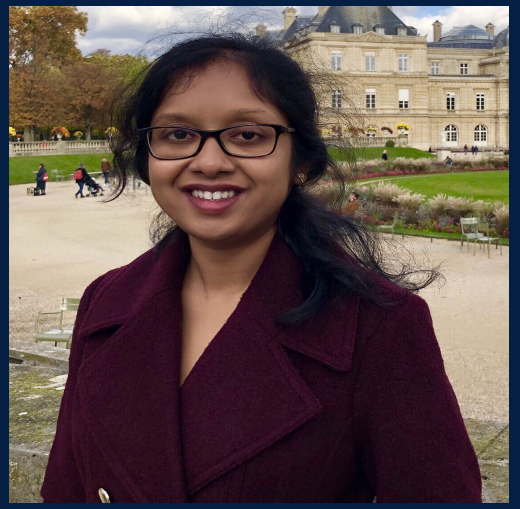
CertEngine

28/08/2020

Walmart Global Tech India

Site Reliability Engineering, Platforms

SRE – CertEngine Team



Sonal Patil

Jessmon George

Nishant Gaurav

Global Tech India

Problem Statement

- **What is the problem and who has it?**
  - ✓ There is no alerting in place which takes care of all the SSL Certificates in the Walmart ecosystem.
  - ✓ Tracking SSL certificate expiries is challenging
  - ✓ No scalable solution available
  - ✓ Previously, incidents have been observed due to lack of awareness on cert expiries causing $$ loss
  - ✓ The solution available such as “Tenable” costs Walmart **$1/IP/Year**, and in Walmart we have millions of Ips (Source IPAM)

- **Where and when does the problem occur?**

  Teams not paying attention to the certificates getting expired.

Impact on Walmart Labs

- **How does this problem affect Walmart's business or it's customers?**

  SSL certificate failures/expiries result in unauthorized activity and loss of security.

  Further, it can cause a lack of service to the customer increasing downtime of application. Resulting in $$ loss

- **How can solving this problem benefit Walmart?**

  Building an end to end solution to inspect certificates and alert customers of its renewal will help in saving $$ in service uptime of all the applications

- **What company objectives are you going to address and achieve?**

  Early detection and alerting

  Improving MTTD and MTTR

Solution

CertEngine – A monitoring tool that flags SSL Certificate expiration with ease and alerts teams. Scans complete Walmart ecosystem for certificates in all market.

- Technologies driving the solution

  The solution is written in Golang

  We are levearaging open source "**ZMAP"** project for fast scanning and certificate extraction

  - Zmap
  - ZGrab2

  Kafka & Elasticsearch

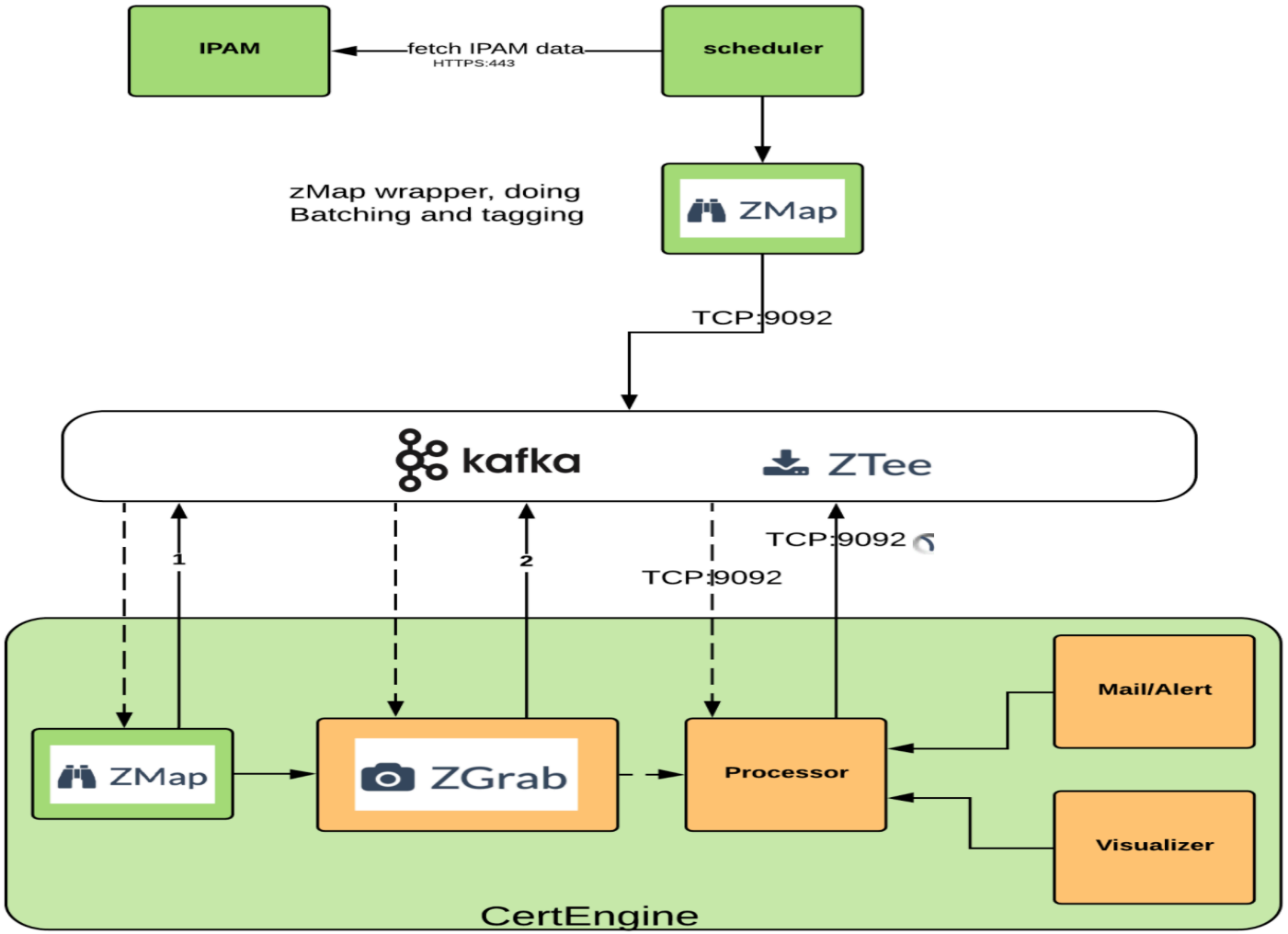
- How does this solution solve the problem
  - ✓ Scans all the IPs in Walmart ecosystem and sends alert to respective teams on daily basis.

    (Only Certs which are about to expire are alerted)

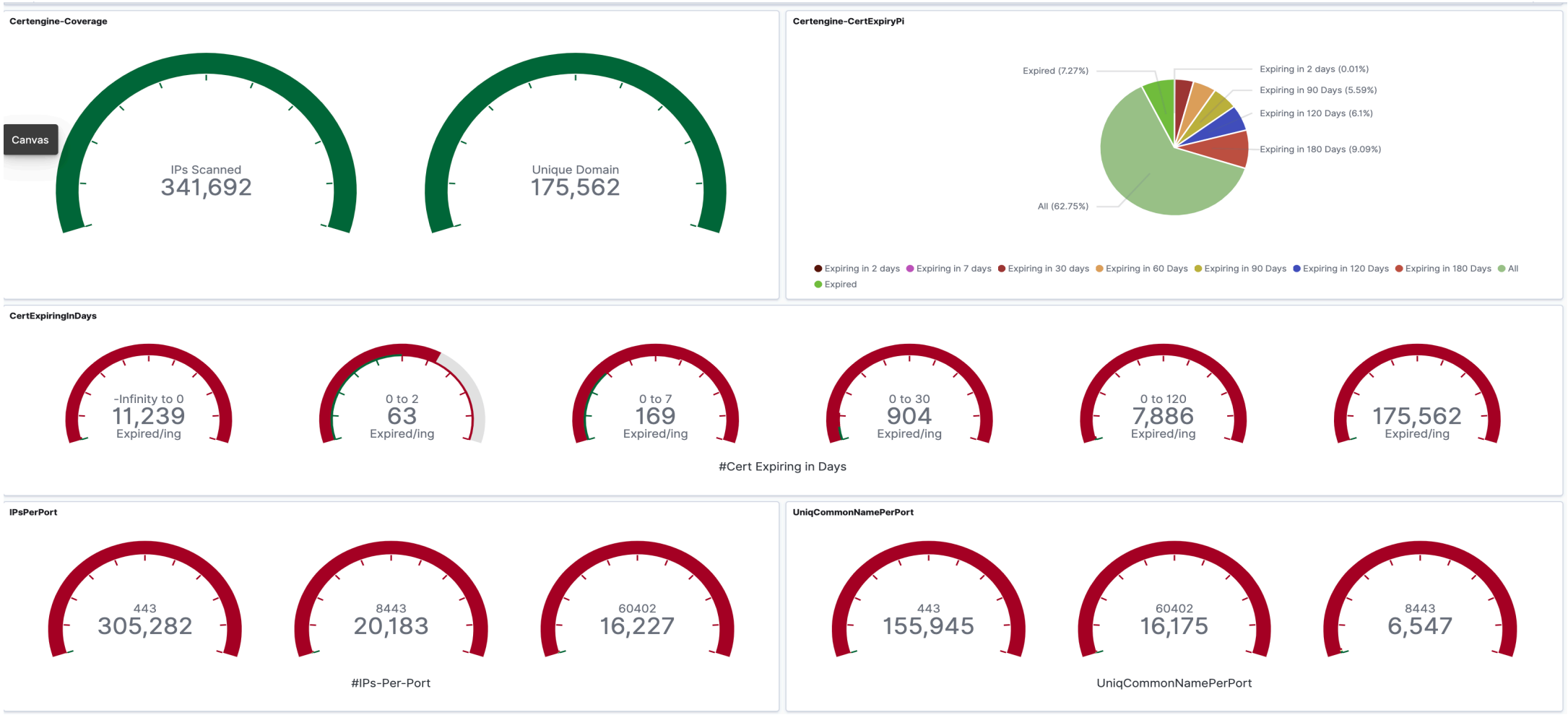
Unique selling points:

- ✓ One stop shop to get domain certificate info
- ✓ The solution is based on IP probes, hence can detect any certificate renewal miss in case, new certificate is not deployed on any IP
- ✓ Scans entire Walmart ecosystem leveraging IPAM info
- ✓ Stores and Ecommerce covered
- ✓ Highly scalable solution, scans complete Walmart ecosystem (IPAM – Source of truth) in few hours

Architecture



CertEngine- Kibana Dashboard



Global Tech India

CertEngine – Mail Alert

[CertEngine Alert] SSL Cert Expiry Report of Private IP Subnet for next 7 Day[s]!

G GTEO-SRE@email.wal-mart.com <GTEO-SRE@email.wal-mart.com> Today at 6:50 AM

Certificate Expiring Domain Detais

Expiry In (days)	Domain/Fqdn	Certificate Owner	VIP IP(s)
0	oneclick.prod.walmart.com	NA	10.247.225.228
0	ampplus.qa.walmart.com	NA	10.65.102.68
0	gain.stg.boprs.prod.walmart.com	NA	10.120.167.61,10.120.163.65
0	rehireeligibility.walmart.com	NA	10.120.161.175,10.118.129.78
0	vn0qsjy.lab-1.canada.walmart.com	NA	10.118.143.46
0	intdeliverymapdev.qa.walmart.com	NA	10.118.79.153
0	girservice.prod8.walmart.com	NA	10.118.100.156
0	sct-search.prod.us.walmart.net	NA	10.12.217.216
0	smartvisiting.walmart.com	NA	10.120.161.176
0	tp309003.homeoffice.wal-mart.com	NA	172.27.19.127
0	dev-api-bssproductivityreport.walmart.com	NA	10.120.132.216,10.227.204.227
0	RxOnlineAccountServices.qa.walmart.com	NA	10.118.69.184
0	lenxclarity01.uk.wal-mart.com	NA	10.41.40.129
0	rxonlineaccountservices-uat.cloud.prod.us.walmart.net	NA	10.12.178.204,10.12.176.10,10.12.179.48

[CertEngine Alert] SSL Cert Expiry Report of Public IP Subnet for next 7 Day[s]!

G GTEO-SRE@email.wal-mart.com <GTEO-SRE@email.wal-mart.com> Today at 6:50 AM

Certificate Expiring Domain Detais

Expiry In (days)	Domain/Fqdn	Certificate Owner	VIP IP(s)
0	www.ygwlgjxx.cn	NA	39.96.90.236
0	www.canpointgz.cn	NA	39.96.60.93
0	wap.qixinge.com	NA	128.1.185.3
0	ap.teogee.com	NA	39.96.165.246
0	omeka.library.cmu.edu	NA	128.2.25.127
0	yyerp.youyuecn.com	NA	39.96.28.253
	SAPS12S05308US.US.Wal-Mart.com,SAPS12S05224US.US.Wal-Mart.com,SAPS11S02442US.US.Wal-Mart.com,SAPS11S03710US.US.Wal-Mart.com,SAPS11S04671US.US.Wal-Mart.com,SAPS11S05170US.US.Wal-Mart.com,SAPS11S05270US.US.Wal-Mart.com,SAPS11S05211US.US.Wal-Mart.com,SAPS11S05228US.US.Wal-Mart.com,SAPS11S05829US.US.Wal-Mart.com,SAPS11S05421US.US.Wal-Mart.com,SAPS11S05670US.US.Wal-Mart.com,SAPS11S05907US.US.Wal-Mart.com,SAPS11S05884US.US.Wal-Mart.com,SAPS11S06932US.US.Wal-Mart.com,SAPS11S05957US.US.Wal-Mart.com,SAPS11S06172US.US.Wal-		

Future Roadmap

- We will enhance the product to integrate with other solutions like
  - ”Team Roaster” to get Org and VP level details
- Enrich the data and provide details in automated manner.
- Create Contact owner mappings
- UI to showcase the data
- Remove dependency from Venafi, Tenable
- Certificate Validation – SAN names missing from the certificates

Thank you!();

}

Nishant Gaurav;
Nishant.Gaurav@walmartlabs.com

Global Tech India

Titan

28/08/2020

Walmart Global Tech India Service Assurance

Service Assurance Functions

SA-Control

- Build the unified devices inventory, remote monitoring, and intelligent on-host changes.
- Deploy globally to Stores, Clubs, DCs, Data Centres, and HO/CO sites.

SA-Insights

- Develop data visualization and correlation, using scalable cloud data lake and analytics.
- Deliver data science-driven insights, to prepare the foundation or AI and self- service dashboards.
- Incident Correlation

SA-Drive

- Deliver smart alerts & notifications, with integrated incident change workflows.
- Build automation to minimize human intervention and enable auto-change.

Problem Statement

Current NNMi tool

- Very expensive for what we use for(~1M $)
- Does not scale well(We are running over 100VMs just to monitor US stores)
- High administrative burden(requires custom scripting)
- Discovery runs once a week and often does not complete
- Each server is an island(If you want data about all stores, you have to go each server and then stitch data together)
- Inflexible(For additional data, we need to develop a new script)
- Single point of failure
- SNMP only
- Minimal support for Access Points

Solution: Titan

- Universal Sensor(Network & Compute)
- Replacement for NNMi (Network Node Manager)
- Provides discovery and monitoring of devices as well as their physical and logical components
- Vendor agnostic data model
- Protocol agnostic(SNMP, ssh, telnet, CLI, netconf, restconf, proprietary API)
- Hardware and firmware inventory
- Monitoring – 1 minute, Discovery – 1 hour

Benefits:

- First, we scale well. We push the hard work to the edge where the scope is smaller.
- By pushing these processes to the edge we reduce the latency to each device. This allows us to collect data faster and more frequently
- Since latency is lower we can use more reliable and secure protocols
- By being protocol flexible we can use whatever means is necessary to collect the data we need
- Discovery is mostly hands off and automated
- Low admin
- Better data accuracy and global data
- Highly available data
- Context(Better correlation of data)

Project Goals

- Find and monitor every single network infrastructure element possible
- Accurate data is our topmost priority
- Low cost
- Efficiency
- Low complexity

Components & Technologies Used

Agents/Sensors:

- Totally stateless
- Protocol independent
- Extremely resource efficient
- Easily extended to collect more information
- Can be scaled vertically(more CPU) or horizontally(zoning)

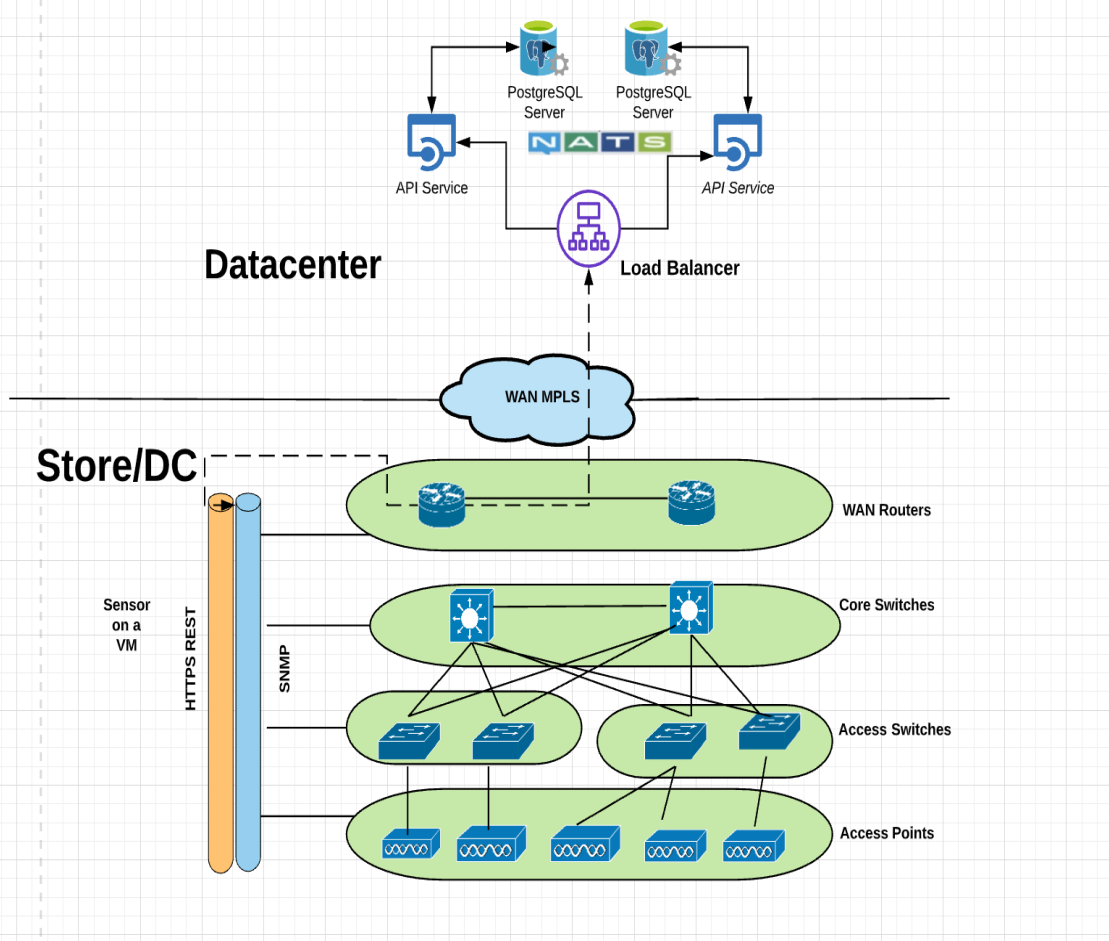
APIs:

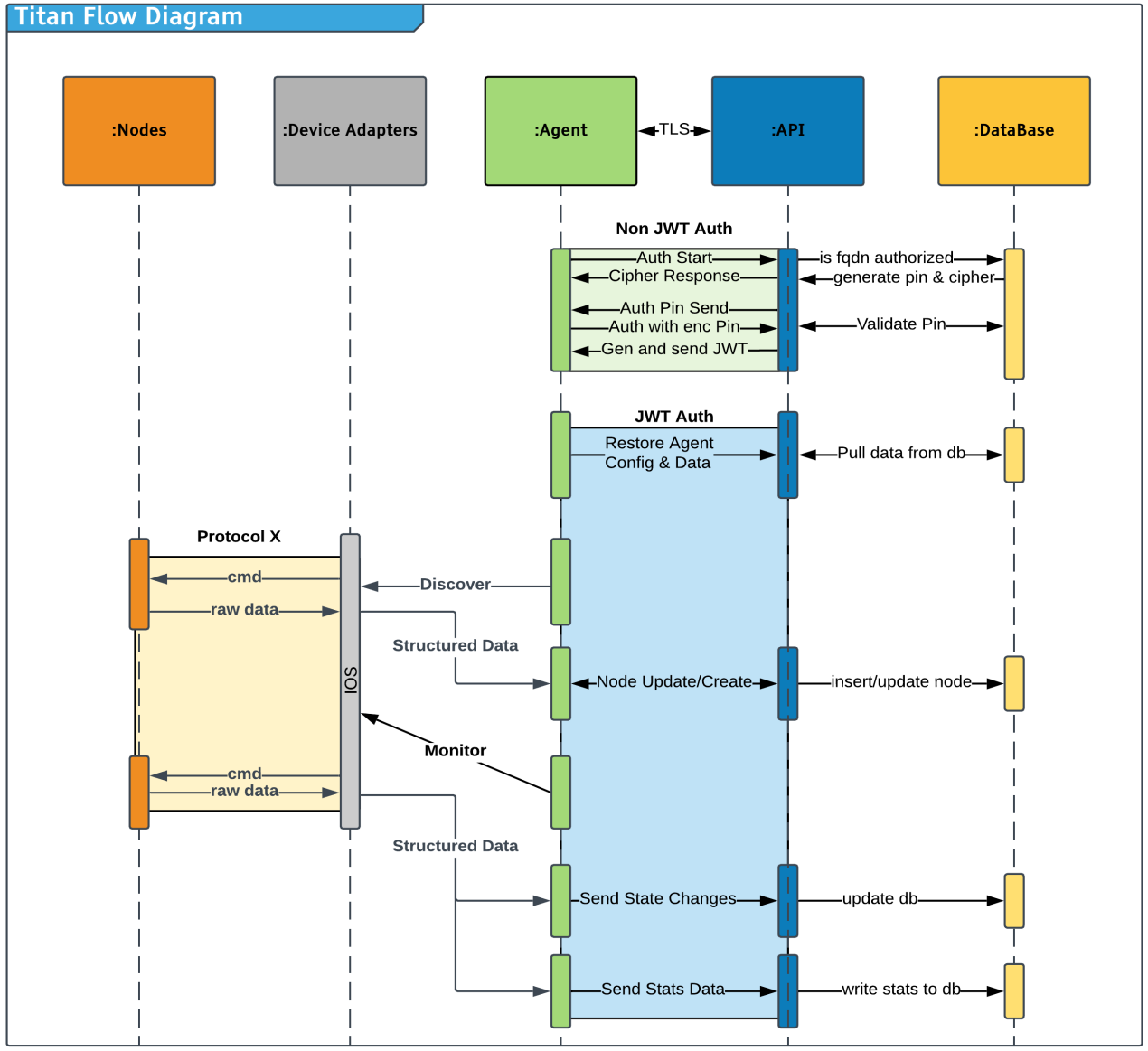
- Also stateless
- Running REST and NATS
- Cloud Ready
- Secure – all sensitive information is encrypted with aes256 at rest and in transit

Technologies Used

- ✓ Golang
- ✓ Postgresql
- ✓ NATS
- ✓ React JS

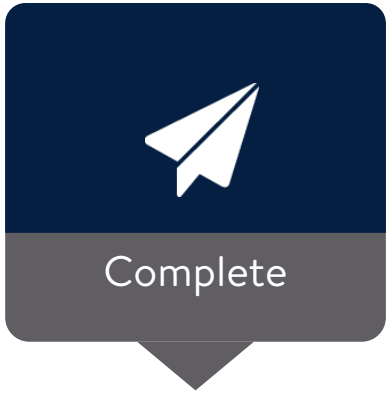
Architecture





Global Tech India

Progress



- ✓ Rollout to entire store chain –US & international
- ✓ Rollout to Data centers and US Distribution centers
- ✓ Rest API, NATS support
- ✓ Device adapters for Cisco, Juniper, NCS, ENCS, Infoblox, F5, Netscalers, Extreme etc
- ✓ Host metrics

- Rollout to international Distribution centers
- Rollout to Pharmacy servers
- Rollout to IDC, SVL and SB campus sites
- SAS ServiceNow Integration
- SACK – CLI tool
- Secured NATS

- Extend scope beyond network infra devices
- Collect more information based on needs

Smart Alerting Services/SAS (WIP)

Core concepts:

Input: An input is a source of data that rules use.

Running input: A running input is actually running connected input.

Rule: Rules are configured with running input, queries, outputs and intervals.

Output: Microservices that receive buffer messages from NATS and translate them to the appropriate destination

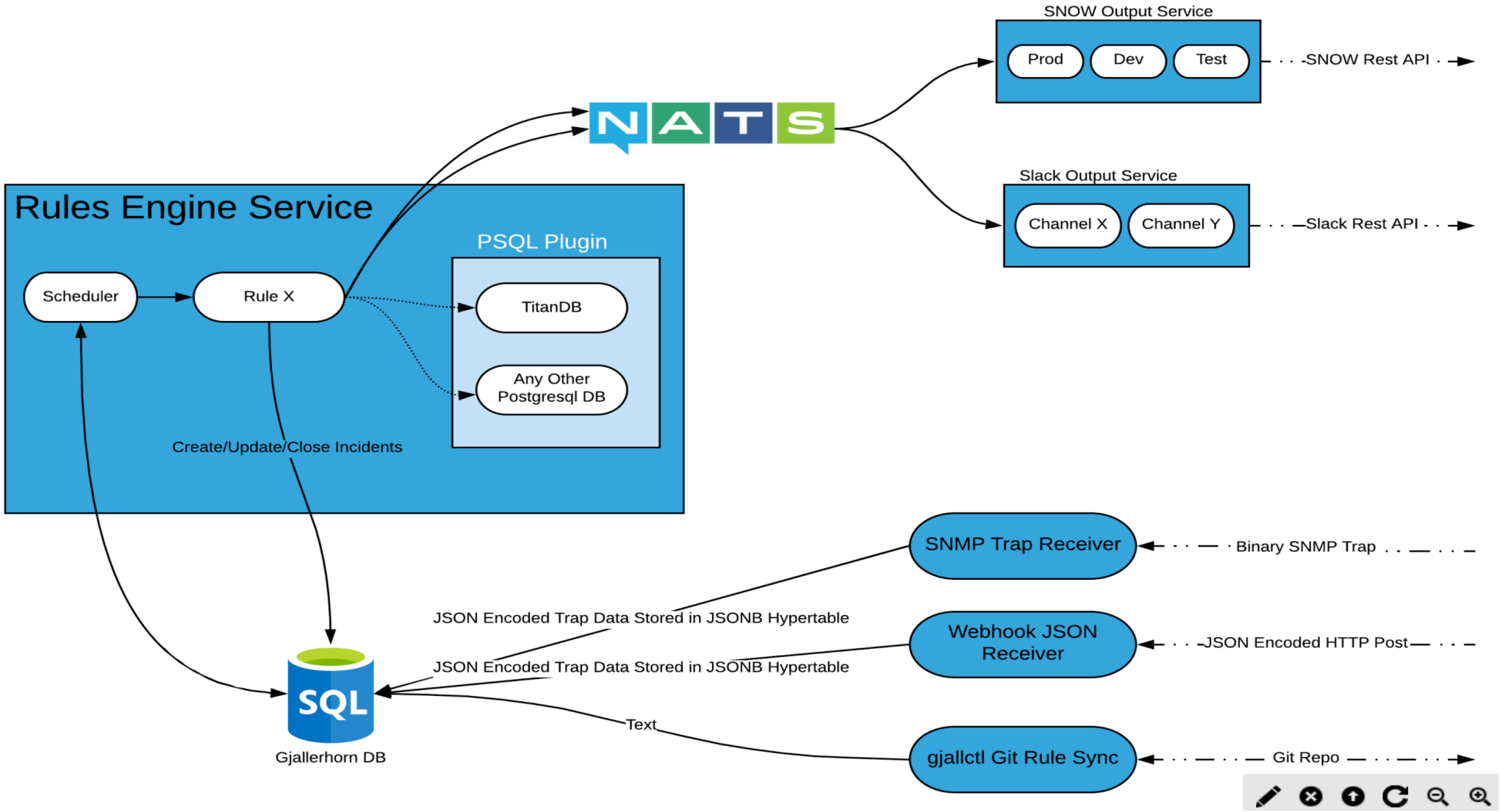
Gjallerhorn is a combination of multiple microservices:

Gjallerhorn Rule engine service(gjalld)

Gjallerhorn SNMP trap receiver service(trapd)

Gjallerhorn ServiceNow output(SNOW)

SAS Architecture



NATS

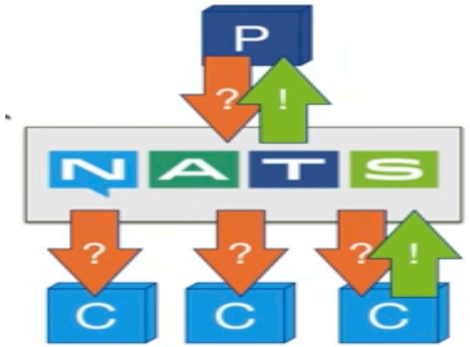
- NATS stands for Neural Autonomic Transport System.
- NATS is simple and secure messaging made for developers and operators who want to spend more time developing modern applications and services than worrying about a distributed communication system.
- Easy to use
- High performance
- Always on and available
- Extremely lightweight
- Support for observable and scalable services and event/data streams
- Clients connect to the NATS system, usually via a single URL, and then subscribe publish messages to subjects
- NATS consists of:

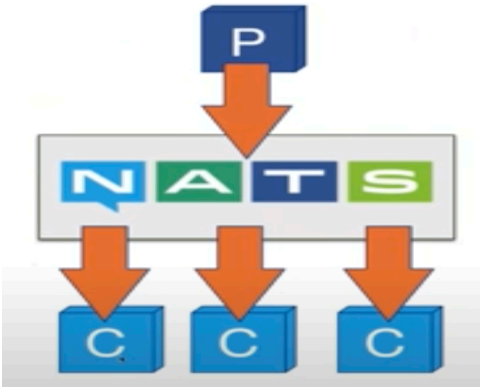
✓ NATS Server

✓ NATS Streaming

✓ Client libraries

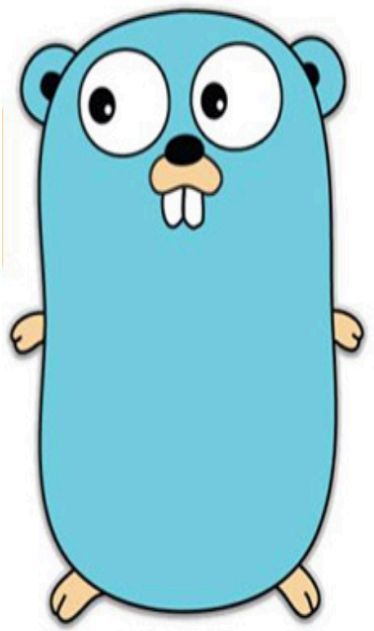
✓ A connector framework





Why Golang?

- High Performance
- Faster and well scaled
- Supports inbuilt concurrency
- Compiles down to 1 binary



Thank you!();

Rohit Cheetu
Rohit.Cheetu@walmart.com

Global Tech India