Swisscom Network Analytics

Cosmos Bright Lights Network Anomaly Detection

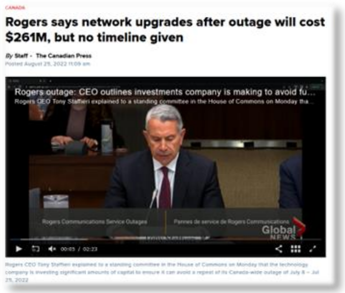
Sharing operational experience in the transition from a Time Series Database to a Real-Time Streaming Processor based system.

thomas.graf@swisscom.com
wanting.du@swisscom.com
alex.huang-feng@insa-lyon.fr
vincenzo.riccobene@huawei-partners.com
antonio.roberto@huawei.com

06. March 2024

Why to automate monitoring

Recognize network incidents faster than humans can



CANADA

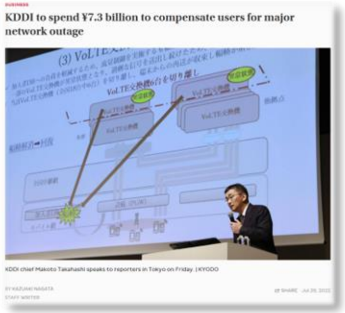
Rogers says network upgrades after outage will cost $261M, but no timeline given

By Staff - The Canadian Press
Posted August 25, 2022 11:09 am

Rogers outage: CEO outlines investments company is making to avoid fu...
Rogers CEO Tony Staffieri explained to a standing committee in the House of Commons on Monday tha...

Rogers Communications Service Outages
Pannes de service de Rogers Communications
Global NEWS
00:03 / 02:23

Rogers CEO Tony Staffieri explained to a standing committee in the House of Commons on Monday that the technology company is investing significant amounts of capital to ensure it can avoid a repeat of its Canada-wide outage of July 8 – Jul 25, 2022



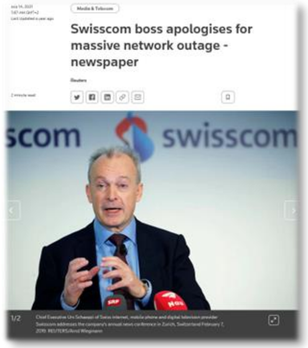
BUSINESS

KDDI to spend ¥7.3 billion to compensate users for major network outage

KDDI chief Makoto Takahashi speaks to reporters in Tokyo on Friday. | KYODO

BY KAZUAKI NAGATA
STAFF WRITER

SHARE Jul 29, 2022



July 14, 2021
7:07 AM GMT+2
Last Updated a year ago

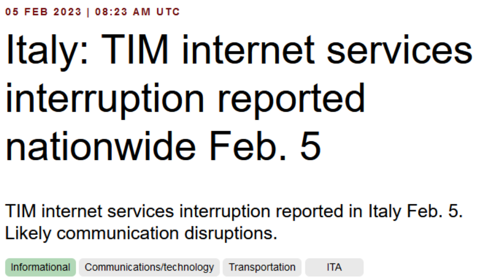
Media & Telecom

Swisscom boss apologises for massive network outage - newspaper

Reuters

2 minute read

1/2 Chief Executive Urs Schaeppi of Swiss internet, mobile phone and digital television provider Swisscom addresses the company's annual news conference in Zurich, Switzerland February 7, 2019. REUTERS/Arnd Wiegmann

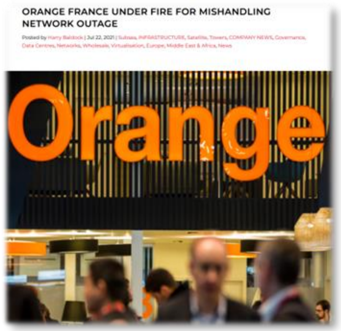


05 FEB 2023 | 08:23 AM UTC

Italy: TIM internet services interruption reported nationwide Feb. 5

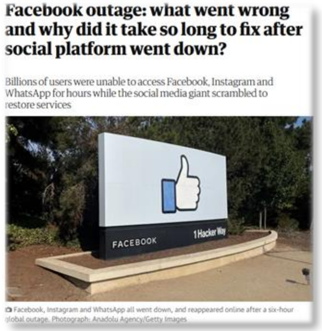
TIM internet services interruption reported in Italy Feb. 5. Likely communication disruptions.

Informational | Communications/technology | Transportation | ITA



ORANGE FRANCE UNDER FIRE FOR MISHANDLING NETWORK OUTAGE

Posted by Harry Baldock | Jul 22, 2021 | Subsea, INFRASTRUCTURE, Satellite, Towers, COMPANY NEWS, Governance, Data Centres, Networks, Wholesale, Virtualisation, Europe, Middle East & Africa, News



Facebook outage: what went wrong and why did it take so long to fix after social platform went down?

Billions of users were unable to access Facebook, Instagram and WhatsApp for hours while the social media giant scrambled to restore services

Facebook, Instagram and WhatsApp all went down, and reappeared online after a six-hour global outage. Photograph: Anadolu Agency/Getty Images

« Customers are always connected, when VPN's changing, regardless due to operational or configurational reasons, network operators are late to react due to missing visibility and automation »

What does Network Anomaly Detection mean

Monitor changes

Network Anomaly Detection

For VPNs, Network Anomaly Detection **constantly monitors and detects any network or device topology changes**, along with their associated forwarding consequences for customers as outliers. Notifications are sent to the Network Operation Center before the customer is aware of service disruptions. **It offers operational metrics for in-depth analysis,** allowing to understand on which platform the problem originates and facilitates problem resolution.

Answers

What changed and when, on which connectivity service, and how does it impact the customers?

Focuses

Provides meaningful connectivity service impact information before customer is aware of and support in root-cause analysis.

Data Mesh

Consumes operational real-time Forwarding Plane, Control Plane and Management Plane metrics and produces analytical alerts.

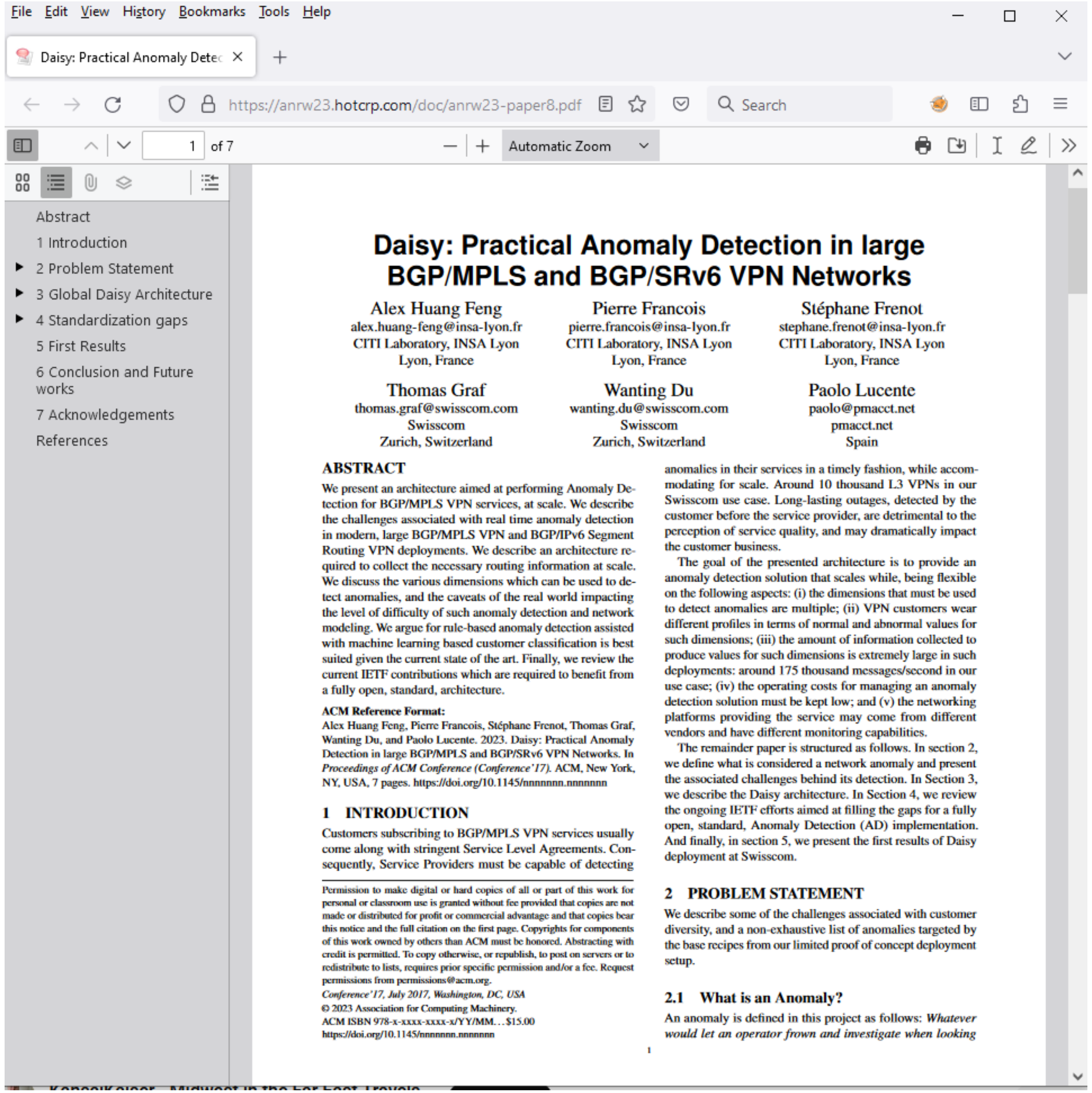
Direction

From connectivity service to network platform.

Presented in ANRW 2023

At IETF 117 San Francisco

« A more detailing paper will be submitted soon to IEEE Transactions on Network and Service Management»



Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks

Alex Huang Feng
alex.huang-feng@insa-lyon.fr
CITI Laboratory, INSA Lyon
Lyon, France

Pierre Francois
pierre.francois@insa-lyon.fr
CITI Laboratory, INSA Lyon
Lyon, France

Stéphane Frenot
stephane.frenot@insa-lyon.fr
CITI Laboratory, INSA Lyon
Lyon, France

Thomas Graf
thomas.graf@swisscom.com
Swisscom
Zurich, Switzerland

Wanting Du
wanting.du@swisscom.com
Swisscom
Zurich, Switzerland

Paolo Lucente
paolo@pmacct.net
pmacct.net
Spain

ABSTRACT

We present an architecture aimed at performing Anomaly Detection for BGP/MPLS VPN services, at scale. We describe the challenges associated with real time anomaly detection in modern, large BGP/MPLS VPN and BGP/IPv6 Segment Routing VPN deployments. We describe an architecture required to collect the necessary routing information at scale. We discuss the various dimensions which can be used to detect anomalies, and the caveats of the real world impacting the level of difficulty of such anomaly detection and network modeling. We argue for rule-based anomaly detection assisted with machine learning based customer classification is best suited given the current state of the art. Finally, we review the current IETF contributions which are required to benefit from a fully open, standard, architecture.

ACM Reference Format:
Alex Huang Feng, Pierre Francois, Stéphane Frenot, Thomas Graf, Wanting Du, and Paolo Lucente. 2023. Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Customers subscribing to BGP/MPLS VPN services usually come along with stringent Service Level Agreements. Consequently, Service Providers must be capable of detecting anomalies in their services in a timely fashion, while accommodating for scale. Around 10 thousand L3 VPNs in our Swisscom use case. Long-lasting outages, detected by the customer before the service provider, are detrimental to the perception of service quality, and may dramatically impact the customer business.

The goal of the presented architecture is to provide an anomaly detection solution that scales while, being flexible on the following aspects: (i) the dimensions that must be used to detect anomalies are multiple; (ii) VPN customers wear different profiles in terms of normal and abnormal values for such dimensions; (iii) the amount of information collected to produce values for such dimensions is extremely large in such deployments: around 175 thousand messages/second in our use case; (iv) the operating costs for managing an anomaly detection solution must be kept low; and (v) the networking platforms providing the service may come from different vendors and have different monitoring capabilities.

The remainder paper is structured as follows. In section 2, we define what is considered a network anomaly and present the associated challenges behind its detection. In Section 3, we describe the Daisy architecture. In Section 4, we review the ongoing IETF efforts aimed at filling the gaps for a fully open, standard, Anomaly Detection (AD) implementation. And finally, in section 5, we present the first results of Daisy deployment at Swisscom.

2 PROBLEM STATEMENT

We describe some of the challenges associated with customer diversity, and a non-exhaustive list of anomalies targeted by the base recipes from our limited proof of concept deployment setup.

2.1 What is an Anomaly?

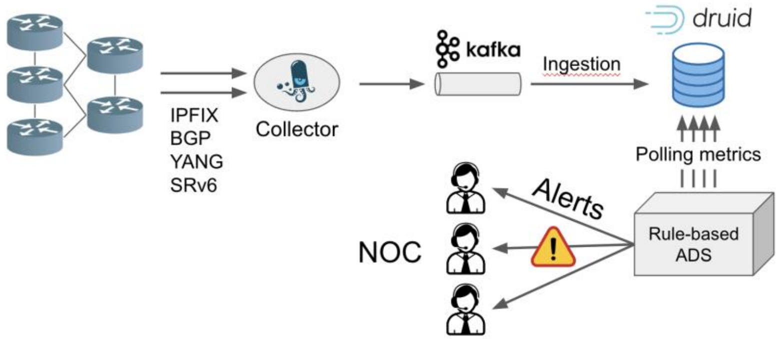
An anomaly is defined in this project as follows: *Whatever would let an operator frown and investigate when looking*

Conference'17, July 2017, Washington, DC, USA
© 2023 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

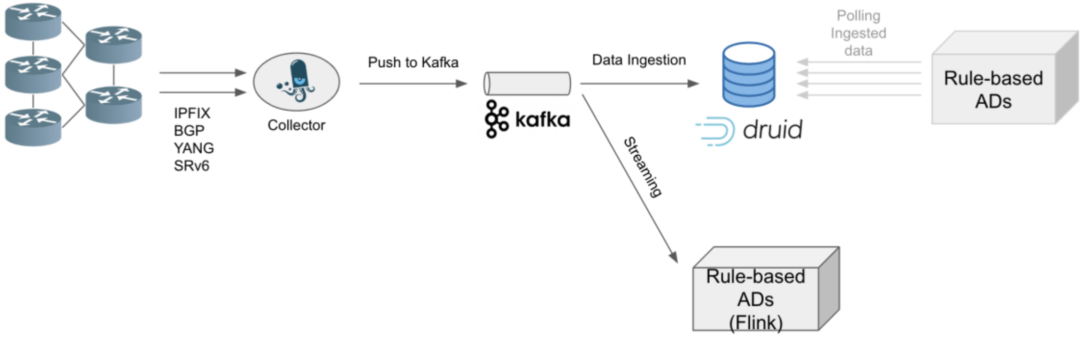
Overwiew of Cosmos Bright Lights

Architecture Comparison

A rule-based approach that actively monitors and promptly detects L3 BGP-MPLS VPN [RFC 4364] anomalies in near real-time. It summarizes and correlates Network Telemetry [RFC 9232] collected metrics from 3 different network planes to identify the possible root.



→

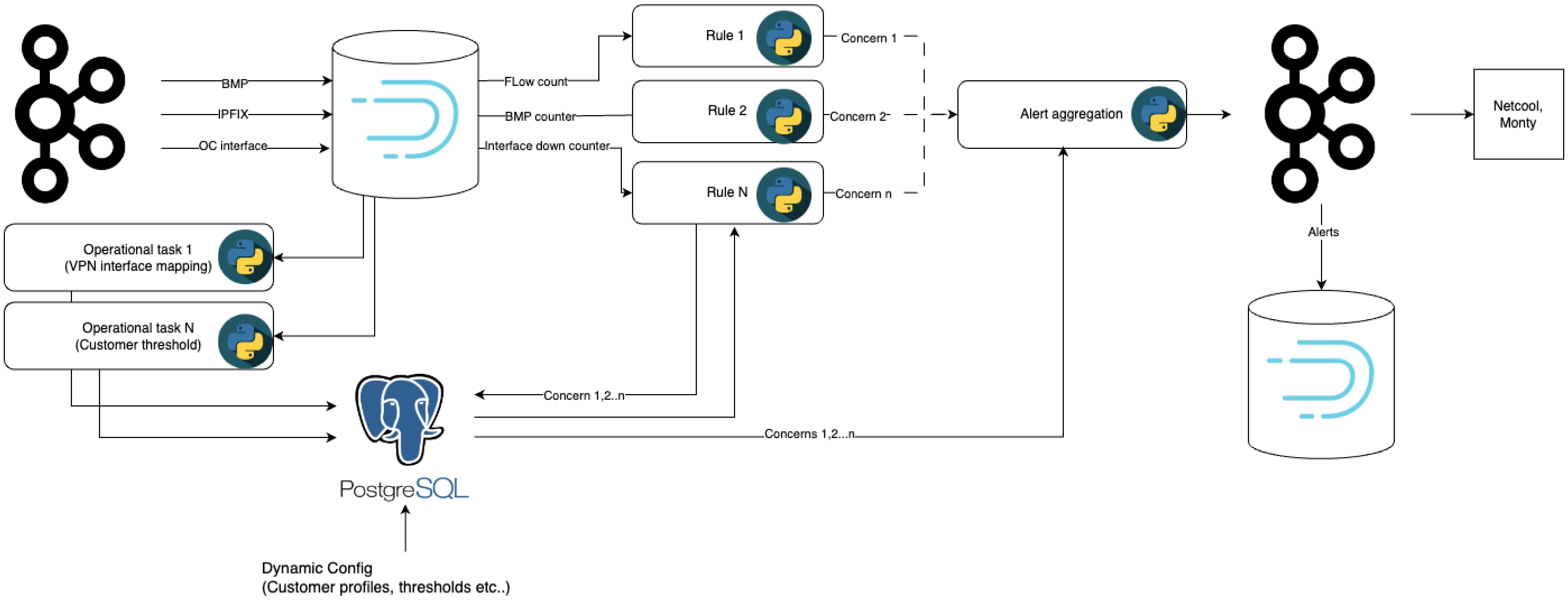


Polling based system architecture with Apache Druid (V0)

Stream based system architecture with Apache Flink (V1)

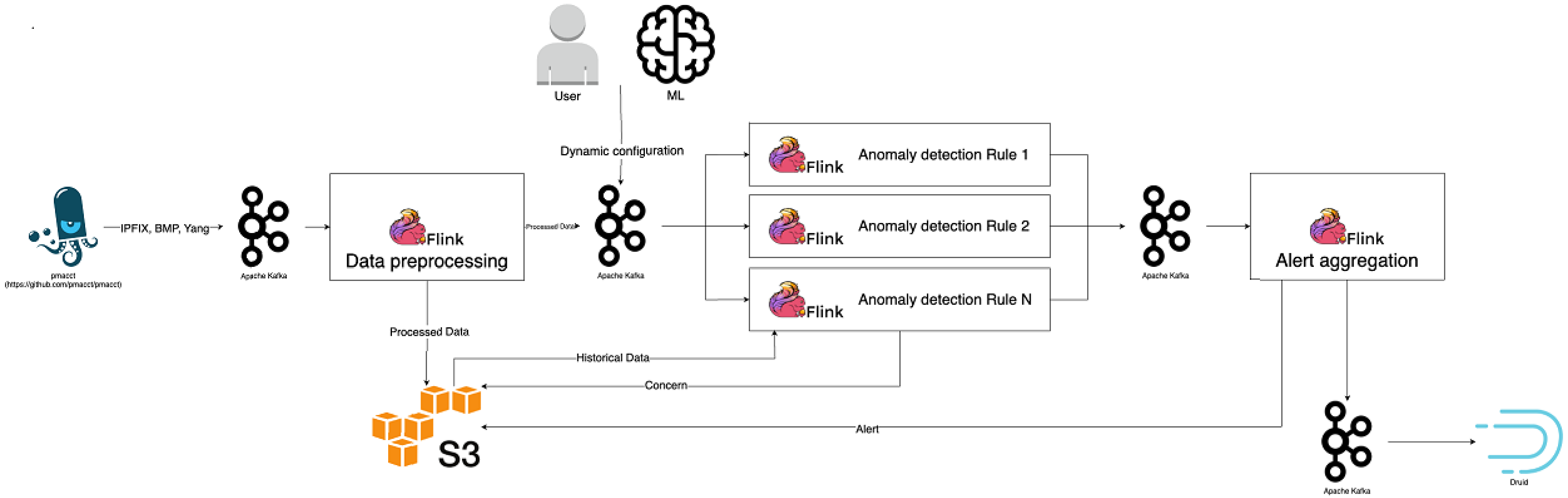
Tech Stack of Cosmos Bright Lights

V0 with Apache Druid Time Series Database



Tech Stack of Cosmos Bright Lights

V1 with Apache Flink Real-Time Streaming Processor



What to monitor

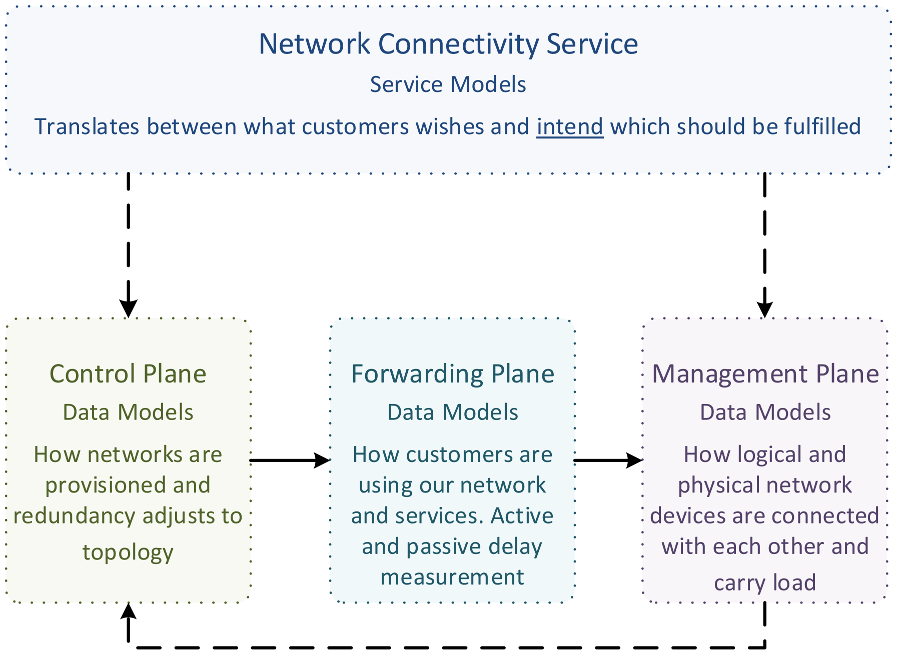
Which operational metrics to verify

Forwarding Plane: Verify wherever traffic is missing (dropped outside the monitored domain), being dropped with IE89 forwardingStatus or transport session count spiked due to retransmissions with IE3 deltaFlowCount.

Control Plane: Verify wherever routing topology changes or peering state changes occurred with BMP message type route-monitoring and peer-down.

Management Plane: Verify wherever interface state changes occurred with YANG Push collected interface metrics.

« Network Telemetry (RFC 9232) describes how to collect data from all 3 network planes efficiently »



Network Connectivity Service

Service Models

Translates between what customers wishes and intend which should be fulfilled

Control Plane

Data Models

How networks are provisioned and redundancy adjusts to topology

Forwarding Plane

Data Models

How customers are using our network and services. Active and passive delay measurement

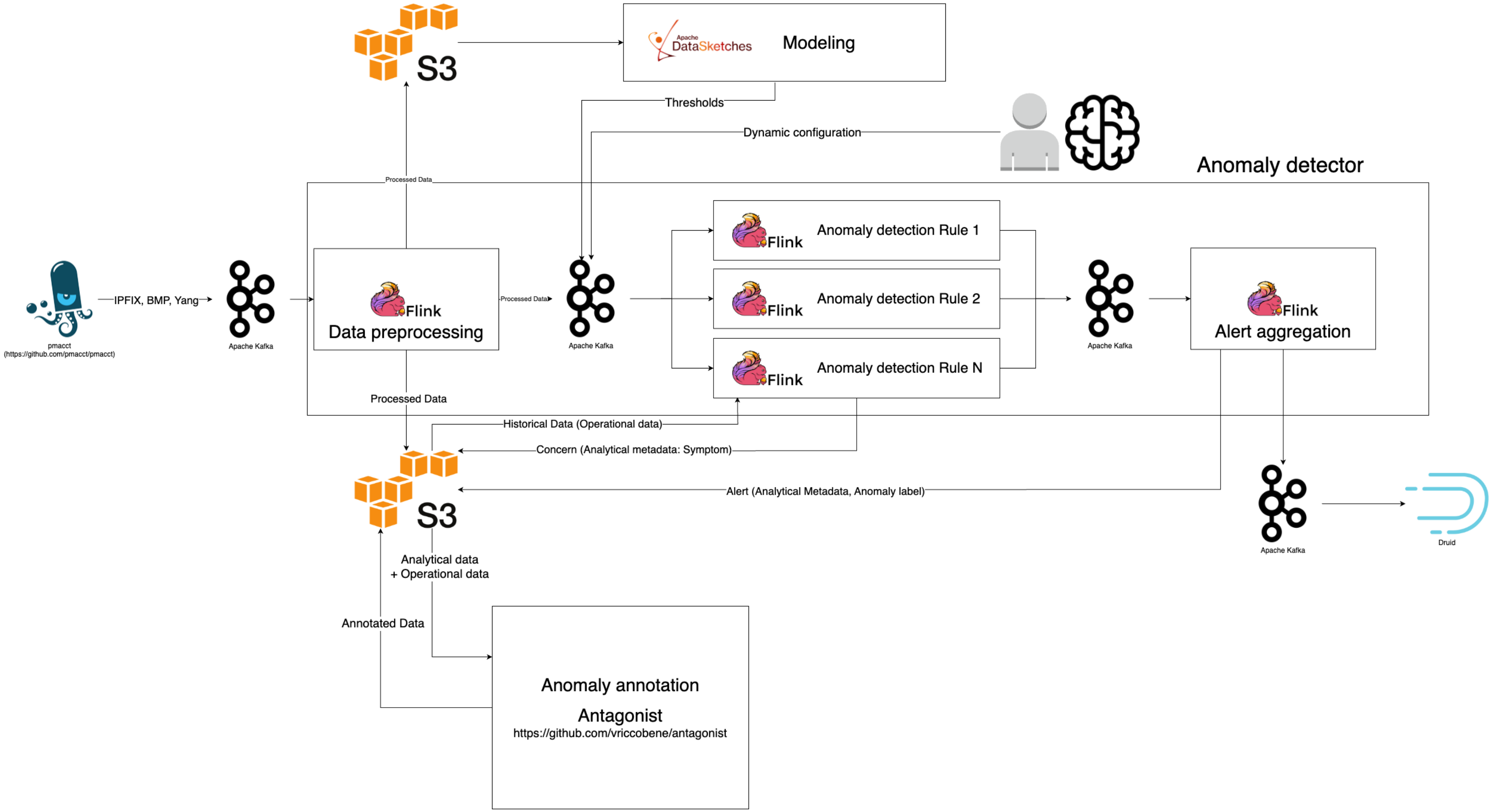
Management Plane

Data Models

How logical and physical network devices are connected with each other and carry load

Next Steps - Semantic Metadata Augmentation

Apache Flink Real-Time Streaming Processor Integration



S3
Apache DataSketches
Modeling
Thresholds
Dynamic configuration
Anomaly detector
Processed Data
IPFIX, BMP, Yang
pmacct
(https://github.com/pmacct/pmacct)
Apache Kafka
Flink
Data preprocessing
Processed Data
Apache Kafka
Flink
Anomaly detection Rule 1
Flink
Anomaly detection Rule 2
Flink
Anomaly detection Rule N
Apache Kafka
Flink
Alert aggregation
Processed Data
Historical Data (Operational data)
Concern (Analytical metadata: Symptom)
Alert (Analytical Metadata, Anomaly label)
S3
Apache Kafka
Druid
Analytical data
+ Operational data
Annotated Data
Anomaly annotation
Antagonist
https://github.com/vriccobene/antagonist