GOAR

Golang Automatic Remediation

Daniel Rodriguez & Marek Denis | NIE/NetPE | Dublin

Execution framework for the Network

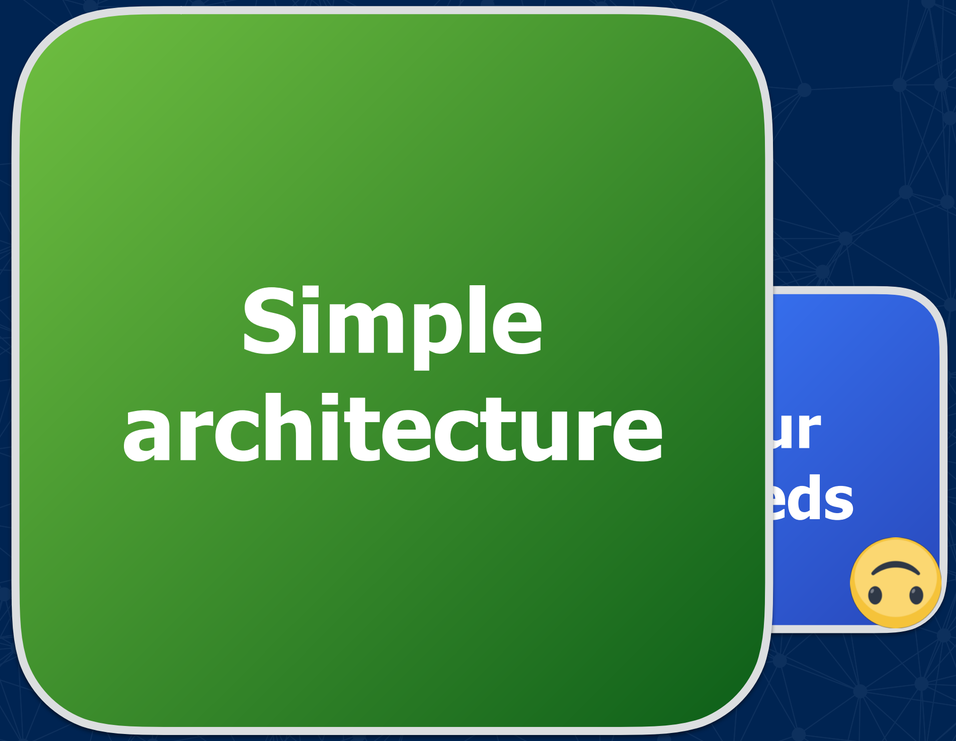
GOAR: why?

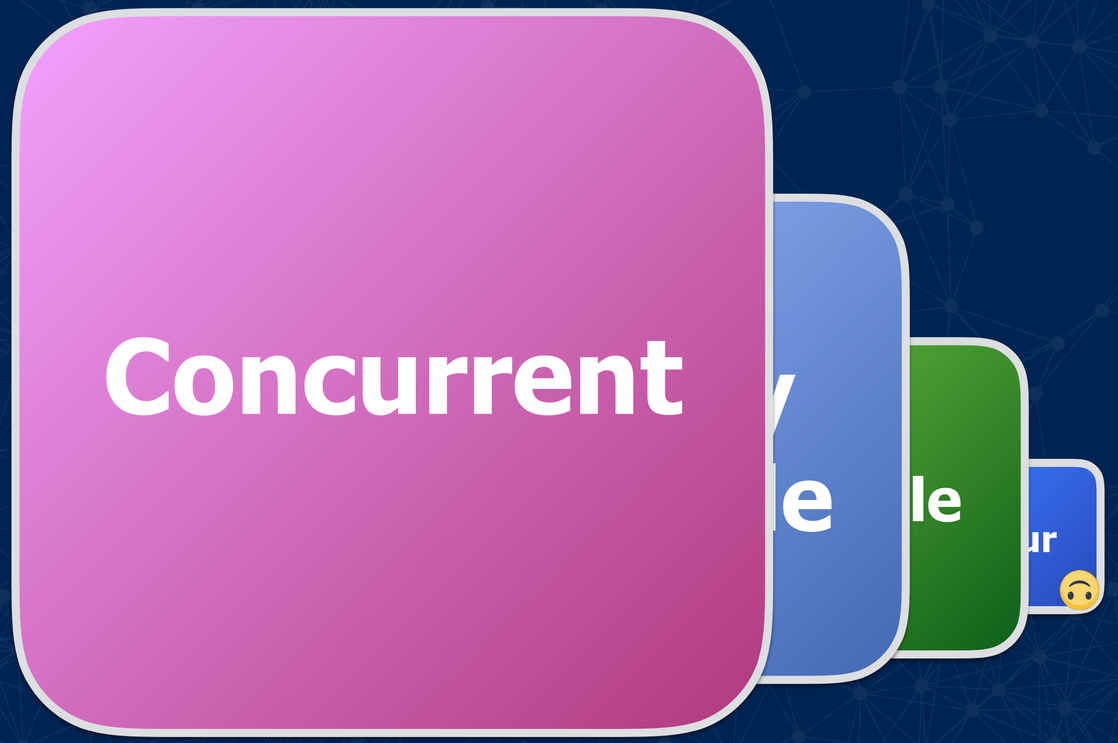
Reason 1

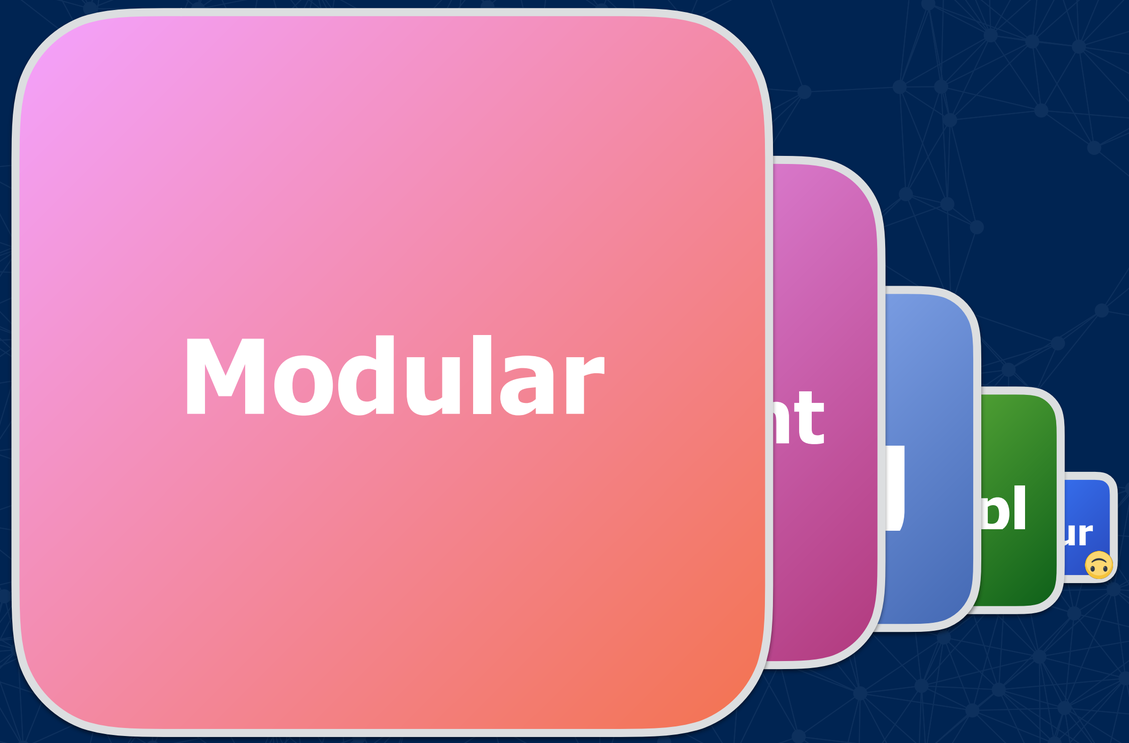
PoC

Our needs

Simple architecture







Flexible

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

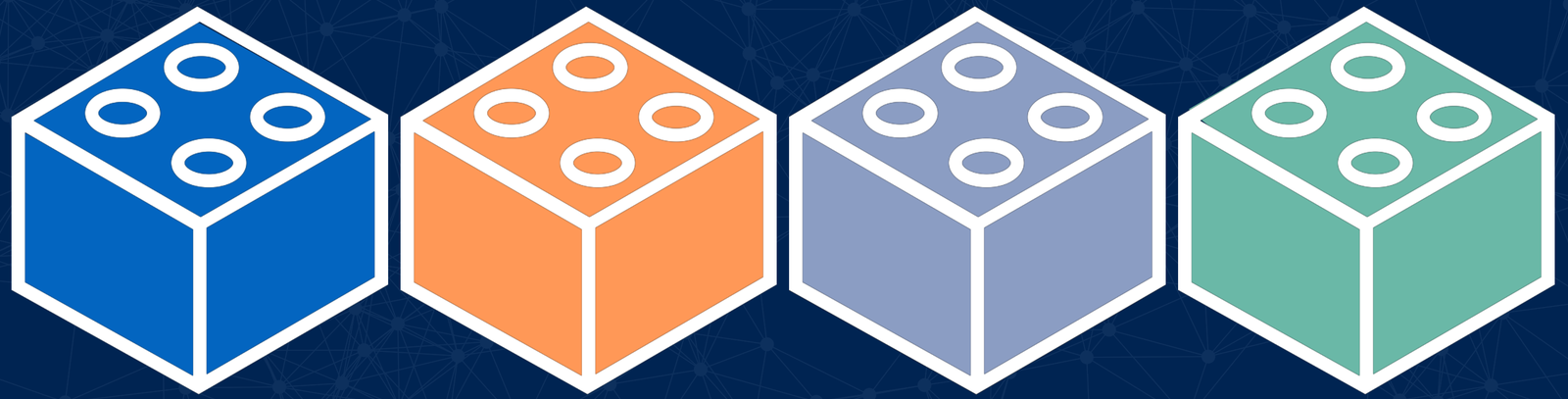
Syslog processing
Act on certain syslog

Job/remediation
Simple self-contain jobs, that modify the state of a device

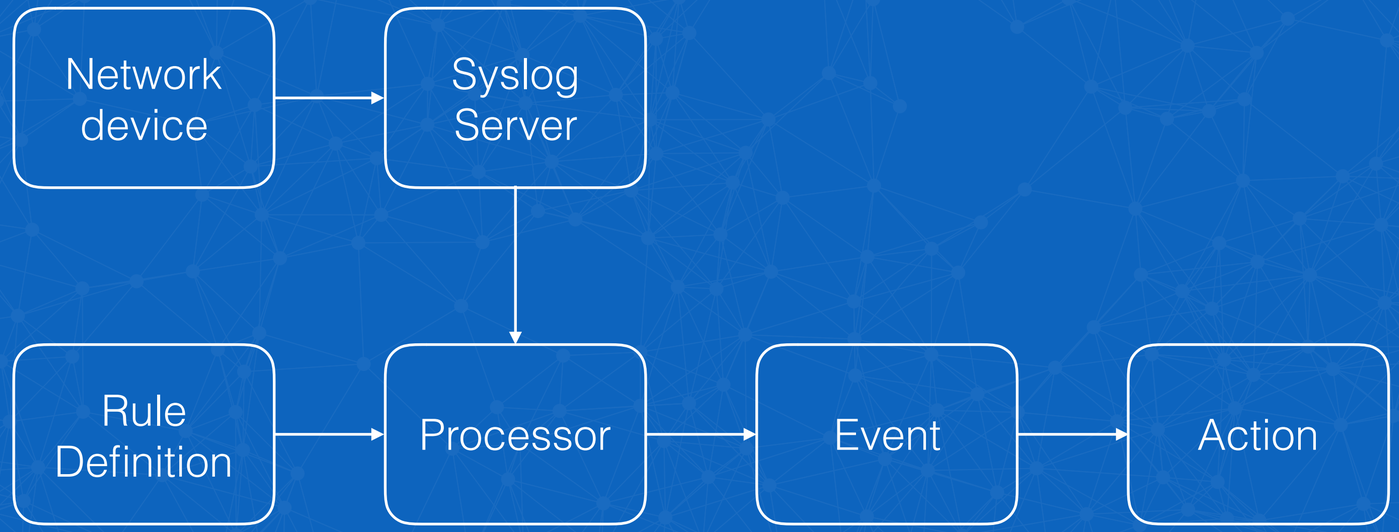
SNMP Processing
Act on certain SNMP traps

Audits
Code that evaluate the state of a device

Use cases

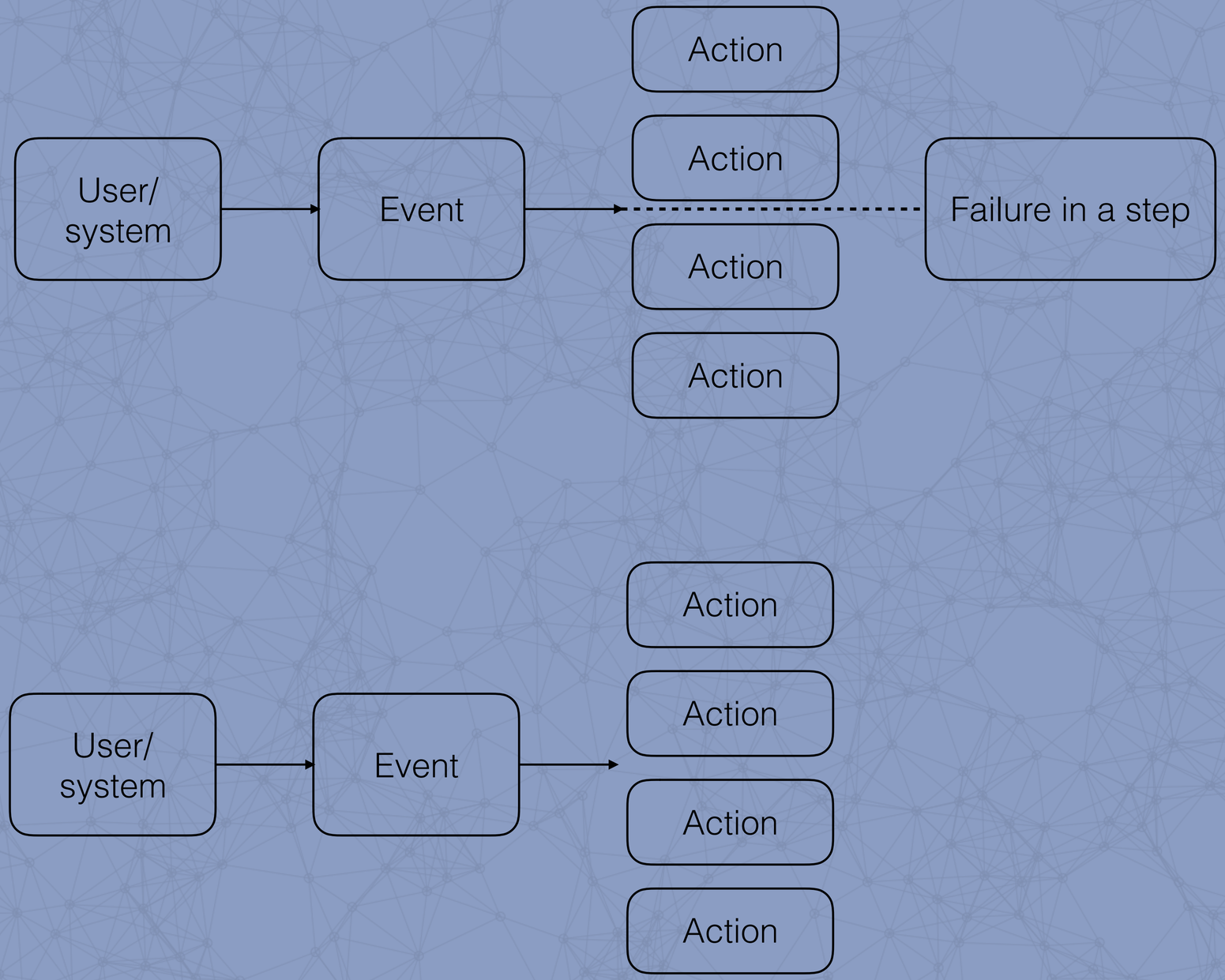


Simple Syslog Matching



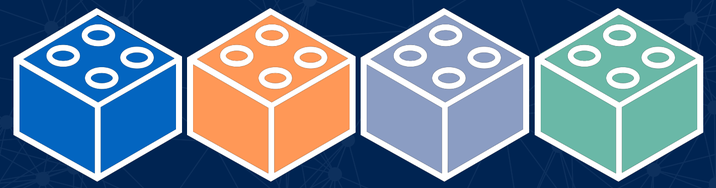
Checking the state

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

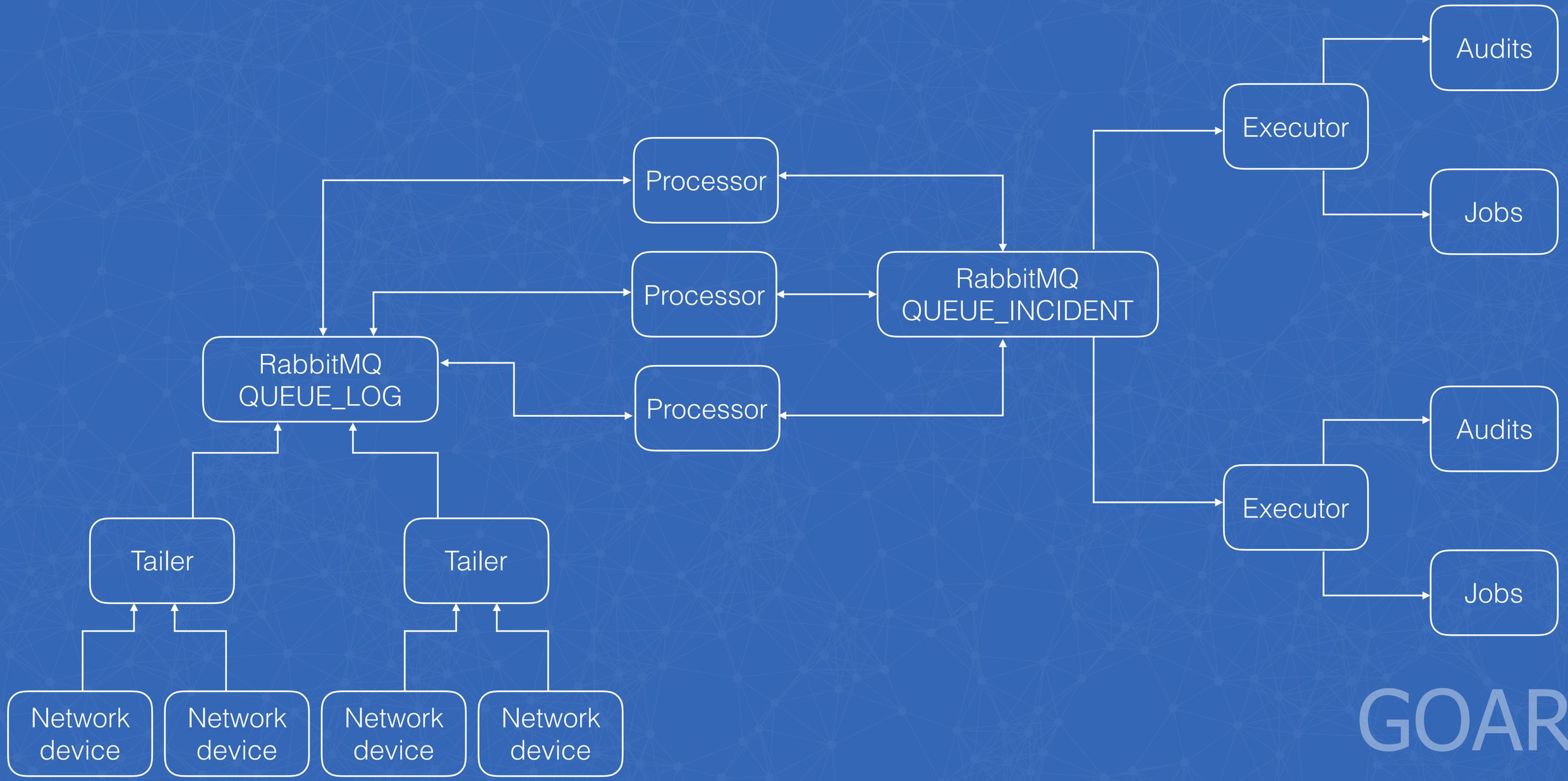
Why Go?

Garbage collection

Why Go?

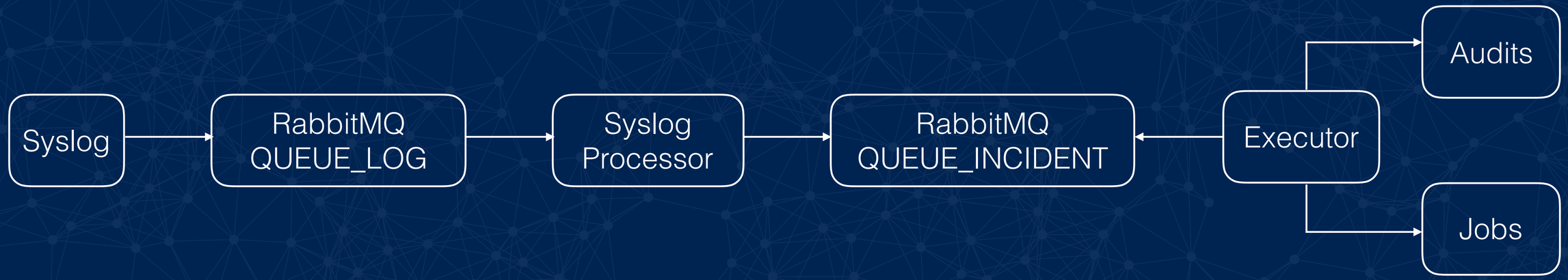
Statically typed

GOAR Architecture



GOAR Architecture

GOAR
Common pipeline

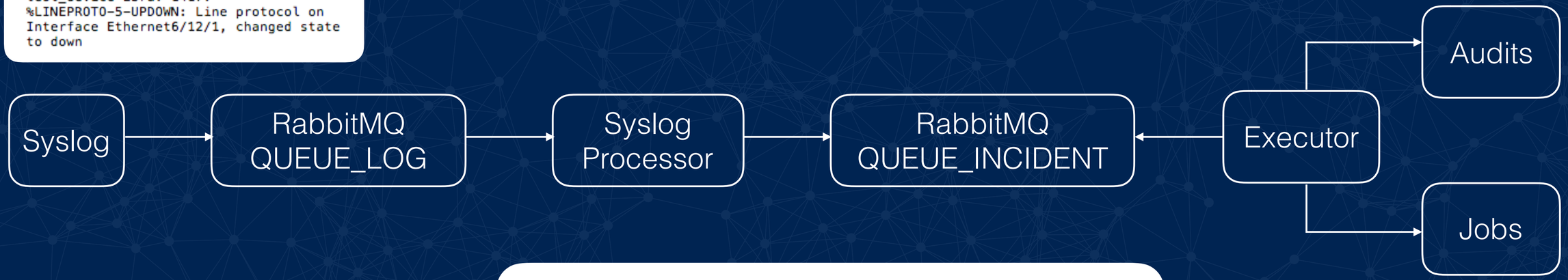


GOAR
Common pipeline

Demos

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

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




```
- 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
```

DRAFT

```
{
Rule:         "check_bgp_redudancy",
RawIncident: "check_bgp_redundancy",
Parameters: {"hostname": test_device},
PreAudits:  "check_bgp_redundancy.py --hostname 'test_device'",
Engine:       "cli",
}
```

The audit call

```
{
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'",
"undrain.py --hostname 'test_device'"],
PostAudits:   ["check_bgp_redundancy.py --hostname 'test_device'",
"check_device_traffic.py --hostname 'test_device'"],
Engine:       "cli",
}
```

Configuration of device

Q&A