HUK-COBURG

Managing Prometheus in a Security-focused Environment

Linux Monitoring at HUK-COBURG

PromCon 2019 | Christian Hoffmann

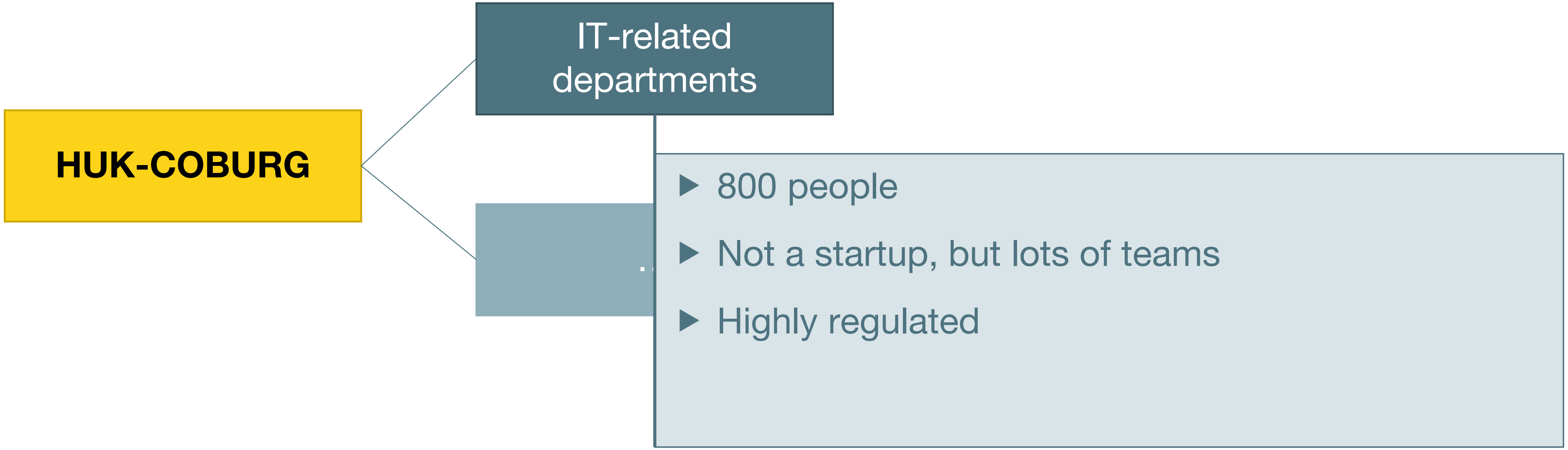
Conway‘s Law?

$ cat /HUK-COBURG

HUK-COBURG

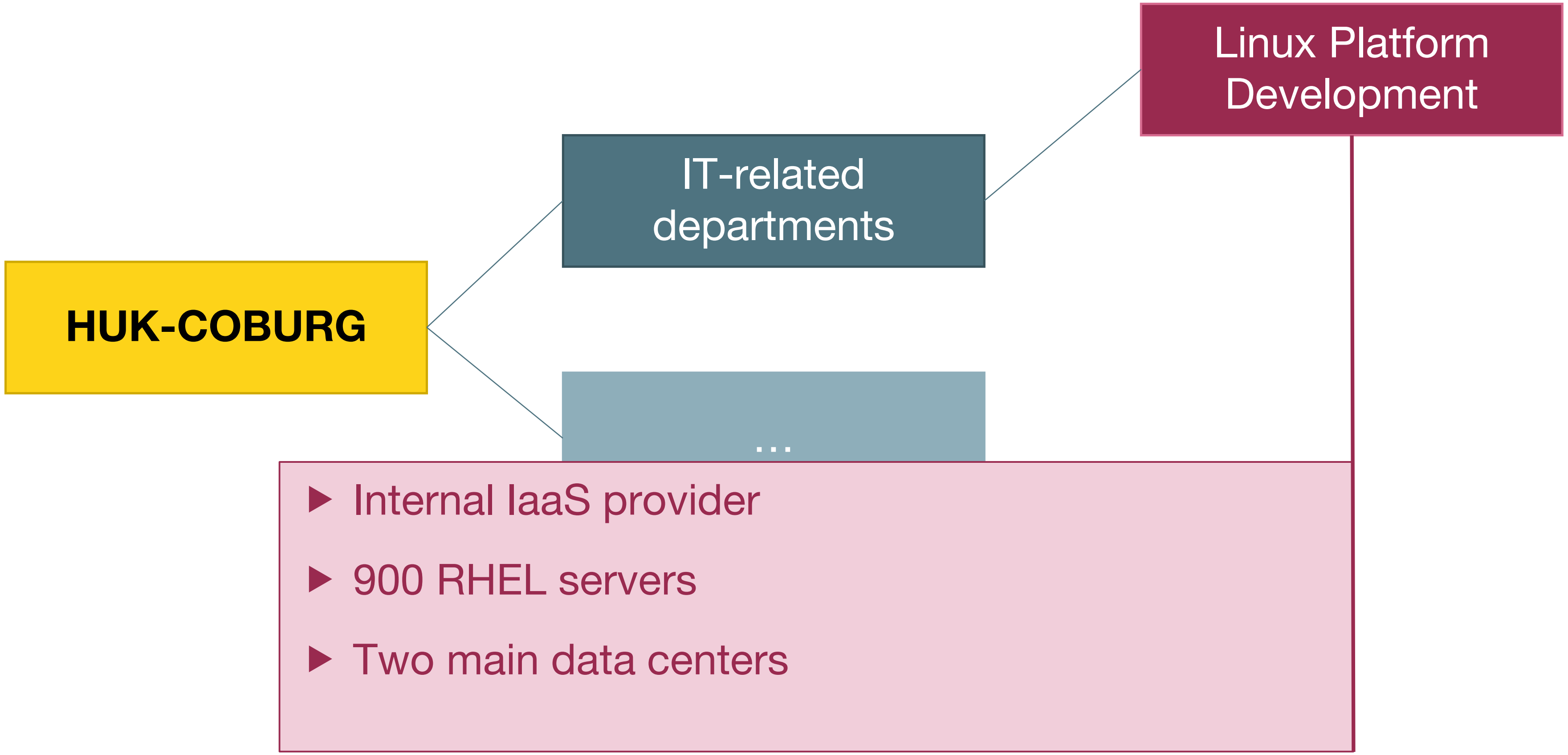
- German consumer insurance company
- Largest car insurance for consumers in Germany
- 12 million customers
- 10.000 employees

$ cat /HUK-COBURG/IT



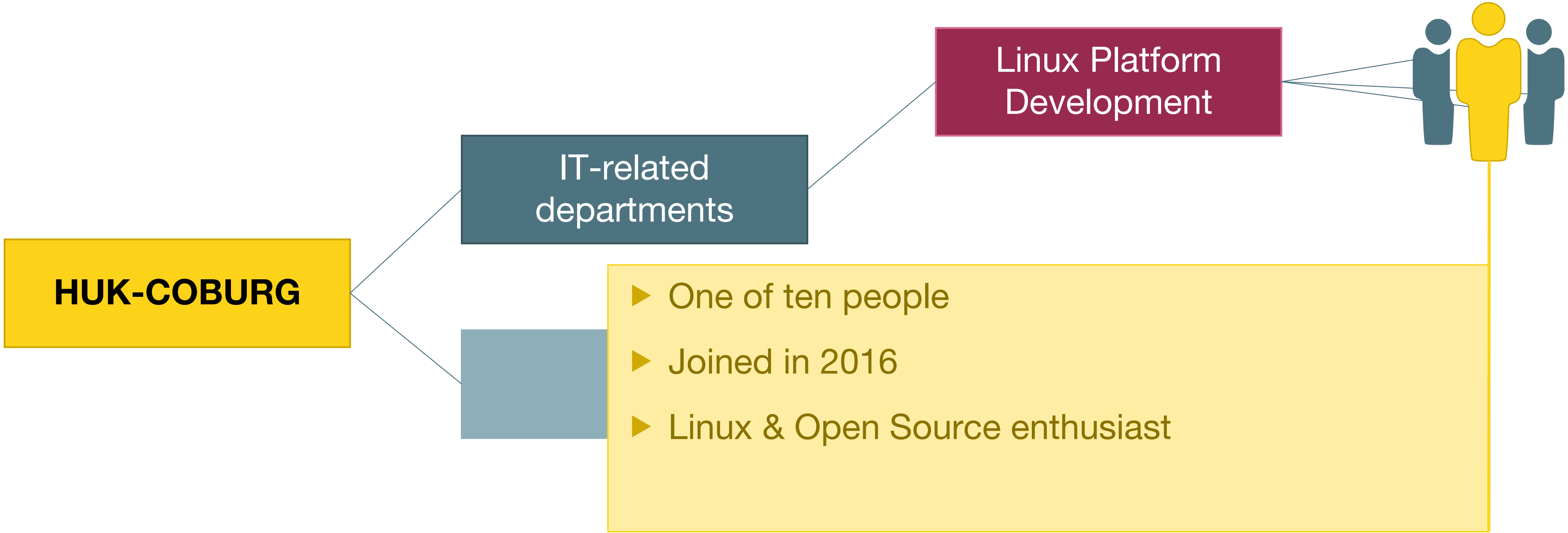
- 800 people
- Not a startup, but lots of teams
- Highly regulated

$ cat /HUK-COBURG/IT/Linux



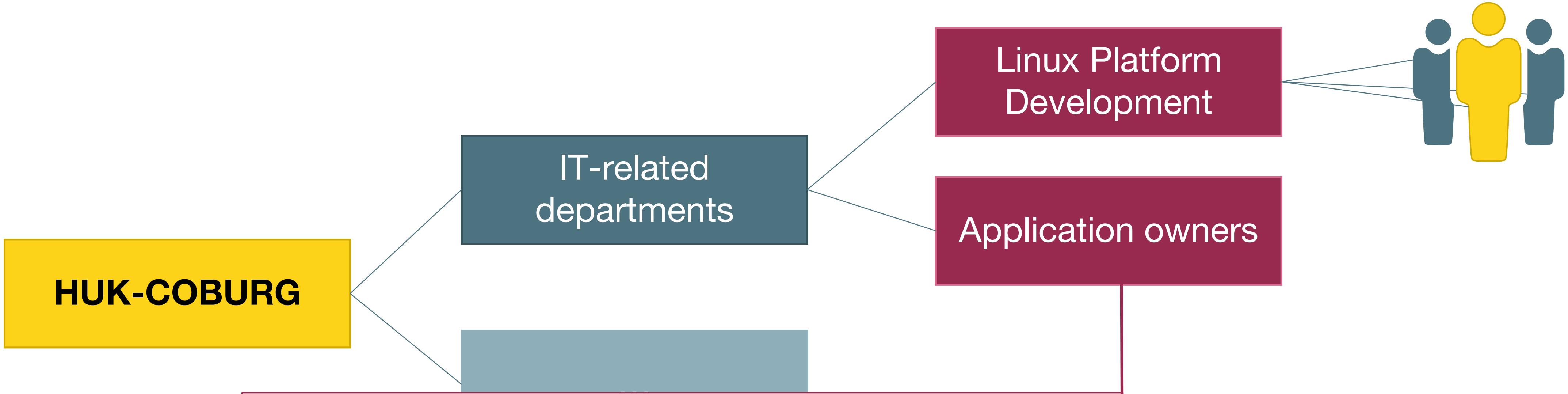
- Internal IaaS provider
- 900 RHEL servers
- Two main data centers

$ cat /HUK-COBURG/IT/Linux/Christian Hoffmann



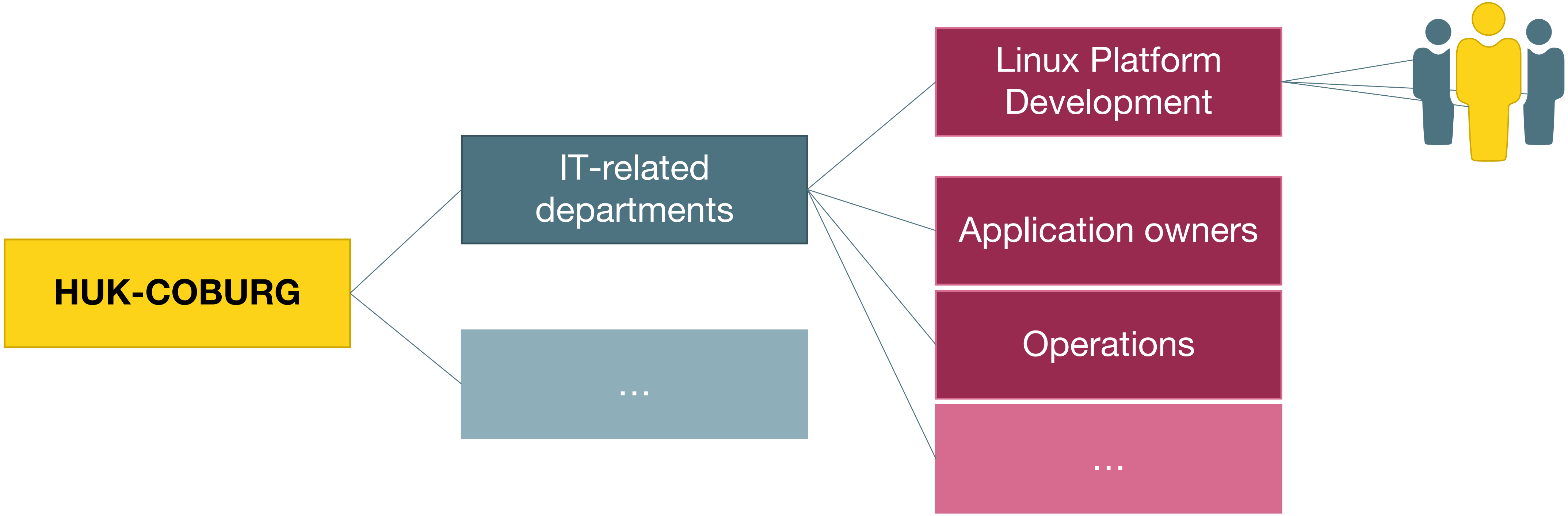
- One of ten people
- Joined in 2016
- Linux & Open Source enthusiast

$ cat /HUK-COBURG/IT/Linux/Application owners

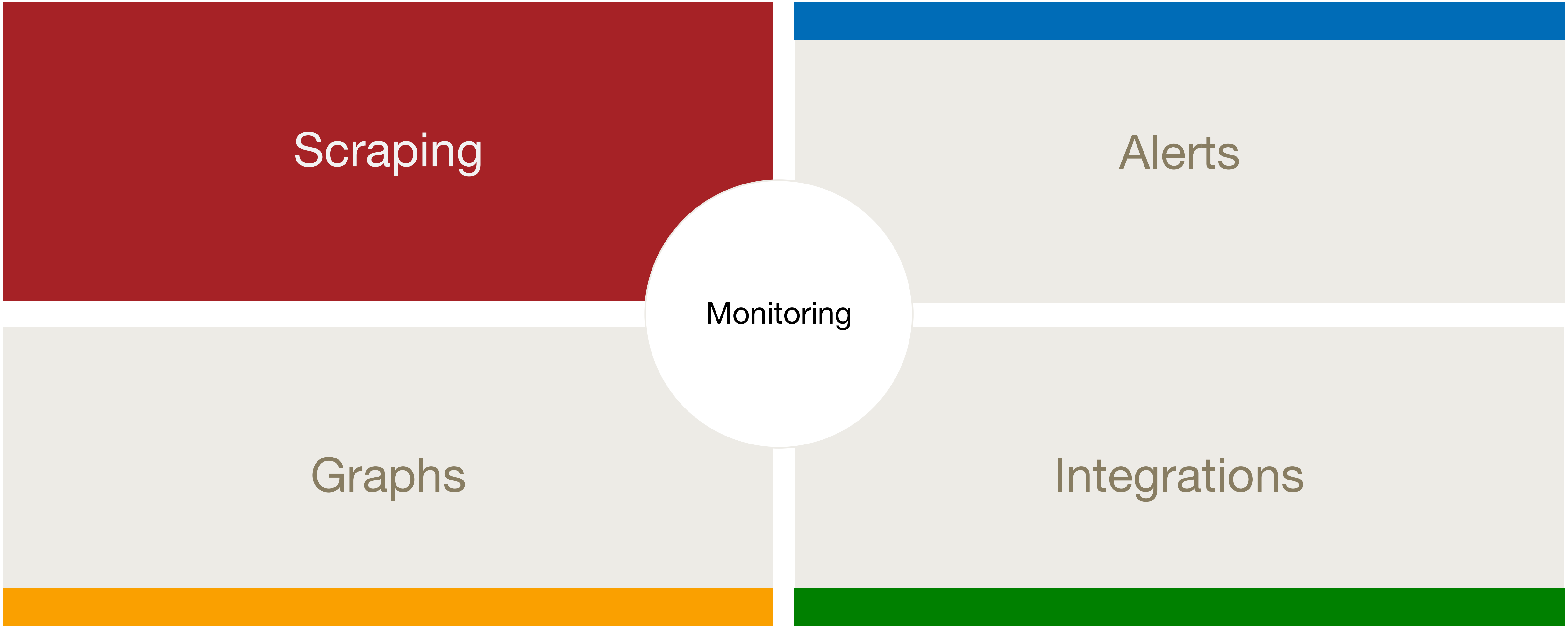


- ▶ About 130 people, running:
  - Databases
  - Web servers
  - …

$ cat /HUK-COBURG/IT/Linux/Others



Overview



Scraping

Alerts

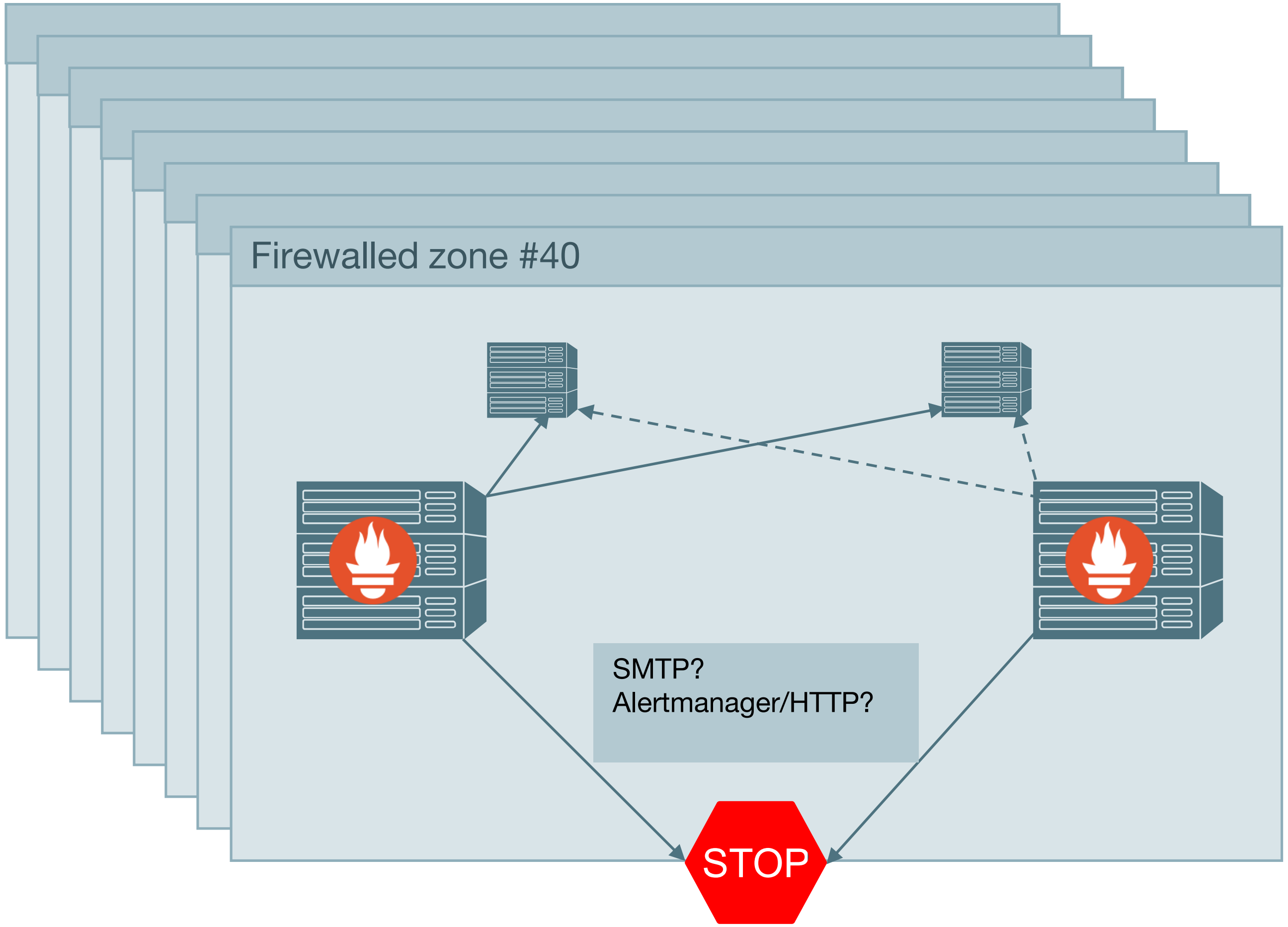
Monitoring

Graphs

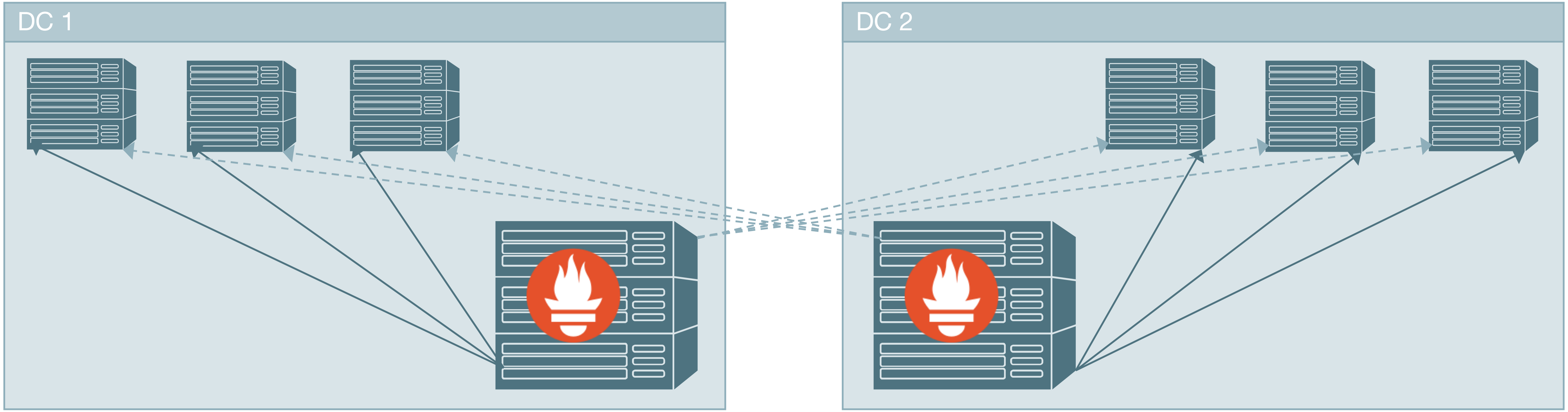
Integrations

Placement of Prometheus Instances

- *Close to the target*
- What does *close* mean?

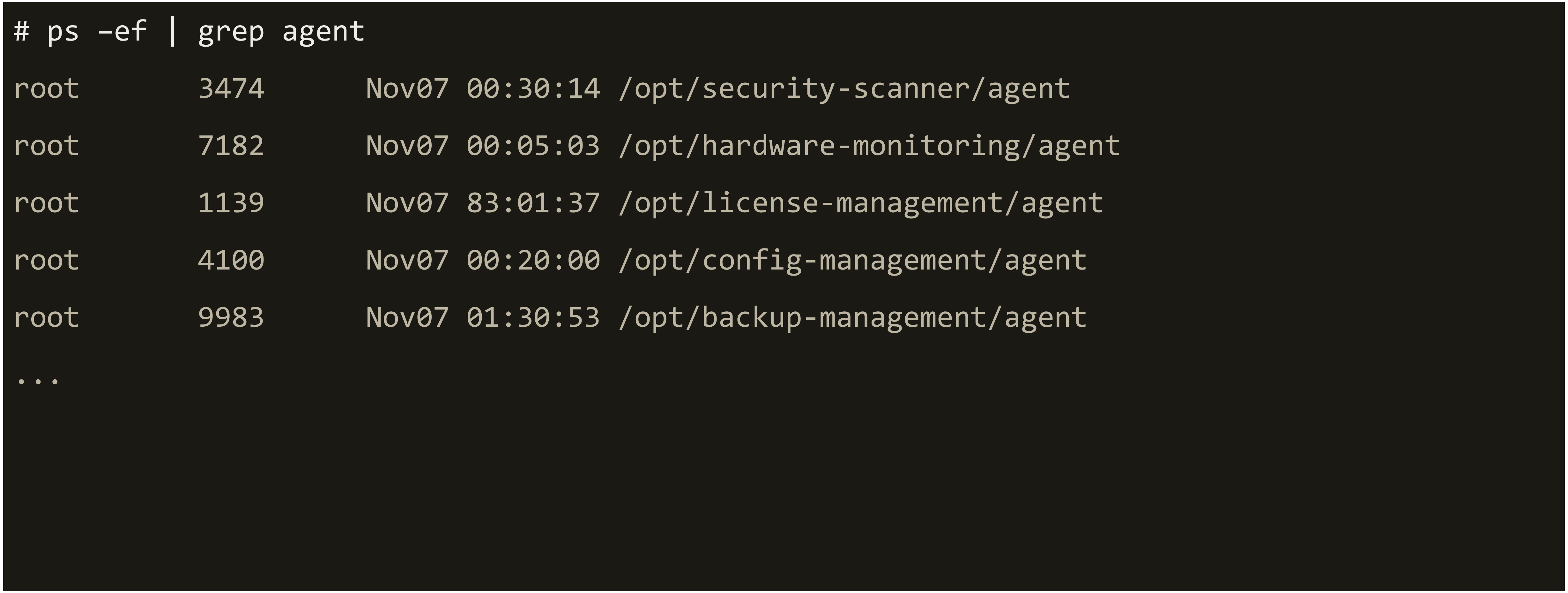


Our setup: One Prometheus per DC



2	4	1.7 M	60s	200
VMs	cores	series	scrape_interval	alert rules
20 GiB	1.2 TiB	30 k	2 600	1 600
RAM	disk	samples/s	file_sd	rec rules

Scraping: Securing and unifying metrics access



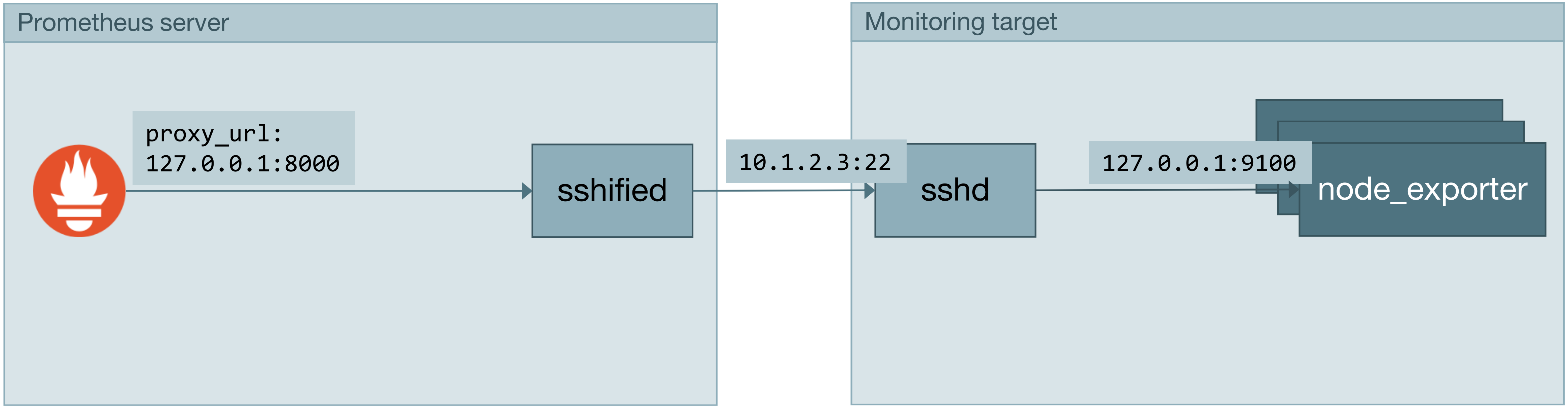
```
# ps -ef | grep agent
root       3474      Nov07 00:30:14 /opt/security-scanner/agent
root       7182      Nov07 00:05:03 /opt/hardware-monitoring/agent
root       1139      Nov07 83:01:37 /opt/license-management/agent
root       4100      Nov07 00:20:00 /opt/config-management/agent
root       9983      Nov07 01:30:53 /opt/backup-management/agent
...
```

So…

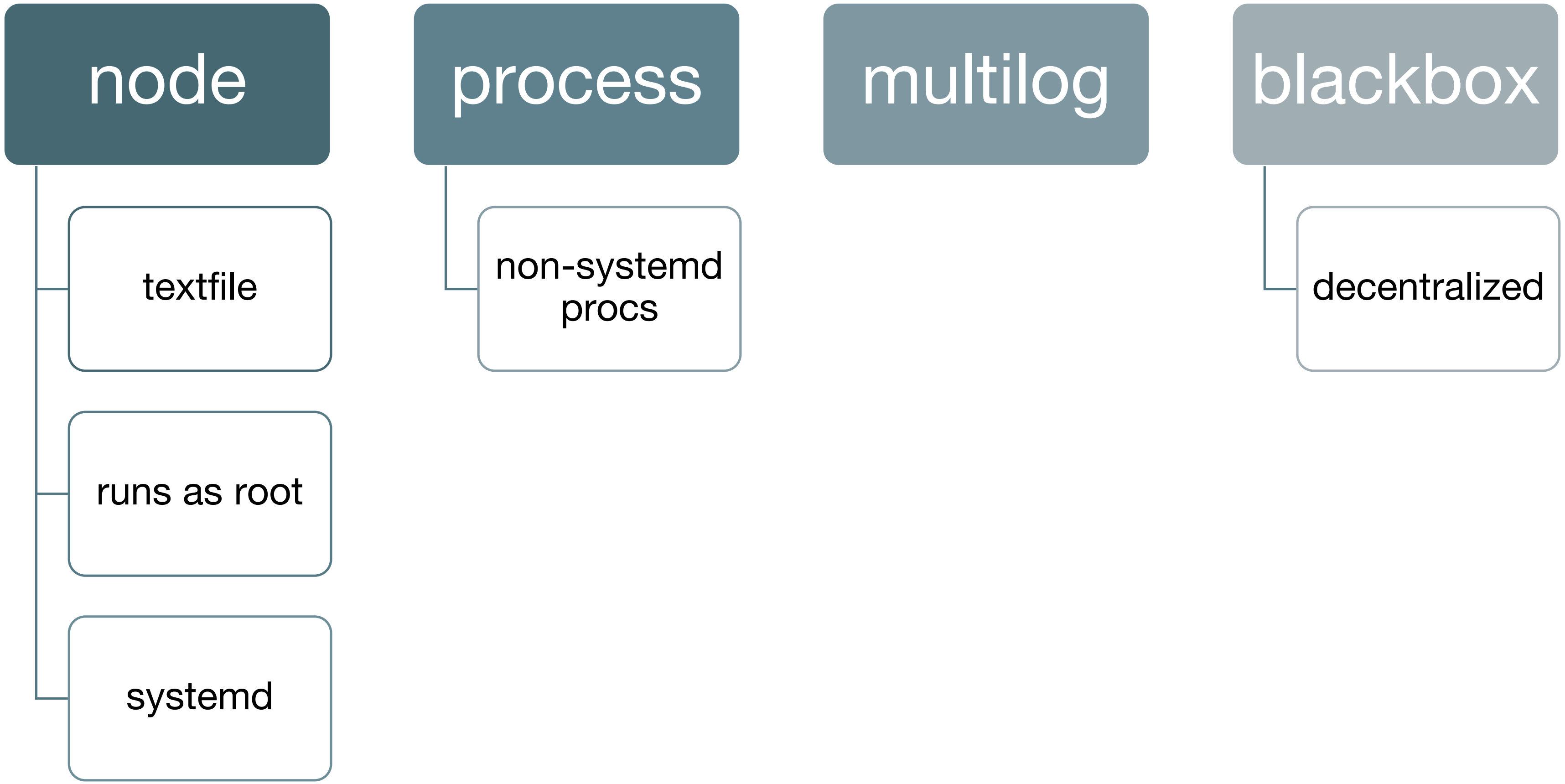
```
# nmap server1001
PORT   STATE SERVICE
22/tcp open  ssh


Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Introducing sshified

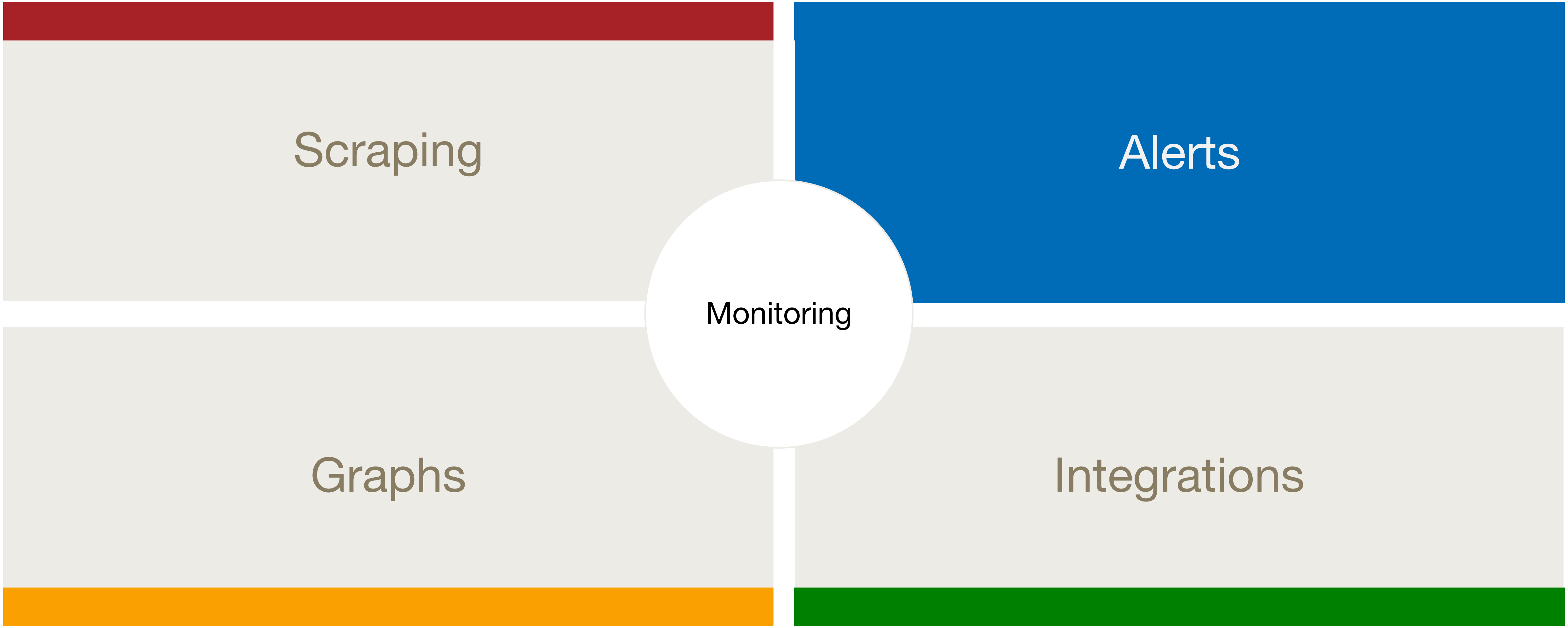


Exporters



- node
  - textfile
  - runs as root
  - systemd
- process
  - non-systemd procs
- multilog
- blackbox
  - decentralized

Overview



Scraping

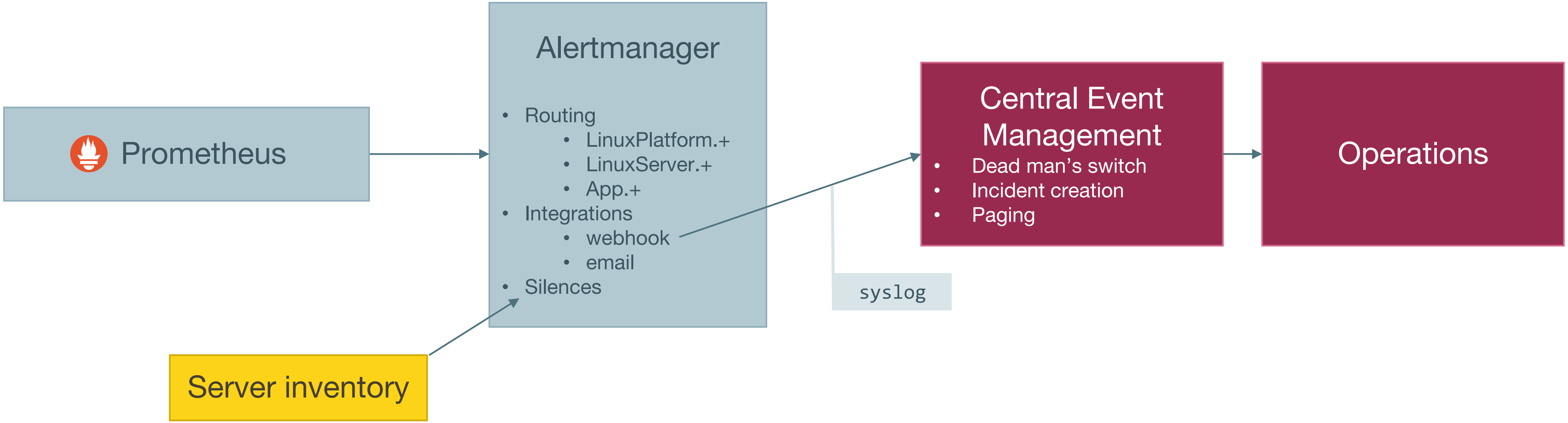
Alerts

Monitoring

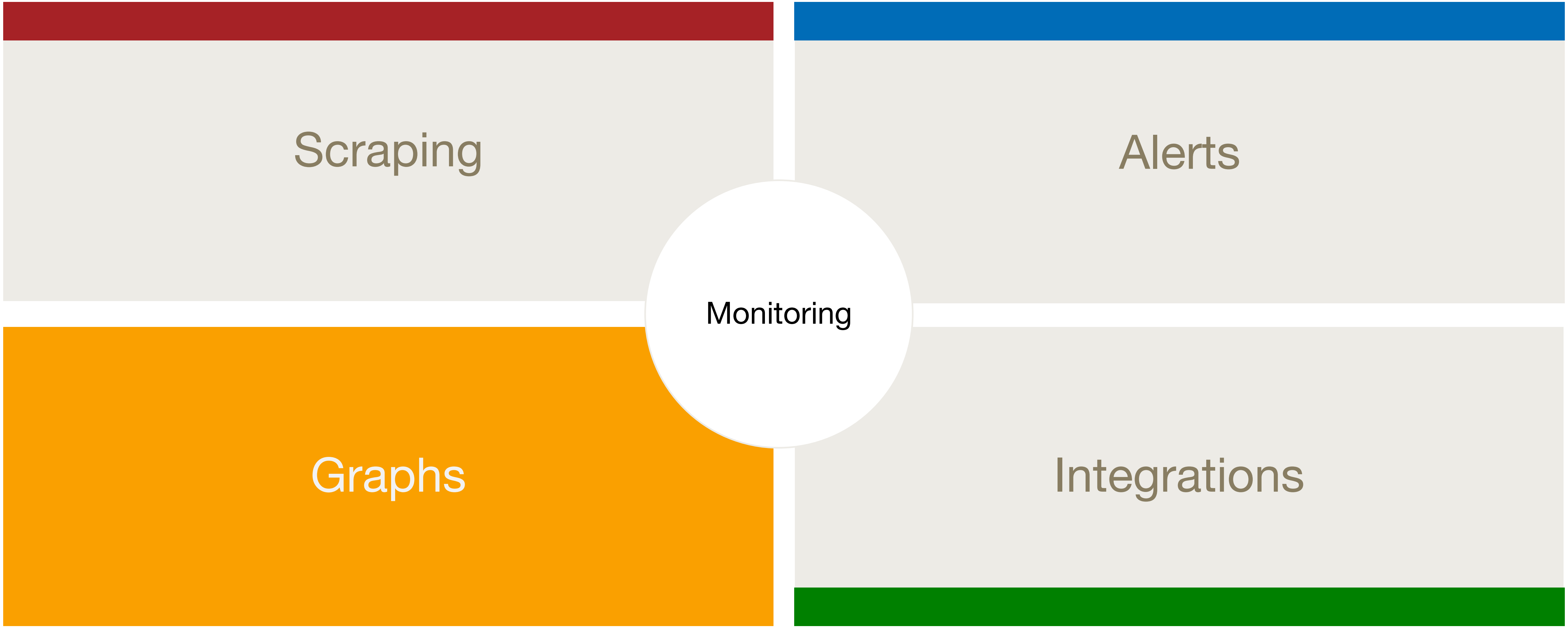
Graphs

Integrations

Alertmanager



Overview



Scraping

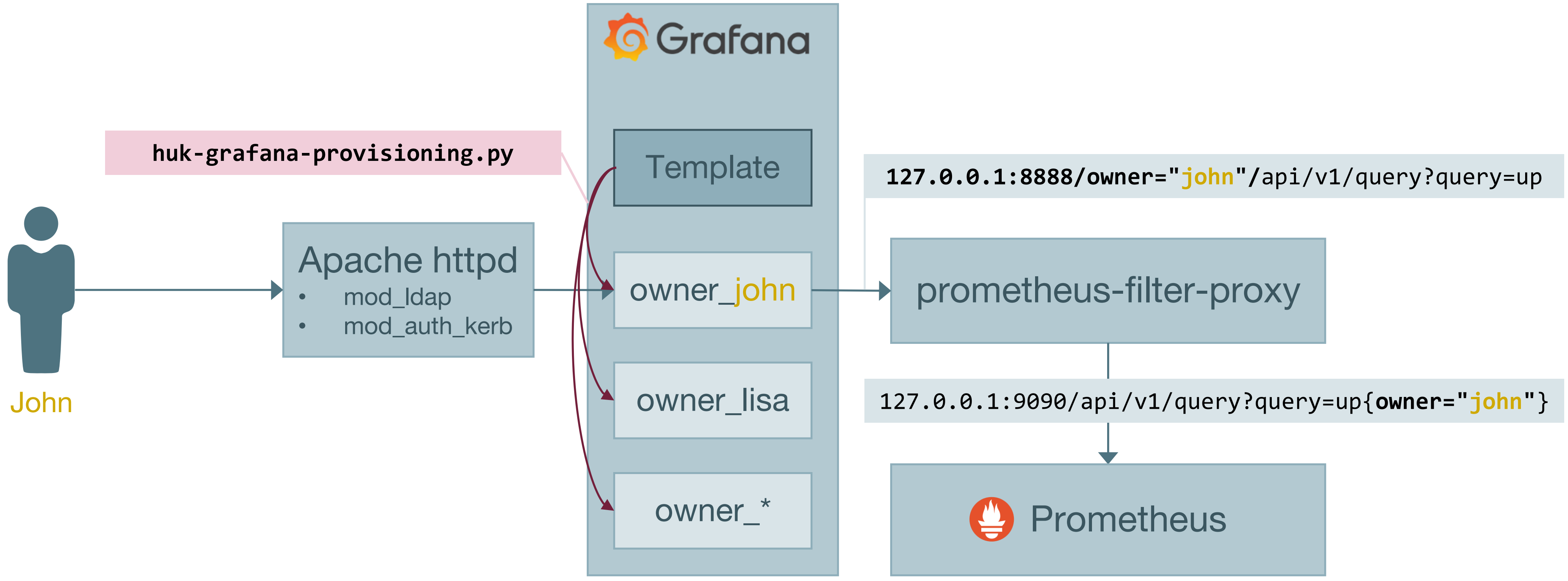
Alerts

Monitoring

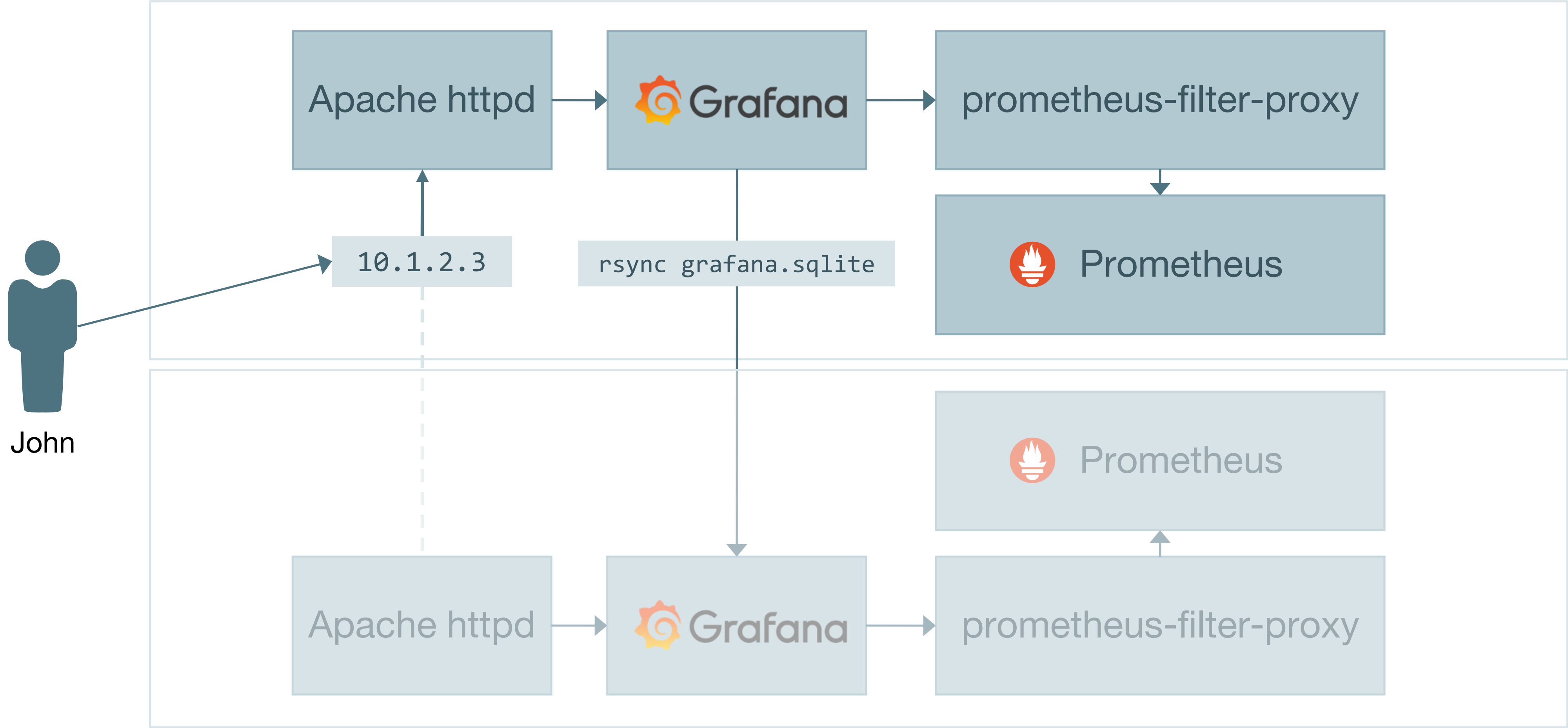
Graphs

Integrations

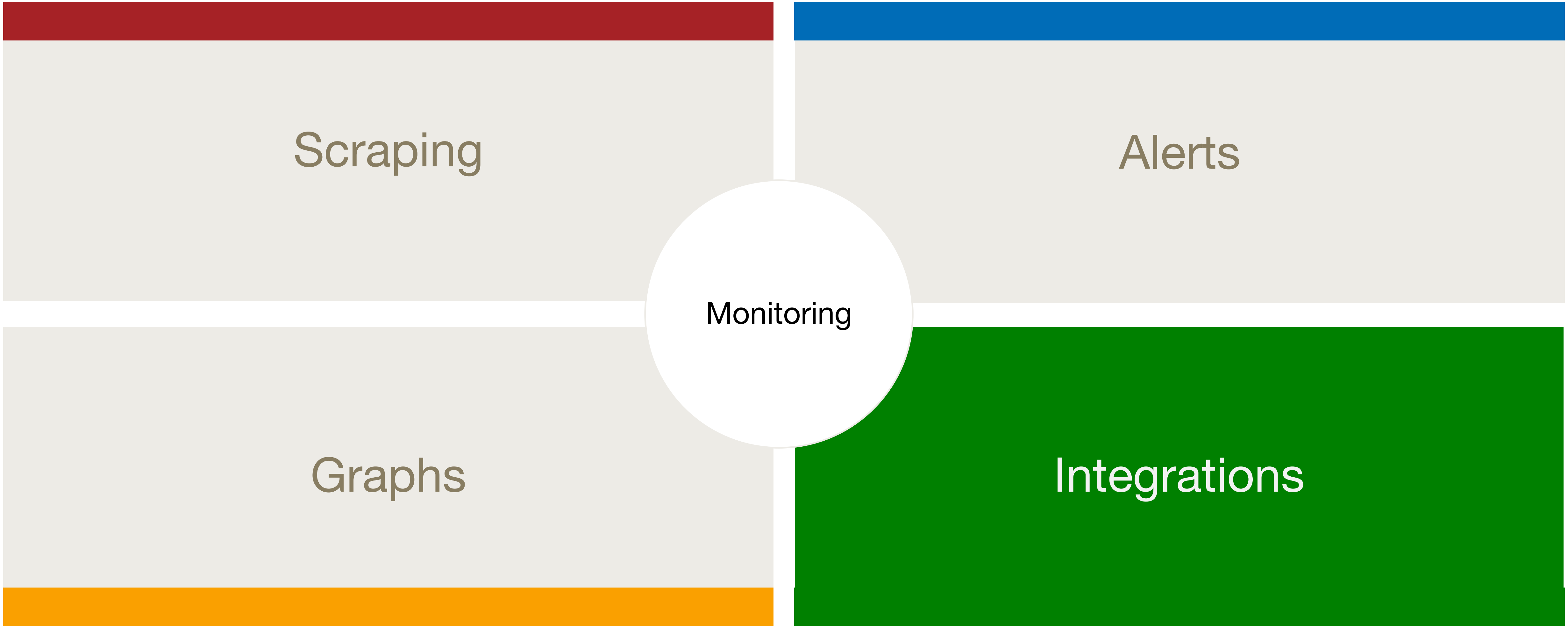
Grafana with basic multi-tenancy


huk-grafana-provisioning.py
John
Apache httpd
• mod_ldap
• mod_auth_kerb
Grafana
Template
owner_john
owner_lisa
owner_*
127.0.0.1:8888/owner="john"/api/v1/query?query=up
prometheus-filter-proxy
127.0.0.1:9090/api/v1/query?query=up{owner="john"}
Prometheus

Grafana with high availability



Overview



Scraping

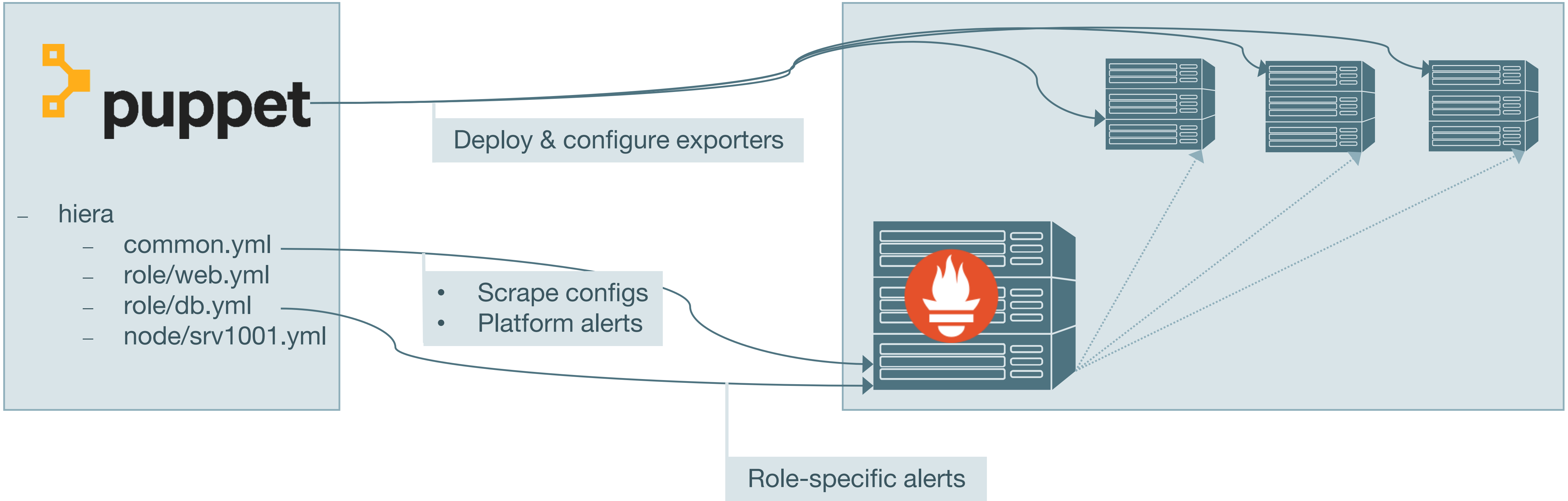
Alerts

Monitoring

Graphs

Integrations

Integrating Prometheus into Configuration Management



puppet

- hiera
  - common.yml
  - role/web.yml
  - role/db.yml
  - node/srv1001.yml

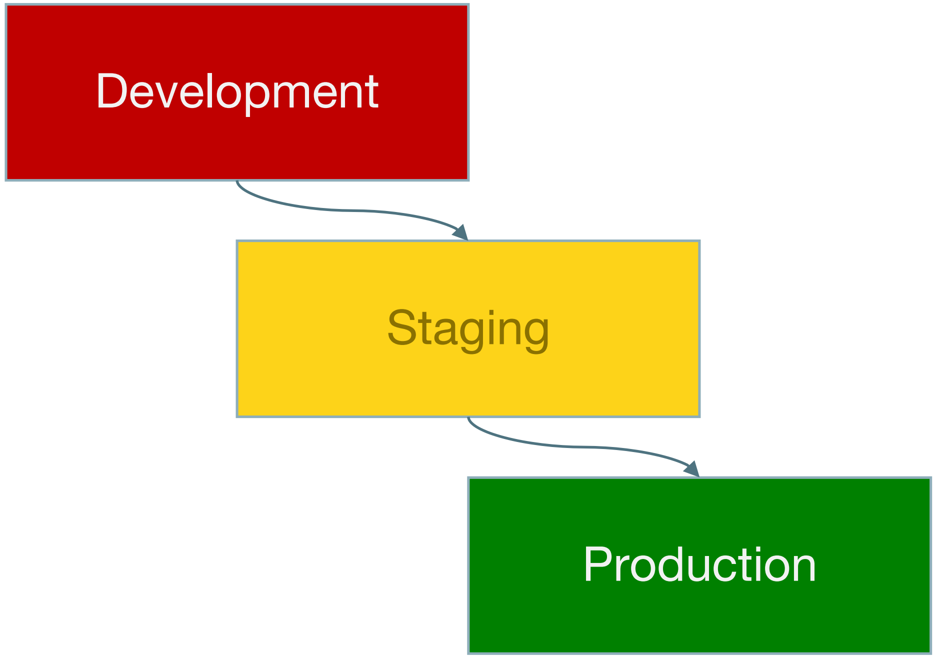
Deploy & configure exporters

- Scrape configs
- Platform alerts

Role-specific alerts

Integrating Patch Management into Prometheus

- Staging of new Linux patches
- Roll-out on application servers



What‘s up next?

- Long Term Storage, Downsampling, „Janitor“
- Dashboard performance
- Lots of additional ideas and areas for work

Benefits & Takeaways

Prometheus and Grafana provide us

- Sufficient **flexibility** in a regulated environment,
- Basic **multi-tenancy** for our teams, and
- Helpful **integrations** into other processes.

Thanks! Any questions?

Christian Hoffmann

Linux System Engineer at HUK-COBURG

christian.hoffmann2@huk-coburg.de

http://github.com/hoffie/sshified

http://github.com/hoffie/prometheus-filter-proxy

http://github.com/hoffie/multilog_exporter