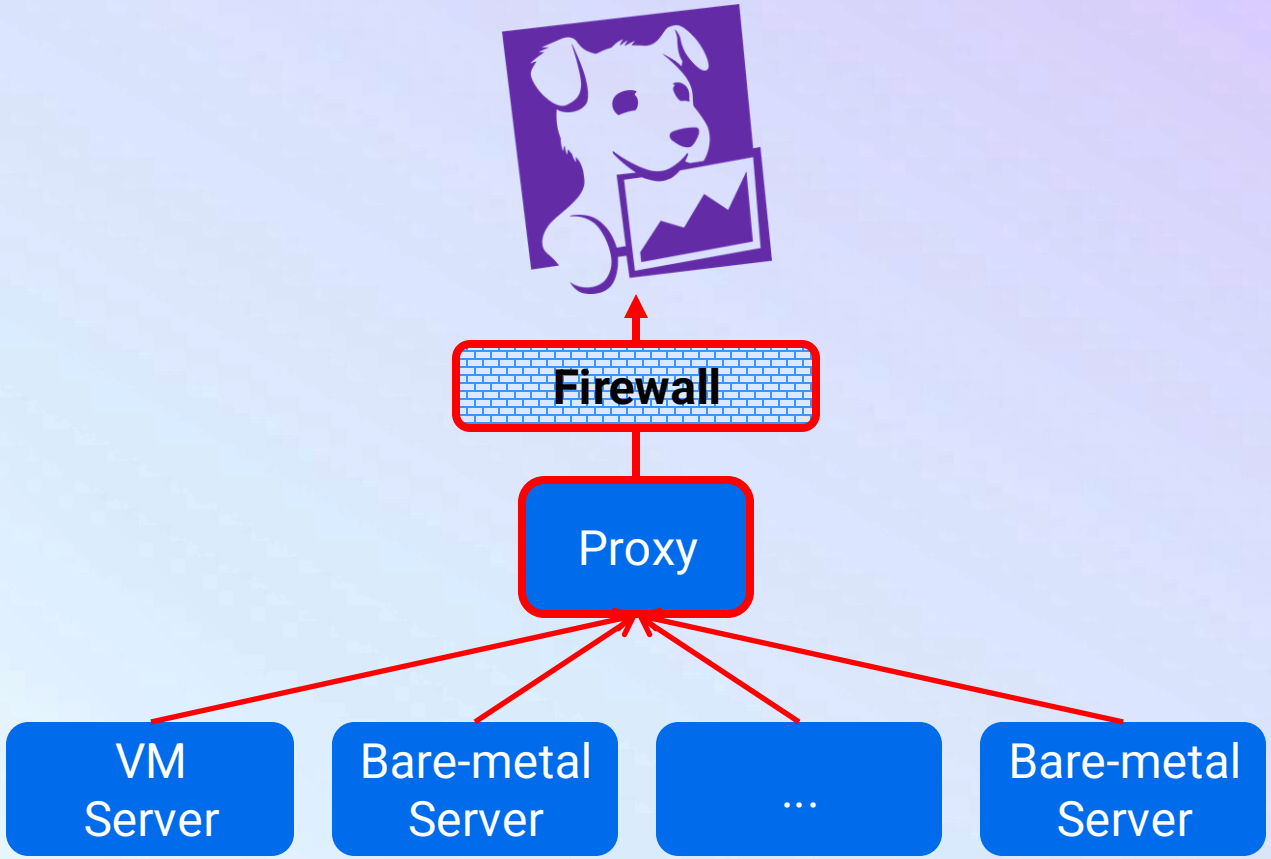
Prevent Internal Data Exposure



Dedicated Route

Proxy Server

Observability Data들을 Proxy Server로 취합 후
해당 서버의 Datadog Service로 전송 예외 처리



Firewall Registration

외부 인터넷 연결을 위해 필요한 결재
업로드 허용 등을 위한 추가 보안성 검토

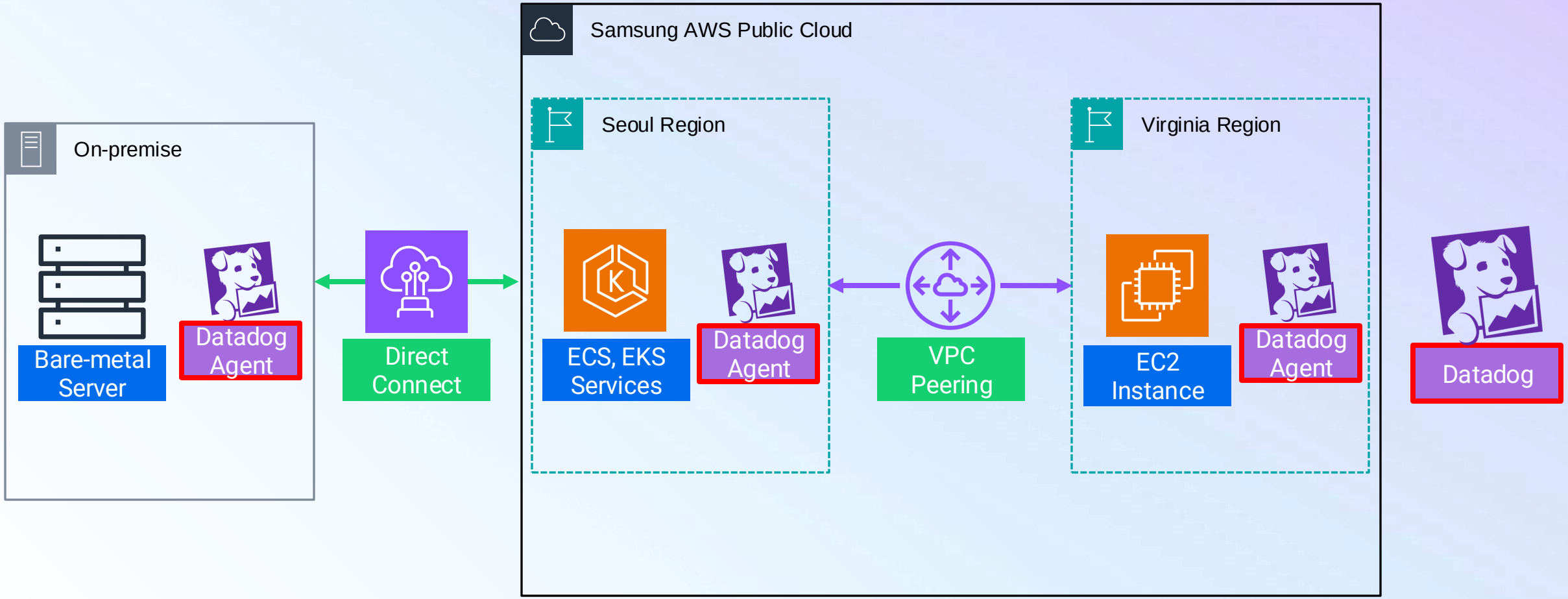
https://www.flaticon.com/free-icon/inspection_17372457

Datadog

Deployment

Public Cloud Architecture

Using Datadog



Complete Quests (Infra)

Deliver Data

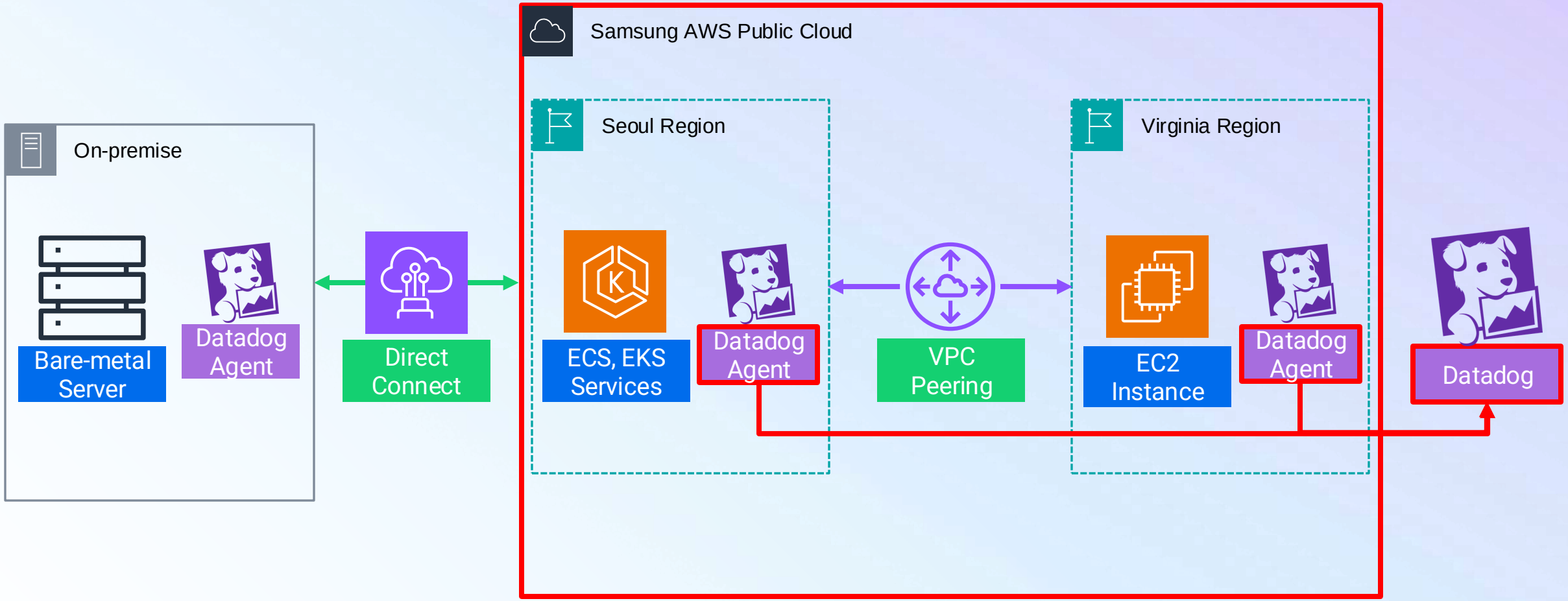
from On-Prem to Public Cloud,

Securely!!

DATADOG

Case 1. From AWS to Datadog

- 가이드 대로. 어렵지 않다!
- AWS PrivateLink를 통해 Datadog에 연결 (datadoghq.com)



Solution: AWS PrivateLink

Datadog VPC Endpoint

Solution: AWS PrivateLink

Datadog VPC Endpoint

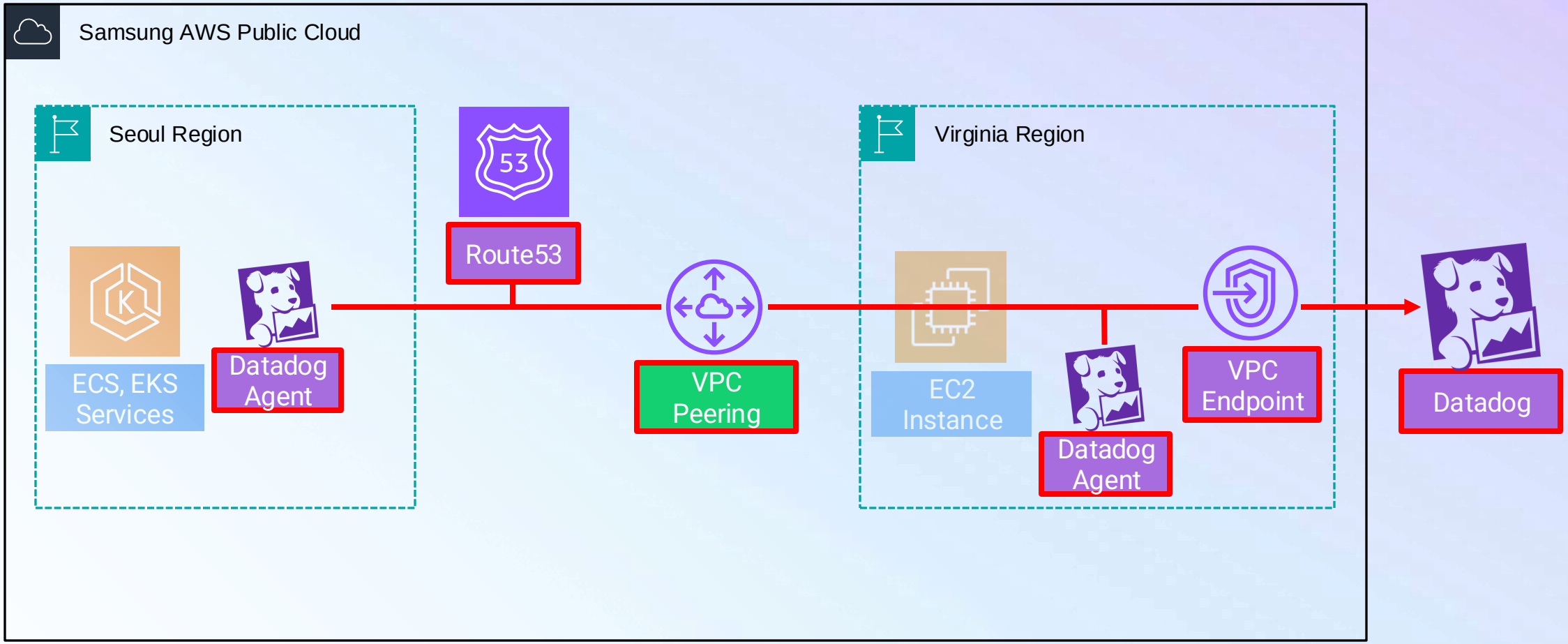
Endpoints (1/20) Info

Search

Name	VPC endpoint ID	VPC ID	Service name	Endpoint type	Status
datadog-prod-API	vpce-0b42cd5ccc14ae334	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Process	vpce-0c13bfaf596cb0fd8	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Containers	vpce-0a23406df2c19fd3a	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Profiling	vpce-05a0c0f543e0f5e0e	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Remote-Config	vpce-050634af0c8be40c3	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Logs-User	vpce-07a0f6818ae12dfe7	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Logs-Agent	vpce-0dc19f2bc5bc374c0	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-DB-Monitoring	vpce-0b5c3111825951a29	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Metrics	vpce-0008754b5e56e809e	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available
datadog-prod-Traces	vpce-0a26f7be8351ea0fe	vpc-006a979624efb5fdf | main-prod	com.amazonaws.vpc...	Interface	Available

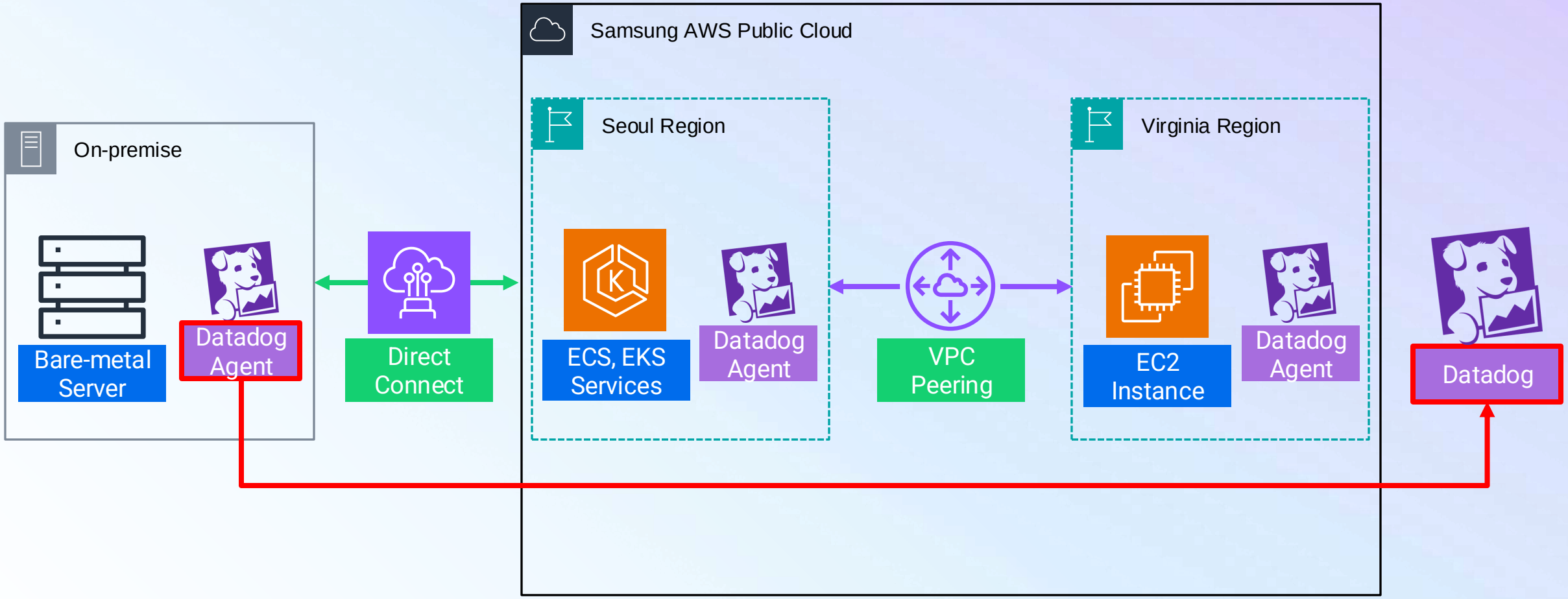
Solution: AWS PrivateLink

Data path using Datadog AWS PrivateLink



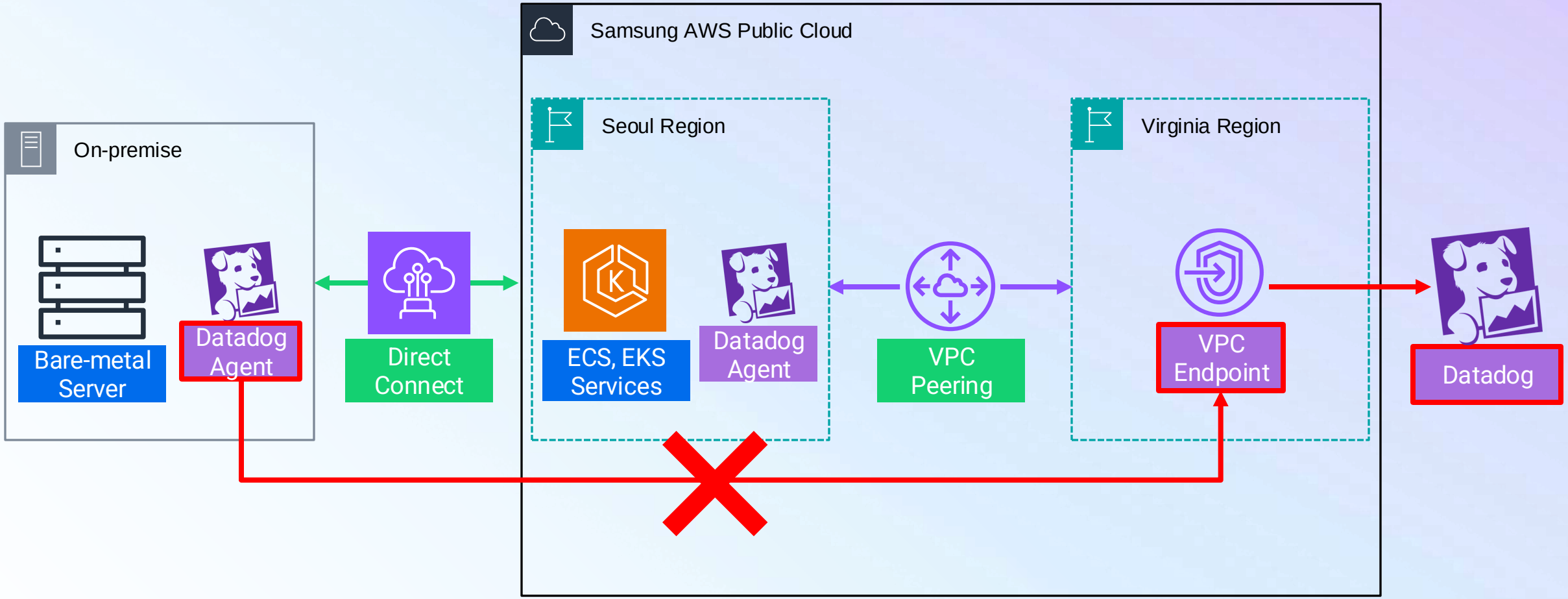
Case 2. From On-premise to Datadog

- 외부 도메인으로 바로 보내는 것은 고려하지 않음 – 추가 보안성 검토 X
- **생각보다 까다로운 제약**



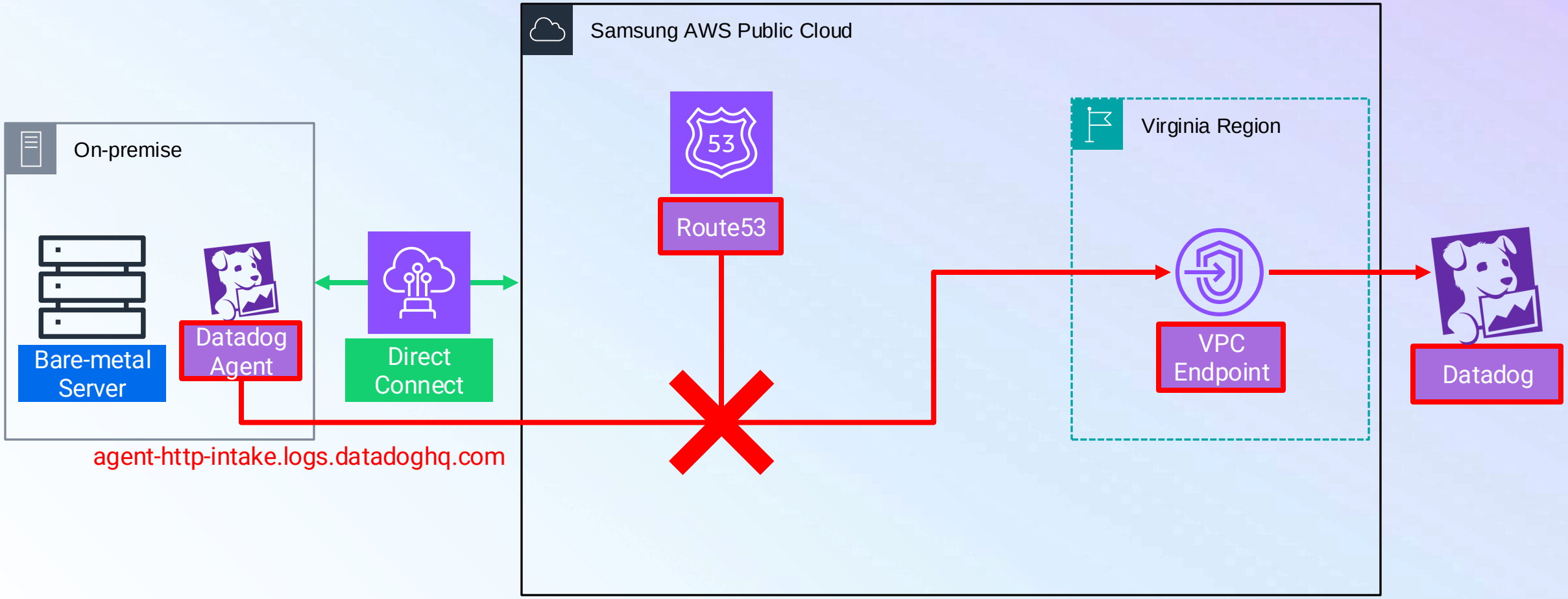
Challenge 1

- 사내에서는 AWS Seoul region으로만 접근 가능함
- Virginia region IP로 직접 접근 불가



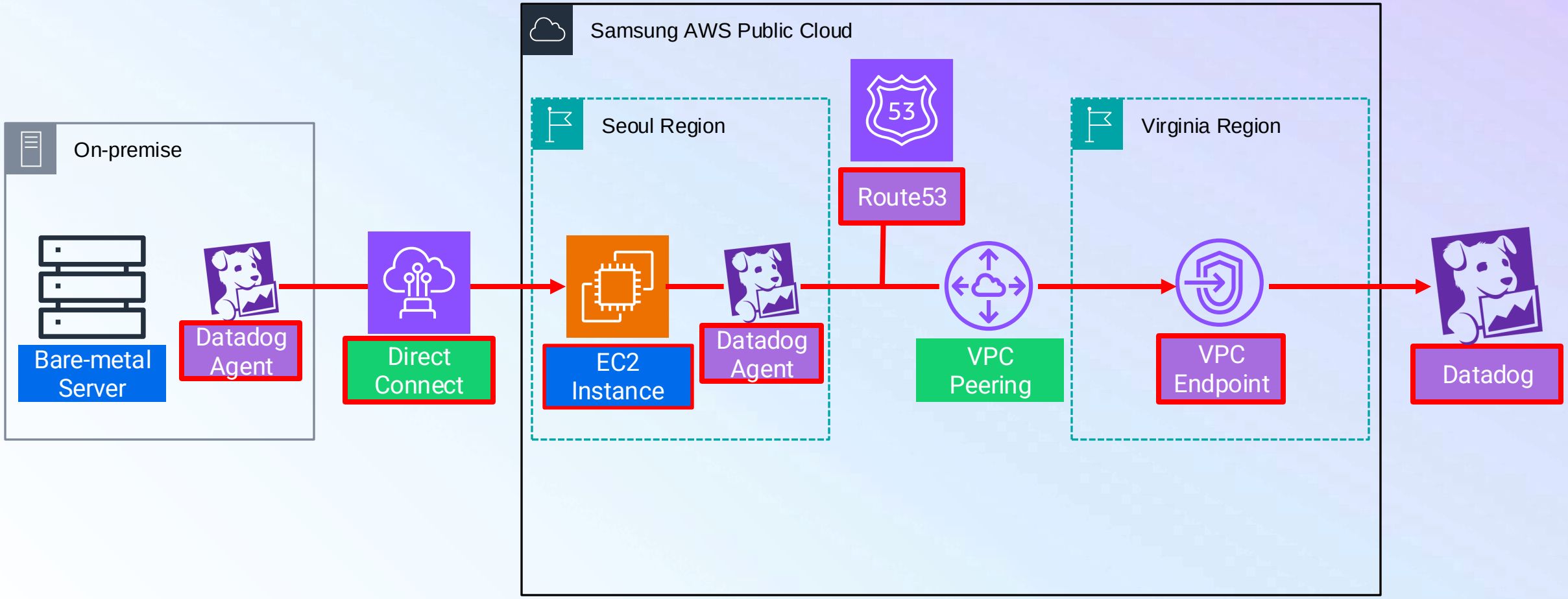
Challenge 2

- 사내에서 AWS를 도메인을 통해 접근하기 위해선 사내 도메인을 신청하여 사용해야 함
- AWS Route53 Domain으로 직접 접근 불가



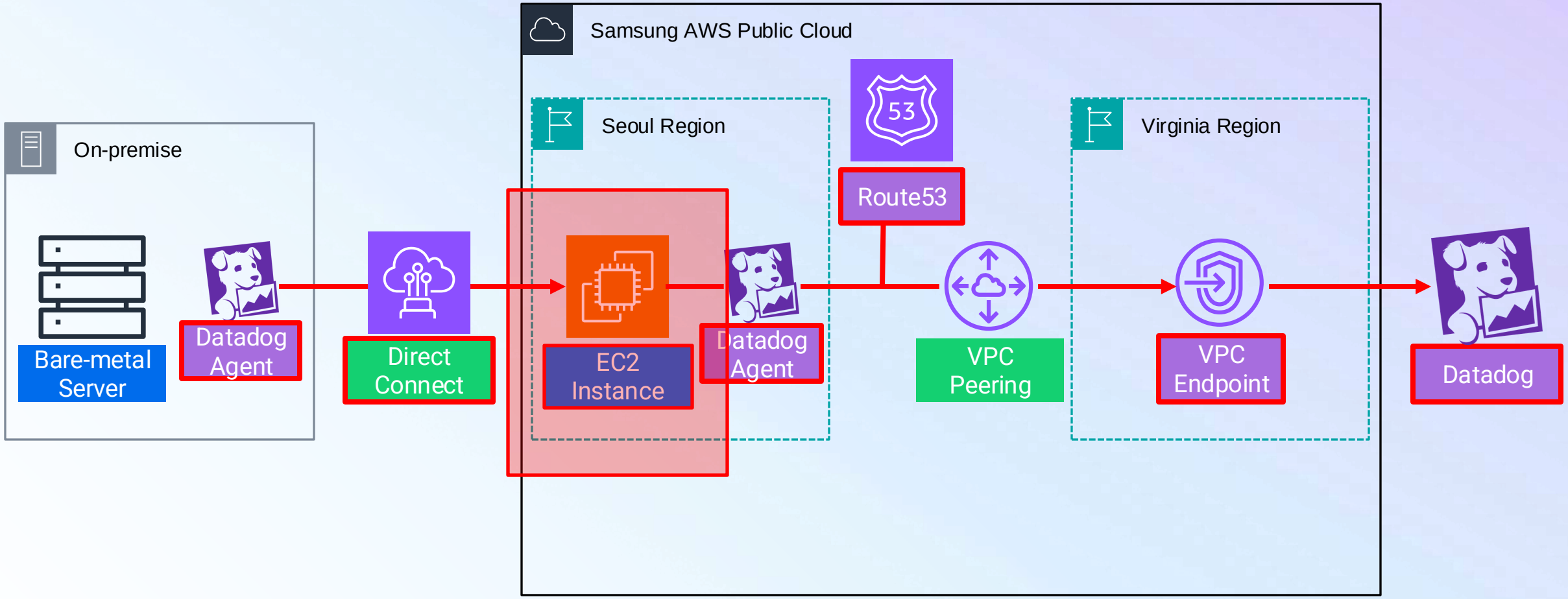
Solution – Proxy Server?

- Seoul region에 loadbalancer 역할의 proxy server EC2 instance 생성
- On-premise aggregation 후 전송



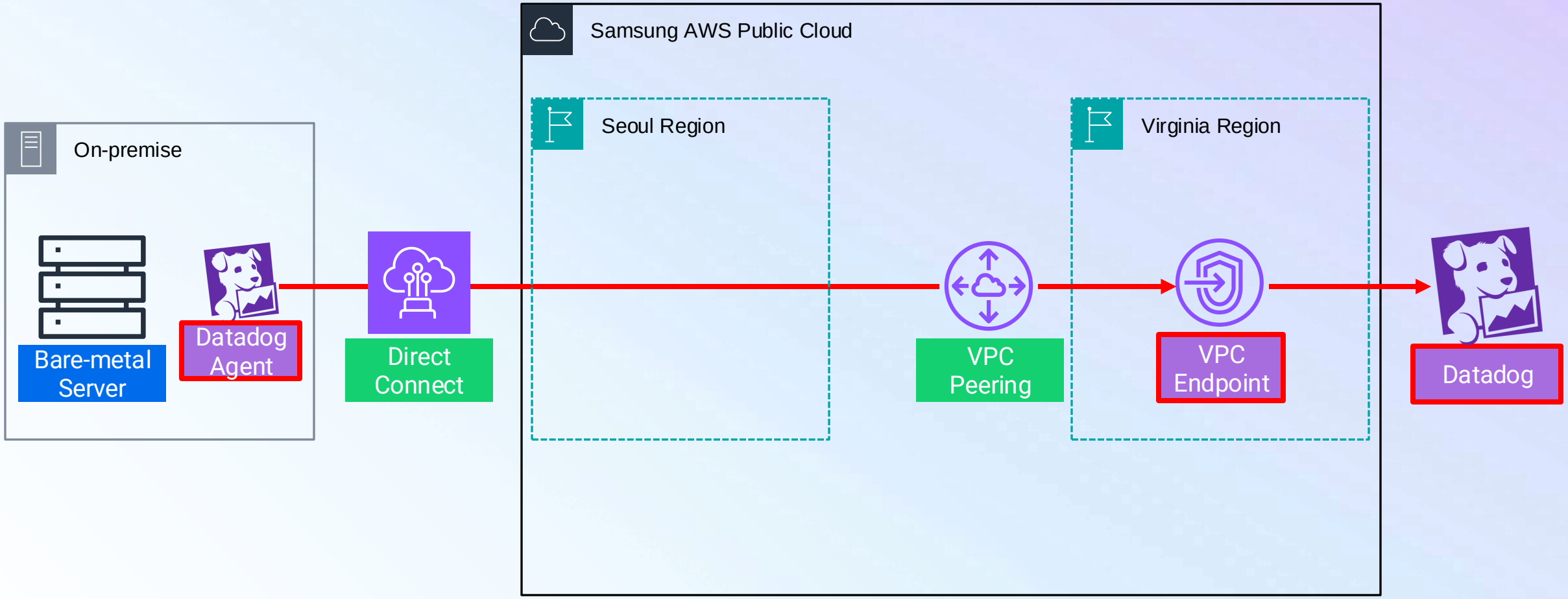
Solution – Proxy Server?

- 복잡한 EC2 내부 Proxy 설정, Routing 설정, 유지 보수 등
- 이게 최선일까?



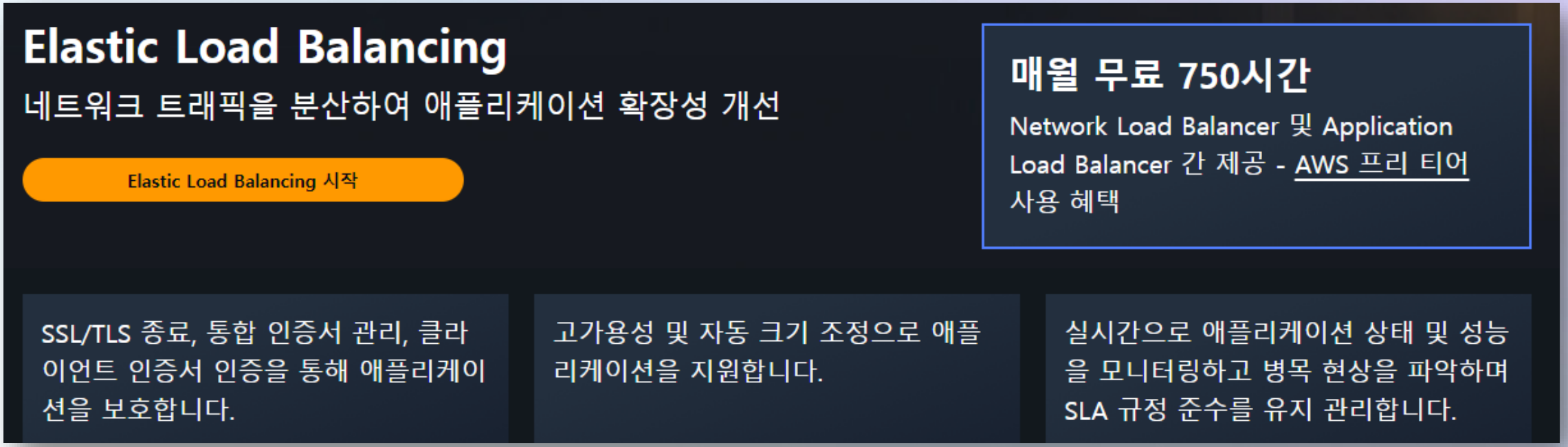
Find Another Solution

- 구성해 놓은 AWS 인프라 Virginia region의 VPC Endpoint로 보내야 한다
- 최대한 기존에 구성된 리소스를 활용하여 적은 노력으로 제약사항을 극복하자



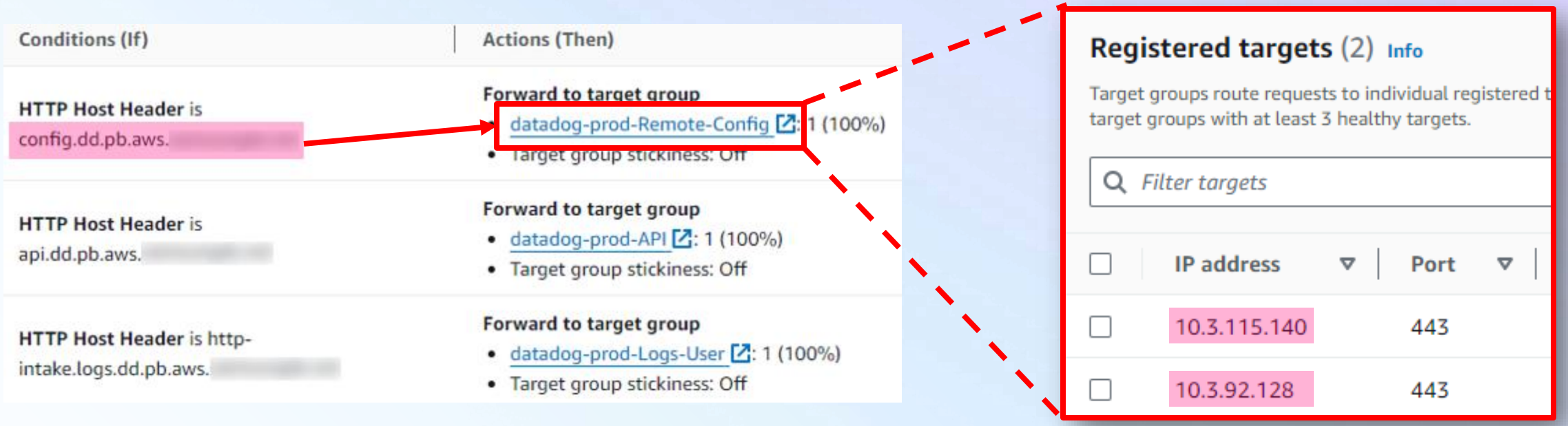
Solution – Elastic Loadbalancer

- 답은 의외로 간단



Elastic Loadbalancer – Application Loadbalancer

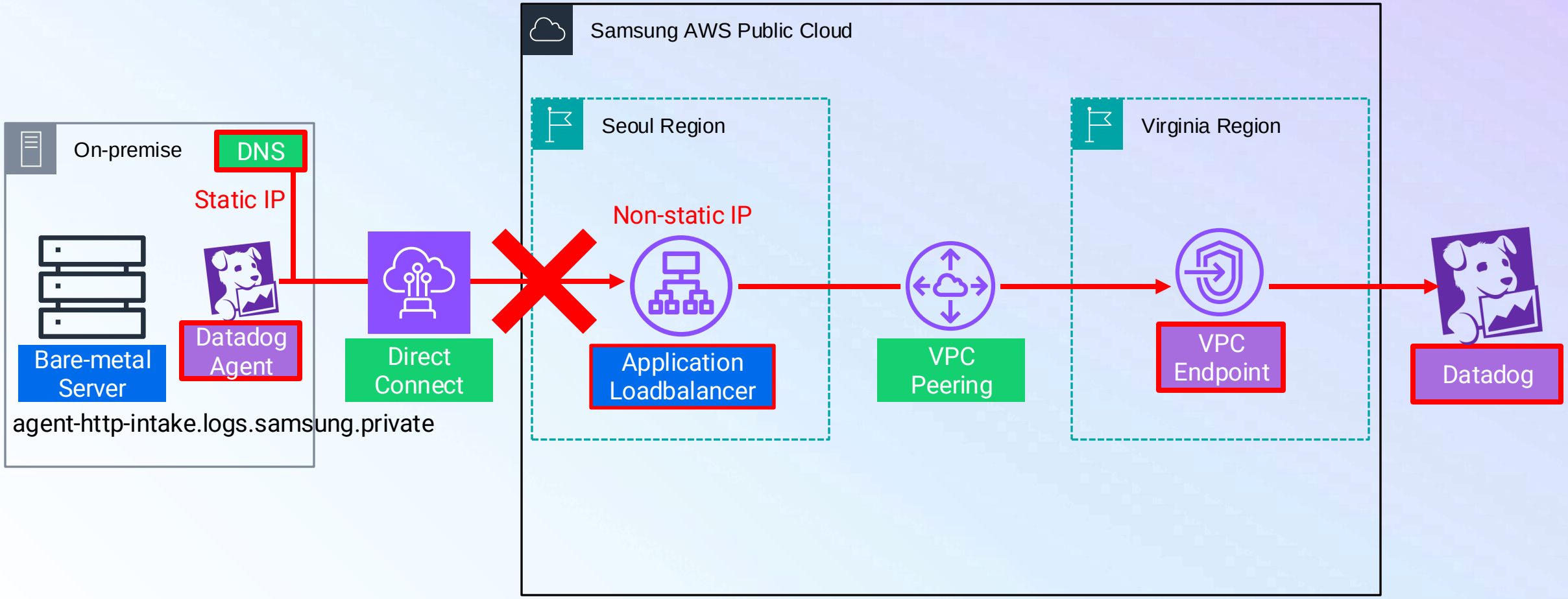
- 기존 구성한 ALB를 통해 Datadog PrivateLink VPC endpoint IP와 연결
- 사내 도메인의 HTTP Host Header로 Service 구분하는 Rule 생성
- 각 도메인 Header에 따라 각 Datadog Service의 VPC endpoint IP로 연결되도록 구성



*.dd.pb.aws.samsung.private → ALB IP로 사내 도메인 신청하면 연결 가능
But!

Challenge 3

- 사내 도메인은 고정된 특정 IP만을 연결할 수 있음
- AWS Application Loadbalancer 로 직접 접근 불가



Solution – Network Loadbalancer

사내에서 도메인을 통해 AWS ALB는 어떻게 접근하지?

1. 어떻게든 ALB의 private IP를 알아낸다.

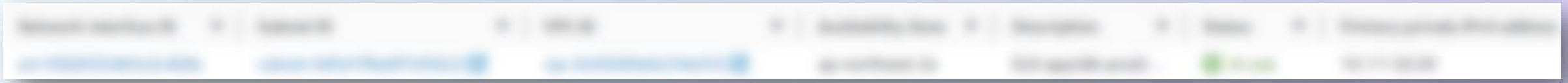
Network interface ID	Subnet ID	VPC ID	Availability Zone	Description	Status	Primary private IPv4 address
eni-03685924b5e2c468e	subnet-0d5d1f9ed97ef2b22	vpc-0c69289afa234a555	ap-northeast-2a	ELB app/alb-prod/...	In-use	10.111.92.93

- 원하는 IP로 설정 불가
- ALB가 배포될 때마다 IP가 변경됨 → 매번 바뀐 IP로 다시 사내 DNS 변경 결재

Solution – Network Loadbalancer

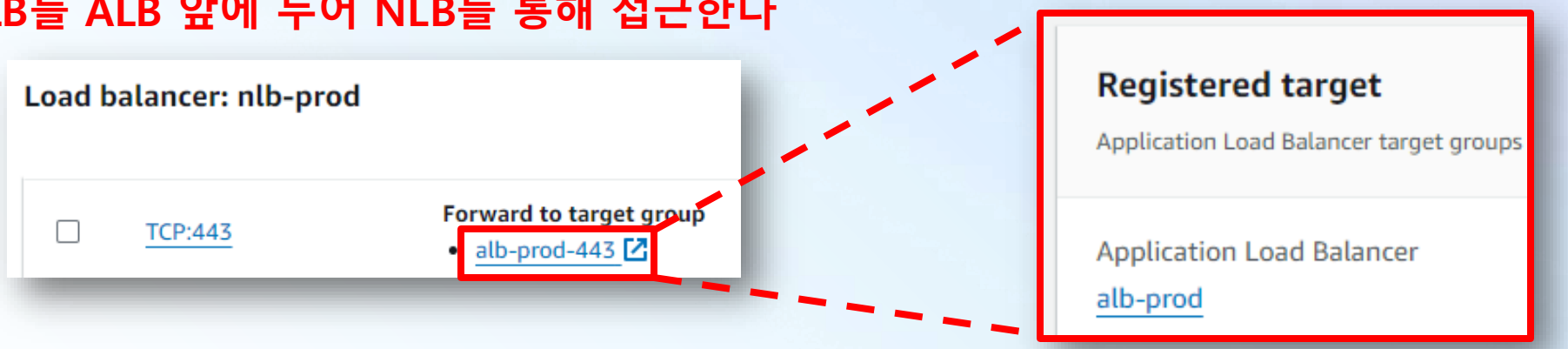
사내에서 도메인을 통해 AWS ALB는 어떻게 접근하지?

1. 어떻게든 ALB의 private IP를 알아낸다.



- 원하는 IP로 설정 불가
- ALB가 배포될 때마다 IP가 변경됨 → 매번 바뀐 IP로 다시 사내 DNS 변경 결재

2. NLB를 ALB 앞에 두어 NLB를 통해 접근한다



- 원하는 IP로 설정 가능 (다시 배포되도 같은 IP)
- NLB는 ALB로 트래픽을 보냄 (ALB 재 배포되도 NLB에서 ALB만 다시 연결만 해주면 됨)

One more thing – Route53 Private Domain

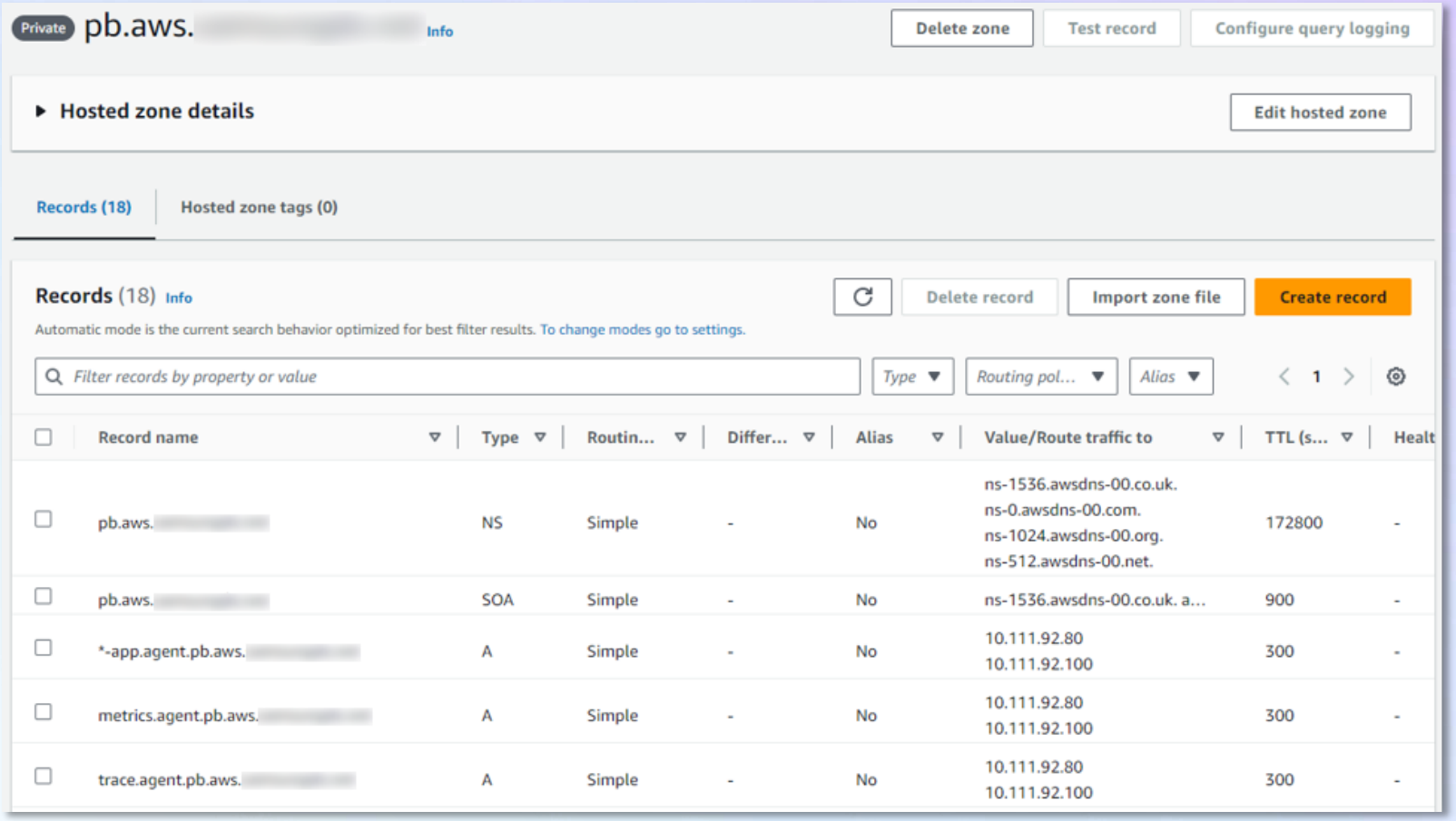
사내, Pubic Cloud 에서 도메인을 통해 AWS NLB는 어떻게 접근하지?

1. 특정 도메인 (*.pb.aws.samsung.private) 에 대해 사내 DNS에서 지정 Route53으로 도메인 질의 전달

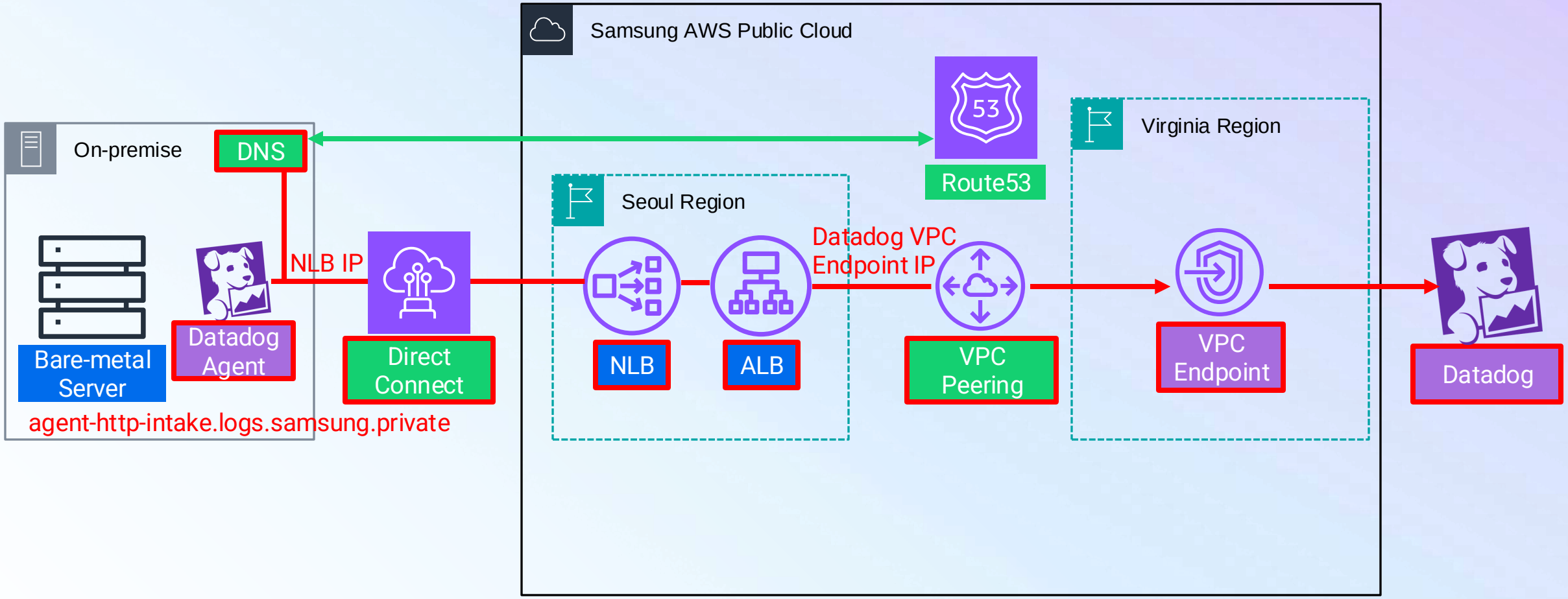
2. 사내에서 접근할 수 있는 AWS 리소스의 도메인을 직접 Route53에서 관리

3. 사내와 Public Cloud 모두 도메인 레코드 조회 가능

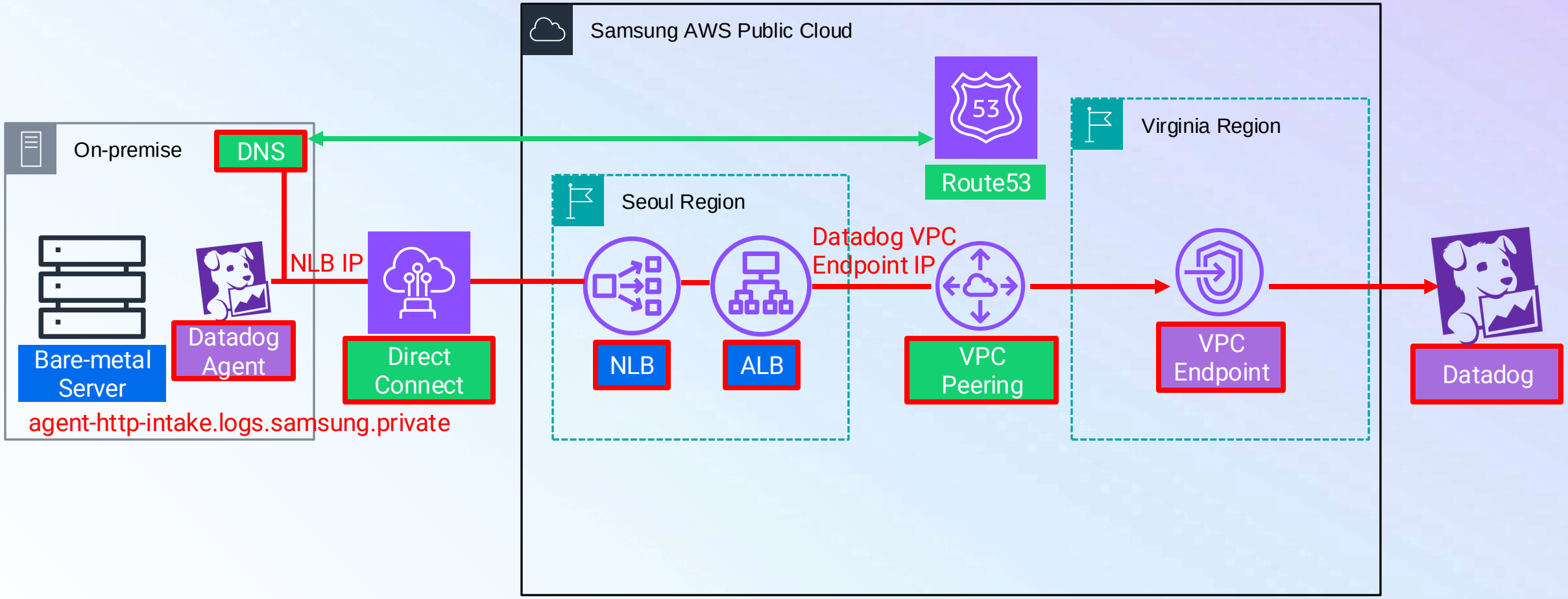
4. 따로 결재 없이 레코드 추가 / 변경 가능, TTL 자체 설정 가능



Observability Data Flow From On-premise to Datadog



Observability Data Flow From On-premise to Datadog



Complete Quests (Agent)

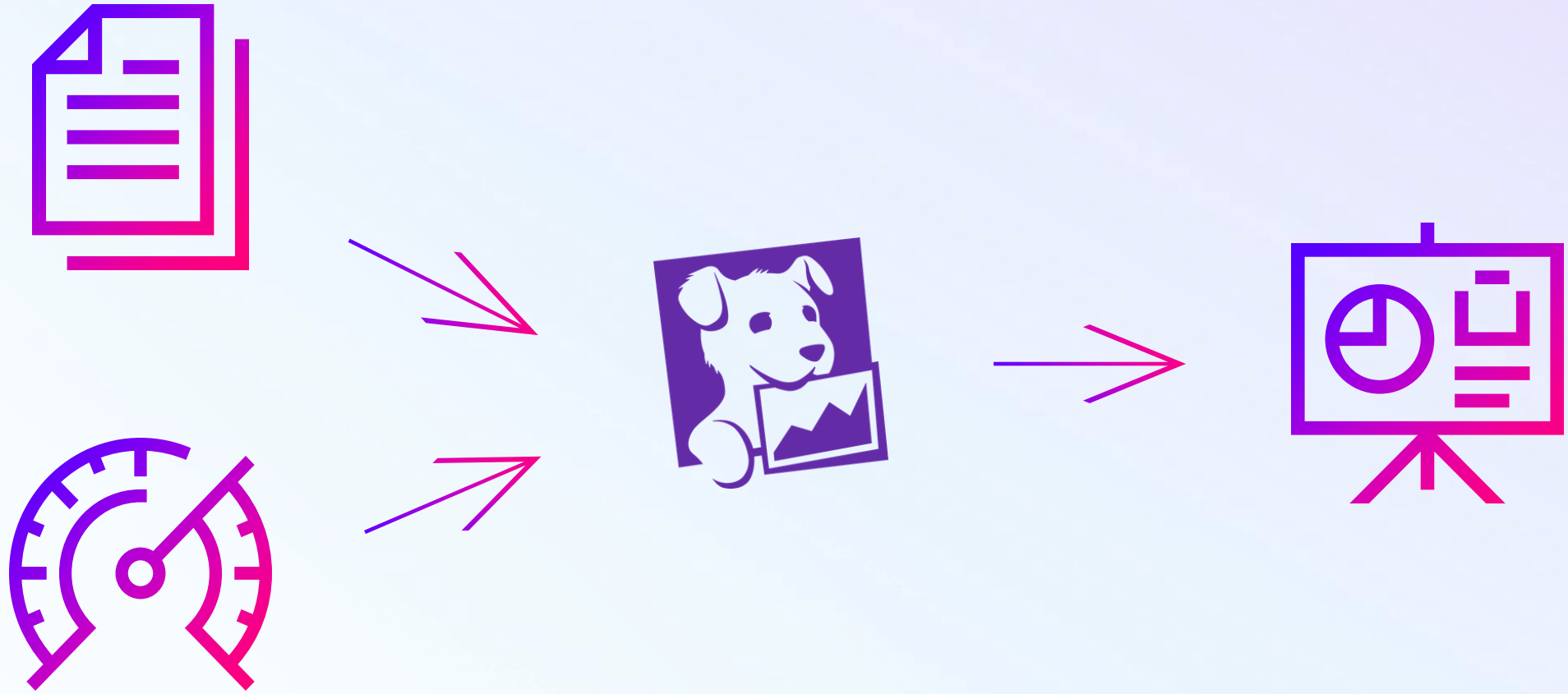
Deliver Data

from On-Prem to Public Cloud,

Securely!!

DATADOG

우리의 목표는?



Datadog Agent에서 접근 시도하는 Subdomain 수집

Datadog Agent가 시도하는 모든 접근을 Private Link로 Cover가 가능할까?

- Custom URL 사용, ALB 사용
  - 각 Subdomain들이 어디로 향해야 할지?

- Datadog 측에서 제공하는 Private Link Endpoint
  - AWS PrivateLink를 통해 Datadog에 연결 (datadoghq.com)
  - Logs, API, Metrics, Containers, Process, Traces, etc: 10

- Datadog Agent의 Log 참조

7-51-0-app.agent
process
config
contlcycle-intake
app
...

DATADOG	PRIVATELINK SERVICE NAME	PRIVATE DNS NAME
Logs (Agent HTTP intake)	com.amazonaws.vpce.us-east-1.vpce-svc-025a56b9187ac1f63	agent-http-intake.logs.datadoghq.com
Logs (User HTTP intake)	com.amazonaws.vpce.us-east-1.vpce-svc-0e36256cb6172439d	http-intake.logs.datadoghq.com
API	com.amazonaws.vpce.us-east-1.vpce-svc-064ea718f8d0ead77	api.datadoghq.com
Metrics	com.amazonaws.vpce.us-east-1.vpce-svc-09a8006e245d1e7b8	metrics.agent.datadoghq.com
Containers	com.amazonaws.vpce.us-east-1.vpce-svc-0ad5fb9e71f85fe99	orchestrator.datadoghq.com
Process	com.amazonaws.vpce.us-east-1.vpce-svc-0ed1f789ac6b0bde1	process.datadoghq.com
Profiling	com.amazonaws.vpce.us-east-1.vpce-svc-022ae36a7b2472029	intake.profile.datadoghq.com
Traces	com.amazonaws.vpce.us-east-1.vpce-svc-0355bb1880dfa09c2	trace.agent.datadoghq.com
Database Monitoring	com.amazonaws.vpce.us-east-1.vpce-svc-0ce70d55ec4af8501	dbm-metrics-intake.datadoghq.com
Remote Configuration	com.amazonaws.vpce.us-east-1.vpce-svc-01f21309e507e3b1d	config.datadoghq.com

Datadog Agent에서 접근 시도하는 Subdomain 수집 (Cont.)

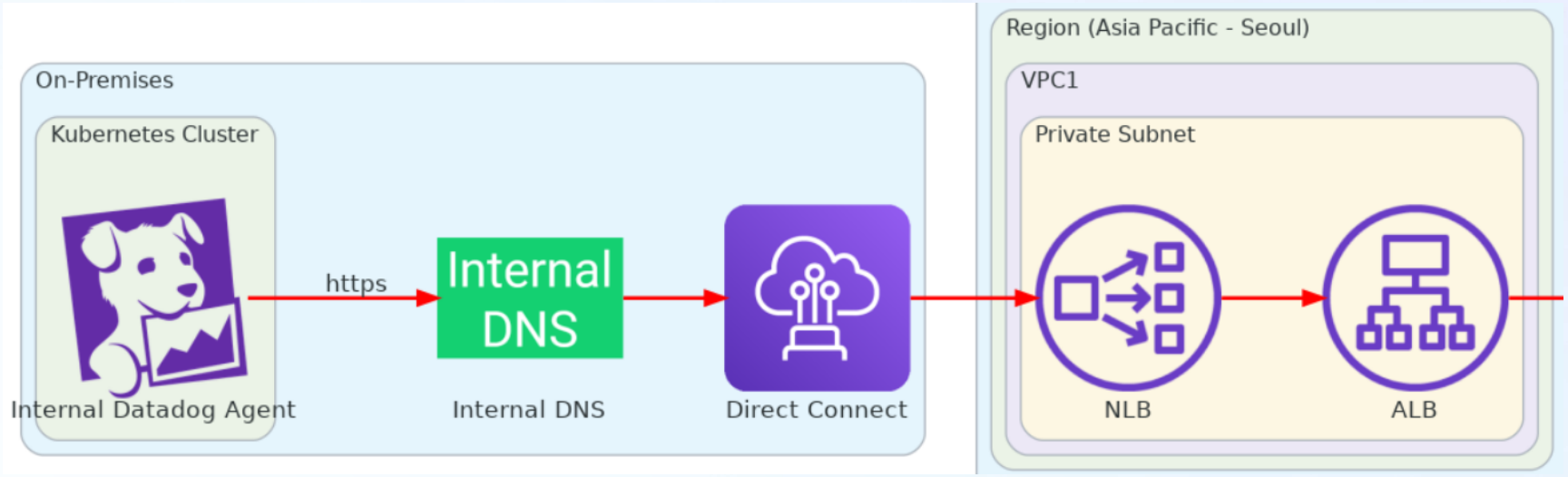
특정 Subdomain들은 Public Internet을 통해야 정상 동작함.

- Private Link를 이용하는 이유와 충돌 발생.
- Public Internet Connection을 필요로 하는 부분, 이용하지 않음.
  - Log, Metric, Infra, Network, Kubernetes Monitoring 등 기본적인 기능 이용에는 지장 없음.
  - 어차피, Air-Gapped 환경이므로, Public Internet Connection 시도는 실패함.
  - ALB Target group에 정의되지 않은 Subdomain은 503 Service Unavailable로 일괄 Fall Through 처리.

Custom URL을 위한 x.509 Certificate 문제

Agent Host와 Proxy가 서로 다른 Network상에 존재

- TLS Encryption 필요
- Datadog Agent Configuration 중 Proxy 관련 설정 Guide
  - 에이전트 프록시 설정 (datadoghq.com)
  - Agent Host와 Proxy가 동일 Network 상에 존재한다는 전제 가정.



Custom URL을 위한 x.509 Certificate 문제 (Cont.)

Datadog Agent가 동작하고 있는 각 Node에 이미 Certificate이 설치되어 있음에도...

- Datadog Agent Log

2024-05-03 01:42:08 UTC | CORE | ERROR | (comp/forwarder/defaultforwarder/worker.go:191 in process) | Error while processing transaction: error while sending transaction, rescheduling it: Post https://app.aws-dev.xxxxxxxxxxx/api/v1/metadata: **tls: failed to verify certificate: x509: certificate signed by unknown authority**
2024-05-03 01:42:08 UTC | CORE | ERROR | (pkg/config/remote/service/service.go:377 in pollOrgStatus) | Could not refresh Remote Config: failed to issue org data request: Get "https://config.aws-dev.xxxxxxxxxxxxxxx/api/v0.1/status": tls: failed to verify certificate: x509: certificate signed by unknown authority

뚫어 봅시다! (Workaround 주의!)

- **Container 내**에 해당 Custom URL을 위한 x.509 Certificate이 설치되어야 함.
  - datadog-operator/docs/configuration.v2alpha1.md at main · DataDog/datadog-operator (github.com)
  - ConfigMap을 통한 Certificate Install.
  - clusterAgent
    - Certificate 위치 후, update-ca-certificates 수행 필요.(/usr/local/share/ca-certificates/...)
    - update-ca-certificates && datadog-cluster-agent start
  - nodeAgent
    - Certificate 위치(/etc/ssl/certs/...)만으로 정상 동작.

Log Transfer Port 변경 문제

보안 정책 상, 80/443 Port만 기본적/제한적으로 사용가능한 On Prem 환경

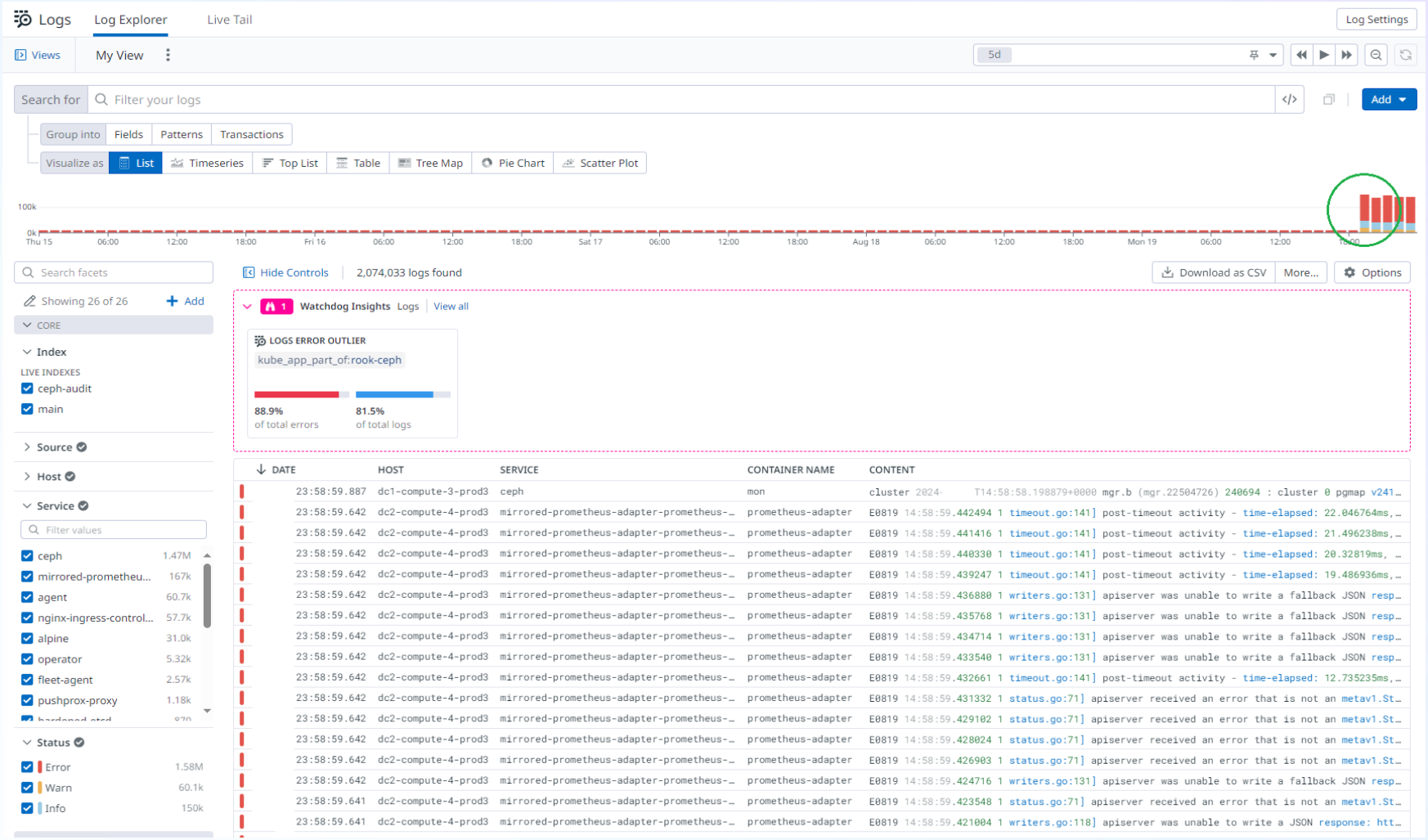
- Datadog Agent Connection 기본 동작
  - Connection Check 시 http 요청에 대한 실패가 발생할 경우, 다른 TCP Port를 Open하여 전송 시도함.

2024-05-03 01:42:08 UTC | CORE | INFO | (pkg/logs/client/http/destination.go:409 in CheckConnectivity) |
Checking HTTP connectivity...
2024-05-03 01:42:08 UTC | CORE | INFO | (pkg/logs/client/http/destination.go:411 in CheckConnectivity) |
Sending HTTP connectivity request to ...
2024-05-03 01:42:08 UTC | CORE | WARN | (pkg/logs/client/http/destination.go:414 in CheckConnectivity)
| **HTTP connectivity failure: Post** ...
2024-05-03 09:09:47 UTC | CORE | INFO | (pkg/logs/client/tcp/connection_manager.go:64 in func1) |
Connecting to the backend: ... :10516, with SSL: 0xc0015b4088

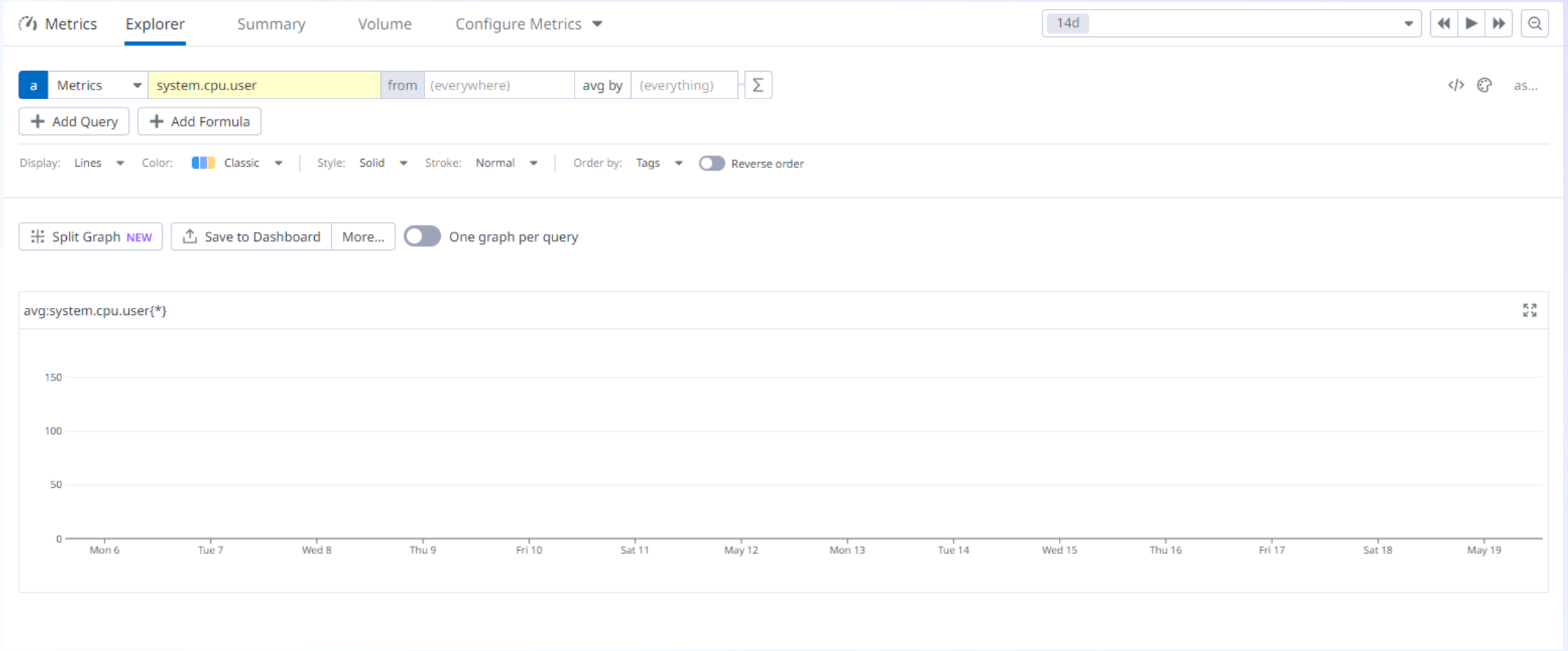
- Connection Check 실패하더라도 항상 80/443 Port로 재시도 하도록, 강제화 함.

```
71      customConfigurations:
72        datadog.yaml:
73          configData: |
74            apm_config:
75              enabled: false
76            logs_enabled: true
77            logs_config:
78              container_collect_all: true
79              force_use_http: true        heesoo84.kim, 3
80            process_config:
81              container_collection:
82                enabled: false
```

오 드디어성공??


Logs
Log Explorer
Live Tail
Log Settings
Views
My View
5d
Search for
Filter your logs
Add
Group into
Fields
Patterns
Transactions
Visualize as
List
Timeseries
Top List
Table
Tree Map
Pie Chart
Scatter Plot
100k
0k
Thu 15
06:00
12:00
18:00
Fri 16
Sat 17
Aug 18
Mon 19
Search facets
Hide Controls
2,074,033 logs found
Download as CSV
More...
Options
Showing 26 of 26
Add
CORE
Index
LIVE INDEXES
ceph-audit
main
Source
Host
Service
Filter values
ceph 1.47M
mirrored-prometheu... 167k
agent 60.7k
nginx-ingress-control... 57.7k
alpine 31.0k
operator 5.32k
fleet-agent 2.57k
pushprox-proxy 1.18k
Status
Error 1.58M
Warn 60.1k
Info 150k
Watchdog Insights
Logs
View all
LOGS ERROR OUTLIER
kube_app_part_of:rook-ceph
88.9%
of total errors
81.5%
of total logs
DATE
HOST
SERVICE
CONTAINER NAME
CONTENT

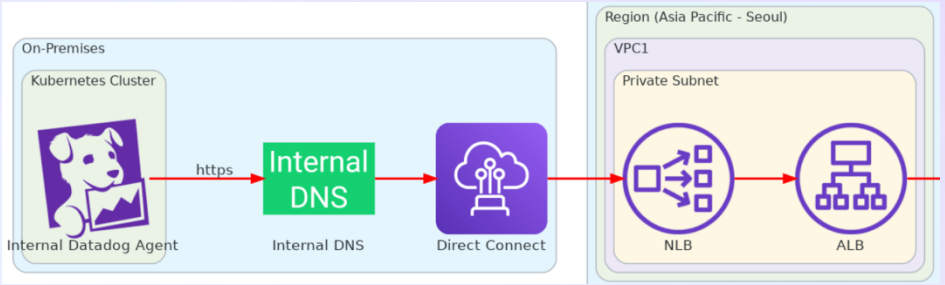
Metric도 한 번 볼까?



Log는 수집이 되는데, Metric은 왜 안되지?

Route53이 아닌 ALB를 사용하고 있었던 점

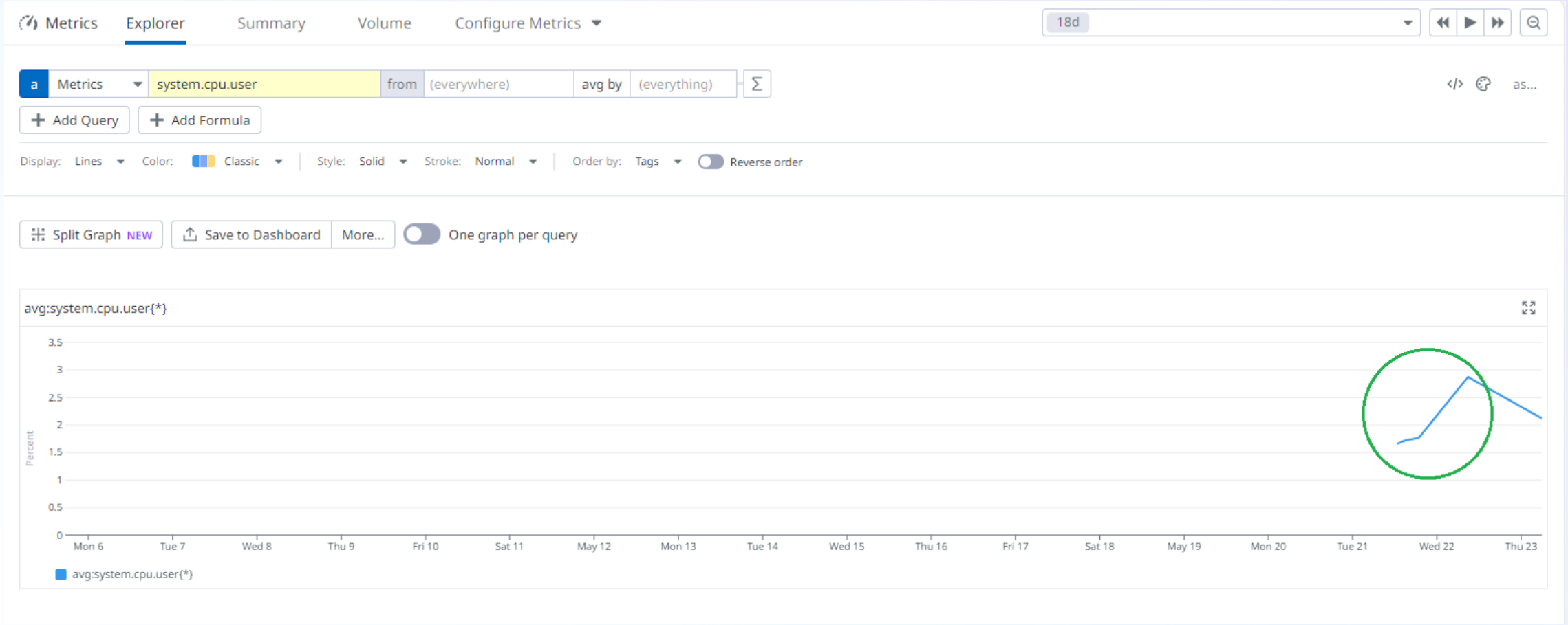
- AWS PrivateLink를 통해 Datadog에 연결 (datadoghq.com)
  - AWS내 Route53 사용에 대한 Guide 제공.
  - Route53이 아닌 NLB – ALB를 사용하게 된 이유?
    - On-Premise에서 Direct Connect를 통해서만 접속가능 -> 정해진 IP 필요
    - ALB 단독으로는 고정 IP 할당이 불가 -> NLB 추가
    - OnPrem -> 사내 DNS -> Direct Connect -> NLB -> ALB -> ...



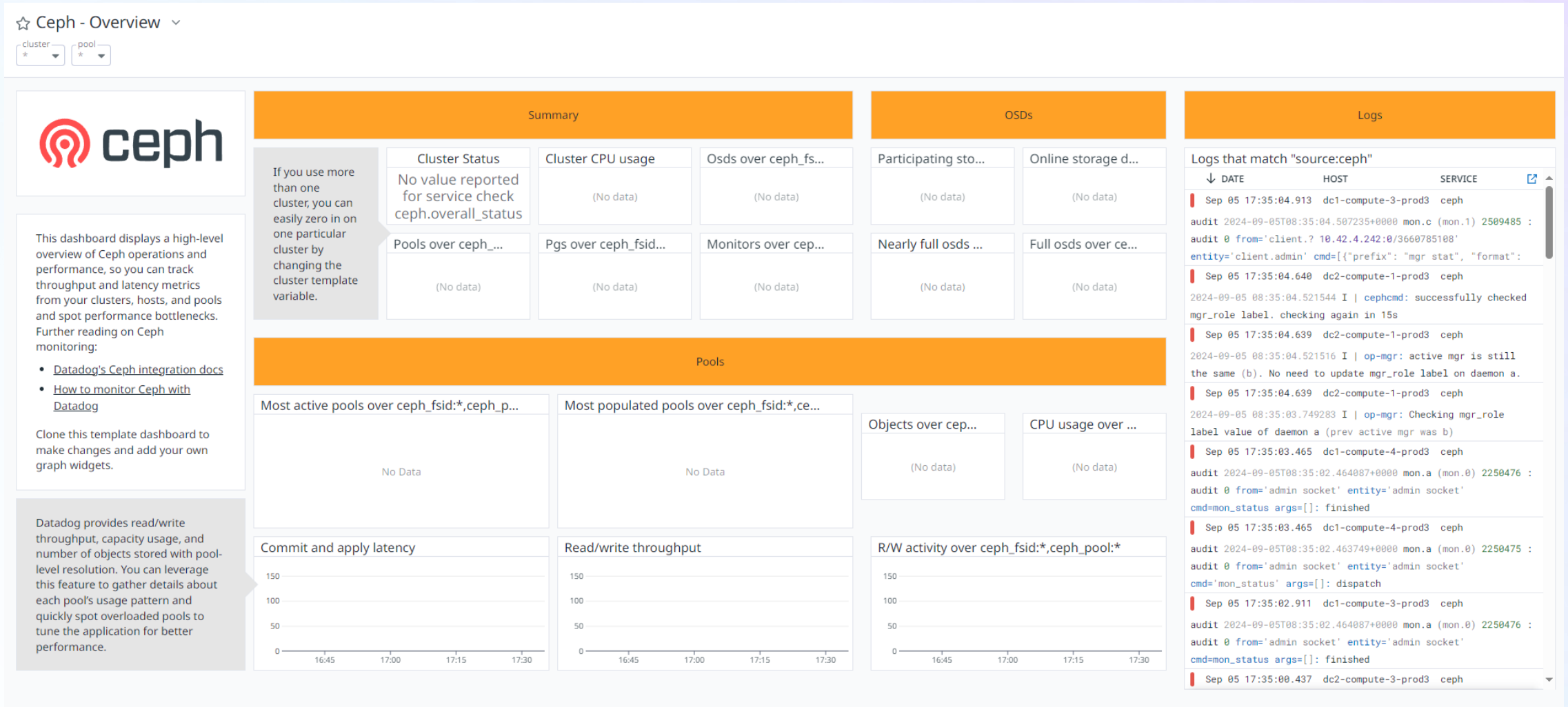
Endpoint에 대한 접근 과정이 모두 동일한데...

- ALB내 Target group 관련, 특정 Subdomain에 대한 Alias 처리가 필요.
  - 명시적인 Private Link Endpoint(Metrics Endpoint) +
    - [version]-app.agent
    - app.agent

드디어!!!???


Metrics
Explorer
Summary
Volume
Configure Metrics
18d
a
Metrics
system.cpu.user
from
(everywhere)
avg by
(everything)
Add Query
Add Formula
Display:
Lines
Color:
Classic
Style:
Solid
Stroke:
Normal
Order by:
Tags
Reverse order
Split Graph
NEW
Save to Dashboard
More...
One graph per query
avg:system.cpu.user{*}
Percent
3.5
3
2.5
2
1.5
1
0.5
0
Mon 6
Tue 7
Wed 8
Thu 9
Fri 10
Sat 11
May 12
Mon 13
Tue 14
Wed 15
Thu 16
Fri 17
Sat 18
May 19
Mon 20
Tue 21
Wed 22
Thu 23
avg:system.cpu.user{*}

끝날 때 까지 끝난 게 아니다



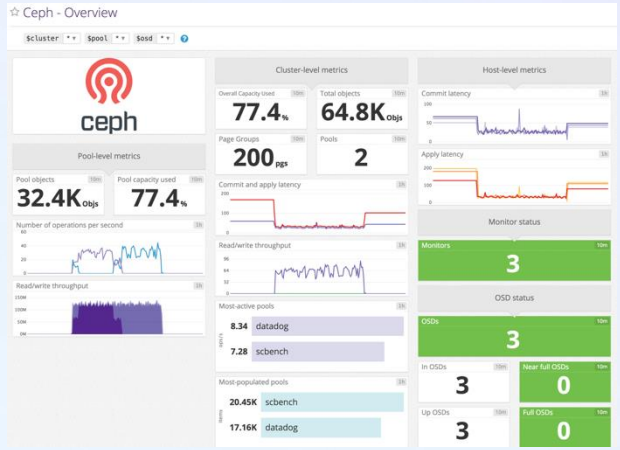
Ceph Integration 적용

Datadog에서 제공하는, 특정 Solution에 대한 Observability Preset 기능

- Ceph (datadoghq.com)
  - Baremetal 기반으로 CephADM 통해서 설치한 Ceph에 대해서만 정상 동작
  - Container native 환경인 K8S 상에 배포 및 관리되고 있는 Ceph (Rook Ceph) 에 대해서는 적용 불가

Alternatives

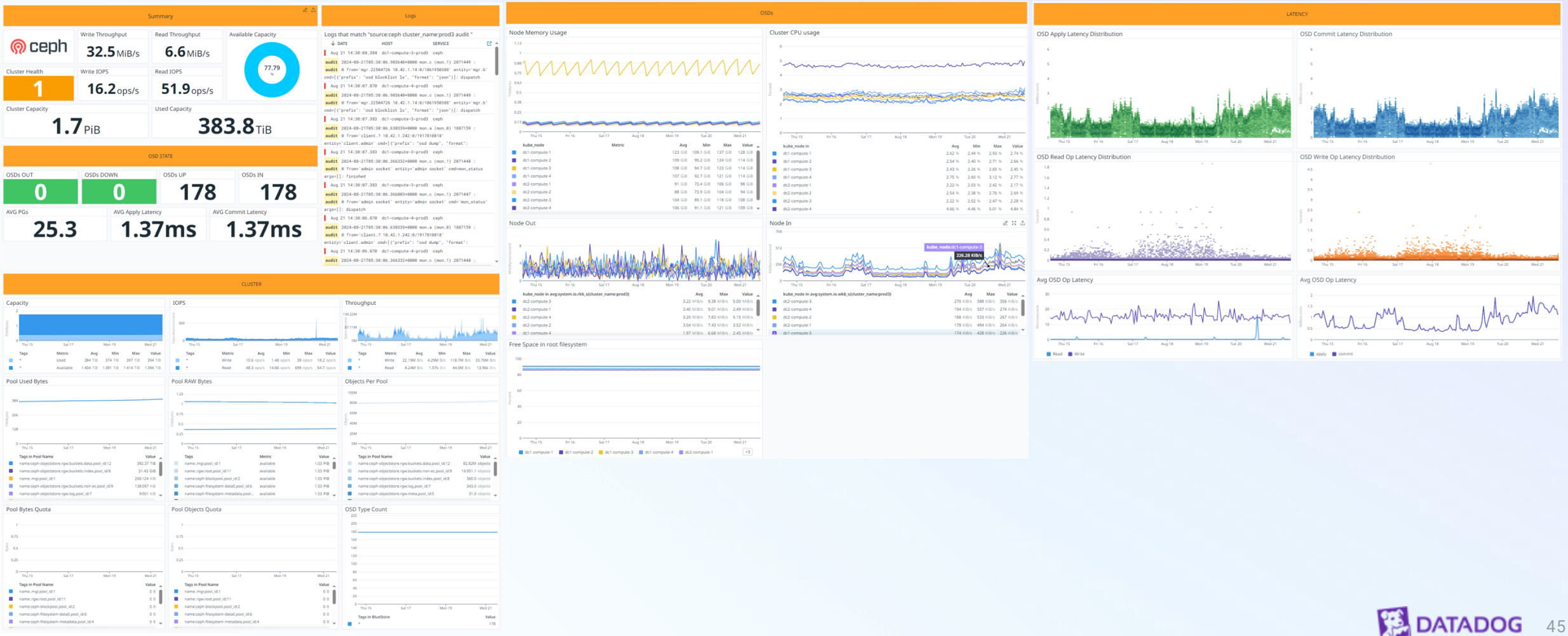
- Sidecar Container를 띄워 각 Ceph 관련 Pod별로 Datadog Agent 배포
  - Agent Container별로 별도 추가 비용 발생
- 필요로 하는 Metric들을 Custom Metric으로 등록하여, 선택적으로 수집 및 사용
  - Custom Metric 개수에 따라(Cardinality 100개당 얼마 형태) 추가 비용 발생
  - Pod용 Annotation을 추가하여, Datadog Auto Discovery 시 명시된 Metric들에 대해서 Custom Metric으로 등록하도록 함.



Storage와 Retention의 가치와 효용을 다시 한 번 느끼게 된 포인트.

Ceph Integration 적용 (Cont.)

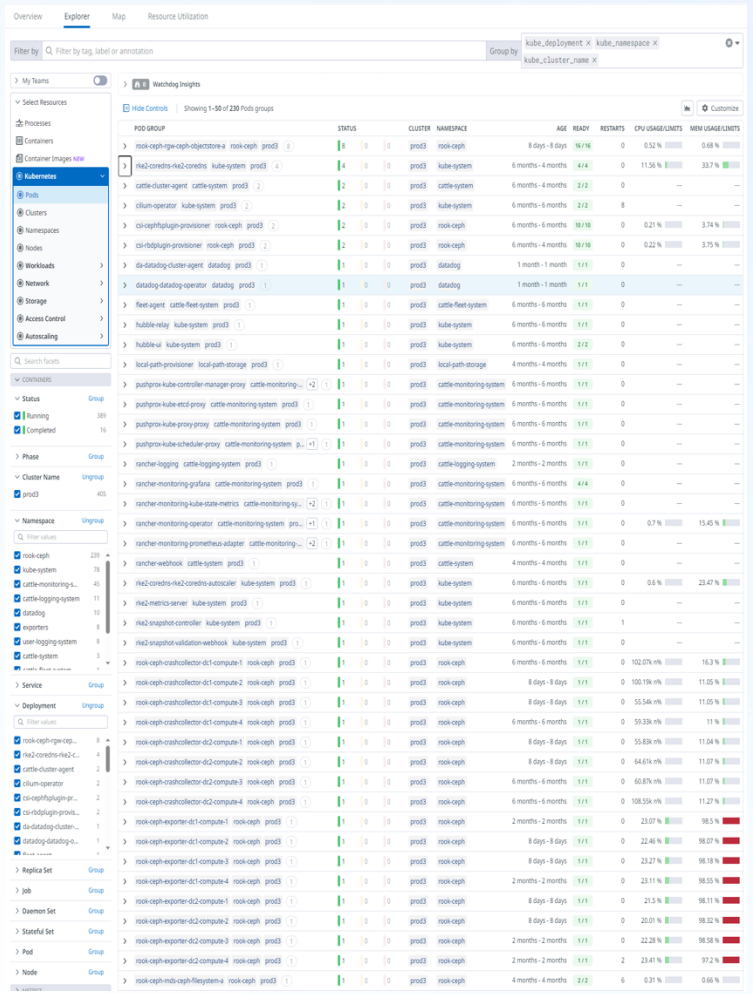
자체 Dashboard 작성 및 사용



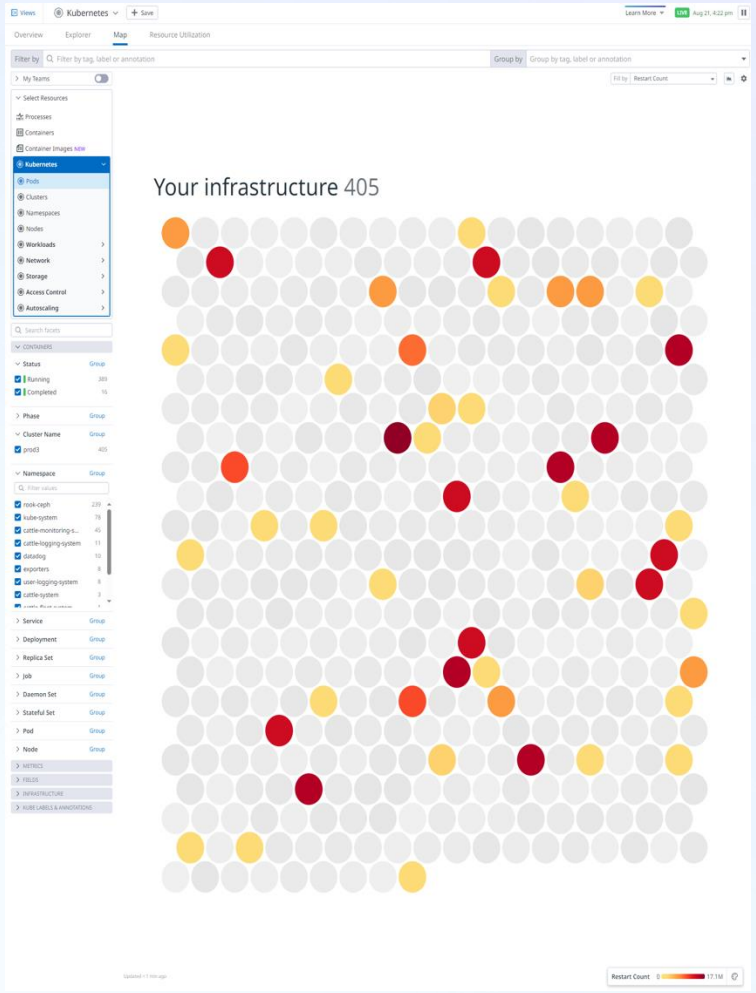
Useful Cases

Kubernetes Resource 확인을 위한 다양한 View 들

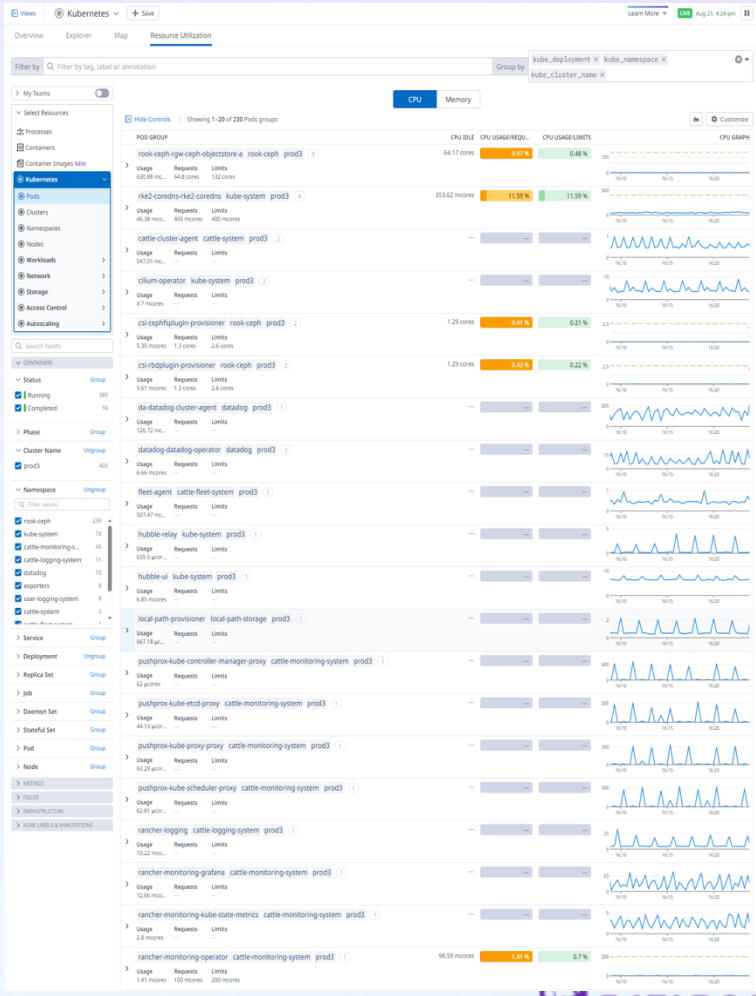
Kubernetes Explorer



Kubernetes Map



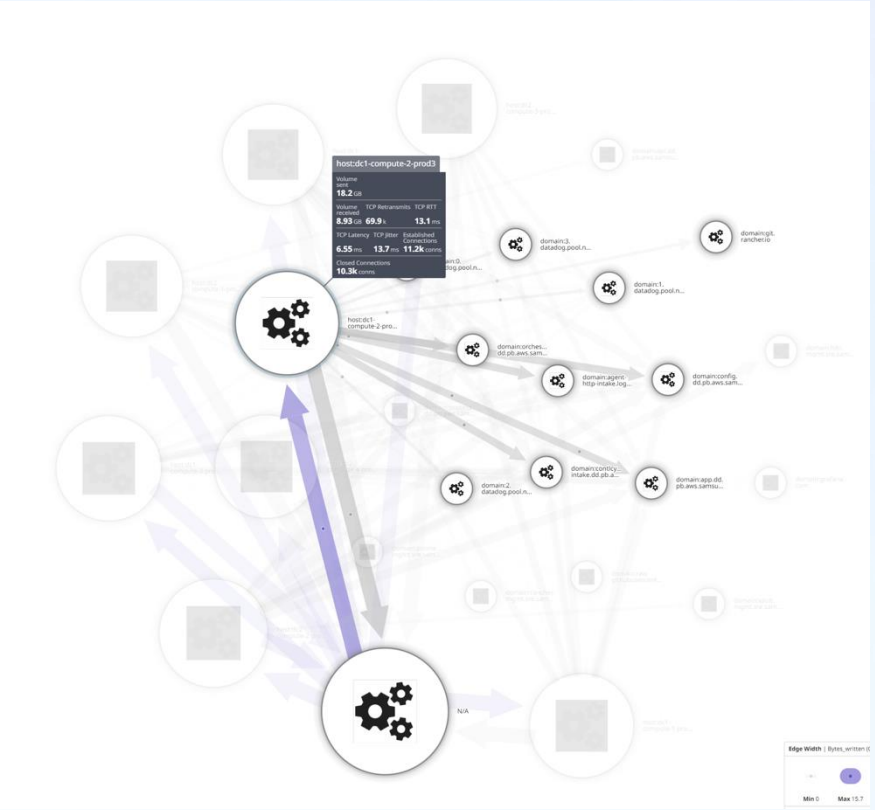
Resource Utilization

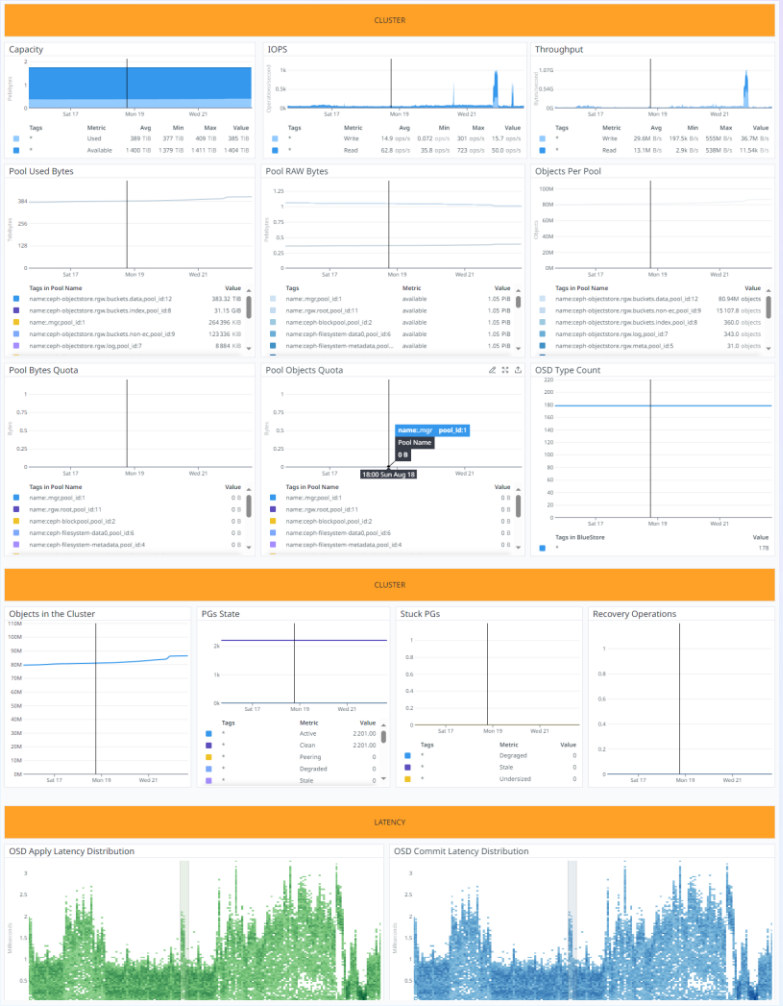


특정 시점에 대한 병렬 분석

특정 포인트에 발생한 이벤트들에 대한 분석 연결성 탁월

- Log -> Network -> Metric -> What ever?

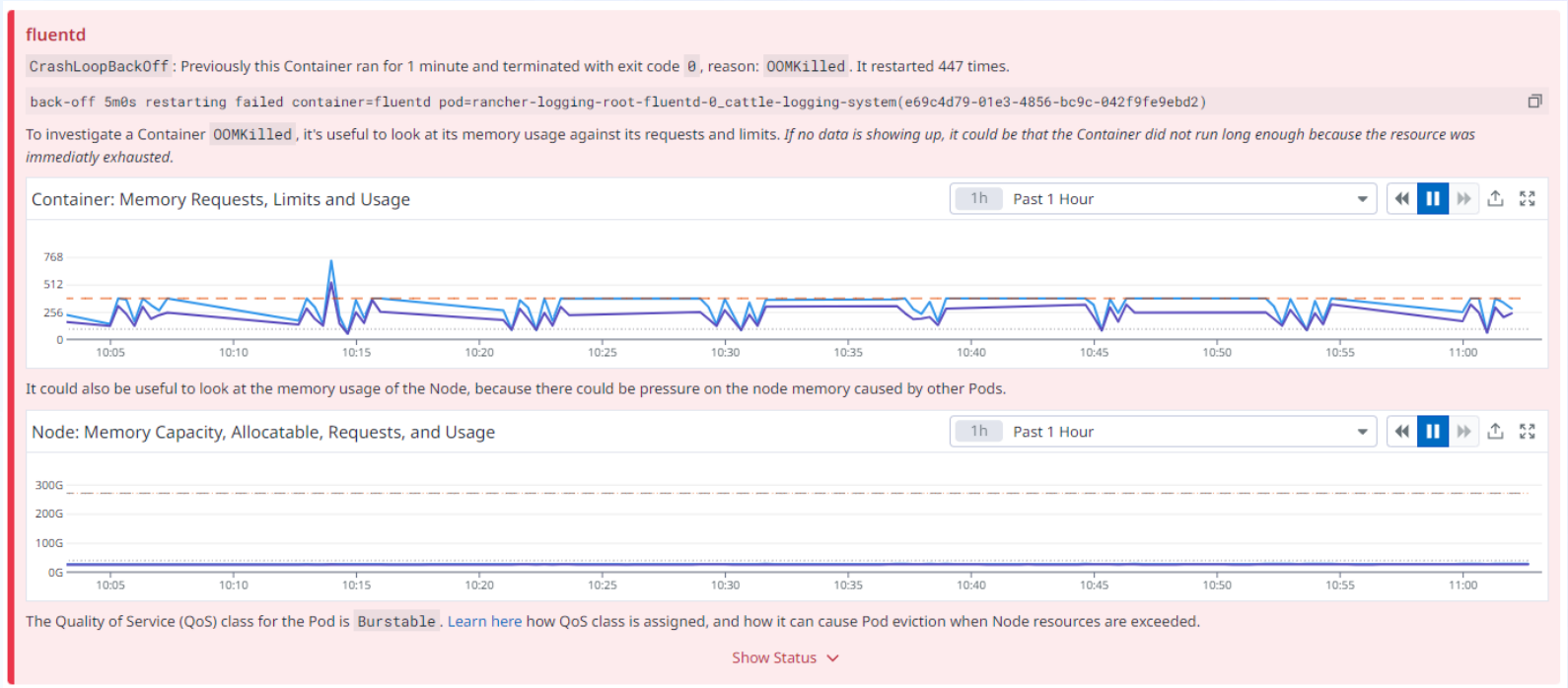




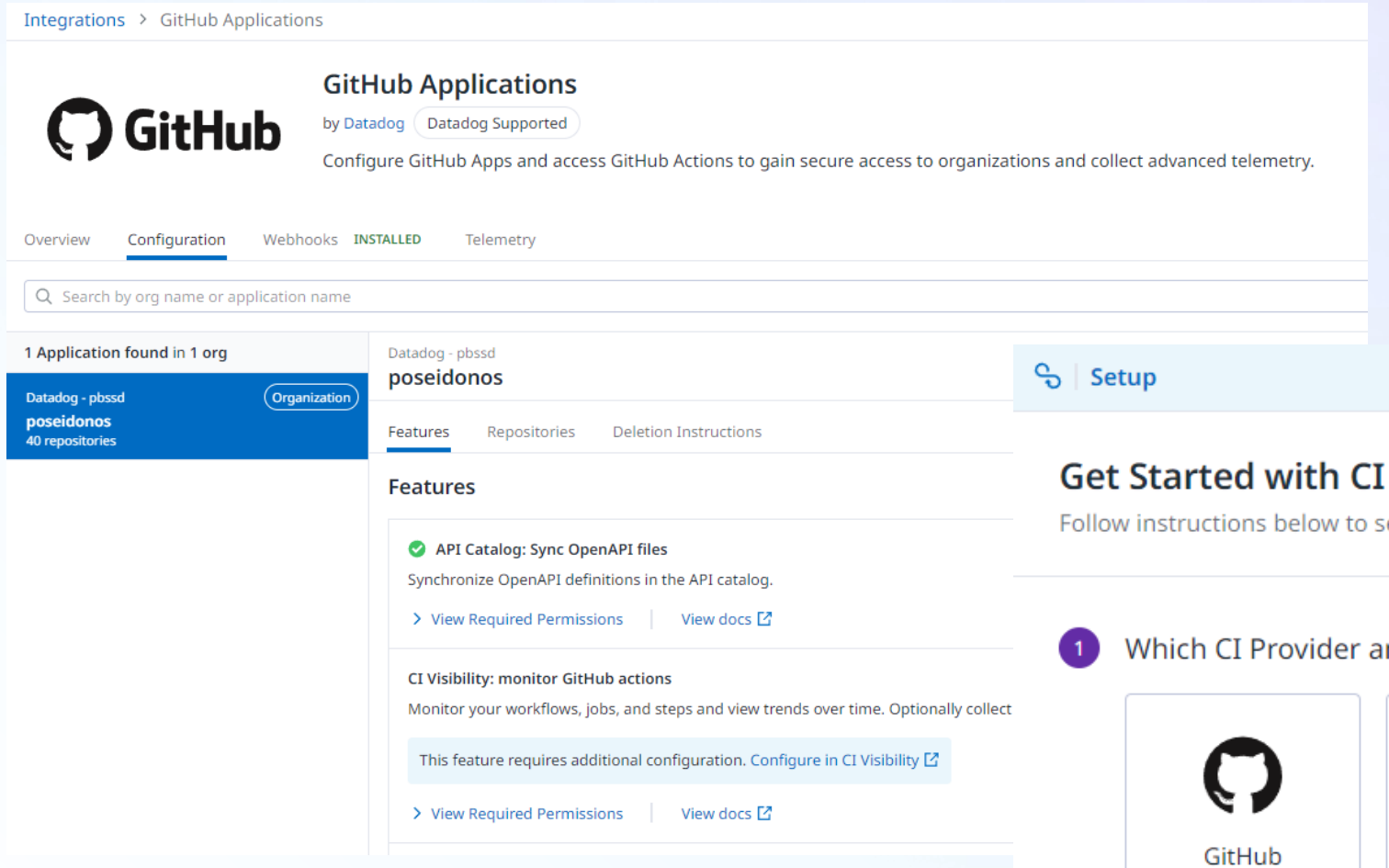
Trouble Shooter

Cluster 내 주기적인 OOM Kill Pod발생

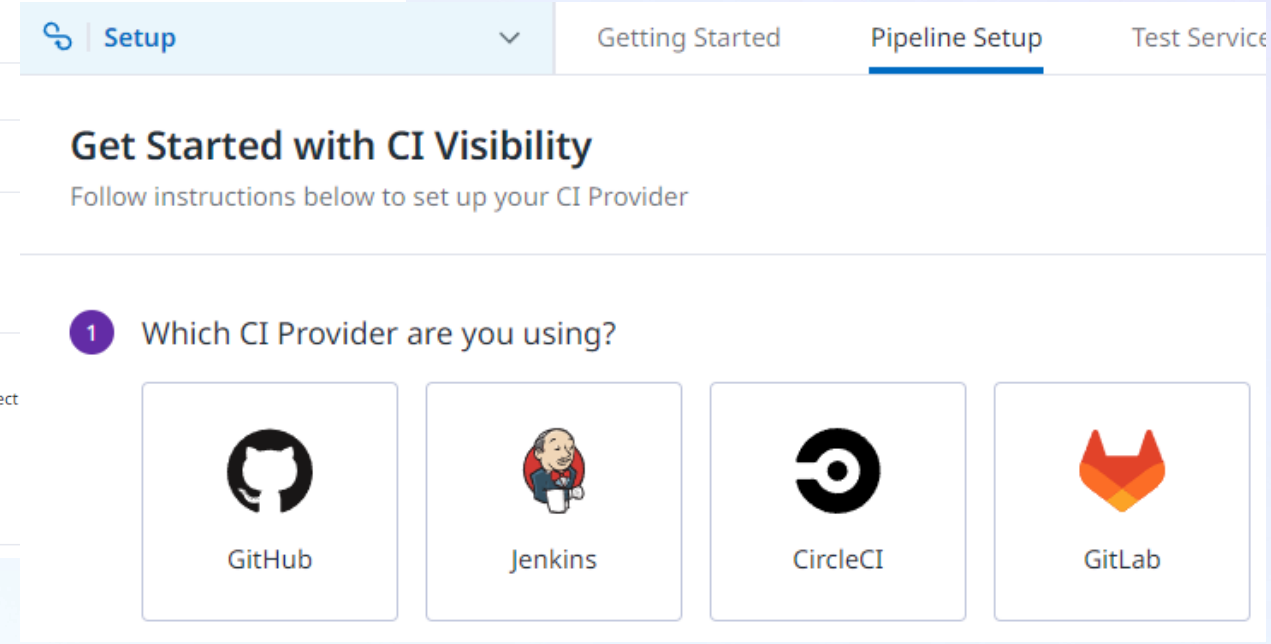
- **On-Prem Cluster 내, 특정 Pod의 주기적 OOM 발생 Detect, 분석, 해결**
- **의심되는 원인에 대한 현상 정보 정리와 함께 관련 Metric 정보를 함께 보여주며, 대응을 위한 실마리를 제시함.**



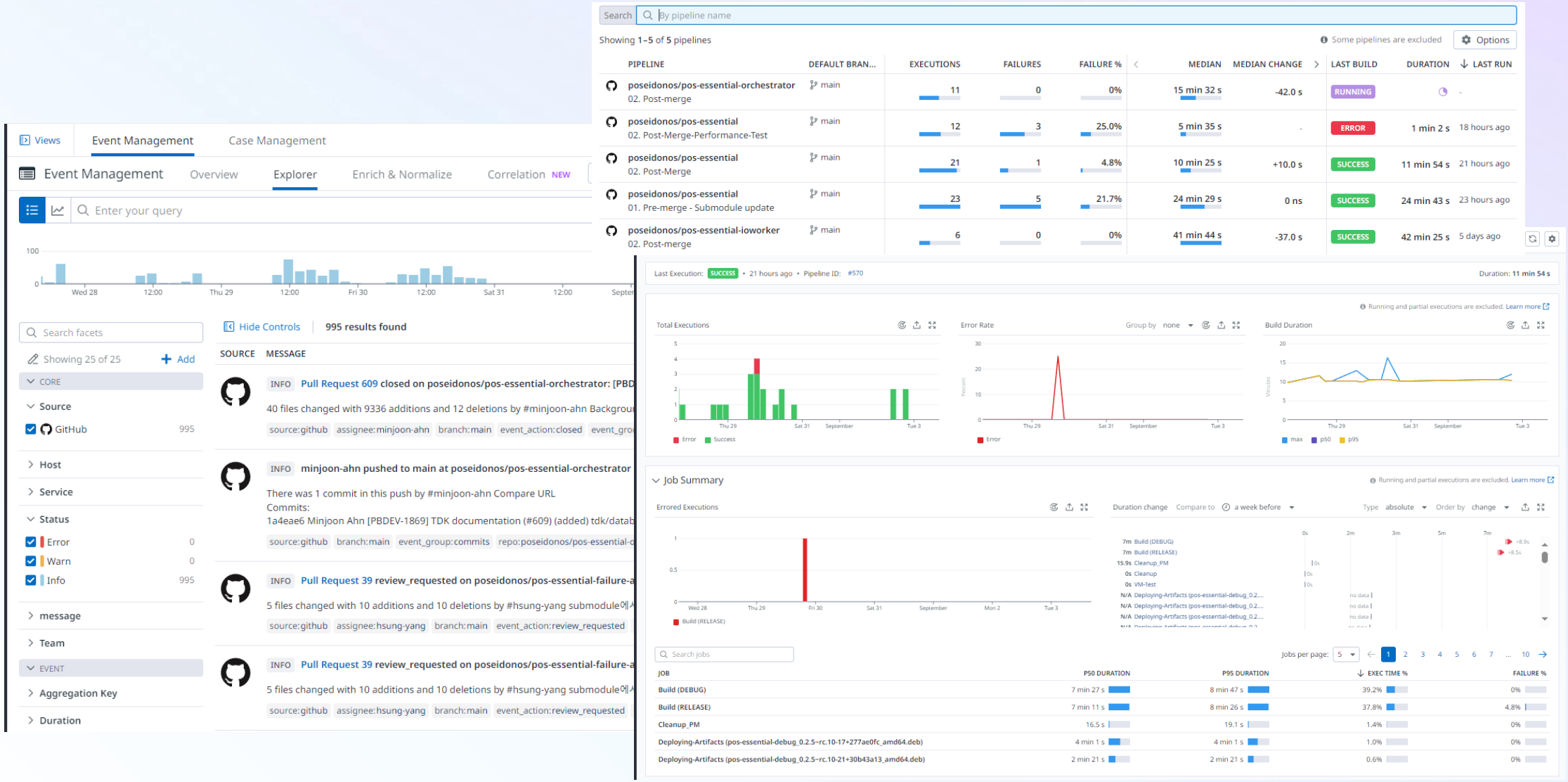
손쉬운 CI Visibility 통합



Several Clicks!!



손쉬운 CI Visibility 통합



Enhancement Points

Enhancement Points

Self-Test Routine? Diagnosis Methods?

- 제대로 연결이 되었는지, 정상적으로 동작하고 있는지 확인할 수 있는 방법?
- Datadog Agent 혹은 그가 속한 Host Node / Host Pod으로 부터 최종 Private Link Endpoint까지 의도대로 정상 동작하도록 연결이 되었는지 손쉽게 확인할 수 있는 방법?
  - 인증 (datadoghq.com)
  - Trouble Shooter의 연장선?

Private Link의 확장?

- 일부 Subdomain 들의 경우, Public Internet을 타게 되어 있음.
  - Private Link 지원의 의미.

Custom URL 사용 및 x.509 Certificate 적용에 대한 공식 Guide?

- Datadog Agent Host와 Proxy가 분리되어 있는 Network에 존재하는 경우 (AirGapped 환경)

Ceph Integration 지원의 확장?

- Container native 환경에서도 지원

Summary

Summary

값진 경험

- Air-gap 환경의 On-Premise 와 Public Cloud(AWS)가 결합된 Hybrid Cloud 형태 구성
- 보안의 중요성 및 최우선 고려 필요 사항
- 최소한의 노력으로 최대 효율 달성 노력: 기존 리소스를 활용하자
- IaC 통한 배포 자동화 구성 필수

기대와 감탄

- Infrastructure Monitoring 및 Event 분석 시, 연속성 있게 다양한 각도로 편하게 분석 가능
- Preset 형태로 제공되는 기능들은 눈이 돌아가고, 숨이 막힐정도로 매력적임 (百聞不如一見)

약간의 개선 포인트

- Customize를 위한 Option에 대한 아쉬움
- 가격...ㄱ 적인...

Thank you

Still Hungry. 부족한 Da린이들의 발표 들어주셔서 감사합니다.