Observability Summit
North America

Implementation of unified observability at scale, from scratch.

Ahmed J.
Platform Engineer @ Emaar

Unified observability or just another marketing scheme?

C

Compliance

One audit trail. Easier to defend.

A

Agents

Everything correlated in one place.

P

Price

One platform. No duplication.

A

Alignment

Same dashboards. Same vocabulary.

The footprint.

200+

SITES

Data centers, malls, hotels, offices in 10+ countries.

2K+

Virtual Machines

Multiple distros.

10K+

NETWORK DEVICES

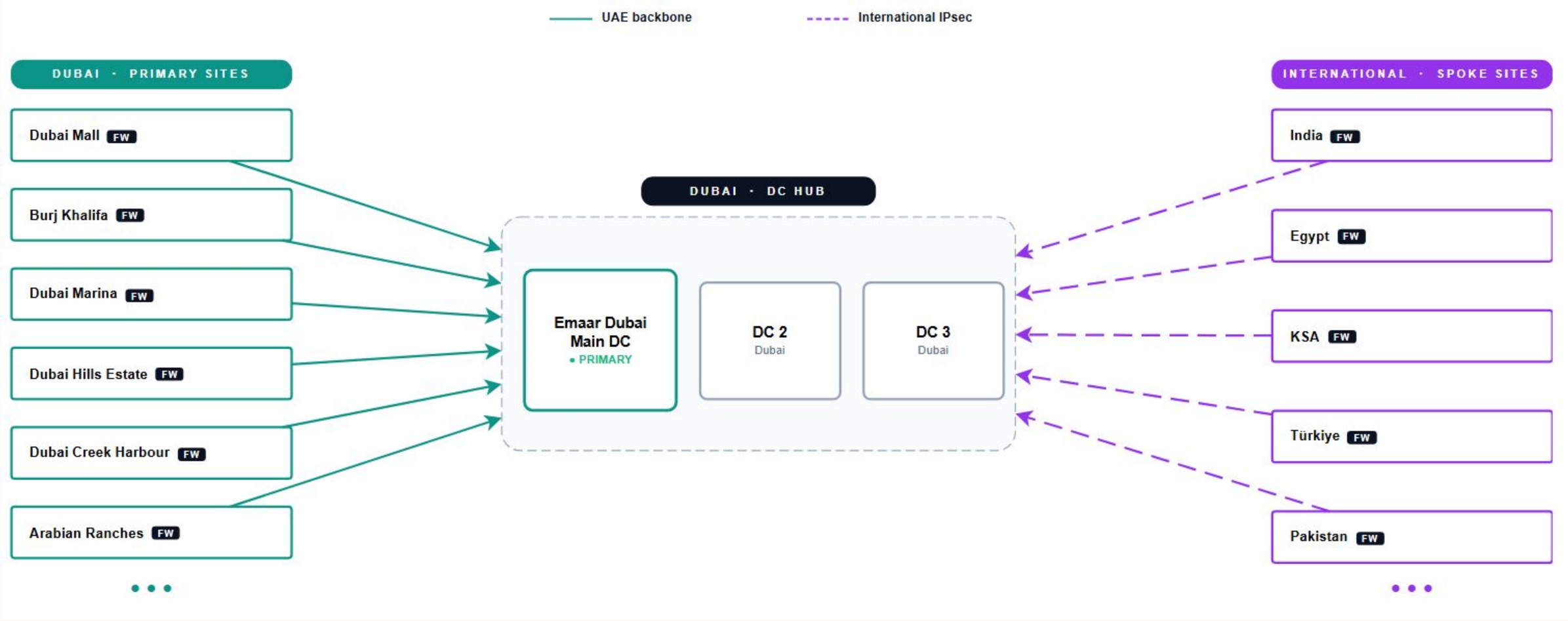
Switches, routers, wireless controllers, etc.

300+

FIREWALLS

Multi-vendor.

High level architecture.



What we integrated.

NETWORK

Switches
Routers
Wireless Controllers
Firewalls
Web Application Firewalls

VIRTUALIZATION

ESXi hosts
vSphere / vCenter
Nutanix

SERVERS

Linux (all distros)
Windows
Solaris

DATABASES

PostgreSQL
MySQL / MariaDB
Oracle DB
MS SQL Server
MongoDB · Redis

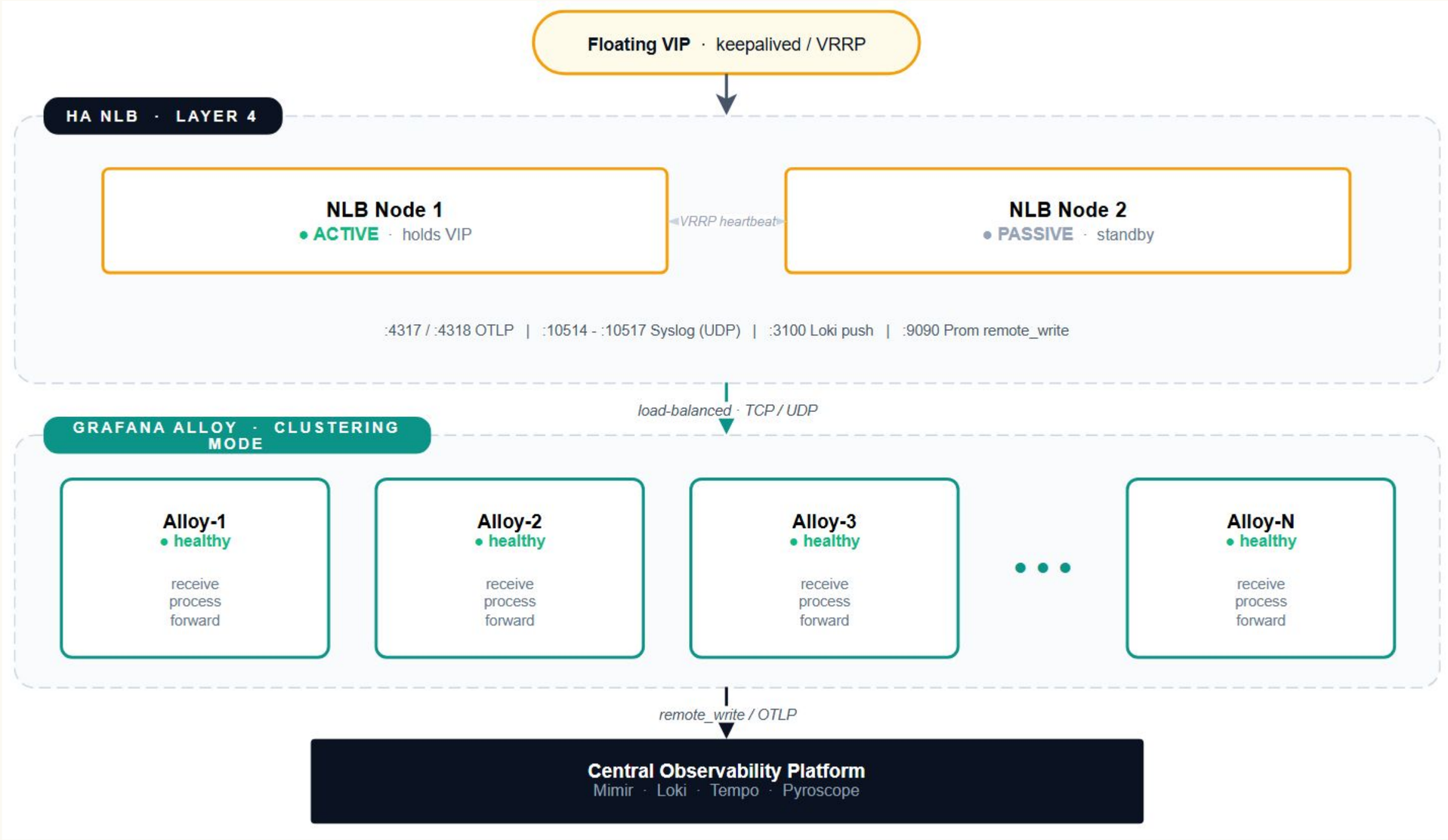
CONTAINERS & APPLICATIONS

Kubernetes clusters
On-prem deployments
Multi-tenant workloads

ALERTING & INTEGRATION

24x7 alerting
Custom ticketing integration

Per-site collection architecture.



Alloy clustering mode vs sharded Prometheus.

ALLOY CLUSTERING MODE

Self-balancing fleet.

Targets sharded automatically across nodes

Rebalances on join, leave, failure

One binary, one config, one mental model

Linear scale-out for collection

Consumes more resources

SHARDED PROMETHEUS

Static, manual, mature.

Targets assigned per shard by config

Federation for the global view

Re-shard on every fleet change

Battle-tested, but operationally heavy

Efficient

Network observability.

SNMP MONITORING

Polling thousands of devices.

Custom MIBs per vendor

Auto-generated exporter configs

Interface, CPU, memory, uptime

SYSLOG INGESTION

Taming a hundred dialects.

RFC 3164 / 5424 via Alloy

rsyslog for edge cases

Custom parsers for Fortinet, Cisco IOS

The cardinality problem. Labels are not free.

Use labels only for **categorical, finite** variables, especially in large scale setups.

Push high-cardinality data into an **external metadata store** . Join at query time.

```
device_interface_traffic_bytes{ip="10.42.18.7", hostna
me="dxb-mall-sw-core-01", vendor="cisco", model="catal
yst-9500", type="switch", role="core", site="dxb-mall-
01", region="ae-dxb", environment="prod", criticality
="tier-1", owner_team="network-ops"} 1.42e9
```

Infrastructure & application observability.

INFRASTRUCTURE

Every host, every engine.

Node & Windows exporters

vSphere & Nutanix integrations

Database exporters per engine

APPLICATION

Traces, metrics, logs.

OpenTelemetry SDKs

RED metrics: rate, errors, duration

Two-click pivot from trace to host

Security & SaaS observability.

SECURITY

WAF + firewall, structured.

Custom parser for WAF logs

Policy, src IP, URI, attack type

Firewall events correlated with app metrics

SAAS

Audit what you don't run.

Audit-trail observability

Logins, exports, permission changes

One store, one query language

What went wrong.

01

Alloy FD exhaustion

`v1.11.x` leaked file descriptors causing alloy to crash.

02

Different behavior across sites

Differences in cloud and on-prem networking to Alloy's behavior.

03

Proprietary syslog formats

No RFC covers real-world network gear. Custom parsers required.

04

Team resistance

Unification is as much a people problem as a technical one.

Everything was great…

…until it wasn't.

Regional AWS Outage out of the blue.

The system we built to watch everything *couldn't watch itself.*

Core functionality recovered in hours, but the gaps in disaster recovery and platform reproducibility were exposed.

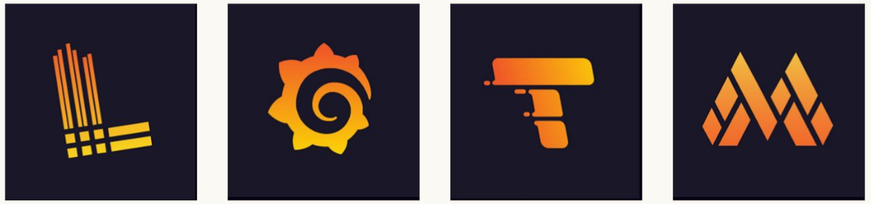
Lessons from the outage.

01 Daily backups of **everything**. Configs, alerts, parsers, the whole platform-as-code.

02 Point-in-time recovery, in progress. Roll back to **any snapshot**.

03 Treat the observability platform as a **tier-one production system**.

Unified observability does work.



One platform across network, infra, app & security

Open-source, end to end

Faster debugging, easier audits, real alignment

6-figure annual savings

Observability Summit
North America

Thank you.

This Presentation

LinkedIn

Ahmed J.
Platform Engineer