Golang Automatic Remediation

Daniel Rodriguez & Marek Denis | NIE/NetPE | Dublin
Execution framework for the Network
GOAR: why?
Reason 1

PoC
Our needs
Our needs

Simple architecture
Highly scalable
Modular
On-demand
Building blocks
Building blocks

Syslog processing
Act on certain syslog
Building blocks

Syslog processing
Act on certain syslog

SNMP Processing
Act on certain SNMP traps
Building blocks

Syslog processing
Act on certain syslog

SNMP Processing
Act on certain SNMP traps

Audits
Code that evaluate the state of a device
Building blocks

- **Syslog processing**: Act on certain syslog
- **SNMP Processing**: Act on certain SNMP traps
- **Job/remediation**: Simple self-contain jobs, that modify the state of a device
- **Audits**: Code that evaluate the state of a device
Use cases
Simple Syslog Matching

Network device → Syslog Server → Rule Definition → Processor → Event → Action
Checking the state

User/system → Event → Action
Execution Workflow
GOAR: Go automatic remediation
https://github.com/facebookexperimental/GOAR
Why Go?
Why Go?

Simple language with basic building blocks
Why Go?

Portability and speed
Why Go?

Easy, simple and efficient concurrency
Why Go?

Safe language with "forced" error checking
Why Go?

Garbage collection
Why Go?

Statically typed
GOAR Architecture
GOAR

Common pipeline
Syslog -> RabbitMQ QUEUE_LOG -> Syslog Processor -> RabbitMQ QUEUE_INCIDENT -> Executor

Audits, Jobs
test_device Err: 1417: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet6/12/1, changed state to down

```json
{
  "Rule": "arista_interface_down",
  "RawIncident": "test_device Err: 1417: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet6/12/1, changed state to down",
  "Parameters": ["hostname": "test_device", "interface": "Ethernet6/12/1"],
  "PreAudit": "interface_check.pl --hostname 'test_device' --interface 'Ethernet6/12/1'",
  "Remediation": "port_down_arista.py --hostname 'test_device' --interface 'Ethernet6/12/1'",
  "Engine": "syslog",
}
```

- **RuleName**: arista_interface_down
- **DeviceType**: ARISTA
- **Regex**: "Line protocol on Interface (?P<interface>[\S]+), changed state to down"
- **Remediations**: 
  - port_down_arista.py
- **AlertType**: Interface Status
The audit call

{  
    Rule: "check_bgp_redundancy",
    RawIncident: "check_bgp_redundancy",
    Parameters: {"hostname": "test_device"},
    PreAudits: "check_bgp_redundancy.py --hostname 'test_device'",
    Engine: "CLI",
}
Configuration of device

```json
{
  Rule: "rebase_device",
  RawIncident: "rebase_device",
  Parameters: ["hostname: test_device"],
  PreAudits: ["capacity_headroom.py --hostname 'test_device'"],
  Remediation: ["configure_ip.py --hostname 'test_device'",
                "configure_bgp.py --hostname 'test_device'",
                "undoip.py --hostname 'test_device'"],
  PostAudits: ["check_bgp_redundancy.py --hostname 'test_device'",
               "check_device_traffic.py --hostname 'test_device'"],
  Engine: ["cli",
            ]
}
```