

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

Agenda

01 Motivation

02 Requirement/Constraint for Datadog Deployment

03 Complete Quests (Infra / Agent)

04 Useful Cases

05 Enhancement Points

06 Summary

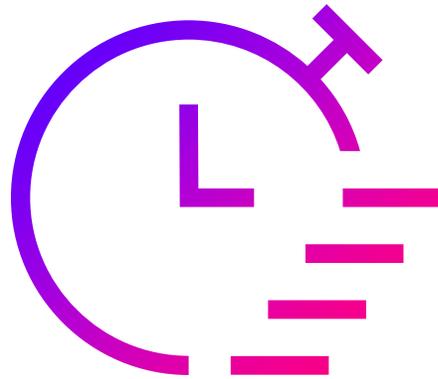
Motivation

Pain Point

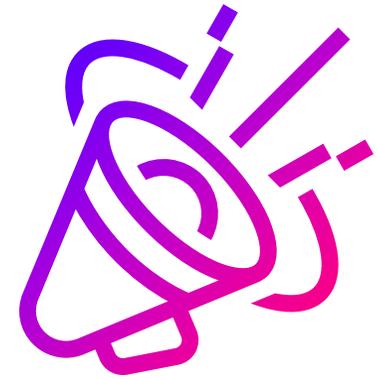
Datadog 도입 동기



**Node / Backend Storage
불안정성**

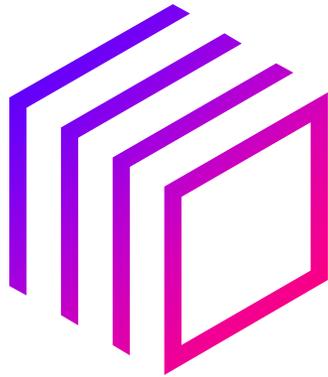


**기존 Logging Stack
느린 검색 성능**

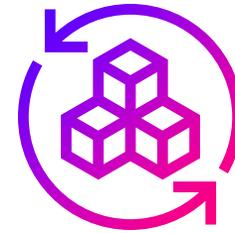


Notification 접근성 제약

Datadog 도입 동기



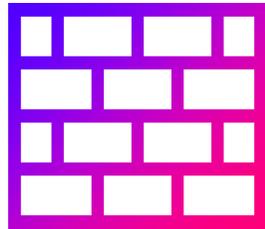
Event / Issue 발생 시
분석의 연계성



CI 통합 Observability 필요

Constraints / Requirements

Constraints & Requirements



**Air-Gapped
Environment**



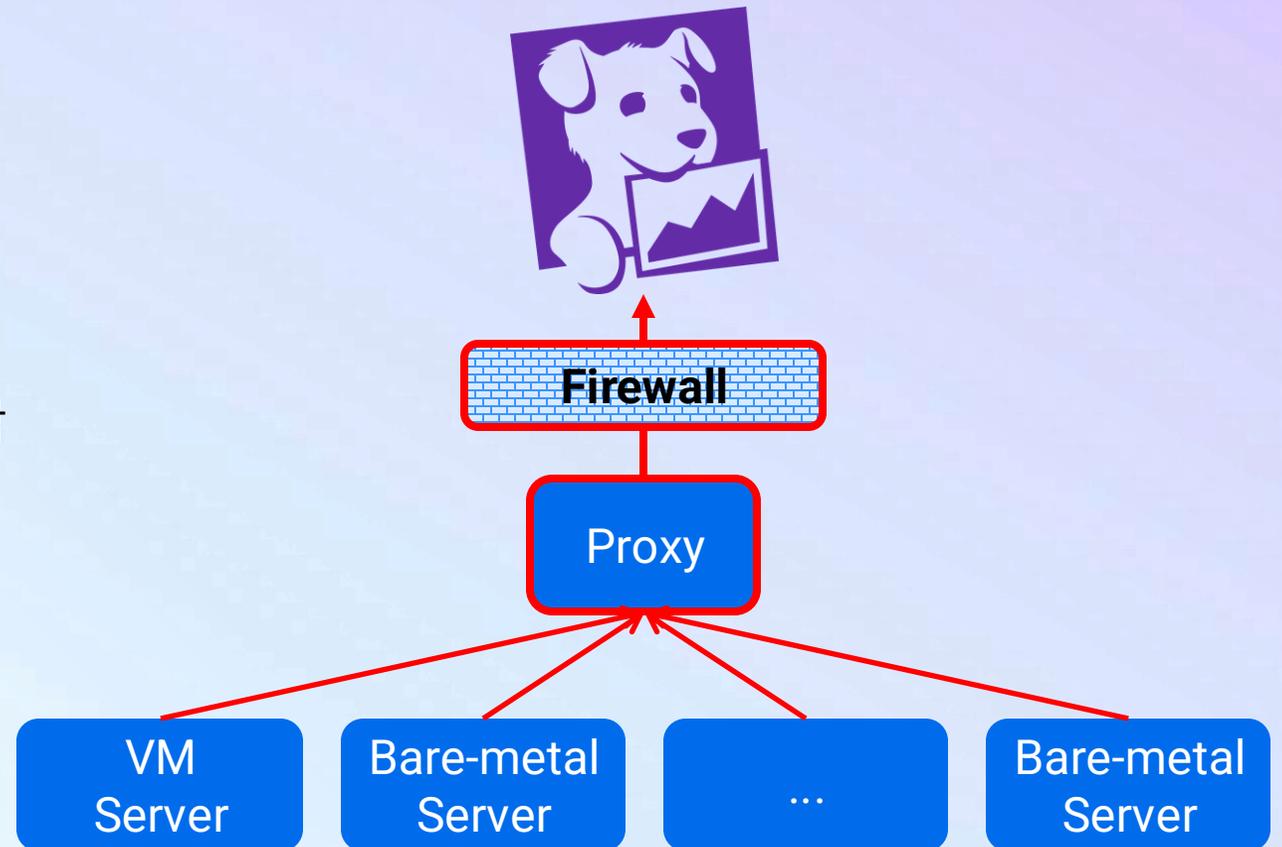
**Prevent
Internal Data Exposure**



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

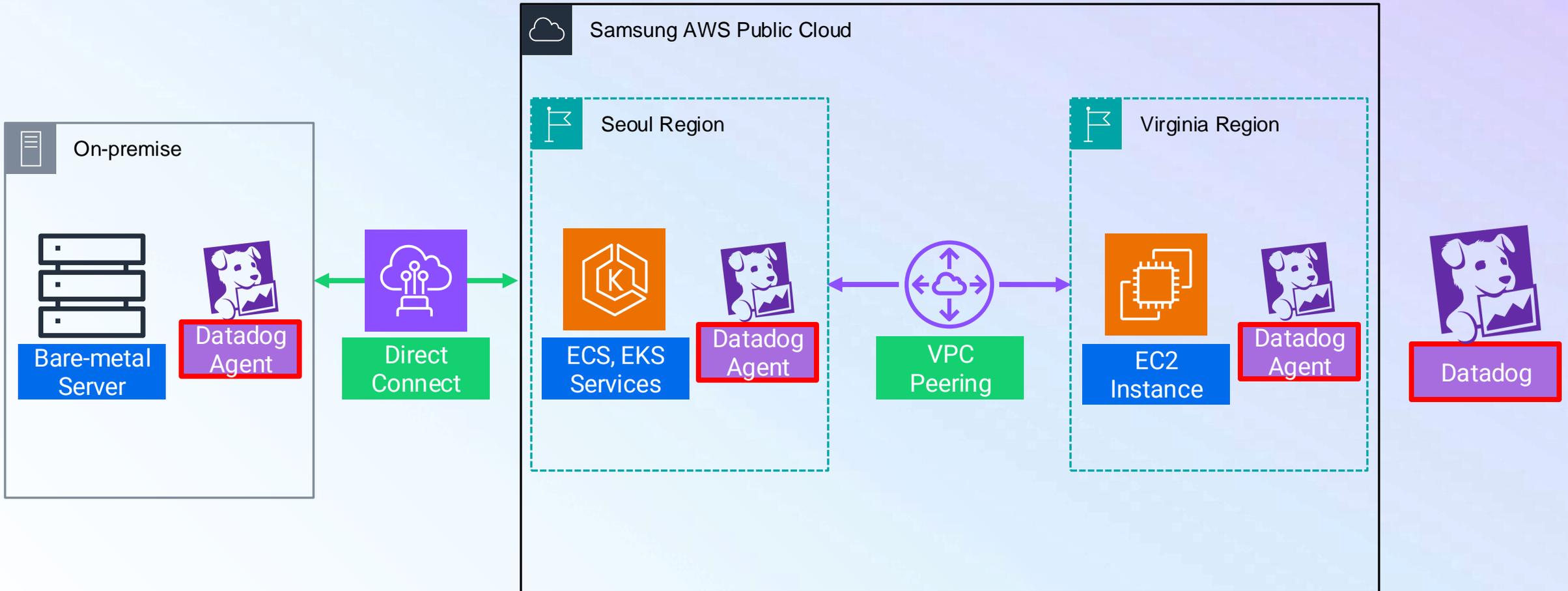


Datadog

Deployment

Public Cloud Architecture

Using Datadog



Complete Quests (Infra)

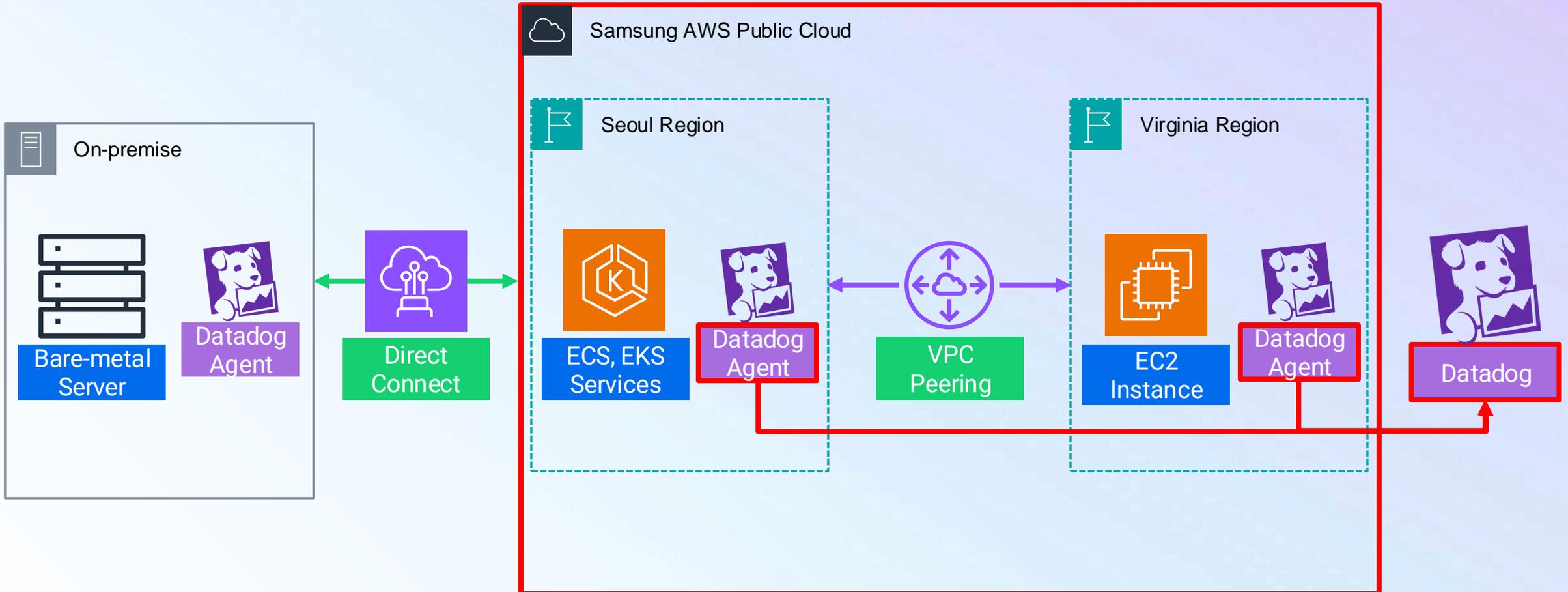
Deliver Data

from On-Prem to Public Cloud,

Securely!!

Case 1. From AWS to Datadog

- 가이드 대로. 어렵지 않다!
- [AWS PrivateLink](https://aws.amazon.com/private-link/)를 통해 [Datadog에 연결 \(datadoghq.com\)](https://datadoghq.com)



Solution: AWS PrivateLink



Datadog VPC Endpoint

AWS PrivateLink

데이터를 인터넷에 노출하지 않고 VPC와 AWS 서비스 간에 연결을 설정합니다.

PrivateLink 시작하기

서비스형 소프트웨어 (SaaS) 애플리케이션과 데이터를 교환할 경우 프라이빗 IP 주소를 사용하여 트래픽의 보안을 유지할 수 있습니다.

간소화된 네트워크 및 방화벽 관리 규칙과 감소된 데이터 출력 및 NAT 비용을 연결할 수 있습니다.

AWS Direct Connect 또는 VPN을 통해 PrivateLink를 결합하여 클라우드 마이그레이션을 가속화할 수 있습니다.

HIPAA, 유럽-미국 프라이버시 실드, PCI, 기타 규제를 준수하면서 SaaS 서비스를 제공할 수 있습니다.

Solution: AWS PrivateLink



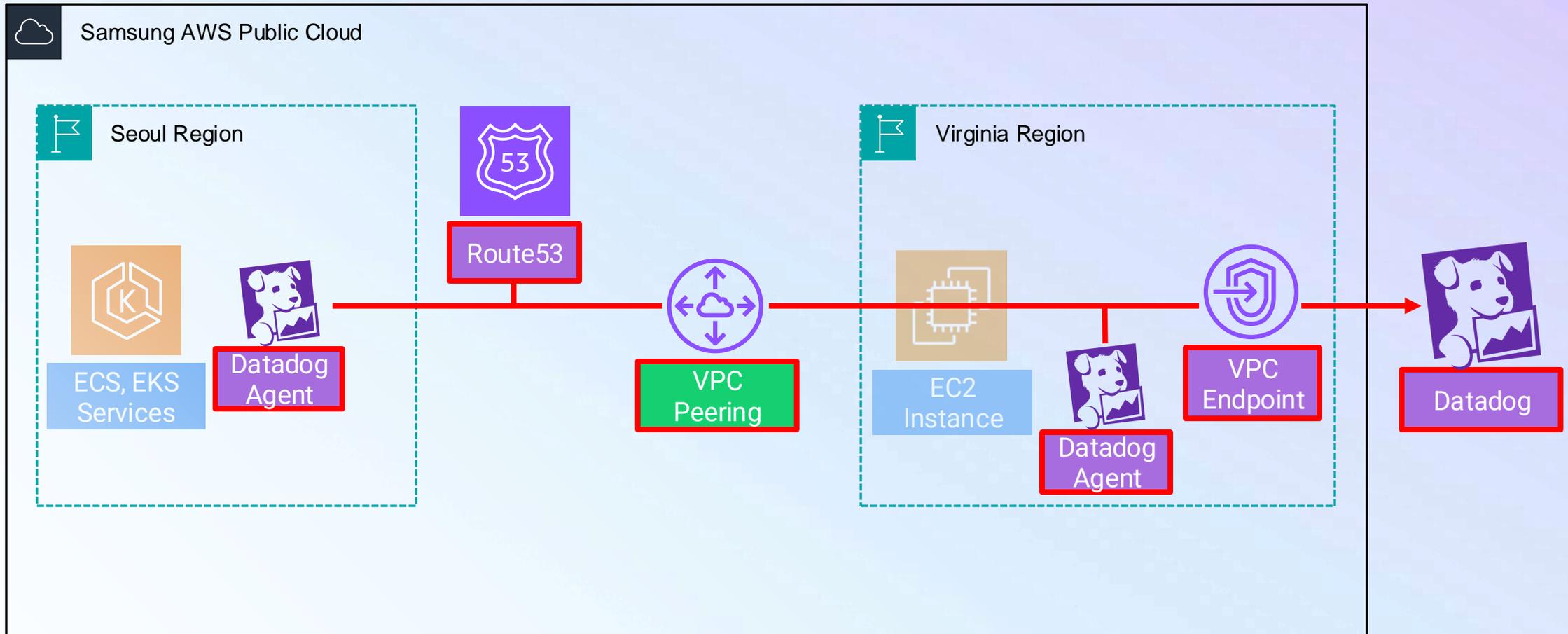
Datadog VPC Endpoint

Endpoints (1/20) [Info](#)

Solution: AWS PrivateLink

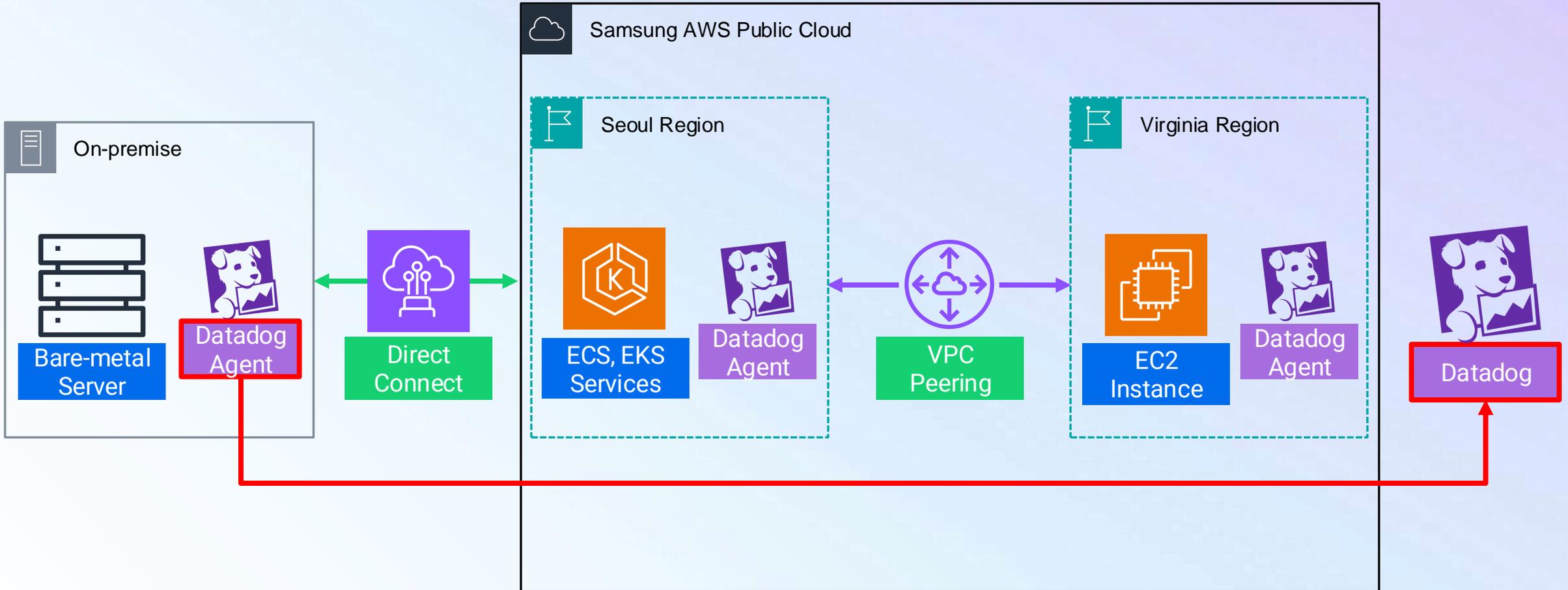


Data path using Datadog AWS PrivateLink



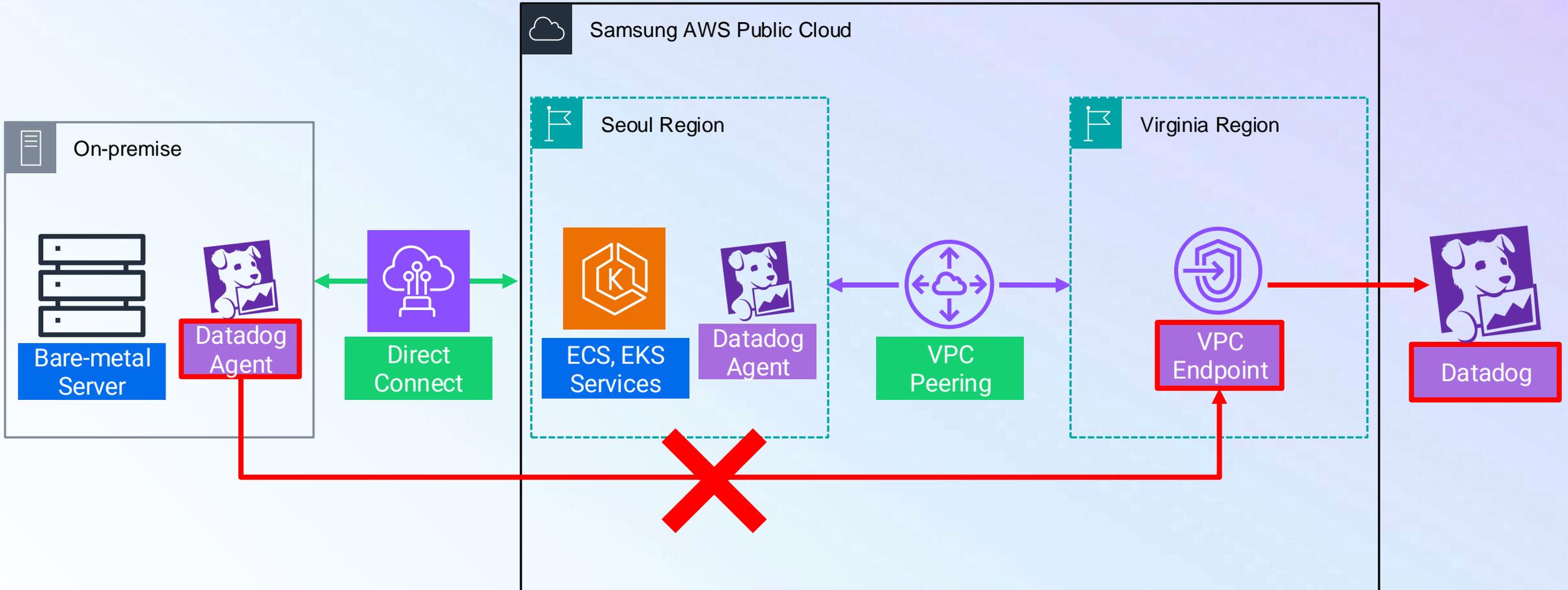
Case 2. From On-premise to Datadog

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



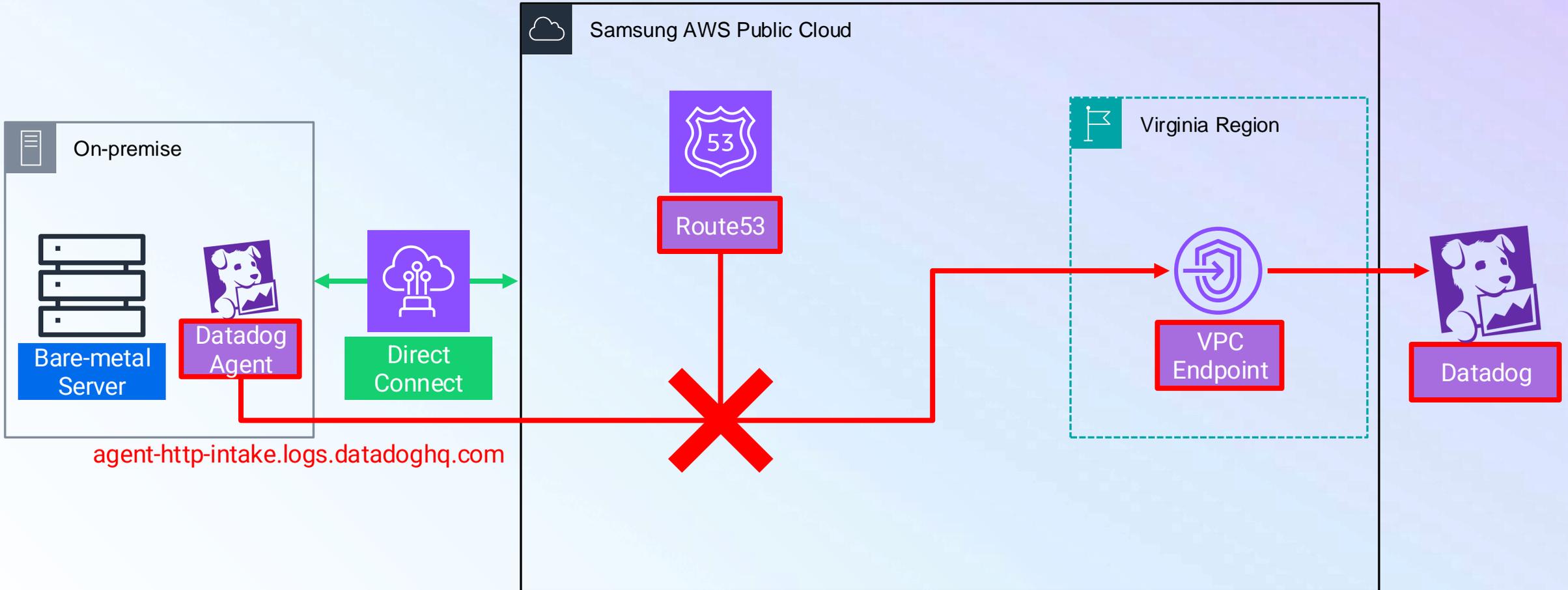
Challenge 1

- 사내에서는 AWS **Seoul region**으로만 접근 가능함
- Virginia region IP로 직접 접근 불가



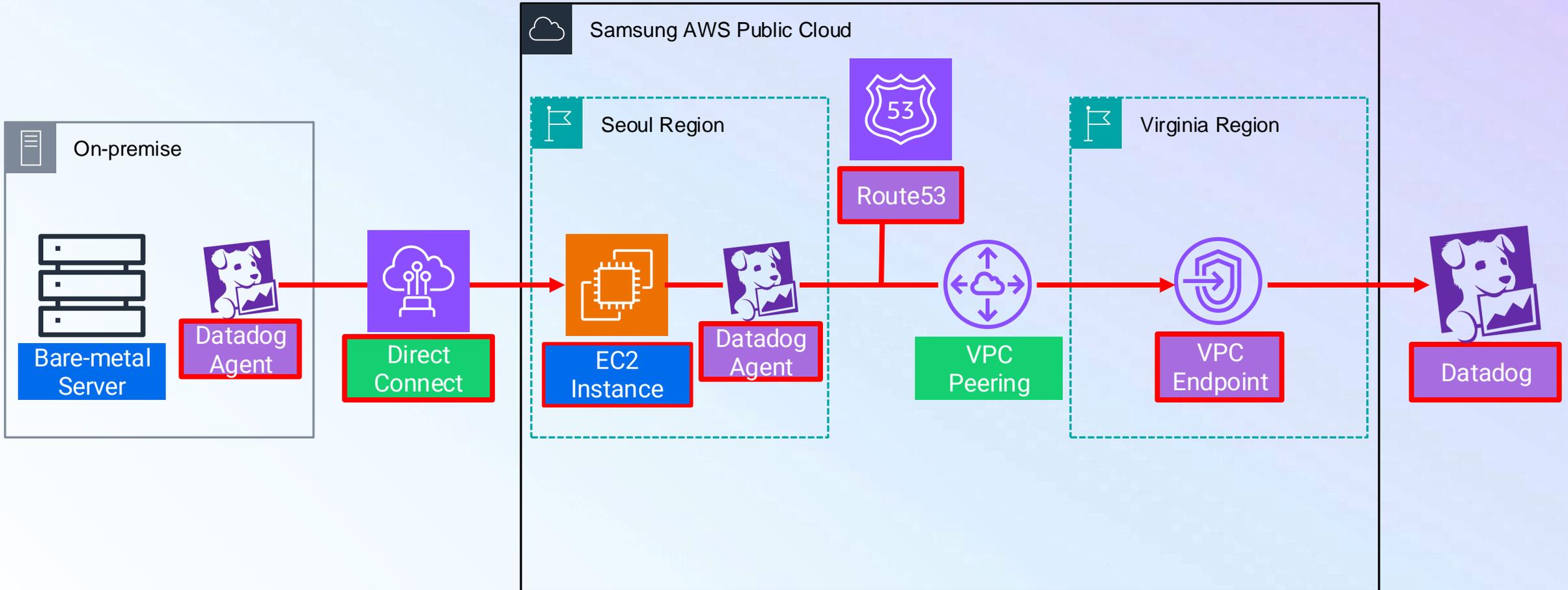
Challenge 2

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



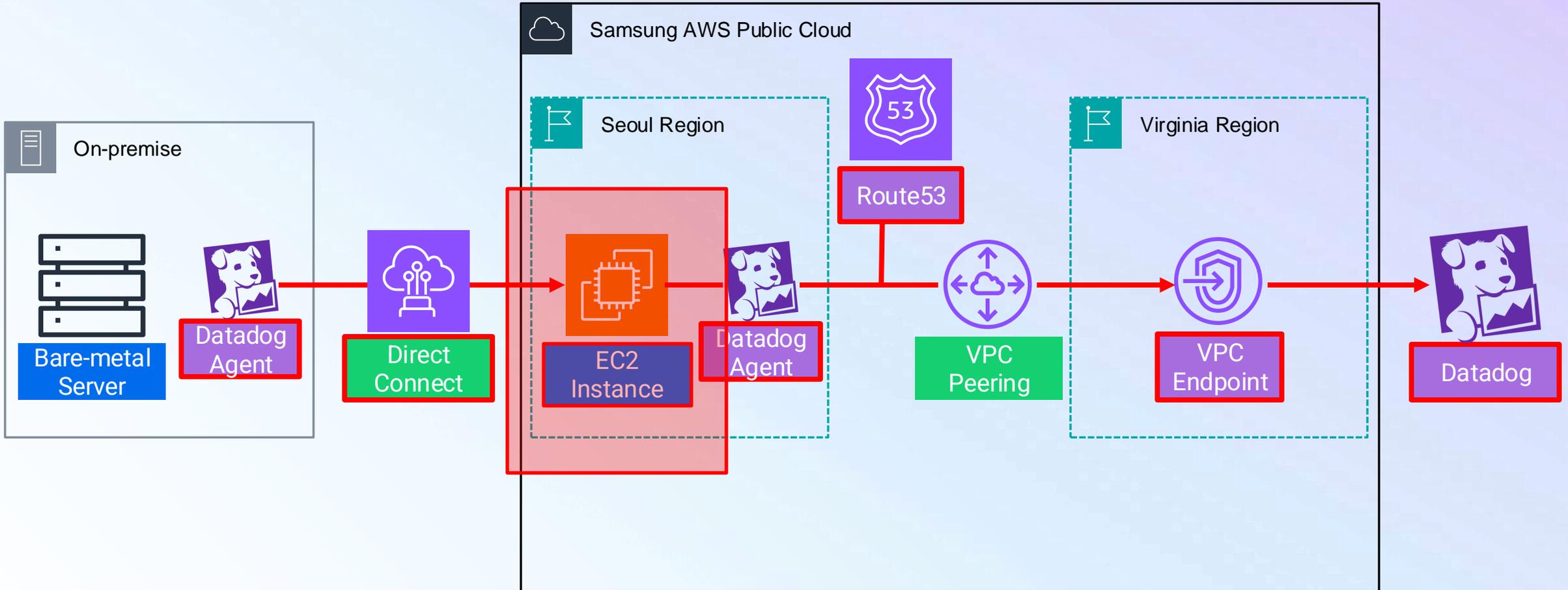
Solution – Proxy Server?

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



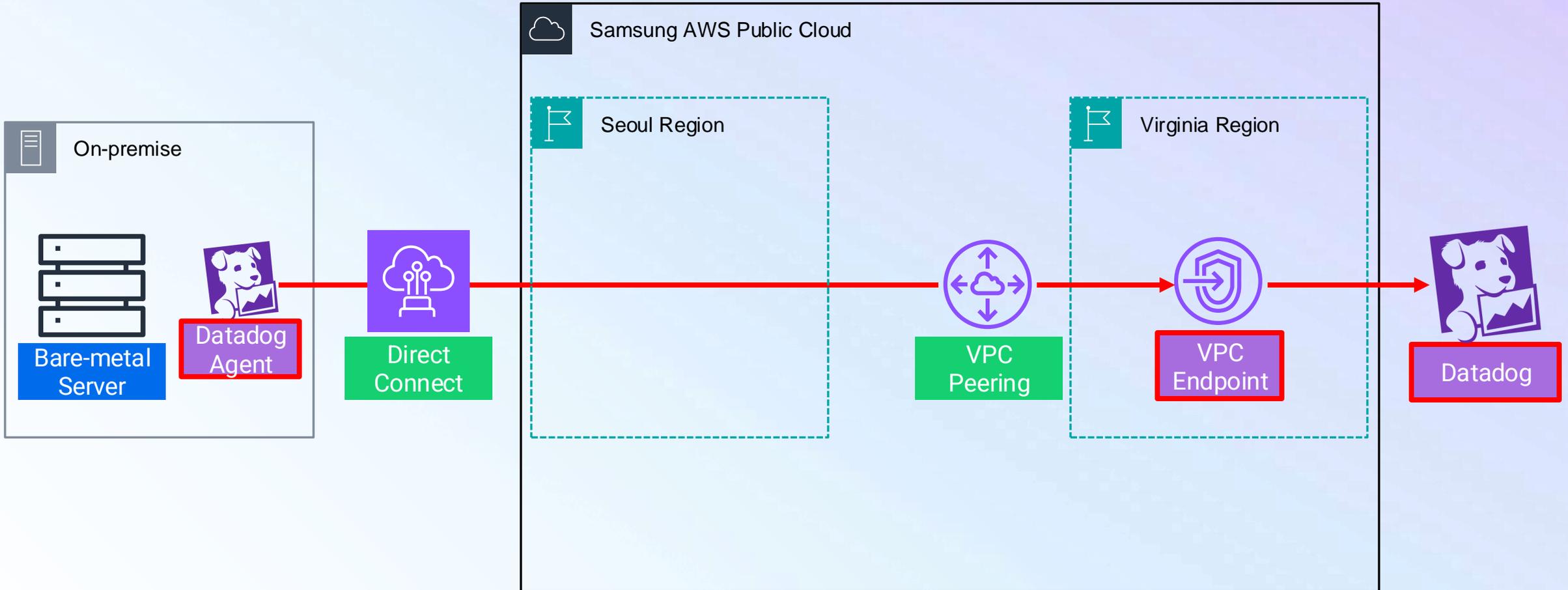
Solution – Proxy Server?

- 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 Load Balancing

네트워크 트래픽을 분산하여 애플리케이션 확장성 개선

Elastic Load Balancing 시작

매월 무료 750시간

Network Load Balancer 및 Application Load Balancer 간 제공 - [AWS 프리 티어](#) 사용 혜택

SSL/TLS 종료, 통합 인증서 관리, 클라이언트 인증서 인증을 통해 애플리케이션을 보호합니다.

고가용성 및 자동 크기 조정으로 애플리케이션을 지원합니다.

실시간으로 애플리케이션 상태 및 성능을 모니터링하고 병목 현상을 파악하며 SLA 규정 준수를 유지 관리합니다.

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

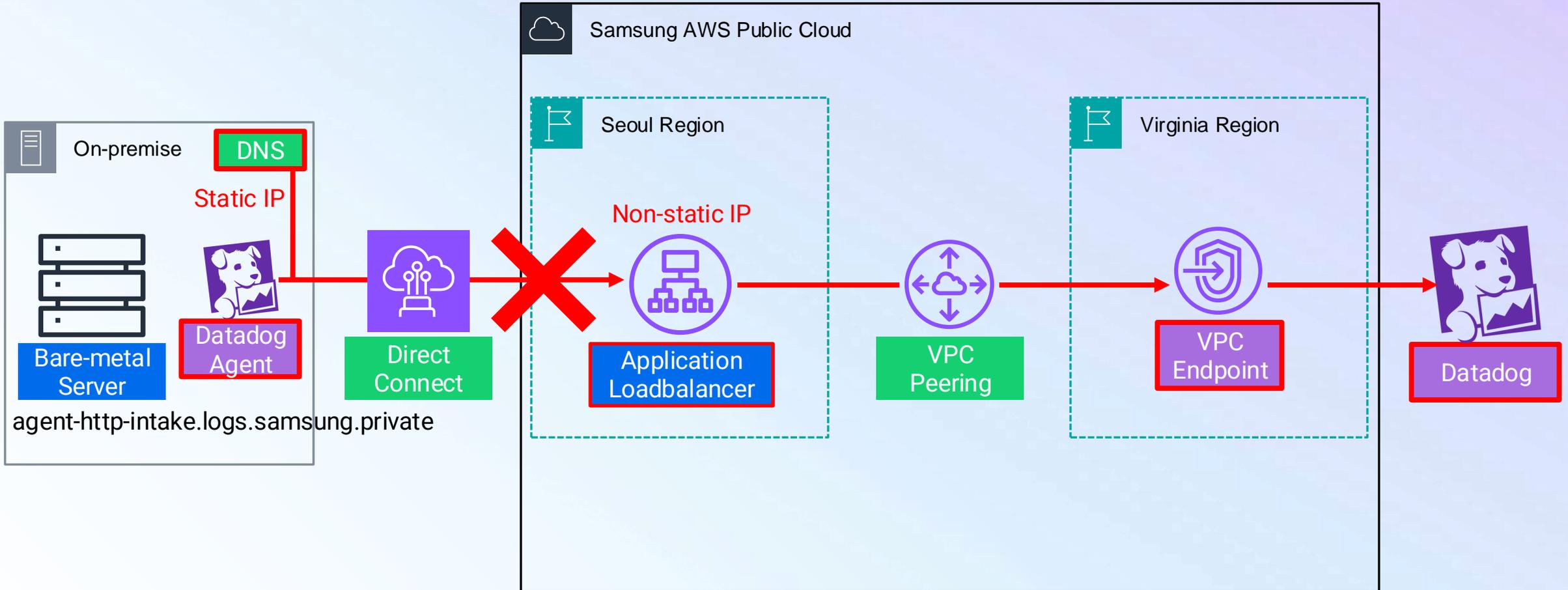
The image shows two screenshots from the AWS IAM console. The left screenshot displays three rules under 'Conditions (If)' and 'Actions (Then)'. The first rule has the condition 'HTTP Host Header is config.dd.pb.aws.' and the action 'Forward to target group' pointing to 'datadog-prod-Remote-Config'. The second rule has the condition 'HTTP Host Header is api.dd.pb.aws.' and the action 'Forward to target group' pointing to 'datadog-prod-API'. The third rule has the condition 'HTTP Host Header is http-intake.logs.dd.pb.aws.' and the action 'Forward to target group' pointing to 'datadog-prod-Logs-User'. A red arrow points from the 'datadog-prod-Remote-Config' link in the first rule to the right screenshot. The right screenshot shows the 'Registered targets (2)' section for the 'datadog-prod-Remote-Config' target group. It lists two targets with IP addresses 10.3.115.140 and 10.3.92.128, both on port 443. A red dashed line connects the two screenshots.

IP address	Port
10.3.115.140	443
10.3.92.128	443

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

Challenge 3

- 사내 도메인은 고정된 **특정 IP**만을 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.

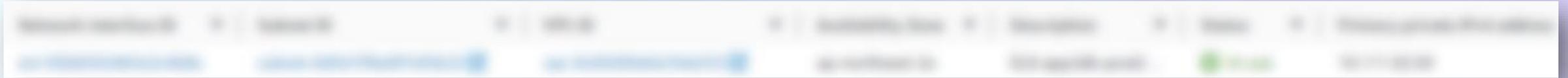
Network interface ID	Subnet ID	VPC ID	Availability Zone	Description	Status	Primary private IPv4 address
eni-03685924b5e2c468e	subnet-0d5d1f9ed97ef2b22	vpc-0c69289afa234a555	ap-northeast-2a	ELB app/alb-prod/...	✔ In-use	10.111.92.93

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

Solution – Network Loadbalancer

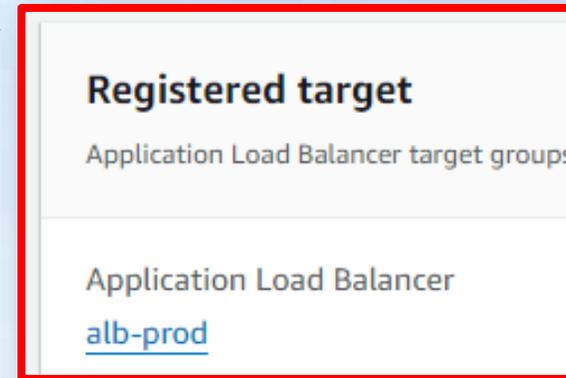
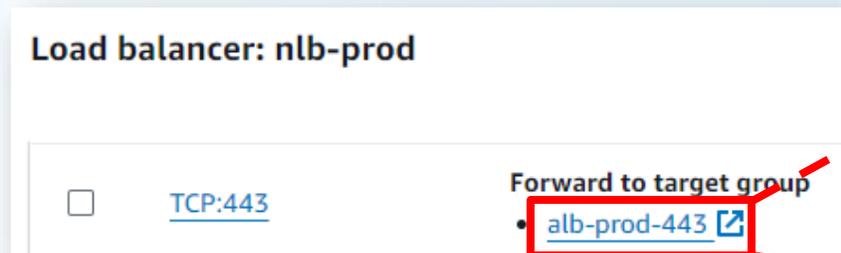
사내에서 도메인을 통해 AWS ALB는 어떻게 접근하지?

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)

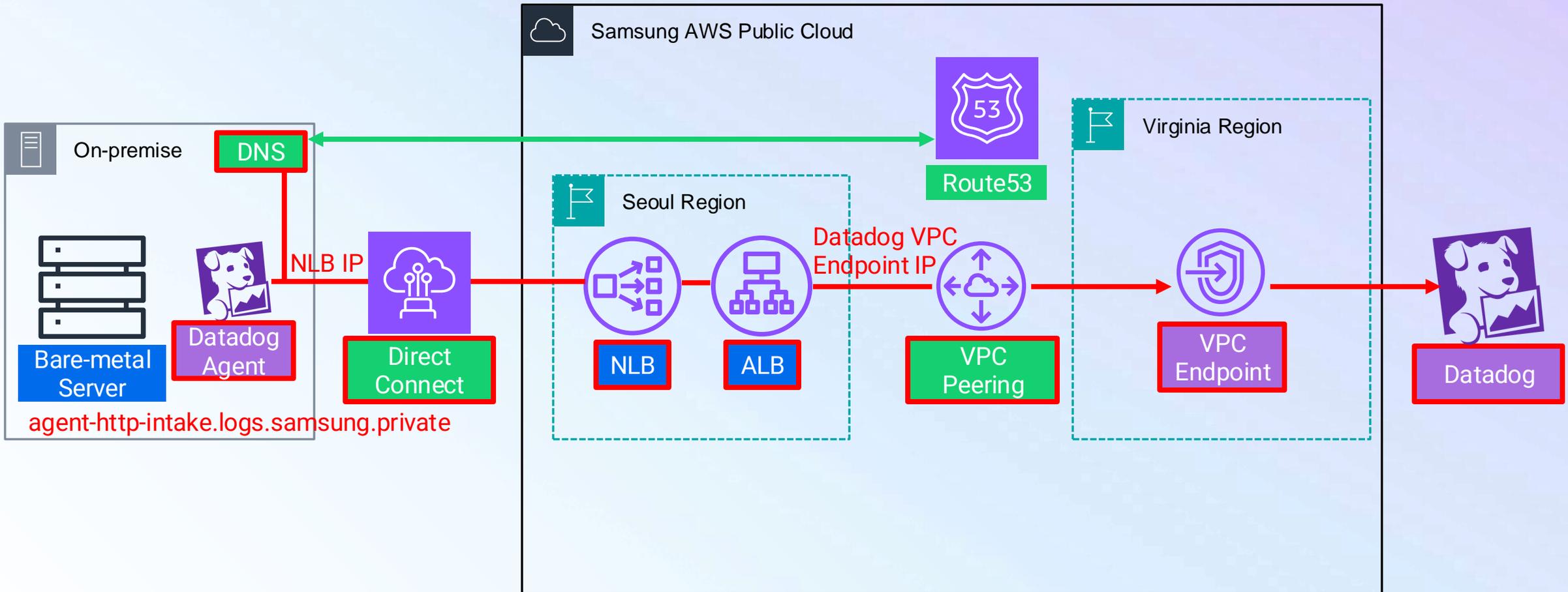
One more thing – Route53 Private Domain

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

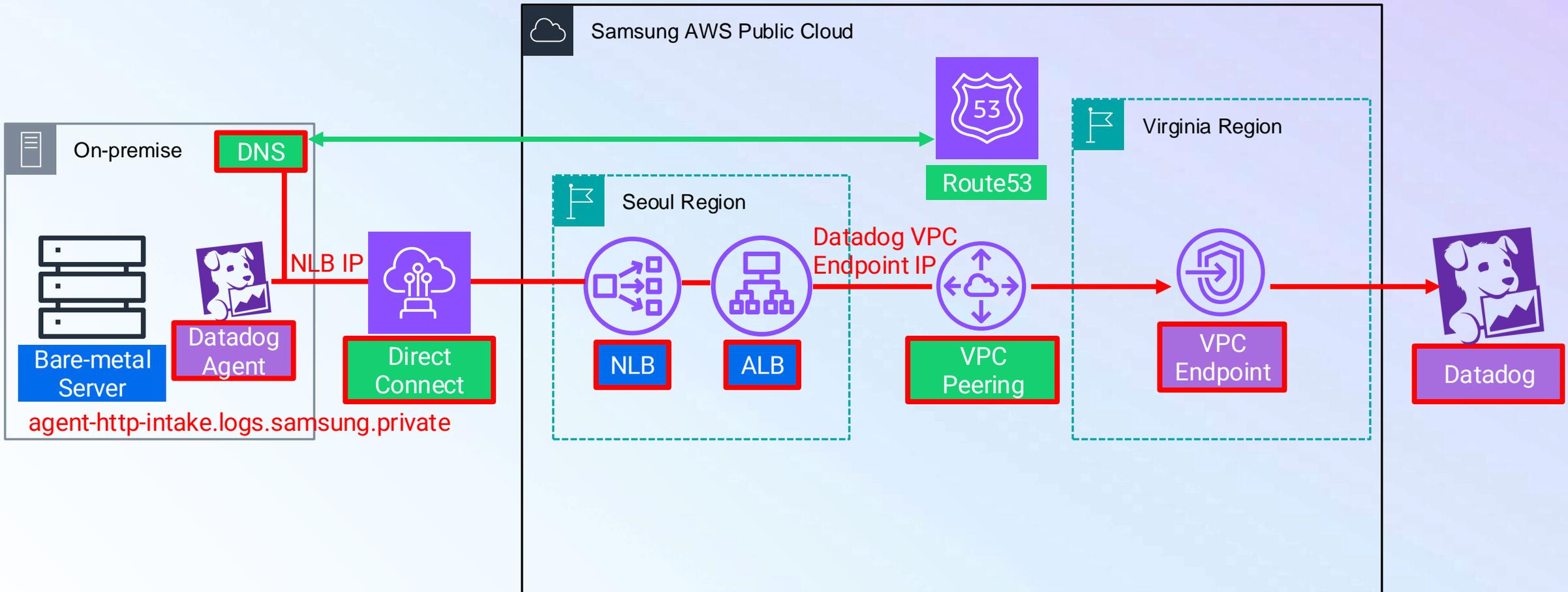
1. 특정 도메인 (*pb.aws.samsung.private) 에 대해 사내 DNS에서 지정 Route53으로 도메인 질의 전달
2. 사내에서 접근할 수 있는 AWS 리소스의 도메인을 직접 Route53에서 관리
3. 사내와 Public Cloud 모두 도메인 레코드 조회 가능
4. 따로 결제 없이 레코드 추가 / 변경 가능, TTL 자체 설정 가능

<input type="checkbox"/>	Record name	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s...)	Health
<input type="checkbox"/>	pb.aws. [redacted]	NS	Simple	-	No	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	172800	-
<input type="checkbox"/>	pb.aws. [redacted]	SOA	Simple	-	No	ns-1536.awsdns-00.co.uk. a...	900	-
<input type="checkbox"/>	*-app.agent.pb.aws. [redacted]	A	Simple	-	No	10.111.92.80 10.111.92.100	300	-
<input type="checkbox"/>	metrics.agent.pb.aws. [redacted]	A	Simple	-	No	10.111.92.80 10.111.92.100	300	-
<input type="checkbox"/>	trace.agent.pb.aws. [redacted]	A	Simple	-	No	10.111.92.80 10.111.92.100	300	-

Observability Data Flow From On-premise to Datadog



Observability Data Flow From On-premise to Datadog

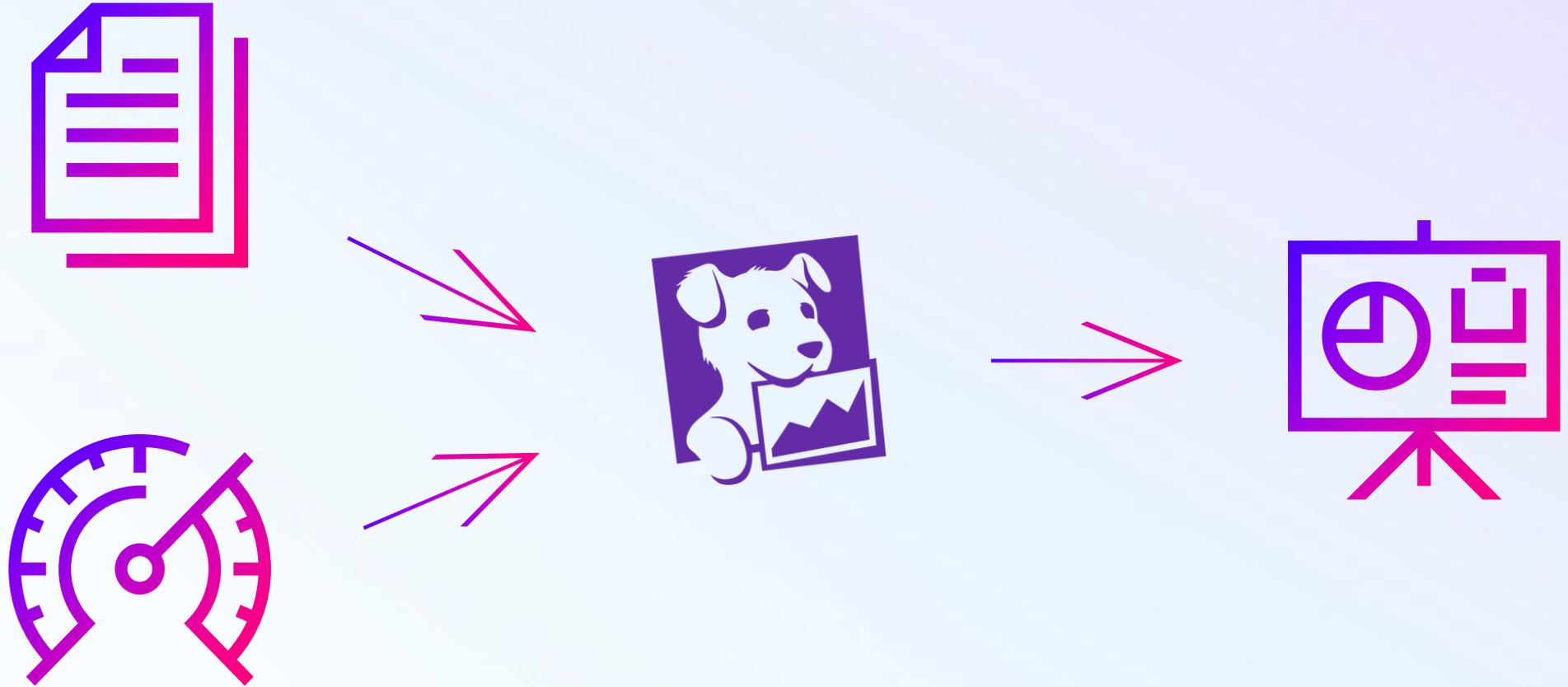


Complete Quests (Agent)

Deliver Data

from On-Prem to Public Cloud,
Securely!!

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 \(datadoghq.com\)](https://aws.amazon.com/privatelink/)
 - 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.)

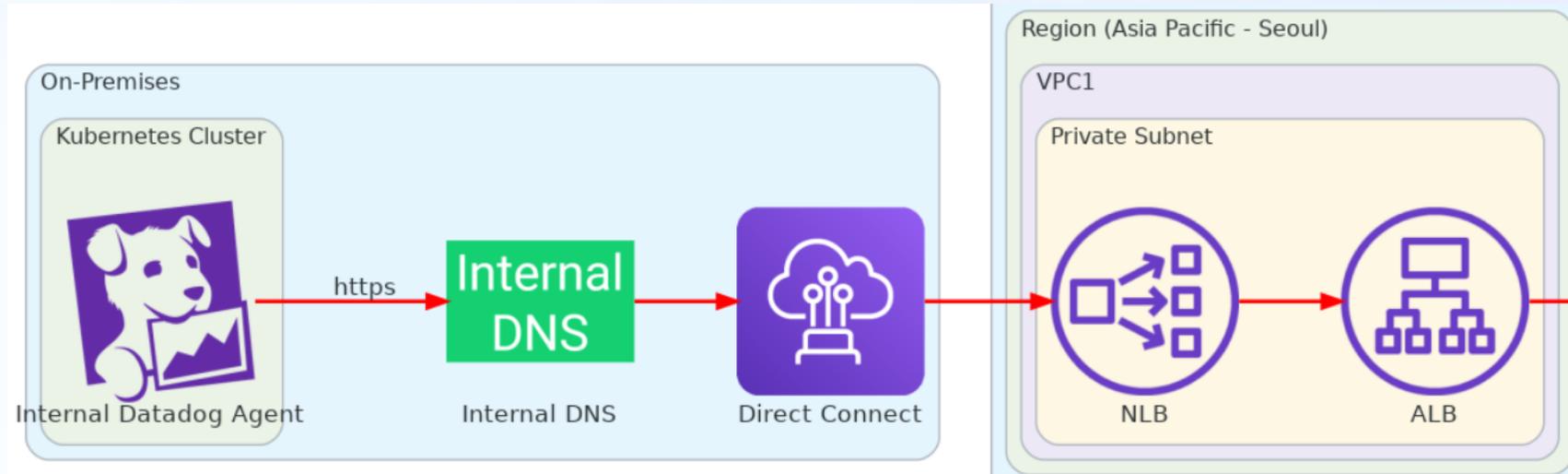
특정 Subdomain들은 Public Internet을 통해야 정상 동작함.

- 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 \(datadoghq.com\)](https://docs.datadoghq.com/agent/faq/proxy/)
 - 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.xxxxxxxx/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.xxxxxxxx/api/v0.1/status": tls: failed to verify certificate: x509: certificate signed by unknown authority
```

뚫어 봅시다! (Workaround 주의!)

- **Container 내에** 해당 Custom URL을 위한 x.509 Certificate이 설치되어야 함.
 - [datadog-operator/docs/configuration.v2alpha1.md at main · DataDog/datadog-operator \(github.com\)](https://github.com/DataDog/datadog-operator/blob/main/docs/configuration.v2alpha1.md)
 - 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.

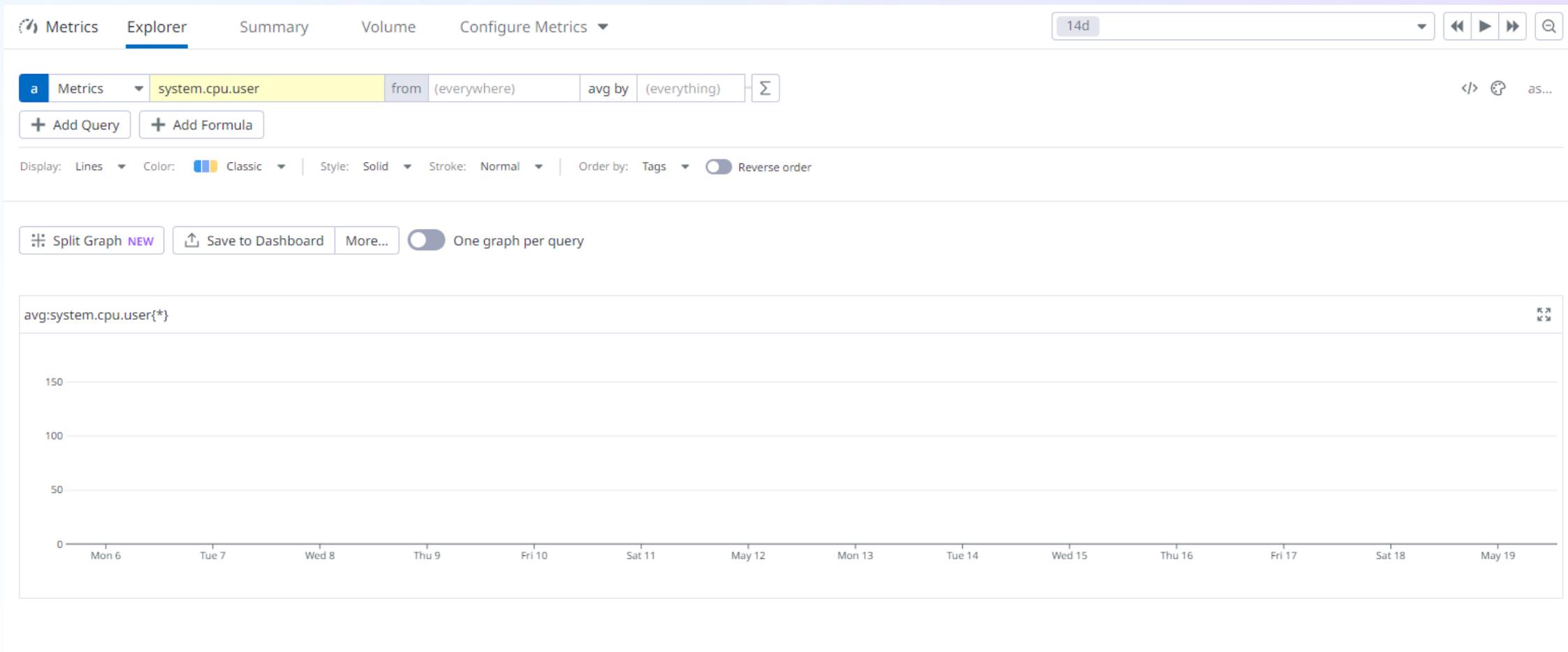
```
71 | customConfigurations:
72 |   datadog.yaml:
73 |     configData: |
74 |       apm_config:
75 |         enabled: false
76 |       logs_enabled: true
77 |       logs_config:
78 |         container_collect_all: true
79 |         force_use_http: true      heesoo84.kim, 3
80 |     process_config: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

오 드디어 성공??

The screenshot shows the Datadog Logs interface. At the top, there are tabs for 'Logs', 'Log Explorer', and 'Live Tail'. Below this, there's a search bar and navigation controls. A sidebar on the left shows filters for 'CORE', 'Index', 'LIVE INDEXES', 'Source', 'Host', and 'Service'. The main area displays a 'Watchdog Insights' alert for 'LOGS ERROR OUTLIER' on 'kube_app_part_of:rook-ceph'. A bar chart shows 88.9% of total errors and 81.5% of total logs. Below the alert is a table of log entries.

DATE	HOST	SERVICE	CONTAINER NAME	CONTENT
23:58:59.887	dc1-compute-3-prod3	ceph	mon	cluster 2024- T14:58:58.198879+0000 mgr.b (mgr.22584726) 240694 : cluster 0 pgmap v241...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.442494 1 timeout.go:141] post-timeout activity - time-elapsed: 22.046764ms, ...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.441416 1 timeout.go:141] post-timeout activity - time-elapsed: 21.496238ms, ...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.440330 1 timeout.go:141] post-timeout activity - time-elapsed: 20.32819ms, ...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.439247 1 timeout.go:141] post-timeout activity - time-elapsed: 19.486936ms, ...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.436880 1 writers.go:131] apiserver was unable to write a fallback JSON resp...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.435768 1 writers.go:131] apiserver was unable to write a fallback JSON resp...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.434714 1 writers.go:131] apiserver was unable to write a fallback JSON resp...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.433540 1 writers.go:131] apiserver was unable to write a fallback JSON resp...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.432661 1 timeout.go:141] post-timeout activity - time-elapsed: 12.735235ms, ...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.431332 1 status.go:71] apiserver received an error that is not an metav1.St...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.429102 1 status.go:71] apiserver received an error that is not an metav1.St...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.428024 1 status.go:71] apiserver received an error that is not an metav1.St...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.426903 1 status.go:71] apiserver received an error that is not an metav1.St...
23:58:59.642	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.424716 1 writers.go:131] apiserver was unable to write a fallback JSON resp...
23:58:59.641	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.423548 1 status.go:71] apiserver received an error that is not an metav1.St...
23:58:59.641	dc2-compute-4-prod3	mirrored-prometheus-adapter-prometheus...	prometheus-adapter	E0819 14:58:59.421004 1 writers.go:118] apiserver was unable to write a JSON response: htt...

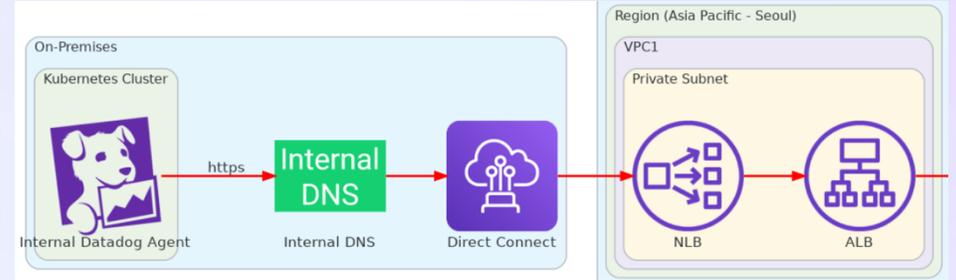
Metric도 한 번 볼까?



Log는 수집이 되는데, Metric은 왜 안되지?

Route53이 아닌 ALB를 사용하고 있었던 점

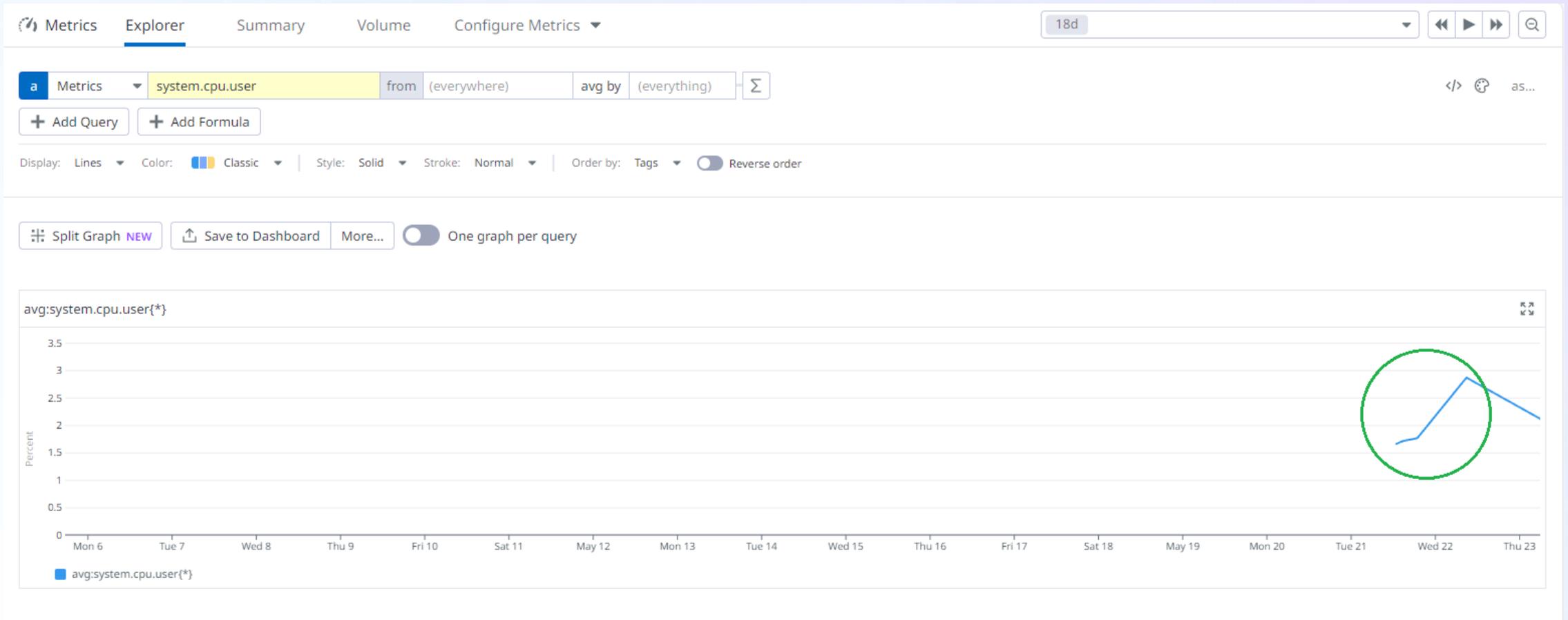
- [AWS PrivateLink를 통해 Datadog에 연결 \(datadoghq.com\)](https://www.datadoghq.com/)
 - AWS내 Route53 사용에 대한 Guide 제공.
 - Route53이 아닌 NLB – ALB를 사용하게 된 이유?
 - On-Premise에서 Direct Connect를 통해서만 접속가능 -> 정해진 IP 필요
 - ALB 단독으로는 고정 IP 할당이 불가 -> NLB 추가
 - OnPrem -> 사내 DNS -> Direct Connect -> NLB -> ALB -> ...



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!!!???



끝날 때 까지 끝난 게 아니다

☆ Ceph - Overview ▾
cluster * pool *



This dashboard displays a high-level overview of Ceph operations and performance, so you can track throughput and latency metrics from your clusters, hosts, and pools and spot performance bottlenecks. Further reading on Ceph monitoring:

- [Datadog's Ceph integration docs](#)
- [How to monitor Ceph with Datadog](#)

Clone this template dashboard to make changes and add your own graph widgets.

Datadog provides read/write throughput, capacity usage, and number of objects stored with pool-level resolution. You can leverage this feature to gather details about each pool's usage pattern and quickly spot overloaded pools to tune the application for better performance.

Summary

If you use more than one cluster, you can easily zero in on one particular cluster by changing the cluster template variable.

Cluster Status No value reported for service check ceph.overall_status	Cluster CPU usage (No data)	Osds over ceph_fs... (No data)
Pools over ceph_... (No data)	Pgs over ceph_fsid... (No data)	Monitors over cep... (No data)

OSDs

Participating sto... (No data)	Online storage d... (No data)
Nearly full osds ... (No data)	Full osds over ce... (No data)

Pools

Most active pools over ceph_fsid:*,ceph_p... No Data	Most populated pools over ceph_fsid:*,ce... No Data
---	--

Commit and apply latency



Read/write throughput



R/W activity over ceph_fsid:*,ceph_pool:*



Logs

Logs that match "source:ceph"

DATE	HOST	SERVICE
Sep 05 17:35:04.913	dc1-compute-3-prod3	ceph
audit 2024-09-05T08:35:04.507235+0000 mon.c (mon.1) 2509485 : audit 0 from='client.? 10.42.4.242:0/3660785108' entity='client.admin' cmd=[{"prefix": "mgr stat", "format":		
Sep 05 17:35:04.640	dc2-compute-1-prod3	ceph
2024-09-05 08:35:04.521544 I cephcmd: successfully checked mgr_role label. checking again in 15s		
Sep 05 17:35:04.639	dc2-compute-1-prod3	ceph
2024-09-05 08:35:04.521516 I op-mgr: active mgr is still the same (b). No need to update mgr_role label on daemon a.		
Sep 05 17:35:04.639	dc2-compute-1-prod3	ceph
2024-09-05 08:35:03.749283 I op-mgr: Checking mgr_role label value of daemon a (prev active mgr was b)		
Sep 05 17:35:03.465	dc1-compute-4-prod3	ceph
audit 2024-09-05T08:35:02.464087+0000 mon.a (mon.0) 2250476 : audit 0 from='admin socket' entity='admin socket' cmd=mon_status args=[]: finished		
Sep 05 17:35:03.465	dc1-compute-4-prod3	ceph
audit 2024-09-05T08:35:02.463749+0000 mon.a (mon.0) 2250475 : audit 0 from='admin socket' entity='admin socket' cmd='mon_status' args=[]: dispatch		
Sep 05 17:35:02.911	dc1-compute-3-prod3	ceph
audit 2024-09-05T08:35:02.464087+0000 mon.a (mon.0) 2250476 : audit 0 from='admin socket' entity='admin socket' cmd=mon_status args=[]: finished		
Sep 05 17:35:00.437	dc2-compute-3-prod3	ceph

Ceph Integration 적용

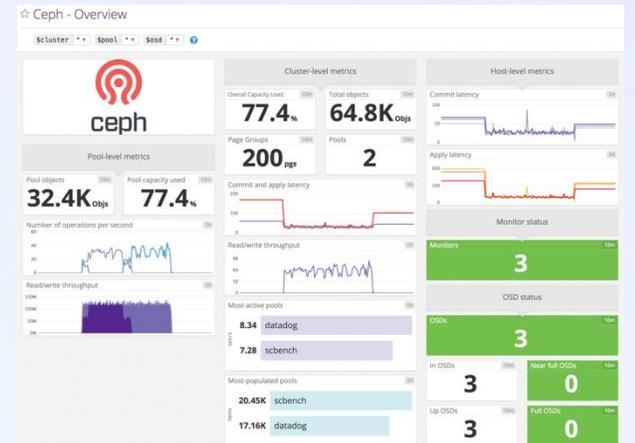
Datadog에서 제공하는, 특정 Solution에 대한 Observability Preset 기능

- [Ceph \(datadoghq.com\)](https://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

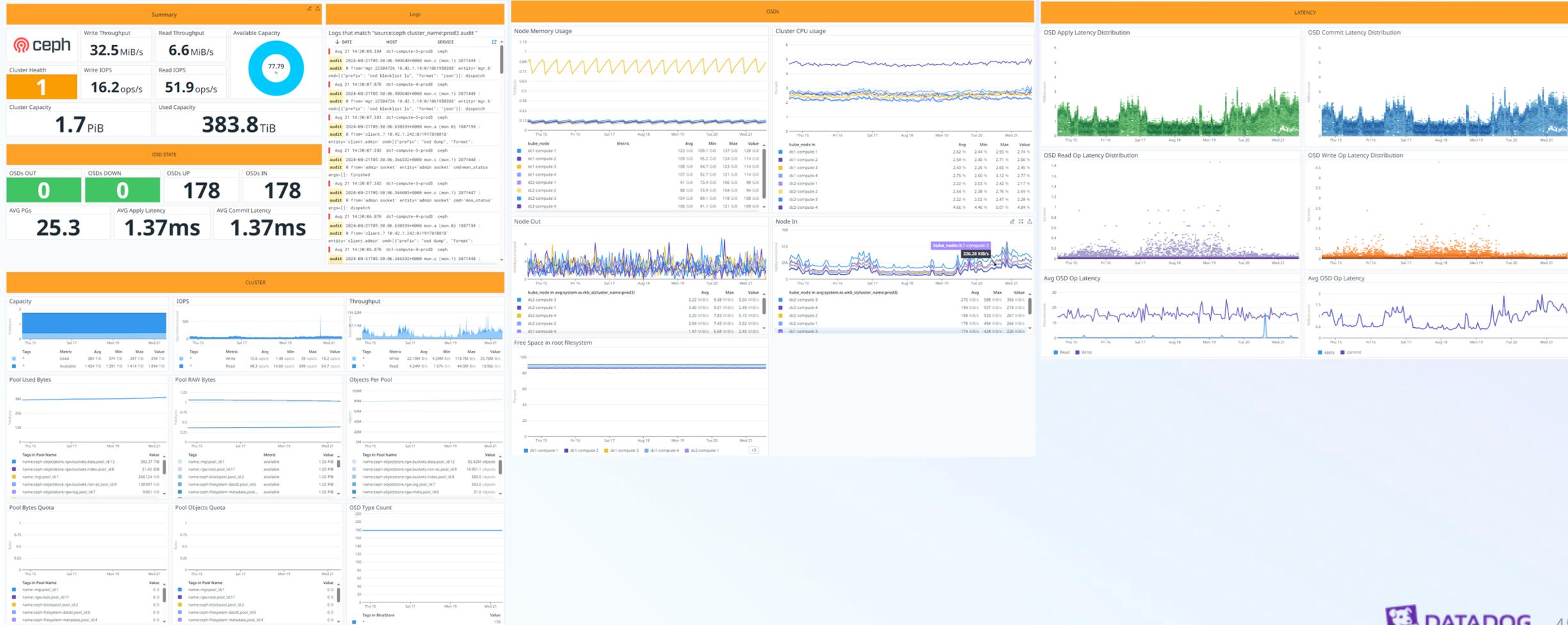
- Sidecar Container를 띄워 각 Ceph 관련 Pod별로 Datadog Agent 배포
 - Agent Container별로 별도 추가 비용 발생
- 필요로 하는 Metric들을 Custom Metric으로 등록하여, 선택적으로 수집 및 사용
 - Custom Metric 개수에 따라(Cardinality 100개당 얼마 형태) 추가 비용 발생
 - Pod용 Annotation을 추가하여, Datadog Auto Discovery 시 명시된 Metric들에 대해서 Custom Metric으로 등록하도록 함.

Storage와 Retention의 가치와 효용을 다시 한 번 느끼게 된 포인트.



Ceph Integration 적용 (Cont.)

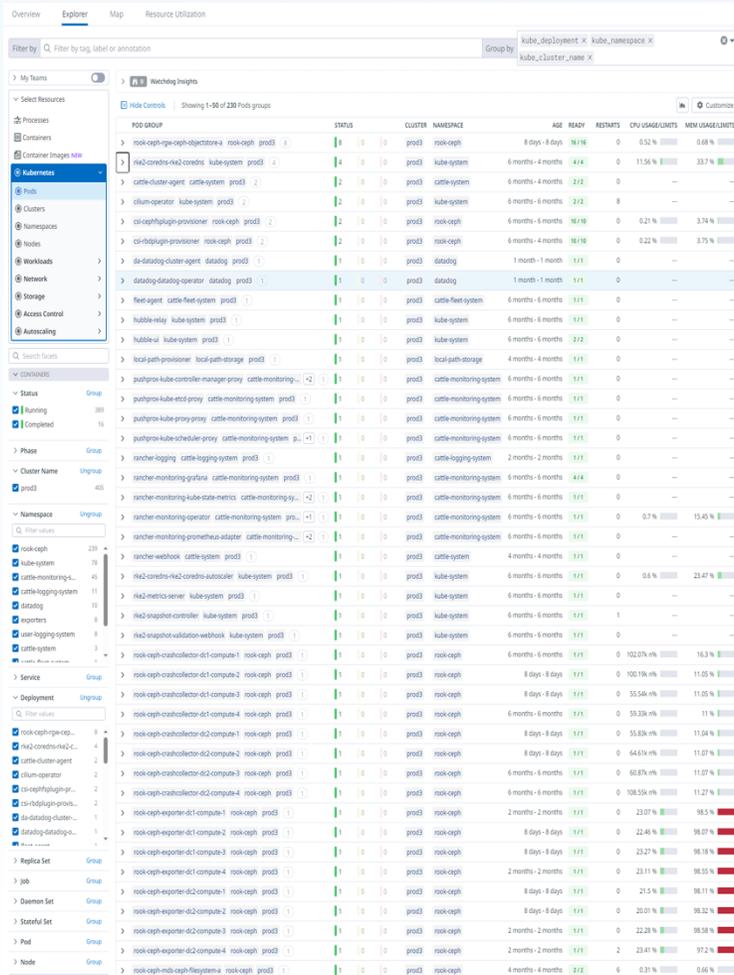
자체 Dashboard 작성 및 사용



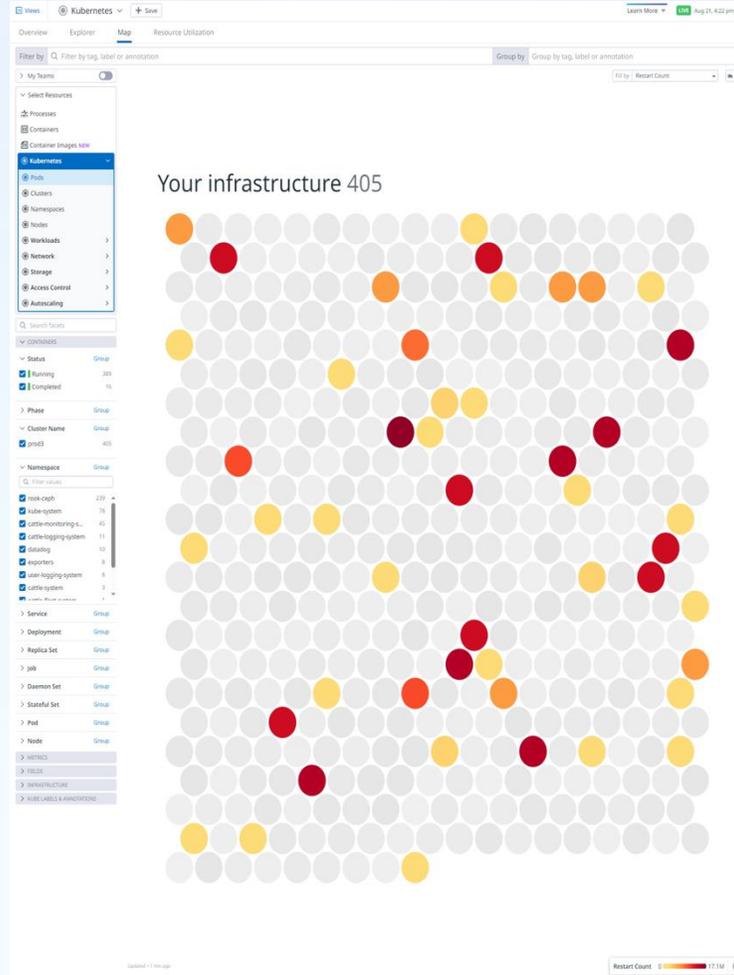
Useful Cases

Kubernetes Resource 확인을 위한 다양한 View 들

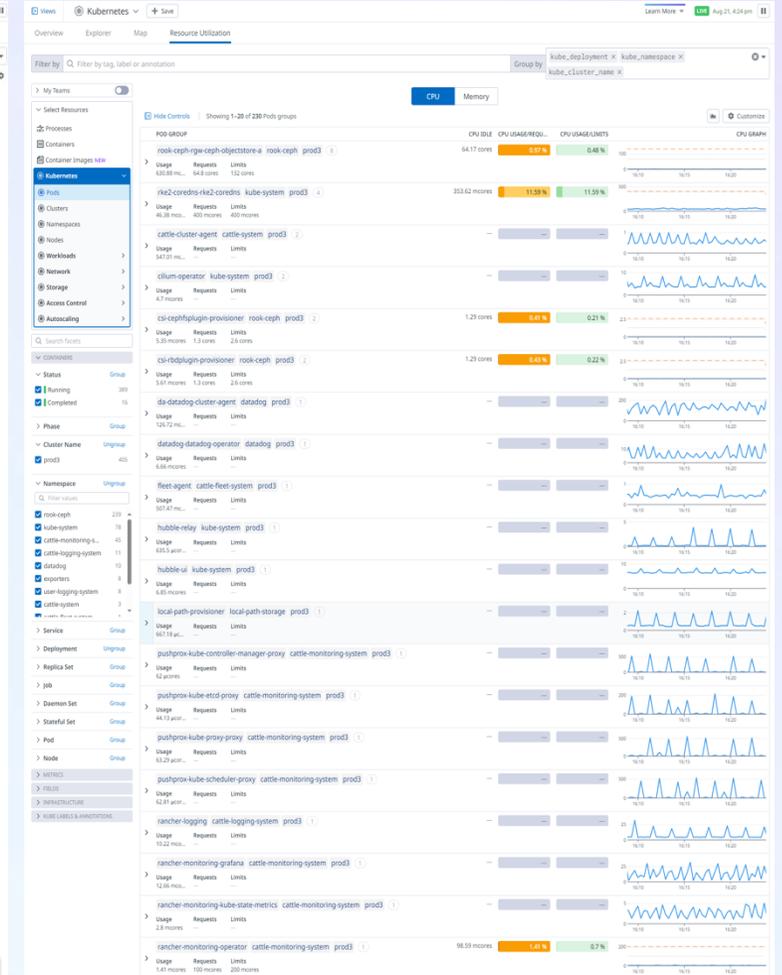
Kubernetes Explorer



Kubernetes Map



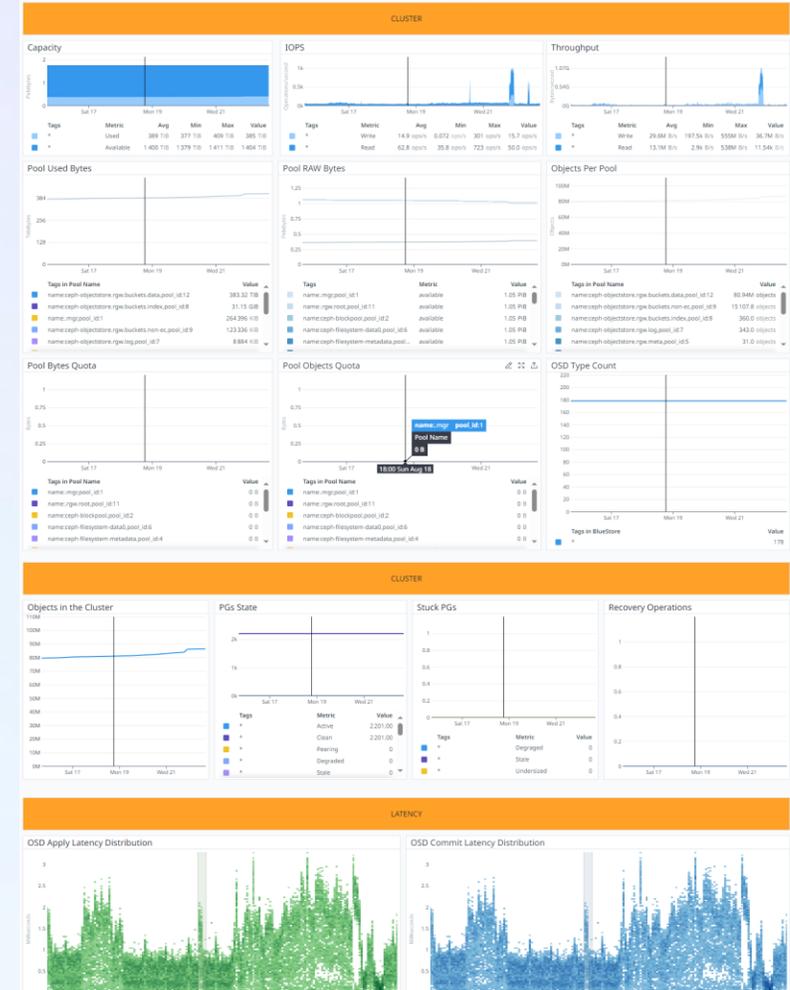
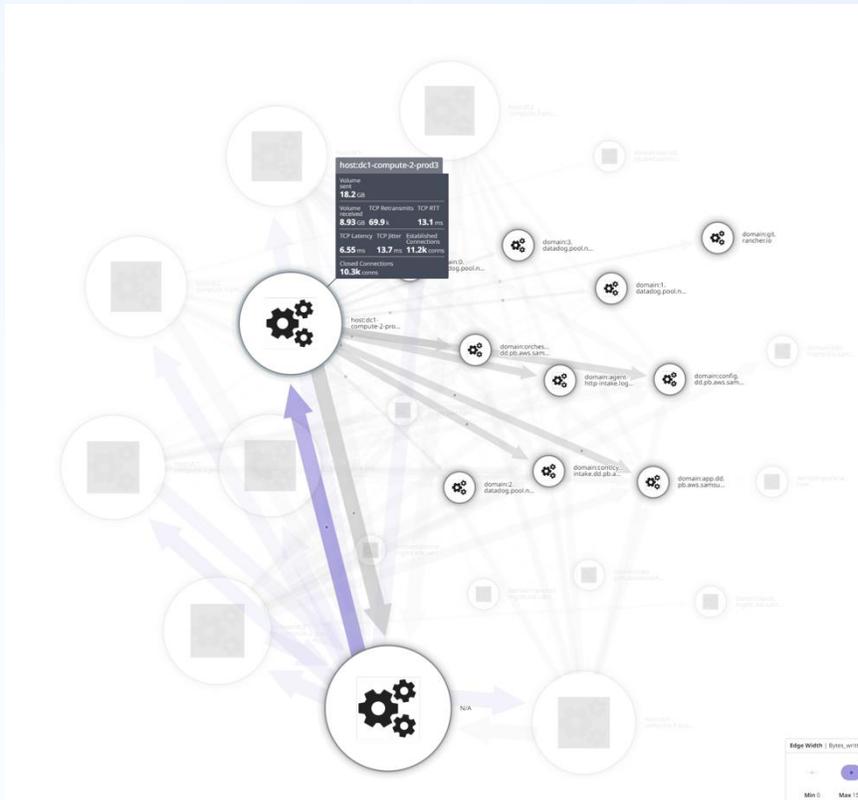
Resource Utilization



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 Pod 발생

- 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

Integrations > GitHub Applications

GitHub Applications

by Datadog Datadog Supported

Configure GitHub Apps and access GitHub Actions to gain secure access to organizations and collect advanced telemetry.

Overview **Configuration** Webhooks **INSTALLED** Telemetry

Search by org name or application name

1 Application found in 1 org

Datadog - pbssd
poseidonos Organization
40 repositories

Features Repositories Deletion Instructions

Features

- ✓ **API Catalog: Sync OpenAPI files**
Synchronize OpenAPI definitions in the API catalog.
[View Required Permissions](#) | [View docs](#)
- CI Visibility: monitor GitHub actions**
Monitor your workflows, jobs, and steps and view trends over time. Optionally collect
This feature requires additional configuration. [Configure in CI Visibility](#)
[View Required Permissions](#) | [View docs](#)

Several Clicks!!

Setup Getting Started **Pipeline Setup** Test Service

Get Started with CI Visibility

Follow instructions below to set up your CI Provider

1 Which CI Provider are you using?

- GitHub
- Jenkins
- CircleCI
- GitLab

손쉬운 CI Visibility 통합

Views | Event Management | Case Management

Event Management | Overview | Explorer | Enrich & Normalize | Correlation NEW

Enter your query

Search facets

Showing 25 of 25 + Add

- CORE
- Source
 - GitHub 995
- Host
- Service
- Status
 - Error 0
 - Warn 0
 - Info 995
- message
- Team
- EVENT
- Aggregation Key
- Duration

Hide Controls | 995 results found

SOURCE MESSAGE

- INFO Pull Request 609 closed on poseidonos/pos-essential-orchestrator: [PBD] 40 files changed with 9336 additions and 12 deletions by #minjoon-ahn Background source:github assignee:minjoon-ahn branch:main event_action:closed event_group:commits
- INFO minjoon-ahn pushed to main at poseidonos/pos-essential-orchestrator There was 1 commit in this push by #minjoon-ahn Compare URL Commits: 1a4eae6 Minjoon Ahn [PBDEV-1869] TDK documentation (#609) (added) tdk/datab source:github branch:main event_group:commits repo:poseidonos/pos-essential-orchestrator
- INFO Pull Request 39 review_requested on poseidonos/pos-essential-failure-... 5 files changed with 10 additions and 10 deletions by #hsung-yang submodule... source:github assignee:hsung-yang branch:main event_action:review_requested
- INFO Pull Request 39 review_requested on poseidonos/pos-essential-failure-... 5 files changed with 10 additions and 10 deletions by #hsung-yang submodule... source:github assignee:hsung-yang branch:main event_action:review_requested

Search

Showing 1-5 of 5 pipelines Some pipelines are excluded Options

PIPELINE	DEFAULT BRAN...	EXECUTIONS	FAILURES	FAILURE %	MEDIAN	MEDIAN CHANGE	LAST BUILD	DURATION	LAST RUN
poseidonos/pos-essential-orchestrator 02. Post-merge	main	11	0	0%	15 min 32 s	-42.0 s	RUNNING		
poseidonos/pos-essential 02. Post-Merge-Performance-Test	main	12	3	25.0%	5 min 35 s	-	ERROR	1 min 2 s	18 hours ago
poseidonos/pos-essential 02. Post-Merge	main	21	1	4.8%	10 min 25 s	+10.0 s	SUCCESS	11 min 54 s	21 hours ago
poseidonos/pos-essential 01. Pre-merge - Submodule update	main	23	5	21.7%	24 min 29 s	0 ns	SUCCESS	24 min 43 s	23 hours ago
poseidonos/pos-essential-ioworker 02. Post-merge	main	6	0	0%	41 min 44 s	-37.0 s	SUCCESS	42 min 25 s	5 days ago

Last Execution: SUCCESS • 21 hours ago • Pipeline ID: #570 Duration: 11 min 54 s

Total Executions Running and partial executions are excluded. Learn more

Error Rate Running and partial executions are excluded. Learn more

Build Duration Running and partial executions are excluded. Learn more

Job Summary Running and partial executions are excluded. Learn more

Errored Executions Compare to a week before Type: absolute Order by: change

Duration change Compare to a week before Type: absolute Order by: change

Jobs per page: 5 | 1 2 3 4 5 6 7 ... 10

JOB	P50 DURATION	P95 DURATION	EXEC TIME %	FAILURE %
Build (DEBUG)	7 min 27 s	8 min 47 s	39.2%	0%
Build (RELEASE)	7 min 11 s	8 min 26 s	37.8%	4.8%
Cleanup_PM	16.5 s	19.1 s	1.4%	0%
Deploying-Artifacts (pos-essential-debug, 0.2.5-rc.10-17+277ae0fc_amd64.deb)	4 min 1 s	4 min 1 s	1.0%	0%
Deploying-Artifacts (pos-essential-debug, 0.2.5-rc.10-21+30b43a13_amd64.deb)	2 min 21 s	2 min 21 s	0.6%	0%

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 \(datadoghq.com\)](https://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
- ~~가거... ㄱ 적인...~~

Thank you

Still Hungry. 부족한 Da린이들의 발표 들어주셔서 감사합니다.



DATADOG