CERN openlab

EOS Winston

Expert Systems for Automated Diagnosis and Remediation

Ishank Arora, IT-ST-FDO

Supervisor: Luca Mascetti

EOS

A disk-based, low-latency storage service

Scale:

- Over 280 PB of raw disk space
- 4.88 billion files
- 50,000 disks
- 25+ namespaces

Issues and Anomalies

It works! It works! Wait a second...

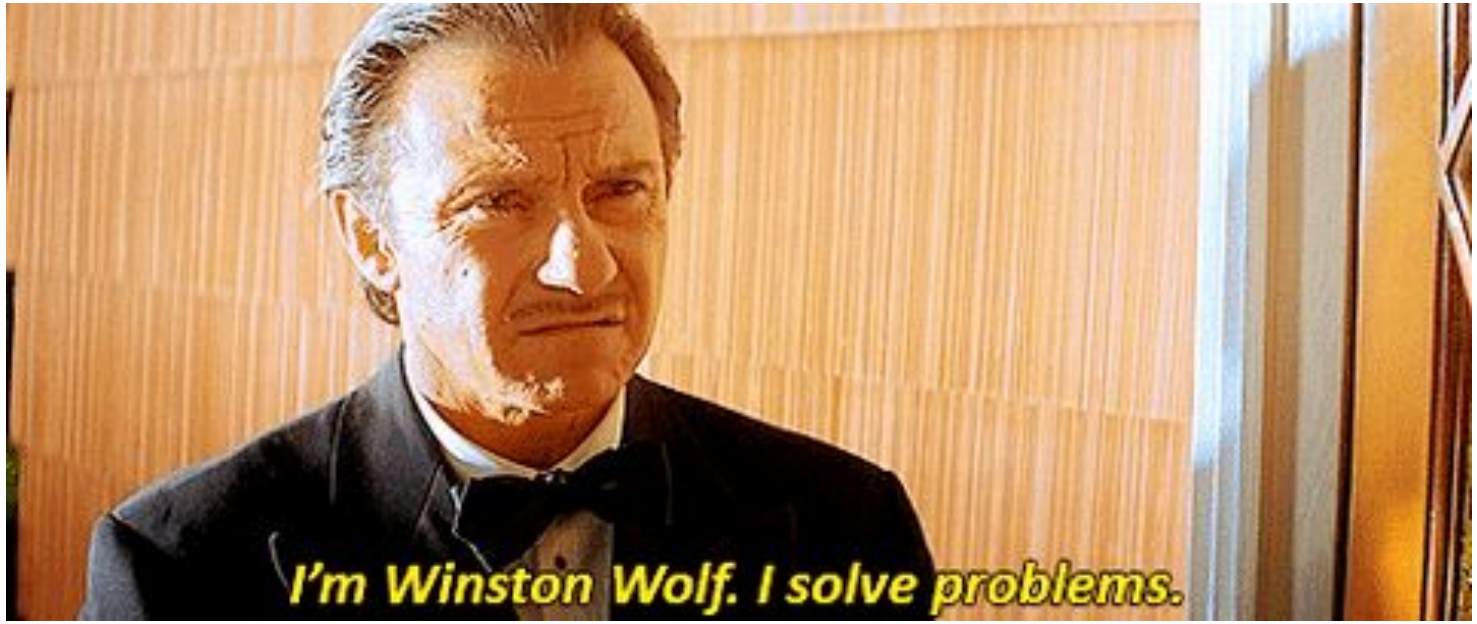
- The `very-critical-mount` on EOSPublic is 95% full (of logs dating a year back).
- User 1729 is performing read operations at 7201.21 Hz.
- Boot failure on 20 nodes in EOSAlice.
- Node `heart-attack.cern.ch` has a heartbeat of 83018 *(actual figures)*.

Project Requirements

Check. Check. Wait a second...

- Reduce MTTR and pager fatigue
- Remove false positives
- Enable the team to focus on the business logic rather than the infrastructure
- Provide a common platform for alerts and collaboration

EOS Winston

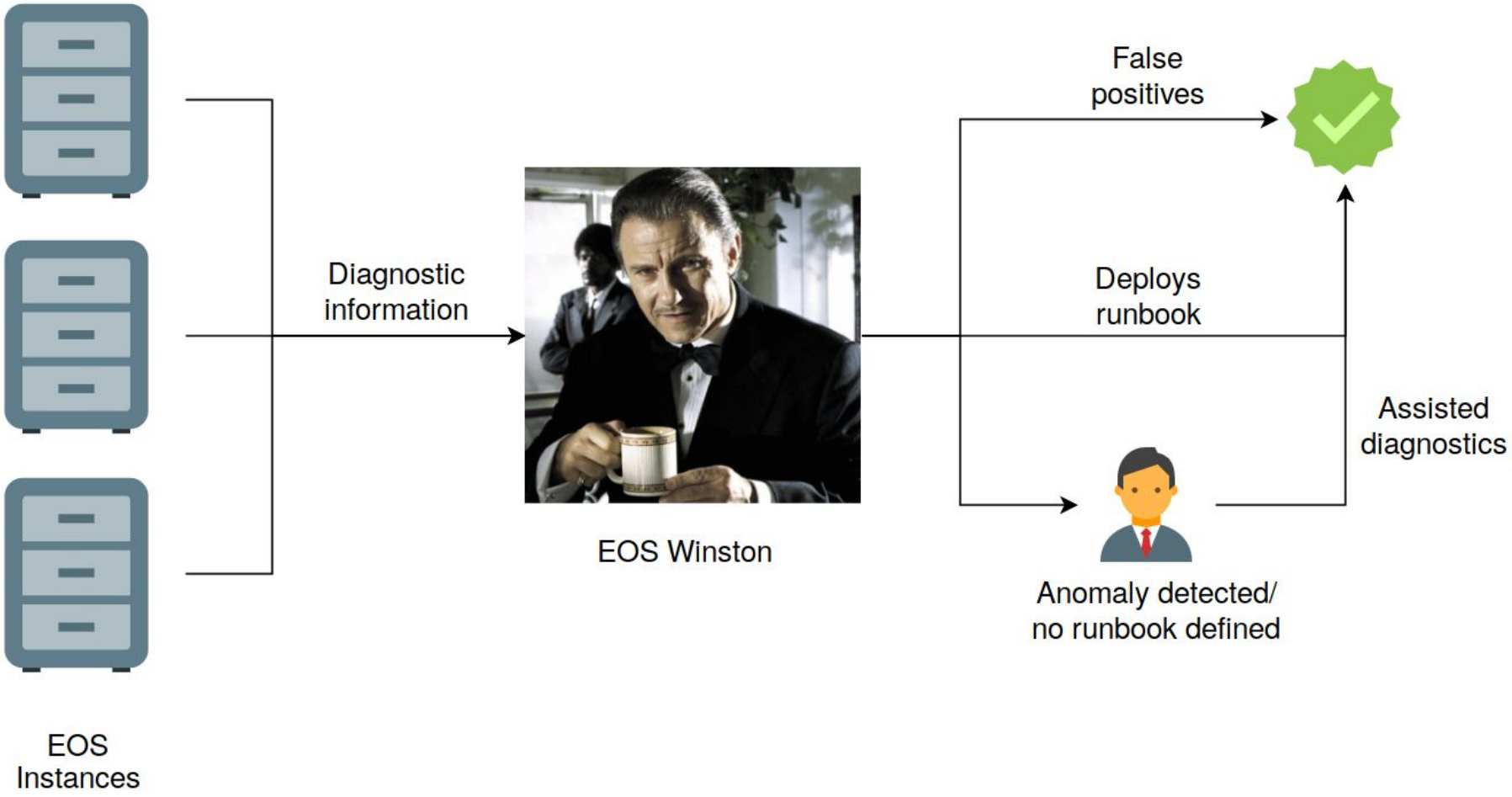


https://giphy.com/gifs/quentin-tarantino-pulp-fiction-harvey-keitel-DeOa0SqsDH5sc

EOS Winston

An event-driven alerting and mitigation automation platform. It employs expert rules and streaming anomaly detection algorithms to categorise events and execute corresponding runbooks.

The architecture



StackStorm[1] for automation

(Thank God for open-source)

- Pluggable rule engine comprising of triggers and actions
- MongoDB for data storage and RabbitMQ for message broking
- Supports a wide variety of interfaces, available as packs
- Deployed by firms such as Netflix[2] and NASA

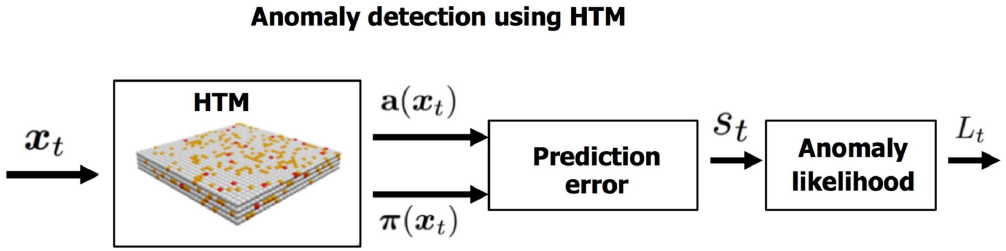
[1]: https://stackstorm.com/

[2]: medium.com/netflix-techblog/introducing-winston-event-driven-diagnostic-and-remediation-platform-46ce39aa81cc

Anomalies in the Average MGM Load

Nupic: Real-time Streaming Anomaly Detection*

- Try to identify if there's a sudden unexplained increase in the average load across all nodes of an EOS instance, or a given user's activity.
- Nupic*, a real-time streaming algorithm, employs Hierarchical Temporal Memory (HTM) networks

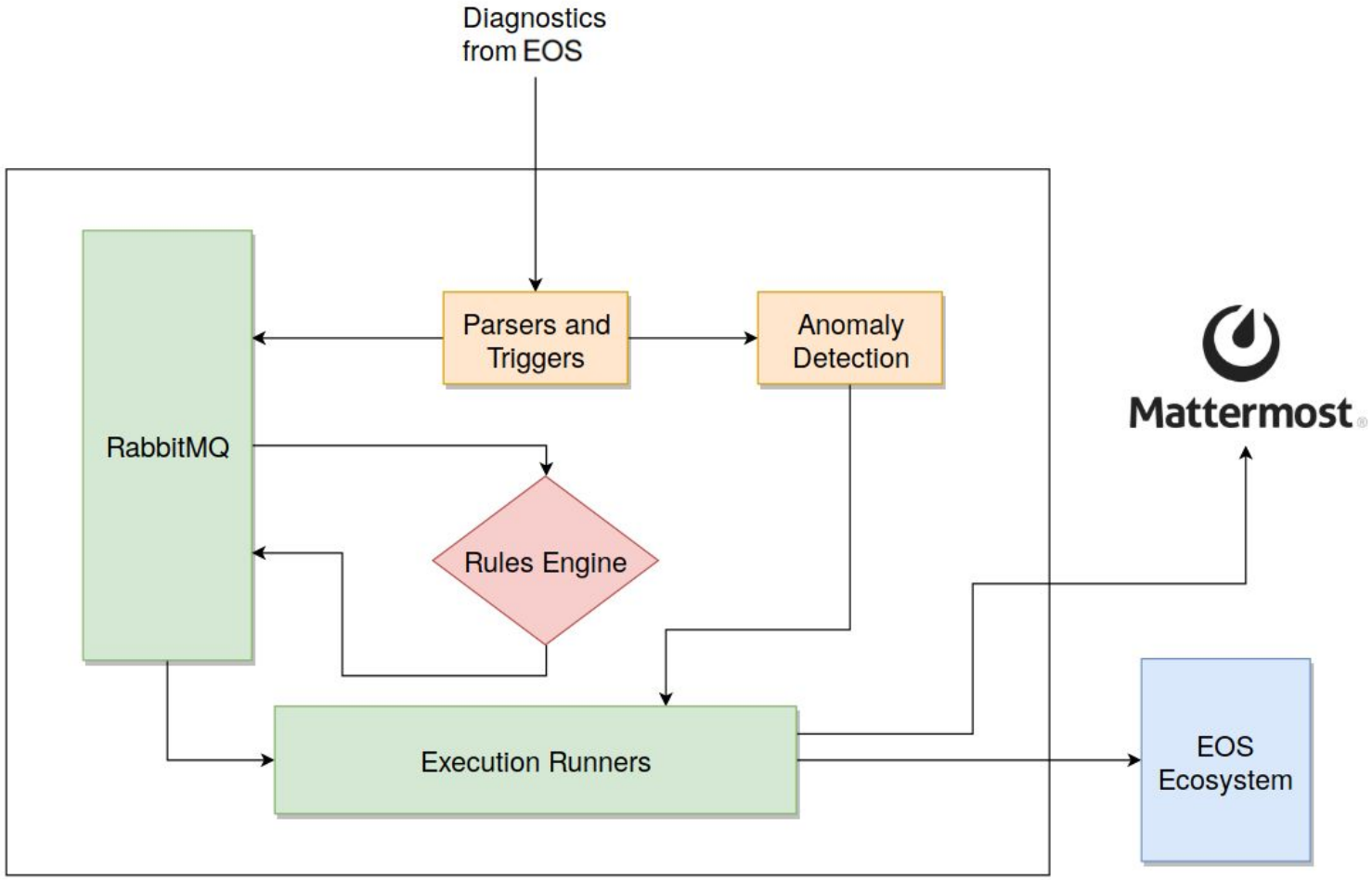


*Ahmad, Subutai, et al. "Unsupervised real-time anomaly detection for streaming data." *Neurocomputing* 262 (2017): 134-147.

Why not LSTMs?

https://twitter.com/mlinterview/status/996570725921181696

An EOS Winston instance



Implemented Runbooks

Winston in action

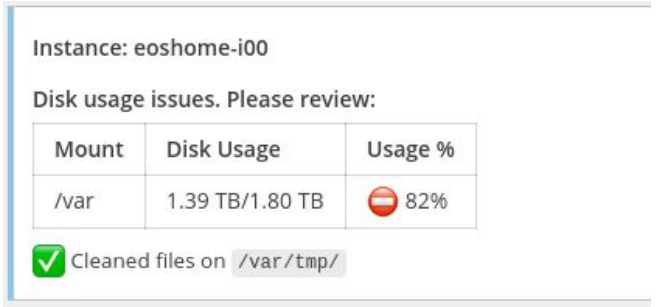
https://giphy.com/gifs/reaction-GnEyBQ2M2Vub6

Implemented Runbooks

Winston in action

- Drain expired:

- /var usage > 80%:



Implemented Runbooks

Winston in action

- User activity through the roof:

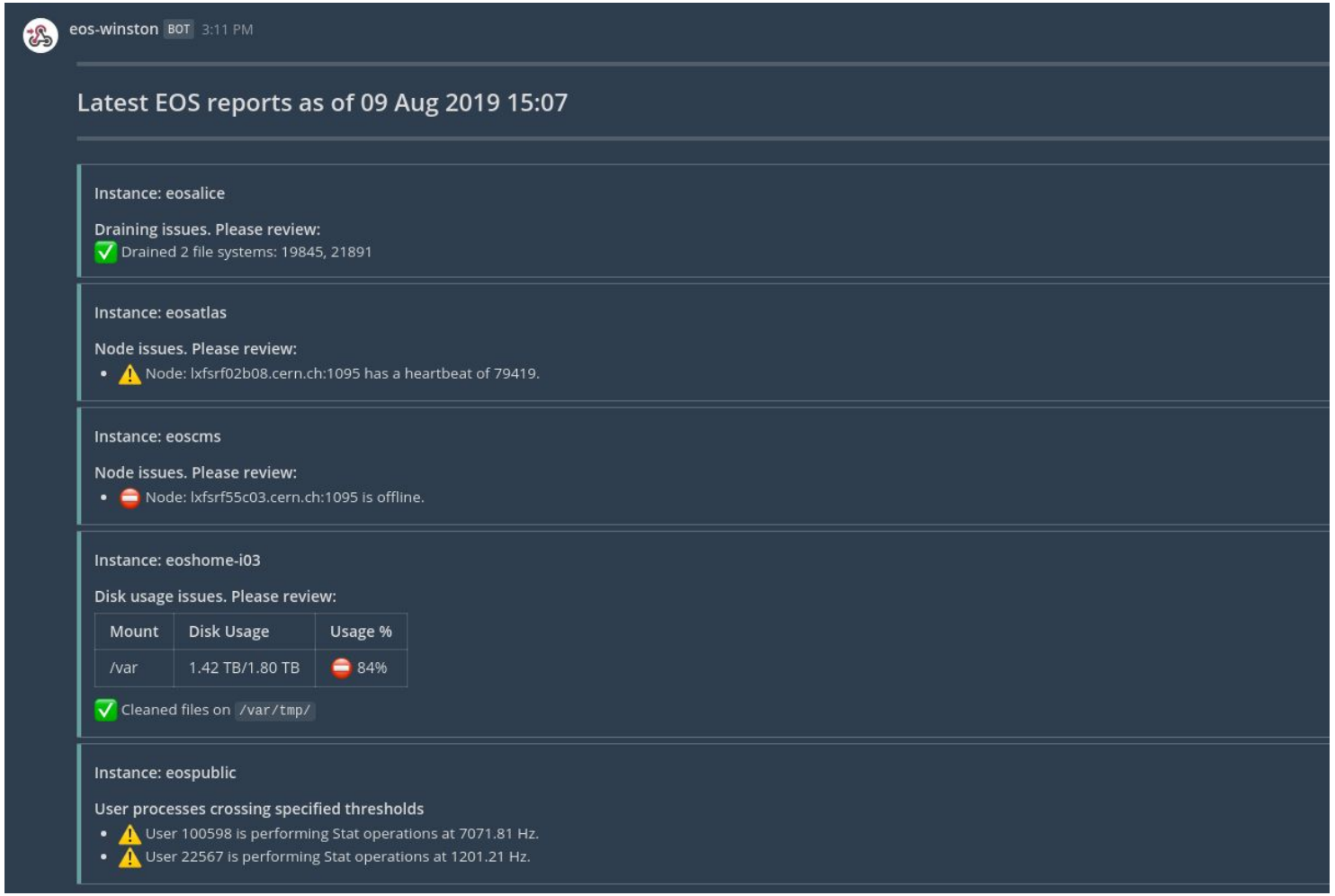
https://tenor.com/view/brooklynninenine-terry-crews-rosa-diaz-brooklyn99-youre-banned-gif-13390256

ChatOps Integration

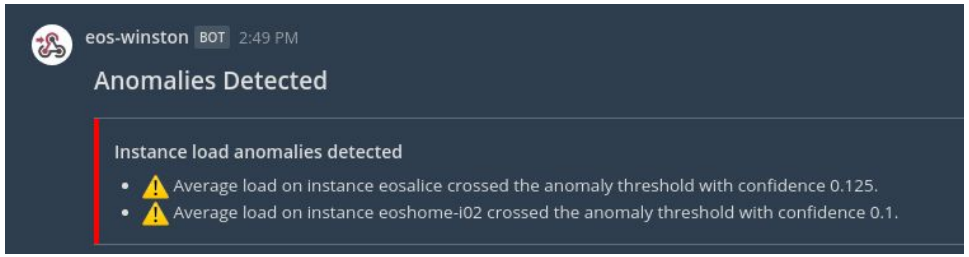
Conversation-driven development

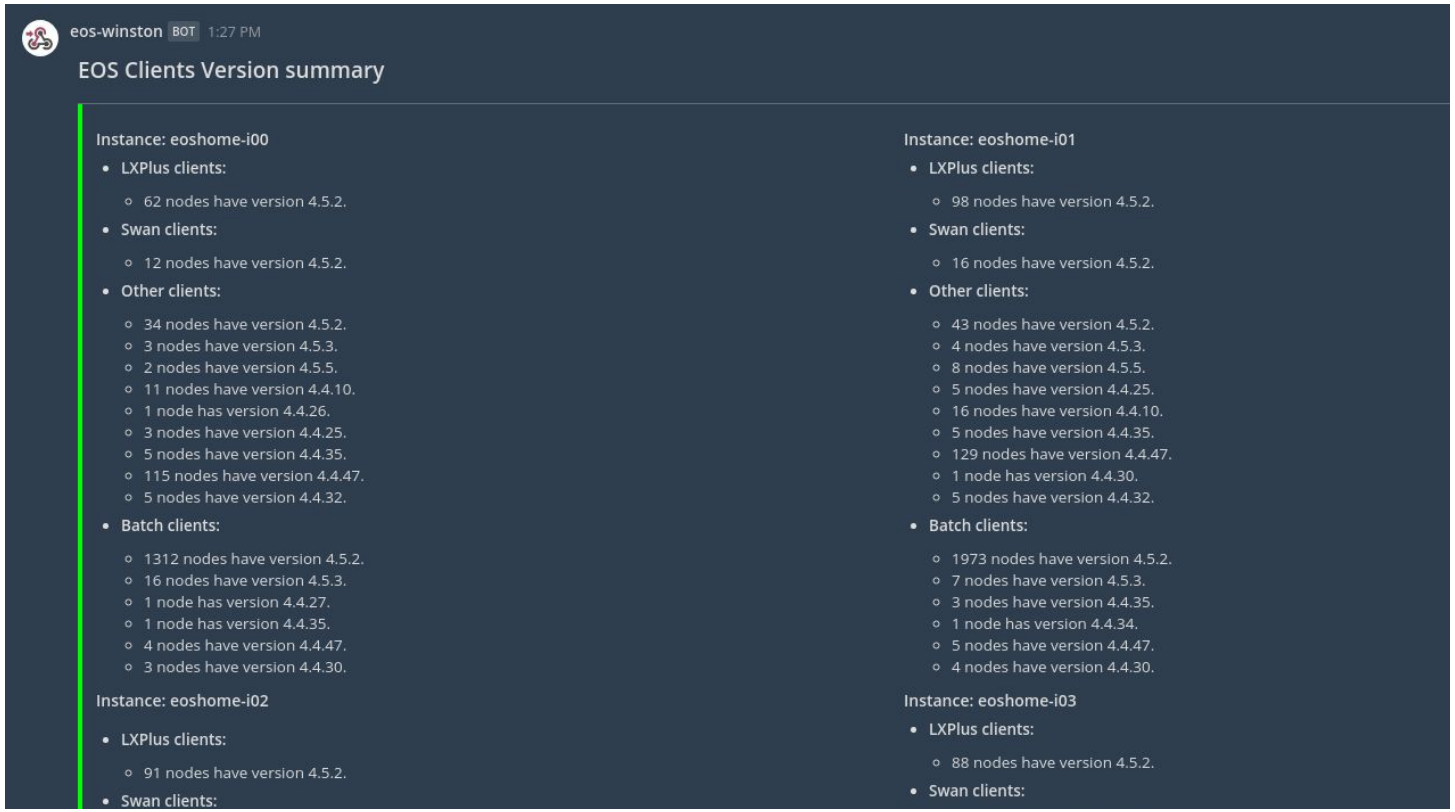
- Execute workflows as commands through Mattermost
- Unifying the communication about what work should get done with the actual history of the work being done
- New commands can be implemented by just adding the business logic

More of Winston



More of Winston (cuz why not)





Impact of the Project

https://www.netflix.com/watch/880640

Thank you!

Questions?

ishank.arora@cern.ch

https://giphy.com/gifs/awkward-pulp-fiction-john-travolta-6uGhT1O4sxpi8