Graph-based ML Anomaly Detection and Insights for Envoy Systems

Presenter: Anoop Koloth, Hanzhang Wang

Team: Anirudh Muralidhar, Kalieswaran Rayar, Phuong Nguyen, Saravana Chilla, Venkatesh Palani

EnovyCon, Nov 18, 2019

Agenda

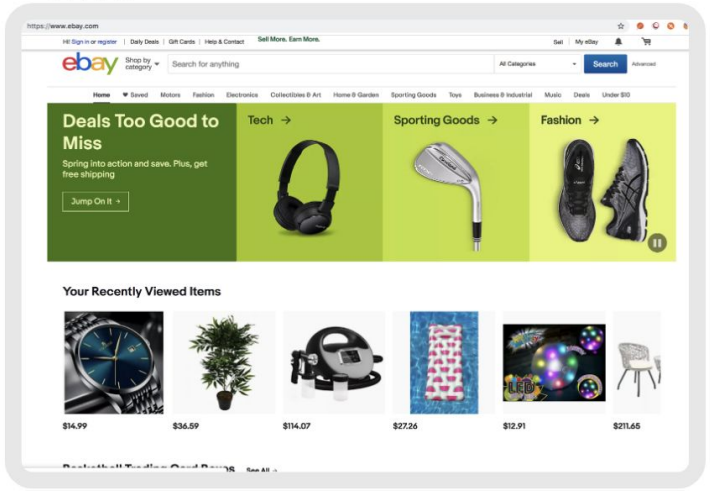
eBay Envoy Ecosystem

Data, Traffic Insights and Anomaly Detection

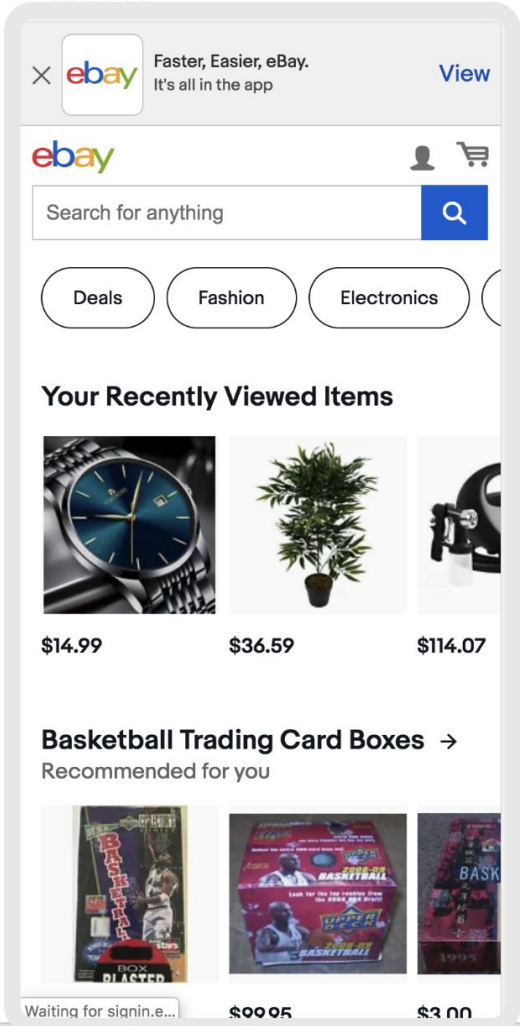
Grano - Graph-based Anomaly Detection

Traffic Engineering

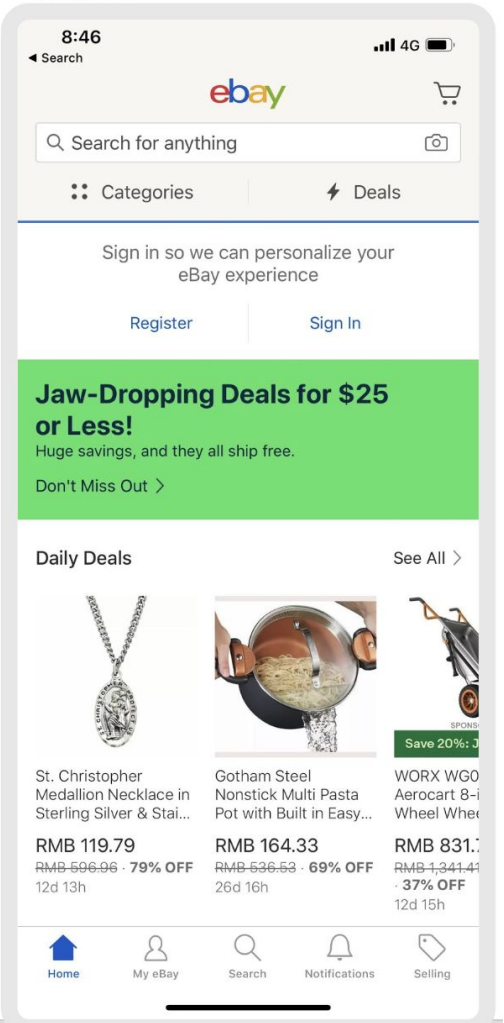
dweb



mweb



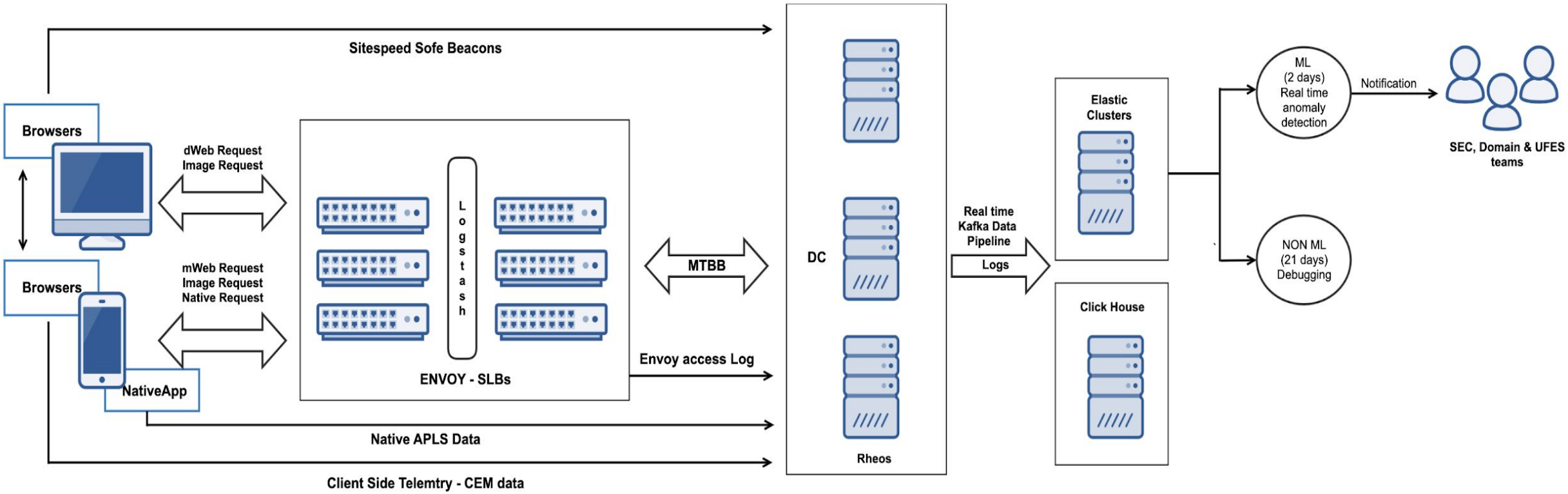
native



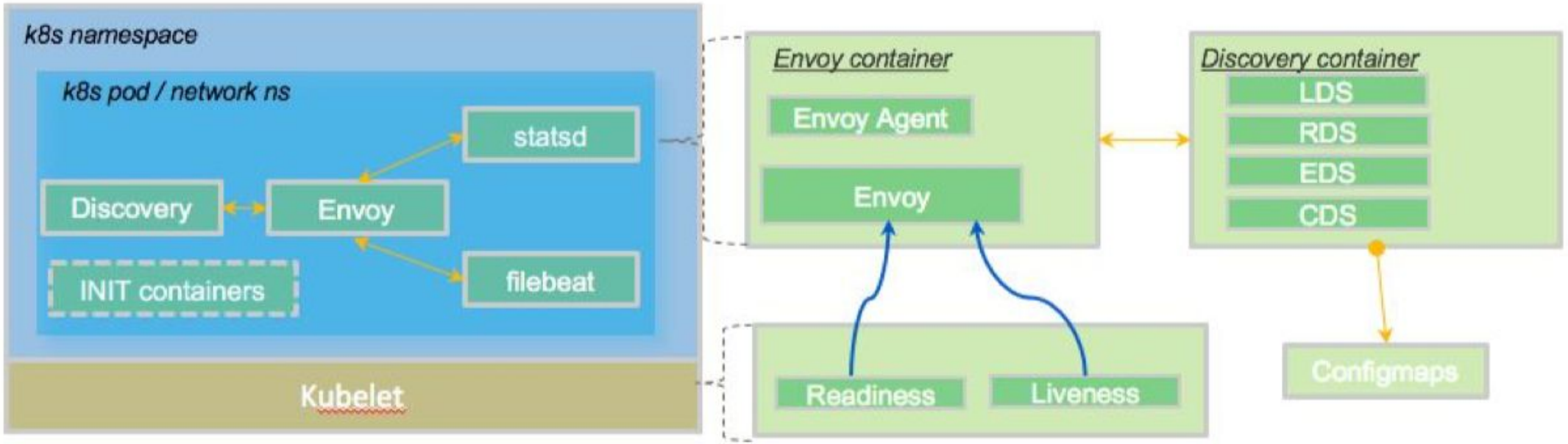
AVAILABILITY

LATENCY

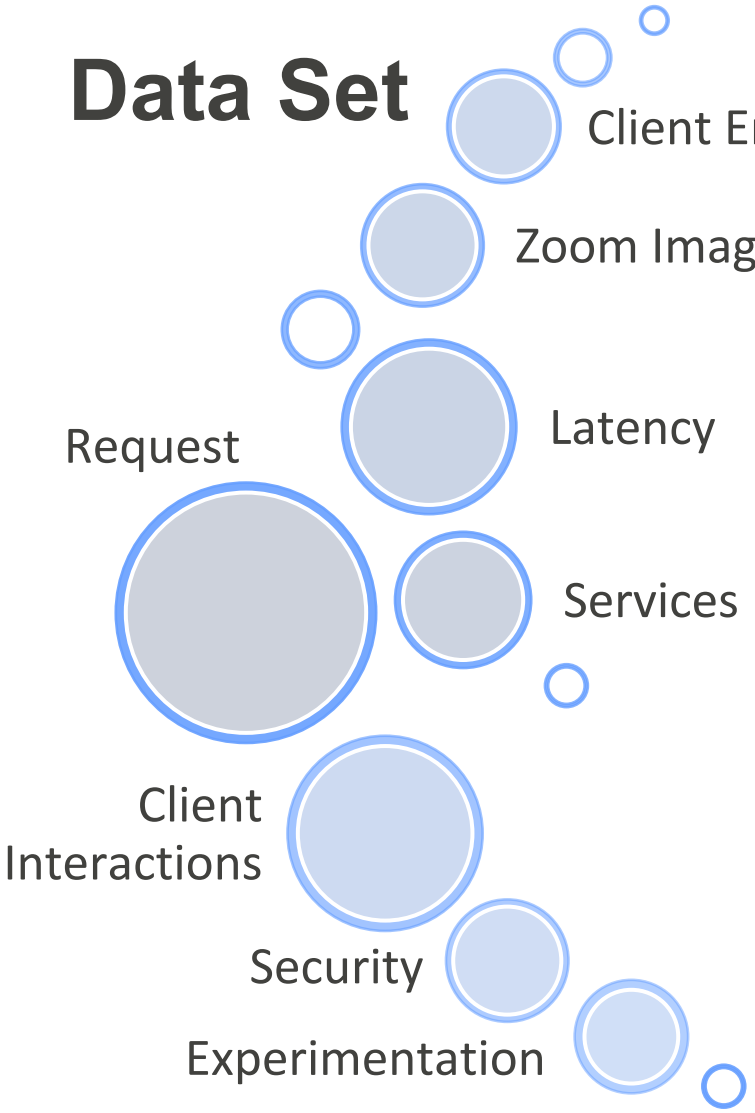
Envoy at eBay



L7 - High Level



Data Set



>12 Billion+ records /day
120+ dimensions
60+ metrics

Anomaly Detection

Ramp Up Decision

Bot/Attack
Remediation

Traffic
Insights

Raw Record

🕒	@timestamp	November 14th 2019, 21:08:38.021
t	@version	1
t	_id	Rrl2bW4B-lxstDMwmTQn
t	_index	envoy-access-nonml-2019.11.14.18.00.12
#	_score	1
t	_type	envoyaccesslog
t	actual	masked
#	actual_pop_dist	masked
t	agent	"eBayiPad/5.38.0"
t	authority	"apisd.ebay.com"
#	bytes_received	94
#	bytes_sent	277
t	city	Hoppers Crossing
t	closest_pop	masked
#	closest_pop_dist	masked
t	cluster_name	SYD
t	country	Australia
t	data_center	LVS
#	duration	148
t	host	masked
t	httpversion	1.1
t	img_pxl_size	-
#	is_right_pop	0
t	isp	telstra internet
t	l7_cluster	nativeapp
t	method	POST
#	offset	masked
t	parent	masked
t	path	/shopping
t	path_f	/shopping
#	popTime	0
t	referer	"-"
t	response	200
t	response_group	2xx
t	rlog_id	-
t	route_name	masked
t	source	/var/log/envoy_access.log
t	ssl_version	masked
🕒	start_time	November 14th 2019, 21:08:37.260
t	state	Victoria
t	tags	envoy, beats_input_codec_plain_applied
#	time_to_first_resp_byte	148
t	type	envoy-access
#	upstream-service-time	148
t	upstream_host	masked
t	upstream_port	443
t	x-forwarded-for	masked
t	x-request-id	masked
t	x_ebay_akamai_9	masked
t	x_ebay_pop_id	UFES2-SYD

route_name , rlogid , isp ,
actual_pop_dist , actual ,
parent , tags ,
upstream-service-time ,
time_to_first_resp_byte,
response_flag

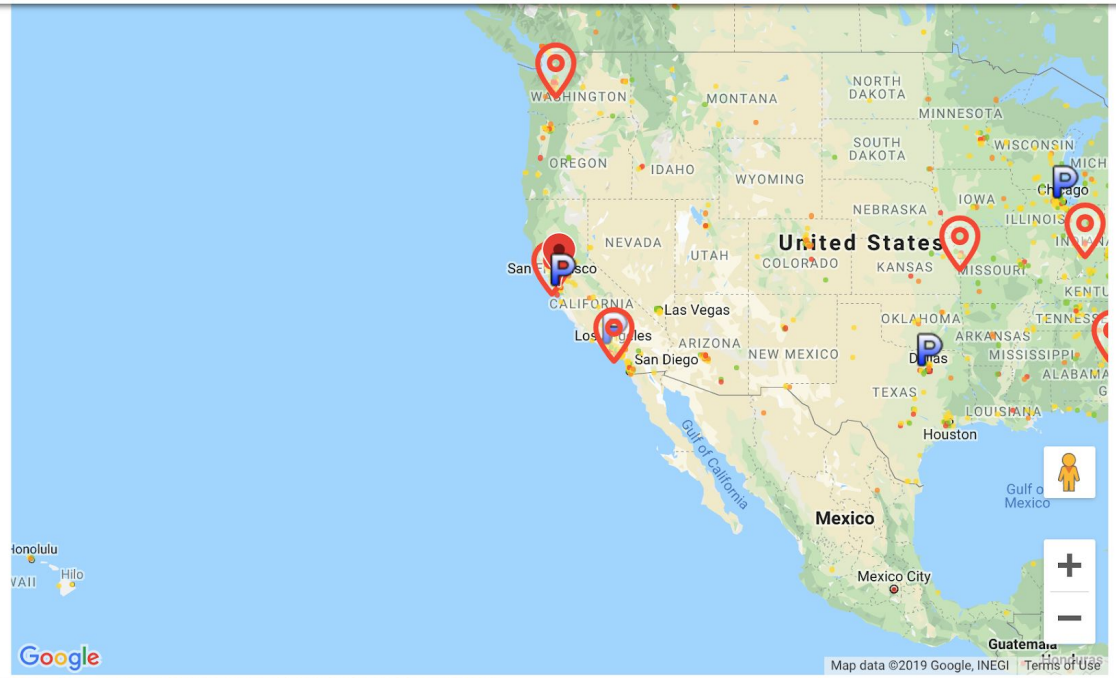
Observability

Traffic Engineering

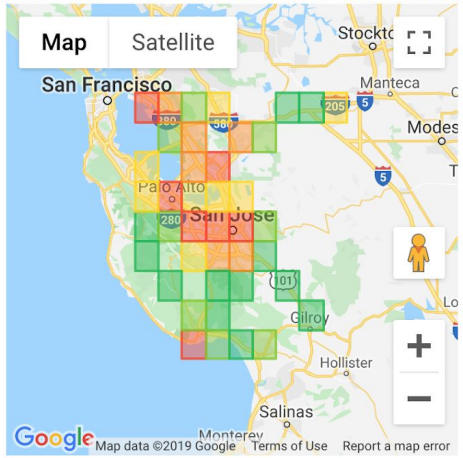
POP:

34412845 hits : Overall

5623179 hits : UFES2-LHR-dweb-2
4876293 hits : UFES2-FRA-dweb-2
3115978 hits : UFES2-SLCAZ01-dweb-1
1704432 hits : UFES2-LHR-dweb-2%2C+UFES1-LHR
1201914 hits : UFES2-MDW-dweb-1%2C+UFES1-MDW
1191351 hits : UFES2-EWR-dweb-1%2C+UFES1-EWR
1156122 hits : UFES2-LVSAZ01-dweb-1
1146849 hits : UFES2-FRA-dweb-2%2C+UFES1-FRA
1121358 hits : UFES2-RNOAZ03-dweb-1
723605 hits : UFES2-SYD-dweb-3
713896 hits : UFES2-DFW-dweb-1%2C+UFES1-DFW
688092 hits : UFES2-EWR-dweb-1
662749 hits : UFES2-AMS-dweb-2
654154 hits : UFES2-MDW-dweb-1
578643 hits : UFES2-SJC-dweb-1%2C+UFES1-SJC
575510 hits : UFES2-LAX-dweb-1%2C+UFES1-LAX
574009 hits : UFES2-MIA-dweb-1%2C+UFES1-MIA
394976 hits : UFES2-DFW-dweb-1
373807 hits : UFES2-SLCAZ01-dweb-2
368938 undefined : UFES2-FRA-dweb-2%2C+UFES1-FRA?
354964 hits : UFES2-SJC-dweb-1
353021 hits : UFES2-LAX-dweb-1
342099 hits : UFES2-MIA-dweb-1
316568 hits : UFES2-SIN-dweb-1%2C+UFES1-SIN
281281 hits : UFES2-FRA-dweb-3
281025 hits : UFES2-LVSAZ01-dweb-2



0-1000 | 1000-2000 | 2000-5000 | 5000-10000 | > 10000 |



119971 score : UFES2-SLCAZ01-dweb-1
49993 score : UFES2-LAX-dweb-1%2C+UFES1-LAX
49699 score : UFES2-SJC-dweb-1%2C+UFES1-SJC
27018 score : UFES2-LHR-dweb-2
5841 score : UFES2-DFW-dweb-1%2C+UFES1-DFW
5591 score : UFES2-MIA-dweb-1%2C+UFES1-MIA

metric	min	median	max
ttfb50	117.5	1539.7	7762.7
tatf50	399	399	399
i29_50	134	134	134
ttfb95	231	231	231
tatf95	754	754	754
i29_95	227	227	227

Anycast

Page:
Overall

POP :

34412845 hits : Overall

5623179 hits : UFES2-LHR-dweb-2
4876293 hits : UFES2-FRA-dweb-2
3115978 hits : UFES2-SLCAZ01-dweb-1
1704432 hits : UFES2-LHR-dweb-2%2C+UFES1-LHR
1201914 hits : UFES2-MDW-dweb-1%2C+UFES1-MDW
1191351 hits : UFES2-EWR-dweb-1%2C+UFES1-EWR
1156122 hits : UFES2-LVSAZ01-dweb-1
1146849 hits : UFES2-FRA-dweb-2%2C+UFES1-FRA
1121358 hits : UFES2-RNOAZ03-dweb-1
723605 hits : UFES2-SYD-dweb-3
713896 hits : UFES2-DFW-dweb-1%2C+UFES1-DFW
688092 hits : UFES2-EWR-dweb-1
662749 hits : UFES2-AMS-dweb-2
654154 hits : UFES2-MDW-dweb-1

First AD Solution

rom: DL-eBay-anomaly-alerts-speed-ufes@ebay.com <DL-eBay-anomaly-alerts-speed-ufes@ebay.com>
ent: Thursday, August 23, 2018 12:00:51 AM
o: DL-eBay-anomaly-alerts-speed-ufes
ubject: Severity : [Critical] - ML Alert for job [envoy_duration_upstreamtime_poptime_by_top50_path_popid_p50]

lastic Stack Machine Learning Alert

ob: envoy_duration_upstreamtime_poptime_by_top50_path_popid_p50
ime: 2018-08-23T06:45:00.000Z
nomaly score: 66

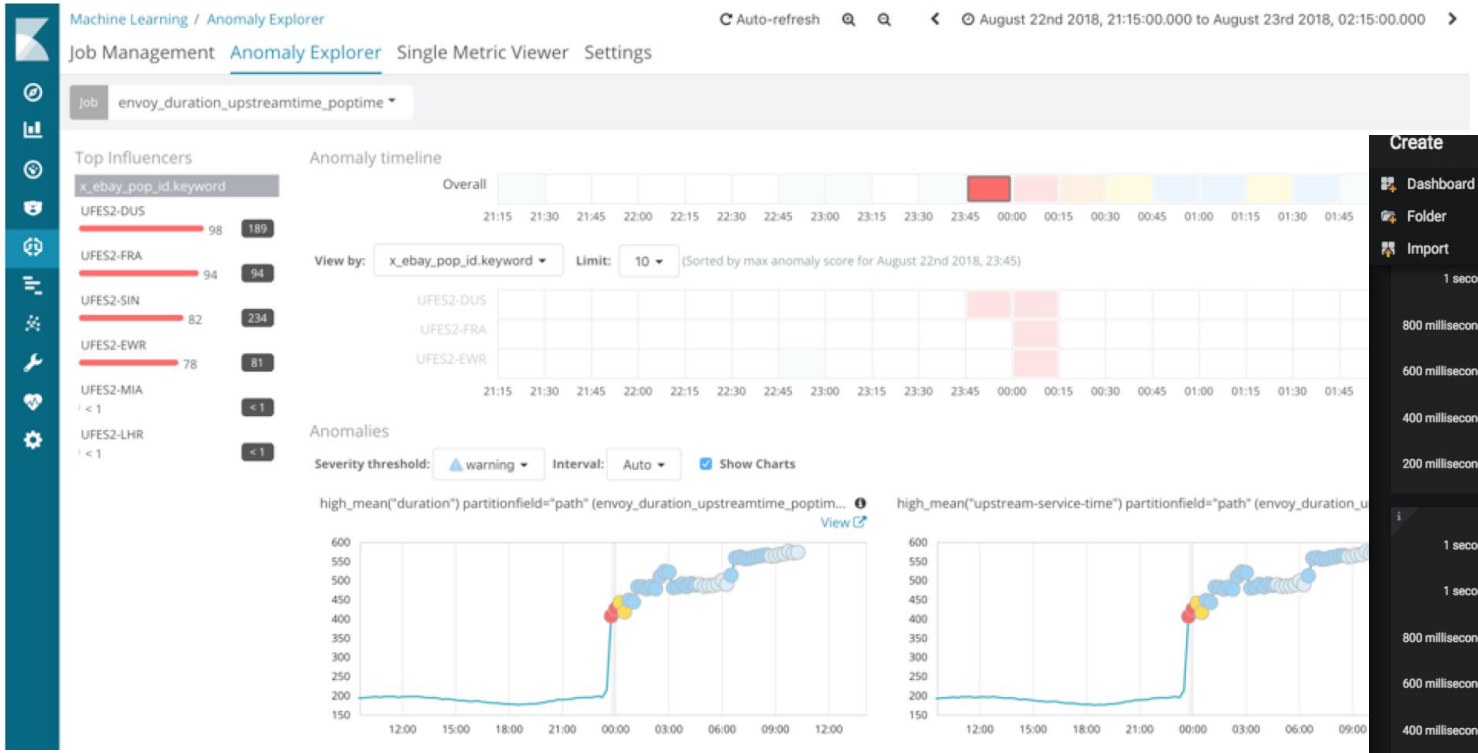
lick here to open in Anomaly Explorer.

op influencers:

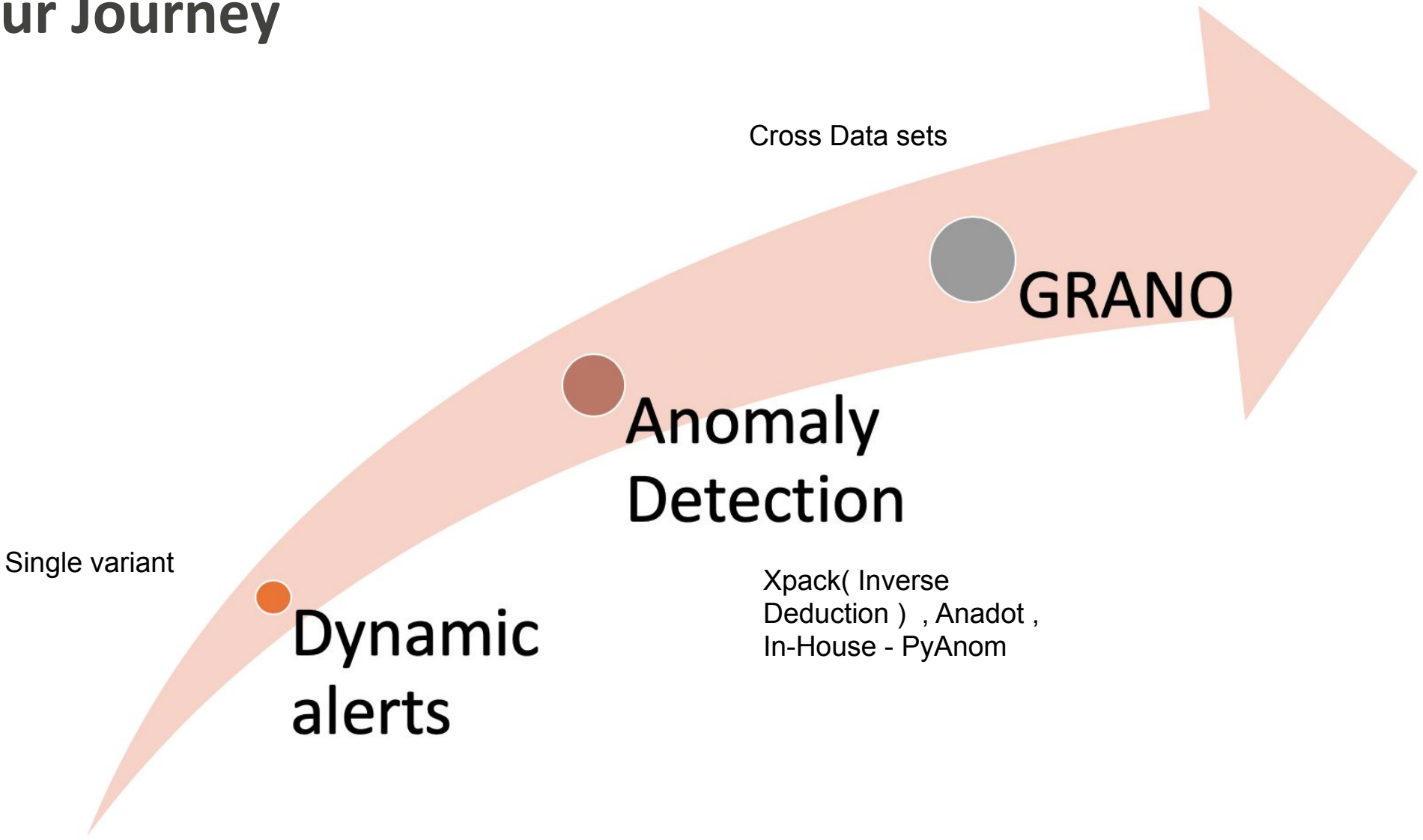
Influencer_field(value)	Score	Severity
x_ebay_pop_id.keyword(UFES2-DUS)	[92]	Critical

op records:

Detector	By_field	Over_field	Partition field	Score	Severity	Actual	Typical
high_mean(duration)			/svcs/services/mobileor/v1/CommonMobileAppService	[100]	Critical	395.36218536825794	187.53703886799974
high_mean(upstream-service-time)			/svcs/services/mobileor/v1/CommonMobileAppService	[100]	Critical	394.98731082228227	187.1285341027986



Our Journey



Grano Vision

“Leverage ML and graph-based solutions to reduce Mean Time to Detect (MTTD) production incidents in distributed systems.”

The time between and incident and somebody’s knowing about it.

- “Somebody” is an automated response system or a person
- “Knowing about” Doesn't count if there's an alert that gets lost in a flood of alerts, even if the monitoring system knew.
- “It” is the incident and the root cause(s).

Grano

Graph-based Anomaly Detection System

GRANO is an *end-to-end* **gra**ph-based **ano**maly detection and root cause analysis system for distributed cloud-native systems

Anomaly Detection
ML time series anomaly detection on metrics

Adaptive Anomaly Graph
Adaptive analysis of all health signals on a real-time property graph of connect metrics/event (or project on a system topology) to identify the root cause

Applications
Alerting, interactive Graph-UI, and integration with monitoring system

Knowledge Graph (or Heterogeneous Graph)

Knowledge Graph:

1. Represents knowledge domain.
2. Connects things of different types in a systematic way.
3. Encode knowledge arranged in a network of nodes and edges rather than tables of rows and columns.

Why graph here?

1. Native method to understand the “Unknown”
2. White box and Visualization
3. The platform and support is ready (e.g. Data, Graph DB, Computation Power)
4. “Get ready for AI” or “translator of AI” analysis (Pattern)
5. Recommendation/Refactoring

Motivating Example

From: "DL-eBay-anomaly-alerts-speed-ufes@ebay.com" <DL-eBay-anomaly-alerts-speed-ufes@ebay.com>
Date: Saturday, October 19, 2019 at 11:14 AM
To: "DL-eBay-anomaly-alerts-speed-ufes@ebay.com" <DL-eBay-anomaly-alerts-speed-ufes@ebay.com>, DL-eBay-ufes-alerts <DL-eBay-ufes-alerts@ebay.com>
Cc: DL-eBay-speed-ad-alerts <DL-eBay-speed-ad-alerts@ebay.com>
Subject: Severity : [Warning] - ML Alert for job [dweb_envoy_duration_upstreamtime_by_clu

Elastic Stack Machine Learning Alert

Job: dweb_envoy_duration_upstreamtime_by_cluster_popid_p50
Time: 2019-10-19T17:45:00.000Z
Anomaly score: 45

Click here to open in Anomaly Explorer.

Top influencers:

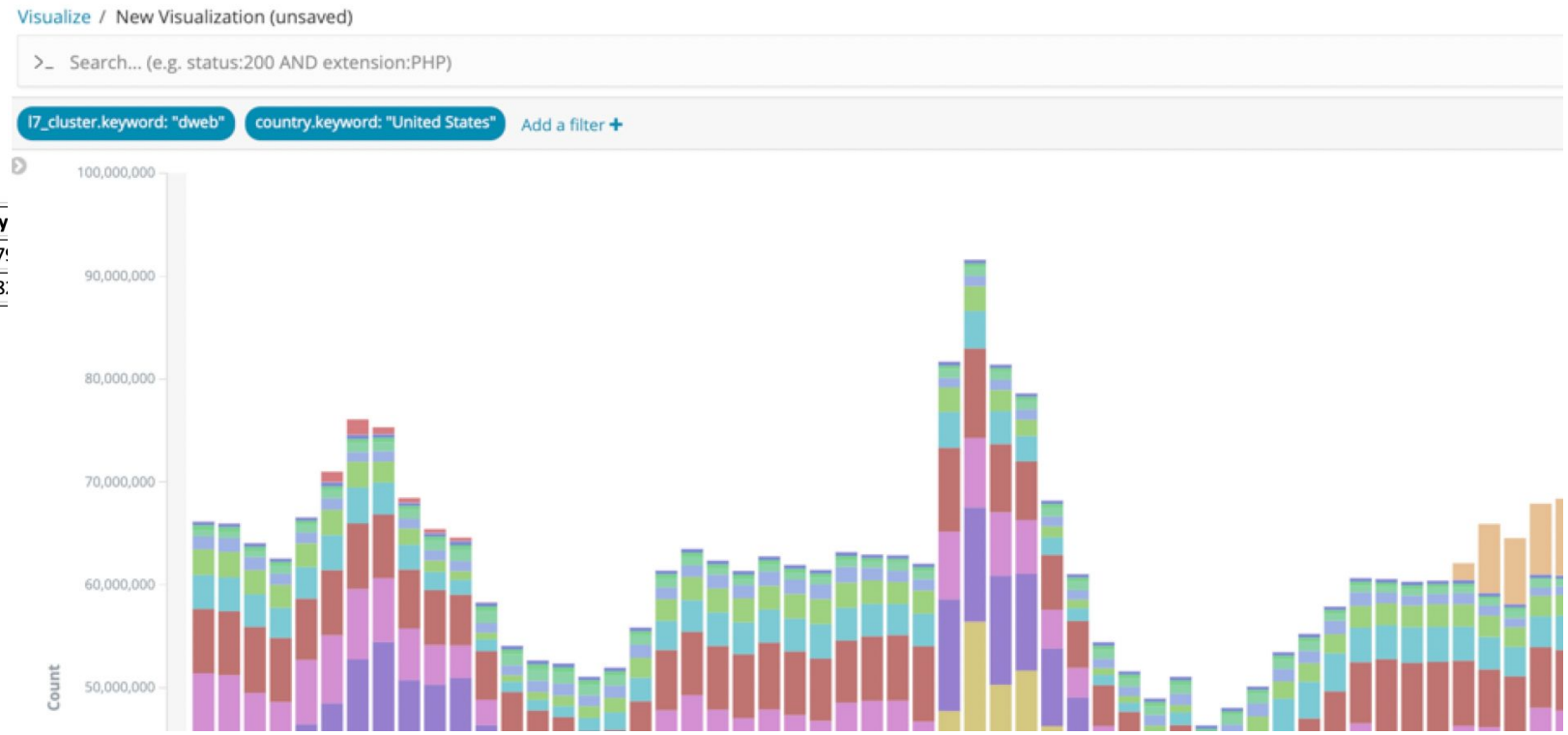
Influencer_field(value)	Score	Severity
x_ebay_pop_id.keyword(UFES2-MDW-dweb-2)	[94]	Critical

Top records:

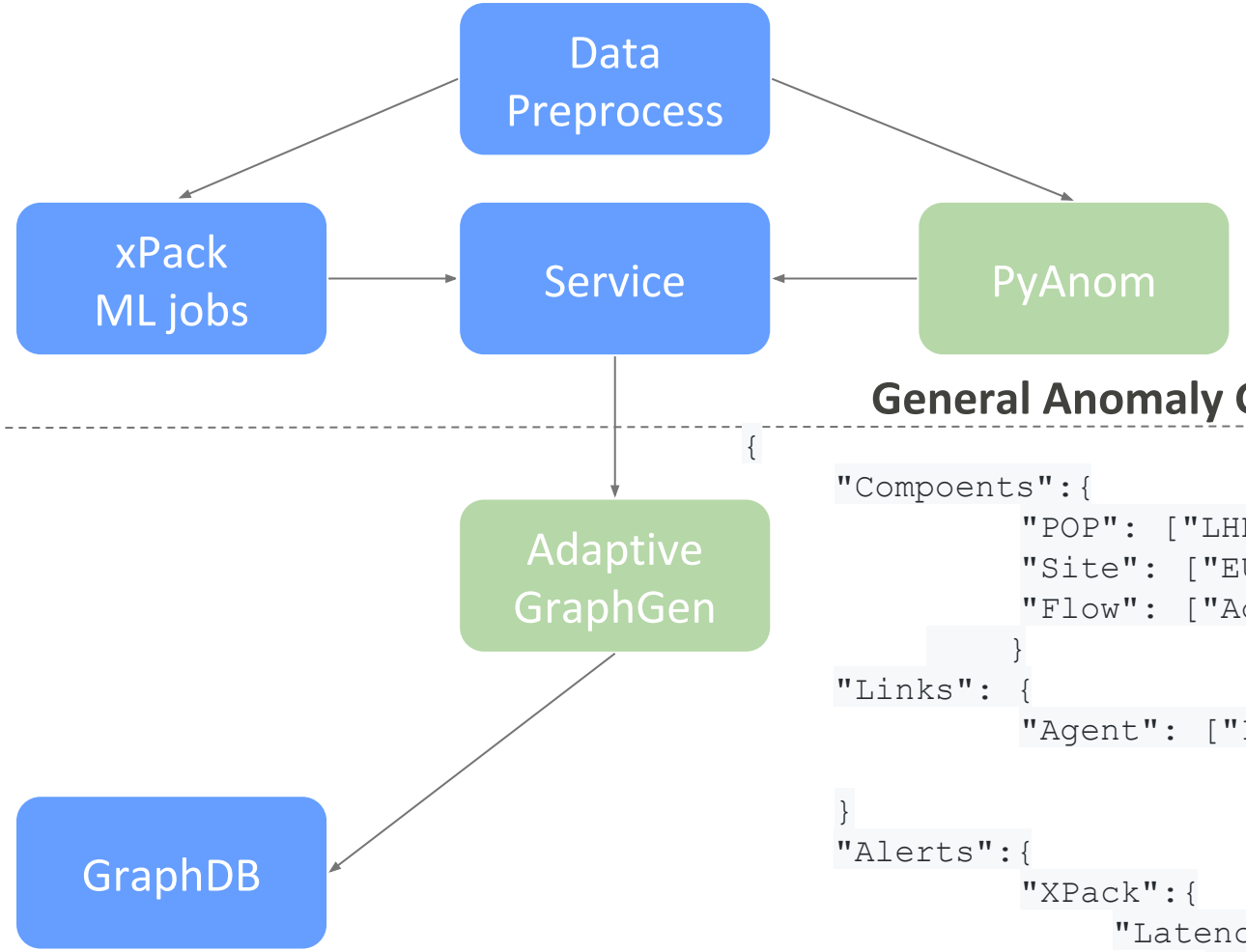
Detector	Partition field	Score	Severity	Actual	Ty
high_mean(upstream-service-time)	MDW	[94]	Critical	296.0211258874482	129.1177
high_mean(duration)	MDW	[92]	Critical	357.8432125356966	147.7838

From: "Rayar, Kalieswaran" <krayar@ebay.com>
Date: Saturday, October 19, 2019 at 11:53 AM
To: DL-eBay-anomaly-alerts-speed-ufes <DL-eBay-anomaly-alerts-speed-ufes@ebay.com>, DL-eBay-ufes-alerts <DL-eBay-ufes-alerts@ebay.com>
Cc: DL-eBay-speed-ad-alerts <DL-eBay-speed-ad-alerts@ebay.com>
Subject: Re: Traffic shifted from SJC & LAX to MDW

This alert is triggered by traffic shift from SJC & LAX to MDW since 5 AM this morning:



Grano Quick Walkthrough

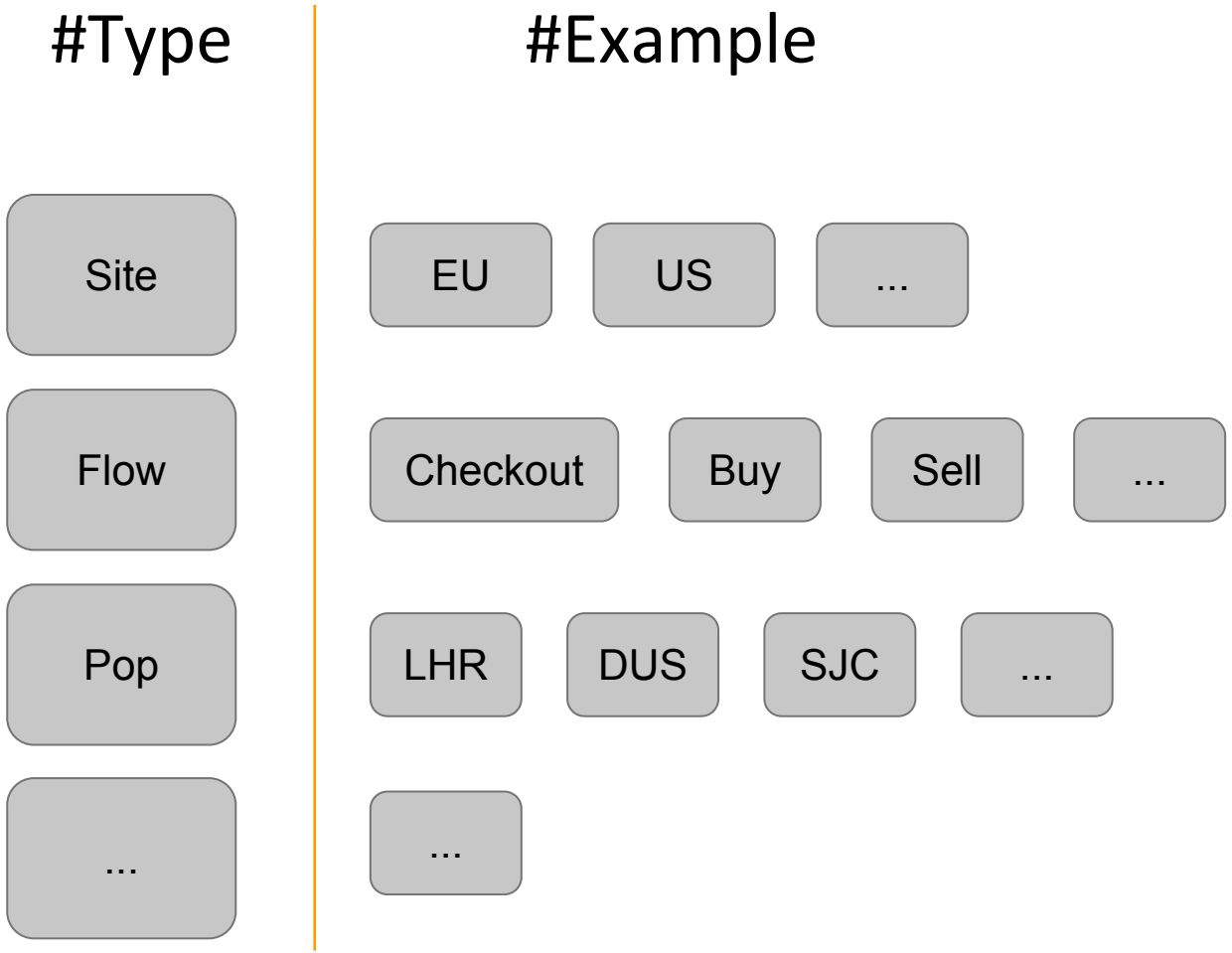


- Additive decomposition forecasting models
- Multivariate clustering models
- Statical-based models

General Anomaly Graph Schema

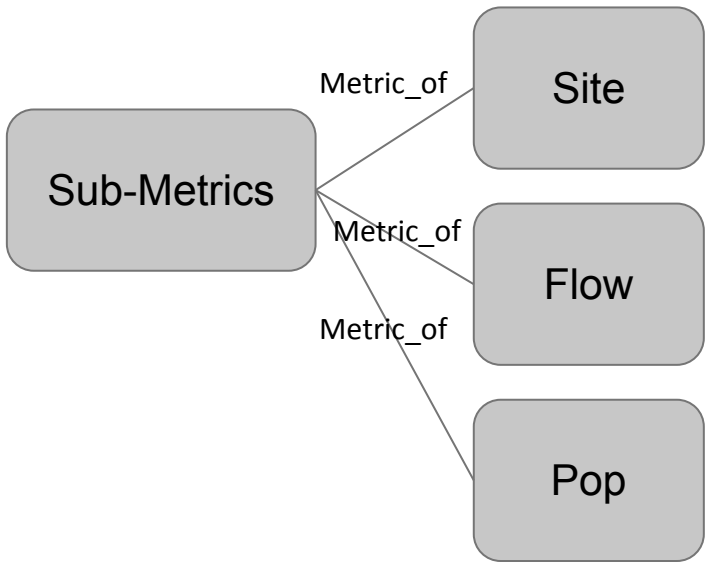
```
{
"Compoents":{
          "POP": ["LHR"]
          "Site": ["EU","US"]
          "Flow": ["AddtoCart", "Checkout"]
        }
"Links": {
          "Agent": ["POP","Flow","Site"]

}
"Alerts":{
          "XPack":{
               "Latency 90":{
                    "LHR": [0,0,0,0.4]
                    "LHR_AddtoCart EU":
                              [0.1,0.3,0.5,0.9]
               }
          }

}
}
```

Adaptive GraphGen

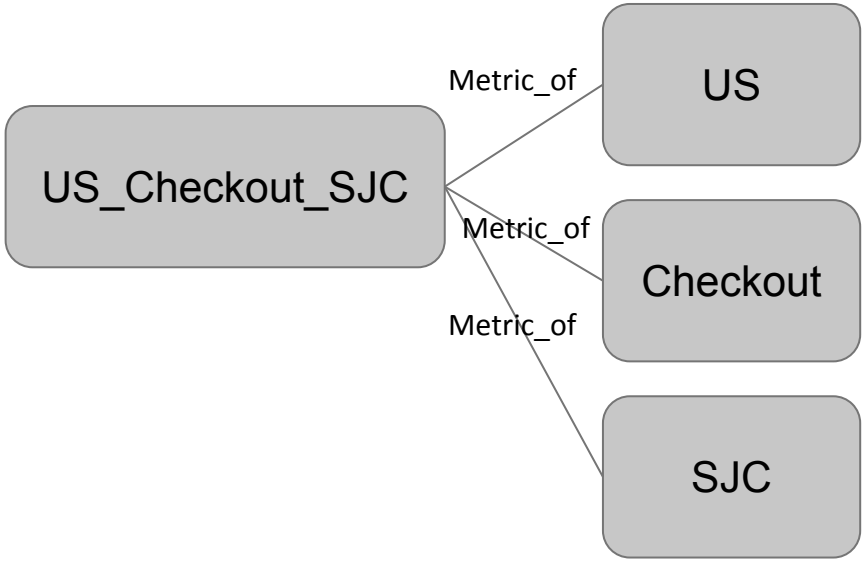


Adaptive GraphGen

#Type

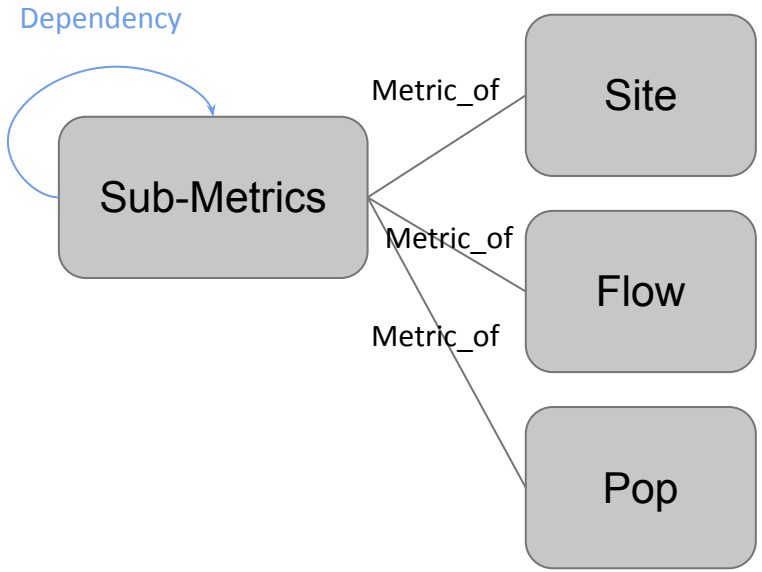


#Example

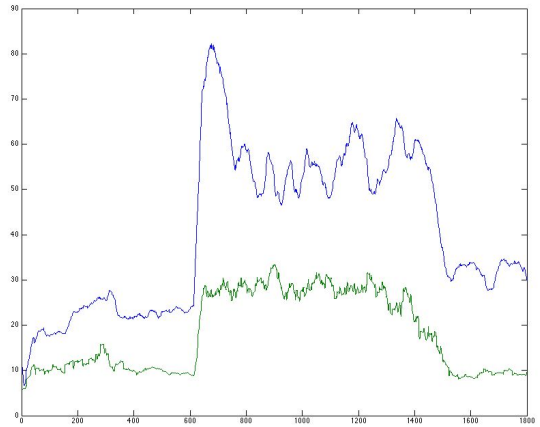


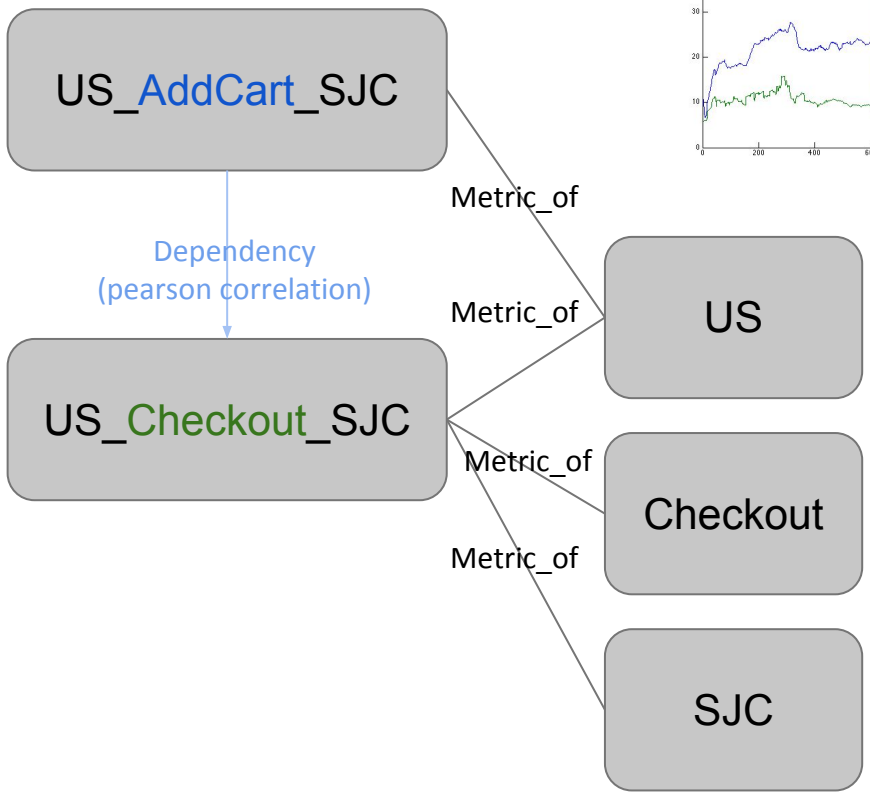
Adaptive GraphGen

#Type

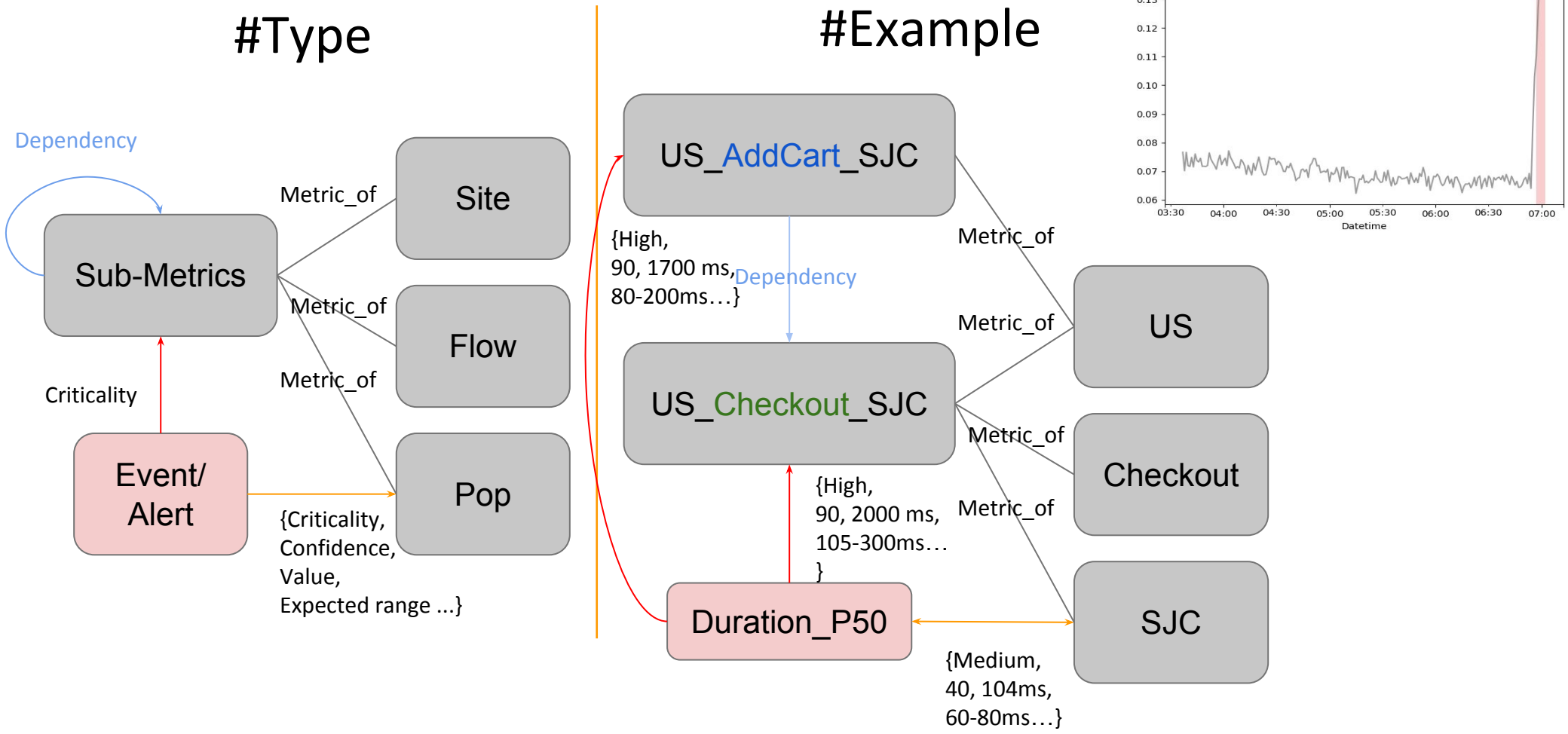


#Example

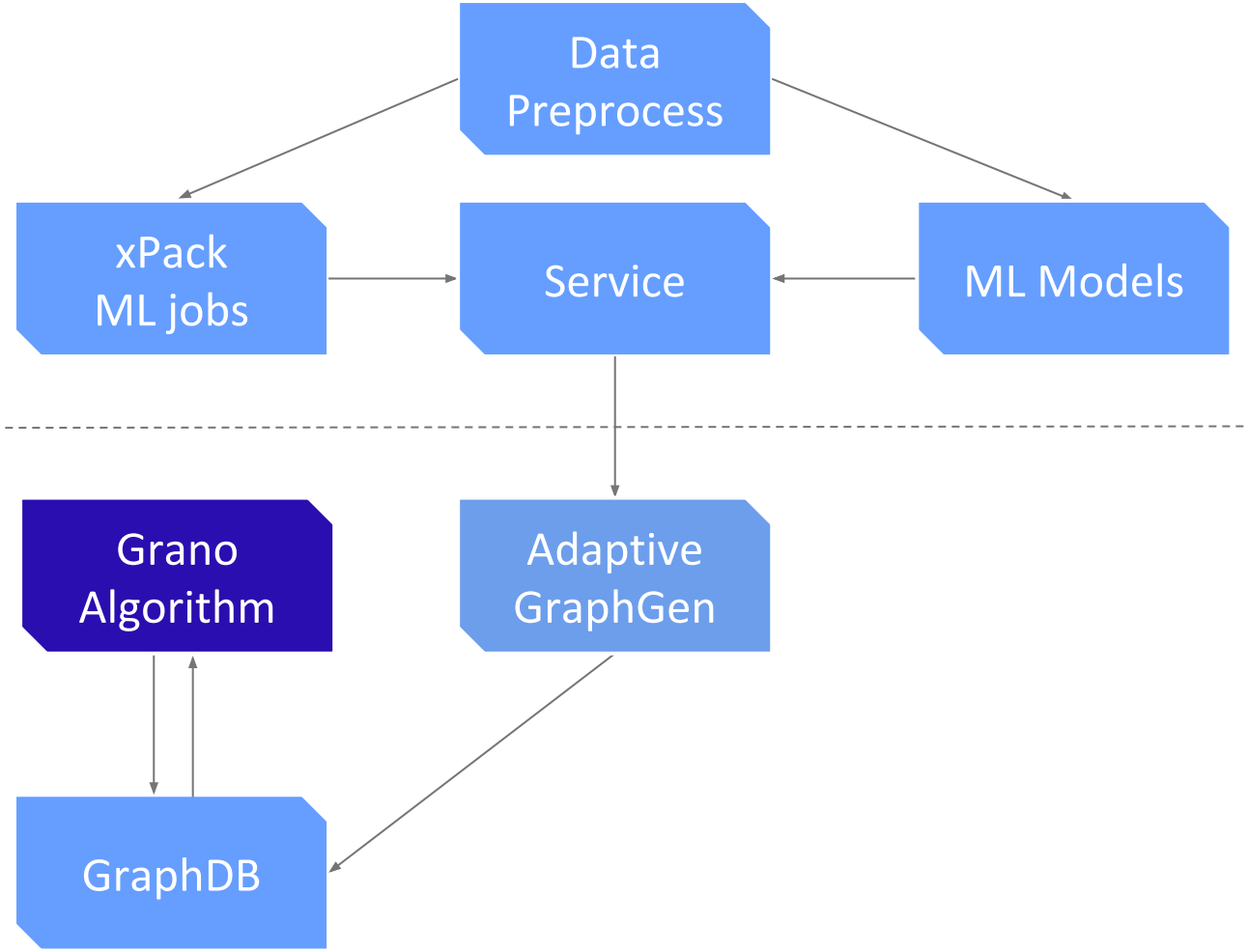




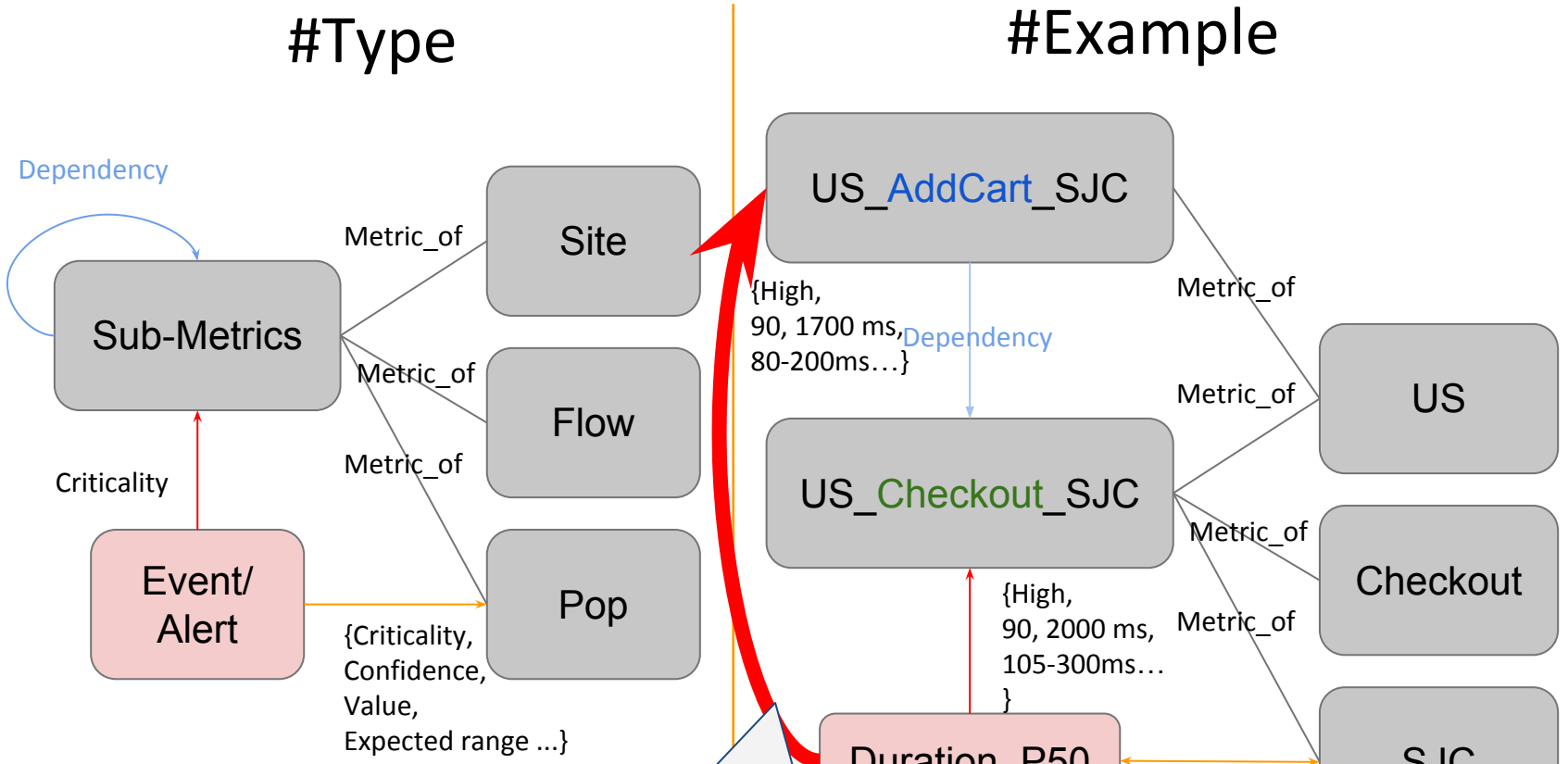
Adaptive GraphGen



Grano Quick Walkthrough



Grano Algorithms



$$\sigma^0_{e(a,c)} = x_0$$

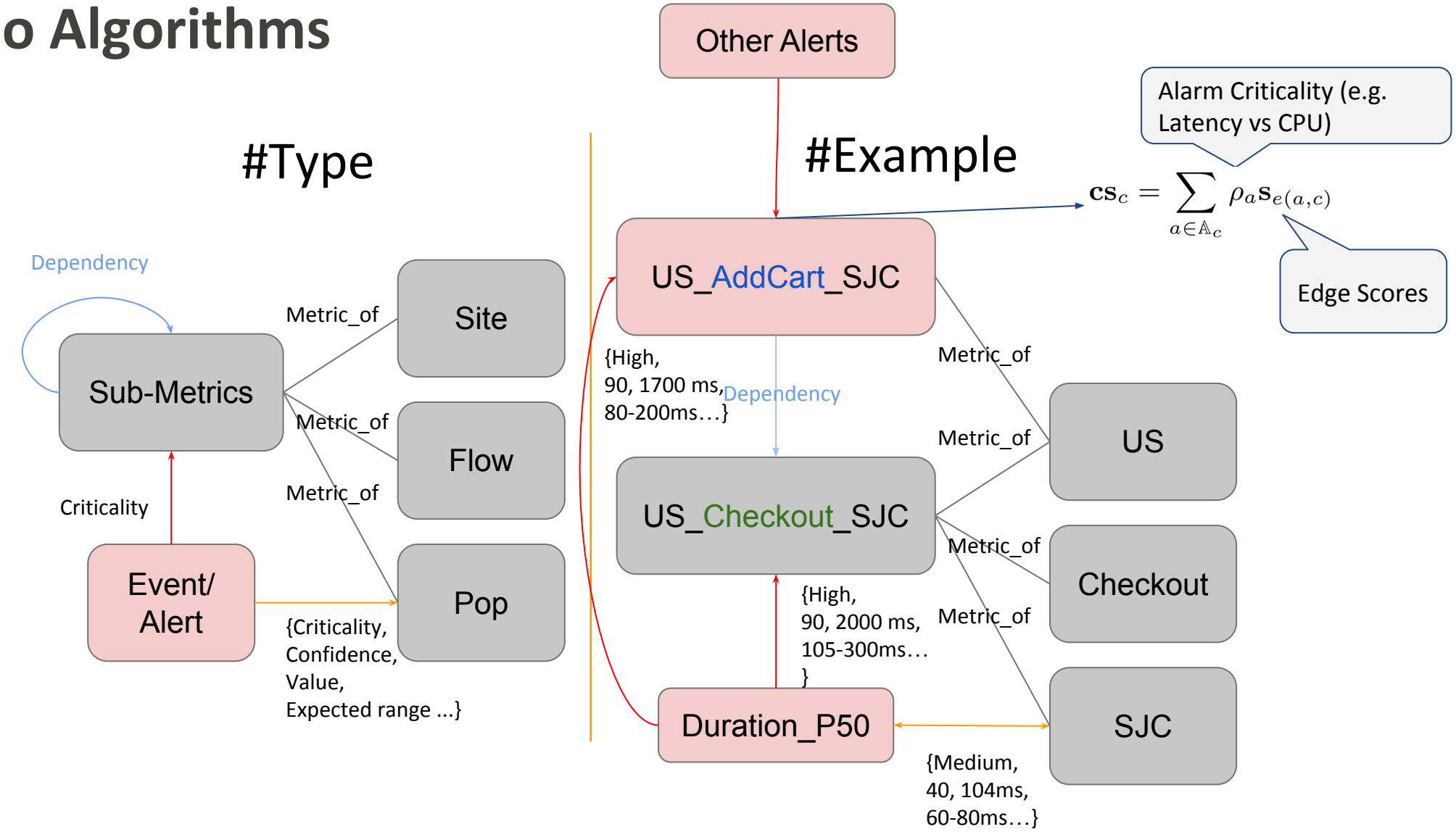
$$\sigma^t_{e(a,c)} = \alpha x_t + (1-\alpha)\sigma^{t-1}_{e(a,c)} (t > 0)$$

$$\mathbf{s}_{e(a,c)} = \sigma_{e(a,c)} \log(\frac{|\mathbf{C}|}{|\mathbb{C}_a|})$$

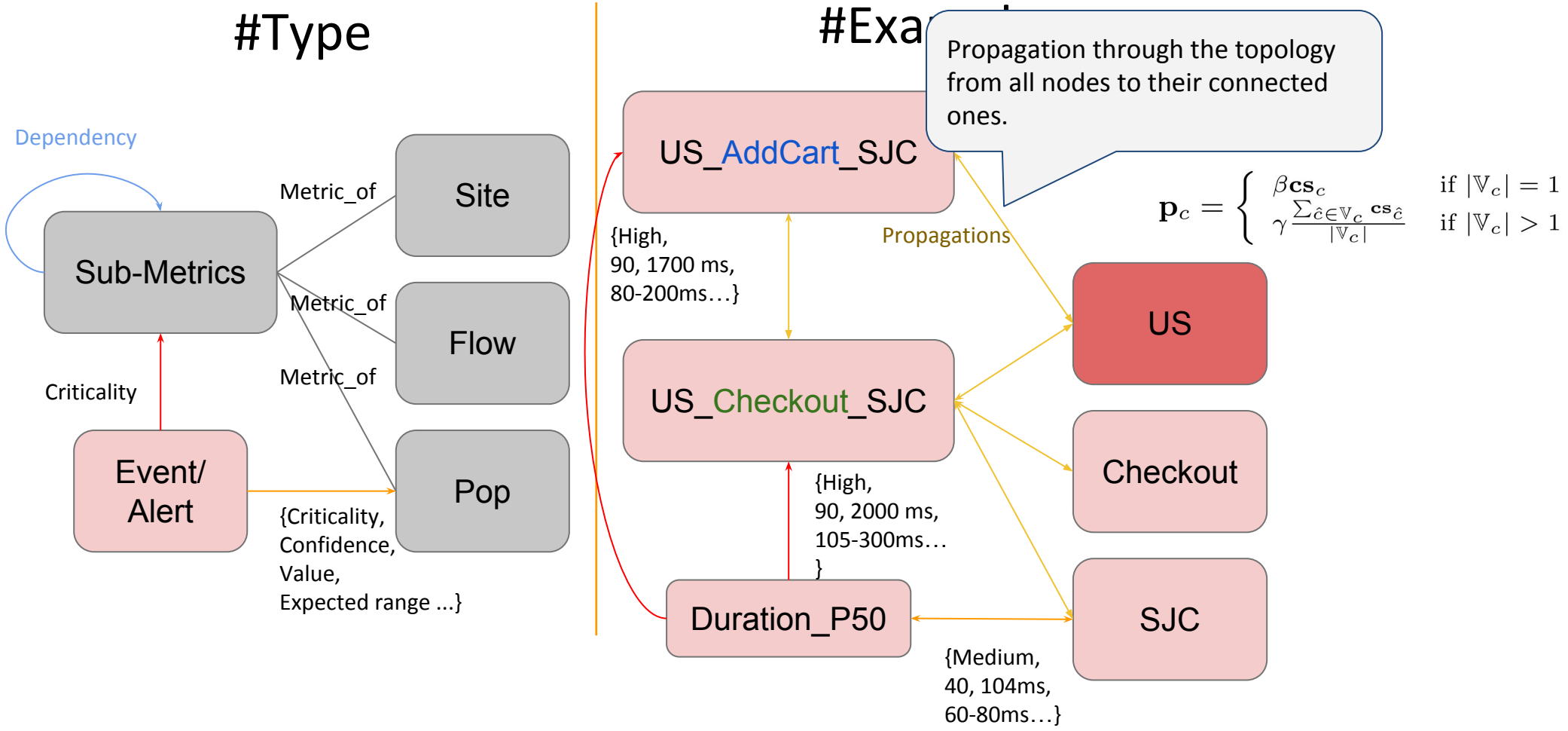
Assign edge score based on:

1. Alarm Severity (Metrics *Dynamics*)
2. Alarm *Connectivities* (at the *Dimension*)

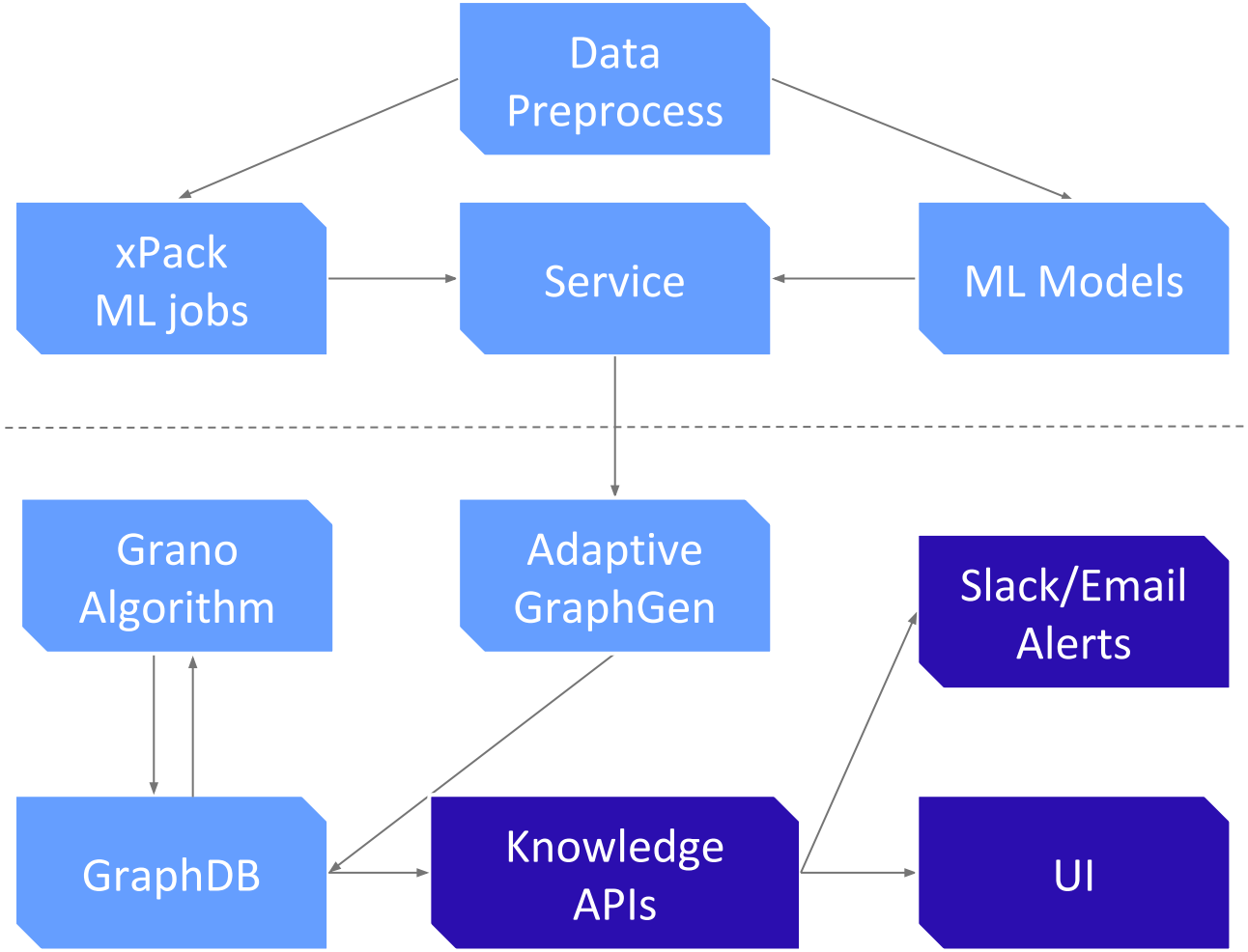
Grano Algorithms



Grano Algorithms



Grano Quick Walkthrough



Grano UI

Grano Insights

77.50 score : SJC-:-POP-:-duration_p50-:-High

52.56 score : Watch-:-Flow-:-upstream_service_time_p50-:-High

51.44 score : LHR-:-POP-:-upstream_service_time_p50-:-High

47.60 score : uk-:-Site-:-upstream_service_time_p50-:-Mid

39.96 score : EWR-:-POP-:-duration_p50-:-Mid

39.54 score : SYD-:-POP-:-duration_p50-:-Mid

33.65 score : MDW-:-POP-:-upstream_service_time_p50-:-Mid

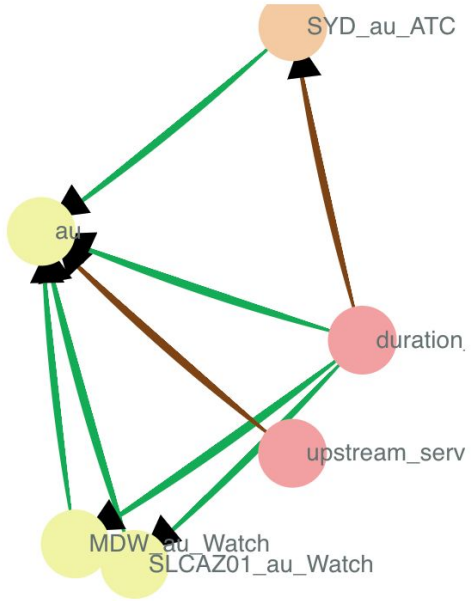
29.65 score : DUS-:-POP-:-upstream_service_time_p50-:-Mid

21.96 score : au-:-Site-:-upstream_service_time_p50-:-Mid

17.63 score : LAX-:-POP-:-duration_p50-:-Low

15.95 score : ATC-:-Flow-:-duration_p50-:-Low

7.49 score : co-:-Site-:-duration_p50-:-Low



87.79 zoe_envoy_traffic_by_4xx_response_code_popid

80.12 zoe_envoy_traffic_by_5xx_response_code_popid

65.57 sitespeed_viewitem_au_latency_by_browsers_p50

55.08 zoe_envoy_traffic_by_responseflags_cluster

89.72 zoe_envoy_traffic_by_4xx_response_code_popid

Takeaway

Envoy enables us for better Observability , Scale , TLS Termination , TCP Congestion BBR and Routing.

Today, we are able to serve experiences(closer and faster) to users with higher ATB powered by our detection.

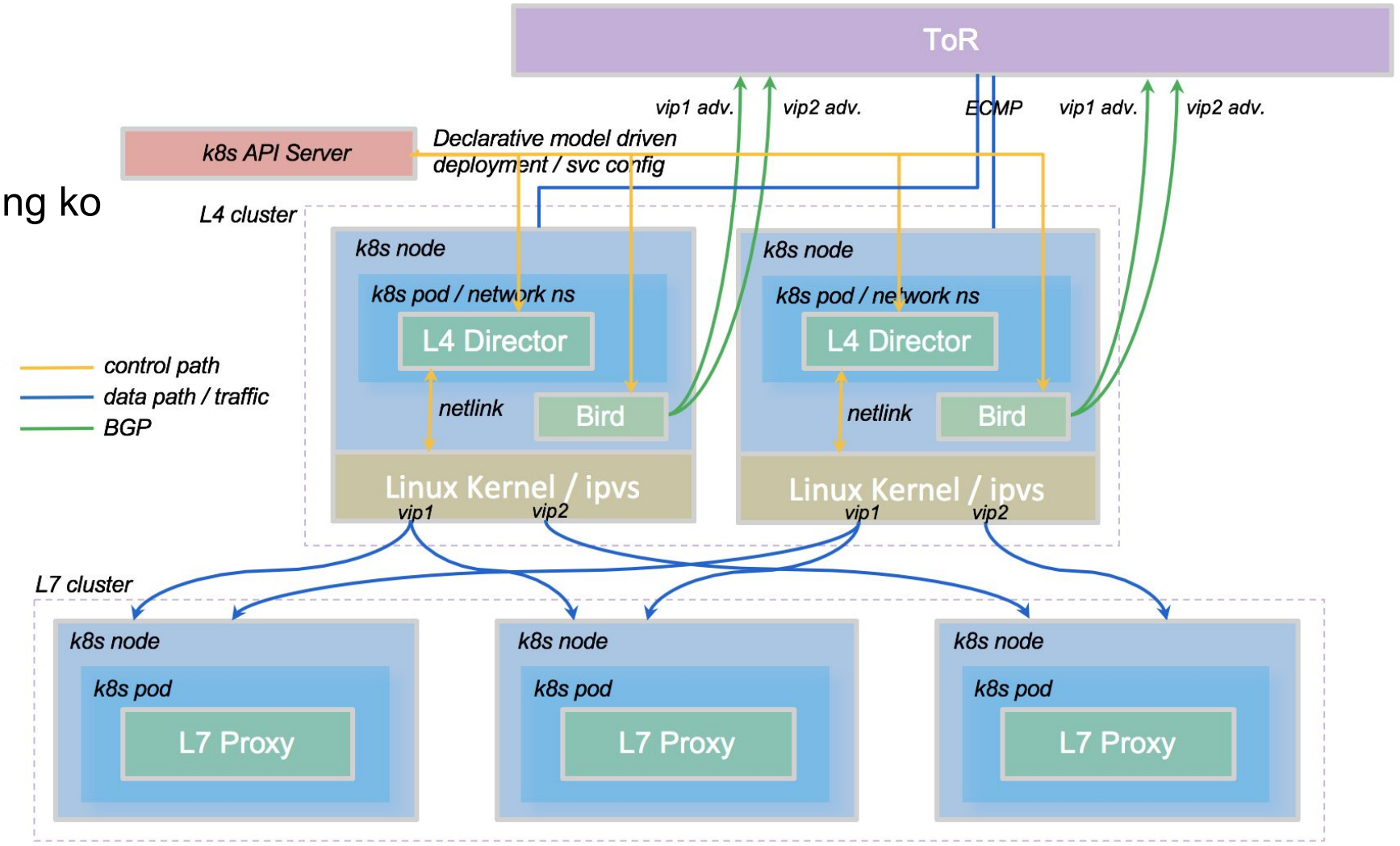
We should leverage ML graph, and knowledge engineering, rather than a relying on one method/metric (single point failure).

Graph is powerful to understand, connect, and make sense out of complex heterogeneous data (e.g., anomalies, metrics, and system event).


envoy
Thank
You
UFES
ebay

L4 Architecture

- IPVS based dataplane
- custom consistent hashing ko
- k8s driven control plane
- k8s native deployment
- horizontally scalable
- DSR
- BGP



Anomaly Detection

m1
--------- d1 (primary)
--------- d2 (secondary / influencers)

Bucket Span + Data History + Exponential Smoothing