Configurations: Do you prove yours?
Continuous configuration, observability, compliance

Alexandre BRIANCEAU
alexandre@rudder.io
@abrianceau
How are the servers doing?

No error nor change in logs means success?

Aren’t we missing something?
Main challenges faced nowadays

Multiple teams, diluted expertise, harder reporting

MGMT  DEV  SEC  OPS  EXTERN

DEV  QA  PRODUCTION  RECOVERY

Heterogeneous systems, reduced visibility, ease of use and understanding
Getting and understanding the info is complex

Operators, Managers, Experts, APIs have different needs

Frustration if we need a third party to get data

We mistrust what we don’t understand
Configuration management is a systems engineering process for establishing and maintaining consistency of a product [...] throughout its life.
How DevSecOps can help to understand?
Let's remember: What does configuration management do?

configuration ➔ target state ➔ configuration ➔ feedback
Let's remember: What does configuration management do?

configuration target state → configuration → feedback → configuration → feedback → configuration
Observability is a measure of how well internal states of a system can be inferred from knowledge of its external outputs.
Monitoring VS Observability: having a factual & deep insight
Why we need Observability in Configuration Management?

- **Causality**: trust and prove configuration states
- **Perspective**: provide insights relevant to different needs
- **Agency**: help teams find the best levers for their job
Let’s take an implementation example...

CONTINUOUS AUDITING & CONFIGURATION
These concepts are core to Rudder

Everyone/thing can be an actor of configuration management
Observability and how Rudder can prove the compliance?

- PARAM
  - Id

- RULE
  - Id
  - (Components)

- DIRECTIVE
  - Id

- GROUP
  - Id

- RUDDER config (global)
  - Policy Mode
  - Schedule...

- NODE
  - Properties
  - Policy Mode
  - Schedule...

Node configuration
- Id:...
- Generated:...

Environmental context

RUN
- Reports
- Reports
- ...
- ...

+ METADATA
  - node id
  - config id
  - run timestamp
  - Signature

Metadata
- Integrity
- Signature

Config
- For Rule R, Directive D1, Component C

Historisation
- Event logs
- Change request

Expected reports
- (node id, config id, timestamp)

Send expected reports

Send configuration reports

Compliance historised

Get config

Historisation

Run reports

Send configuration reports
French, mature and open-source of continuous configuration compliance

Manage OS, middleware and software level

Team oriented (WebUI, CLI, API)

Audit only or automatic drift remediation

Continuous reporting and dashboarding
Thank you!

Any questions?

5mn Survey on SecOps:
bit.ly/pts19-secops