Monitoring and Alerting with Prometheus

Phil Fenstermacher
pcfens@wm.edu

WILLIAM & MARY
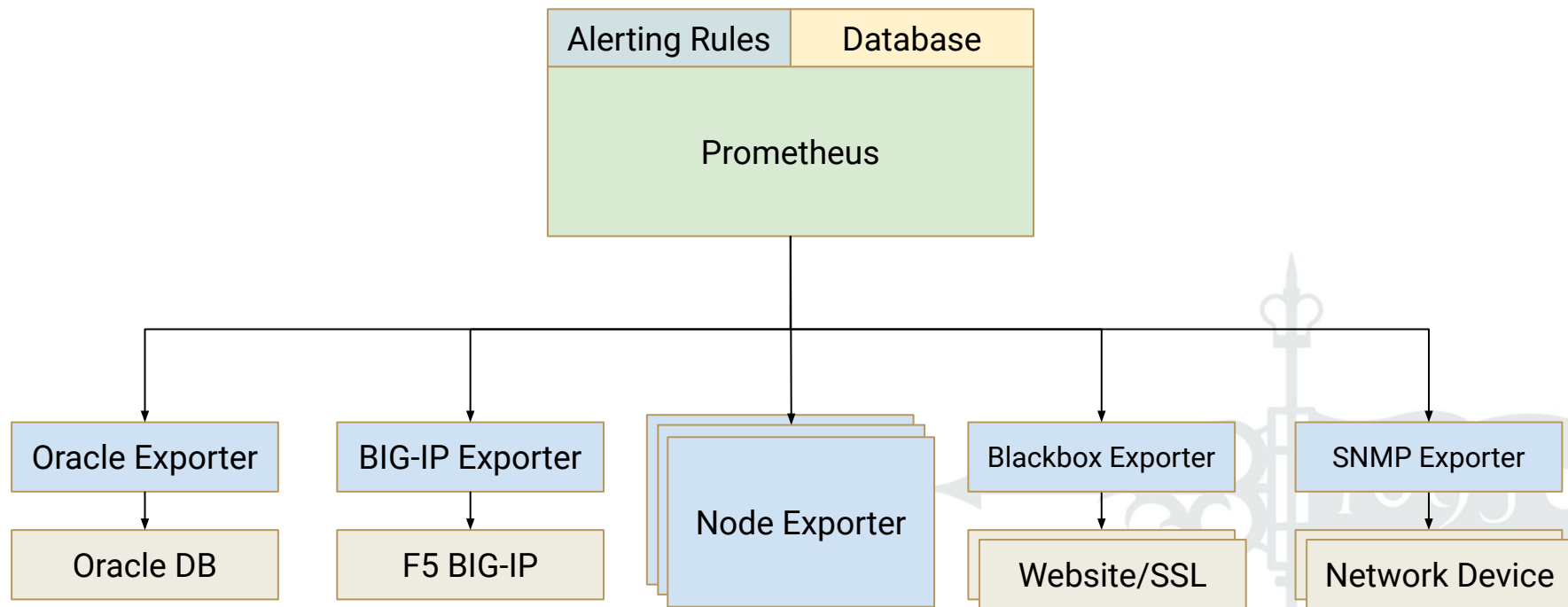
CHARTERED 1693

Monitoring vs. Alerting

- Monitoring is collecting data
- Alerts are what create work

Prometheus

- Discovery
- Metrics Collection
- Time Series Database
- Alerting Engine
- Alert Manager

Alerting Rules | Database

Prometheus

Oracle Exporter

BIG-IP Exporter

Node Exporter

Blackbox Exporter

SNMP Exporter

Oracle DB

F5 BIG-IP

Website/SSL

Network Device

Finding Things

- Traditional Discovery
  - Configuration Files
- API Based
 - Consul
  - Cloud Discovery
  - Kubernetes

Exporters

- Official and community exporters
- Unofficial list maintained on GitHub
- Some software natively exposes metrics

Collecting Metrics

- Exposed by exporters
- Scraped over HTTP
- Metrics have labels
- Everything is a number
- Collected often

```
node_up 1
node_filesystem_avail_bytes{device="/dev/sda2",fstype="ext4",mountpoint="/boot"} 1.42868e+08
node_filesystem_avail_bytes{device="/dev/sda3",fstype="btrfs",mountpoint="/"} 2.40339107e+10
node_sockstat_TCP_inuse 89
```
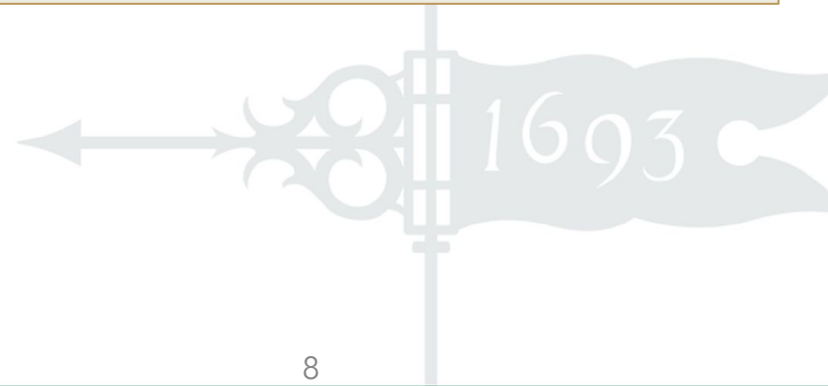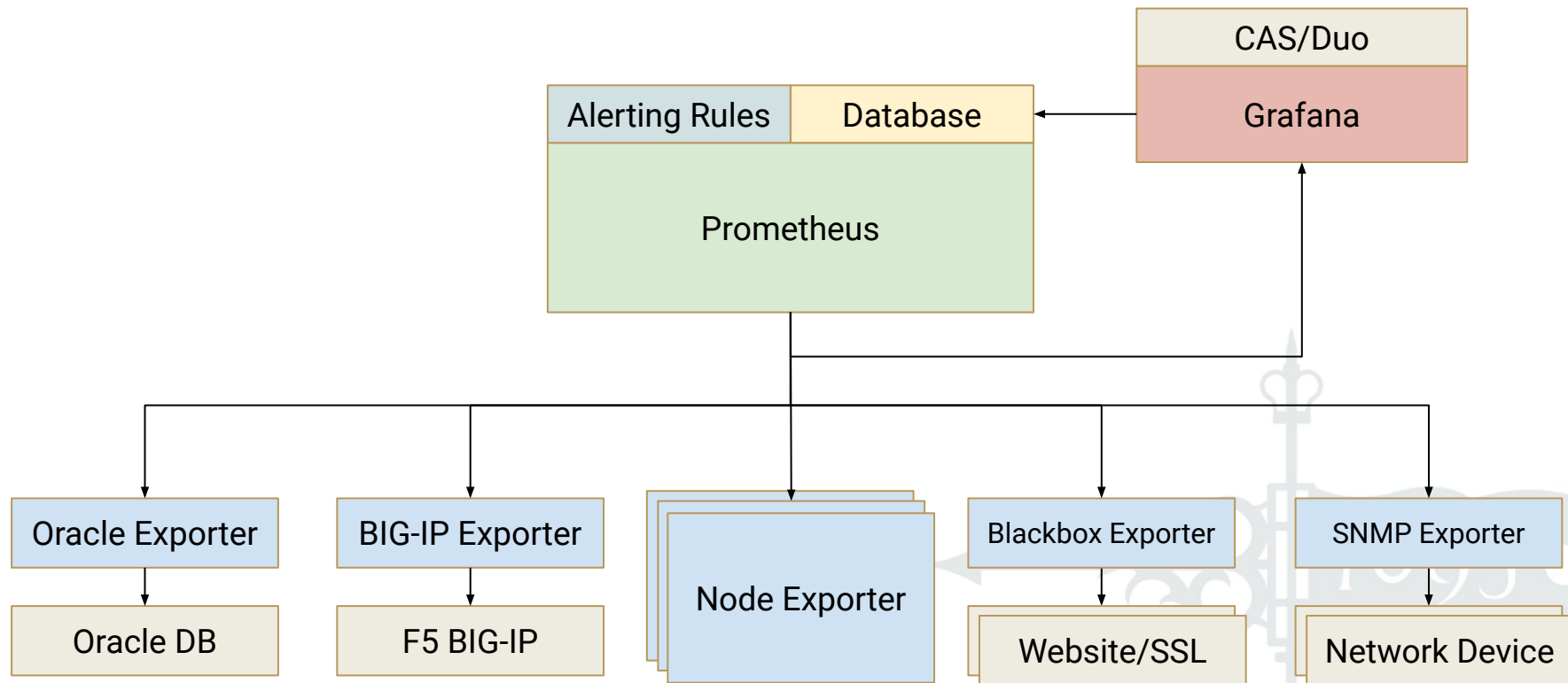
Viewing Metrics

- Quickstart with community dashboards
- Drill in to find interesting trends
- Functions expose hard to see data
  - Predict future state (linearly)
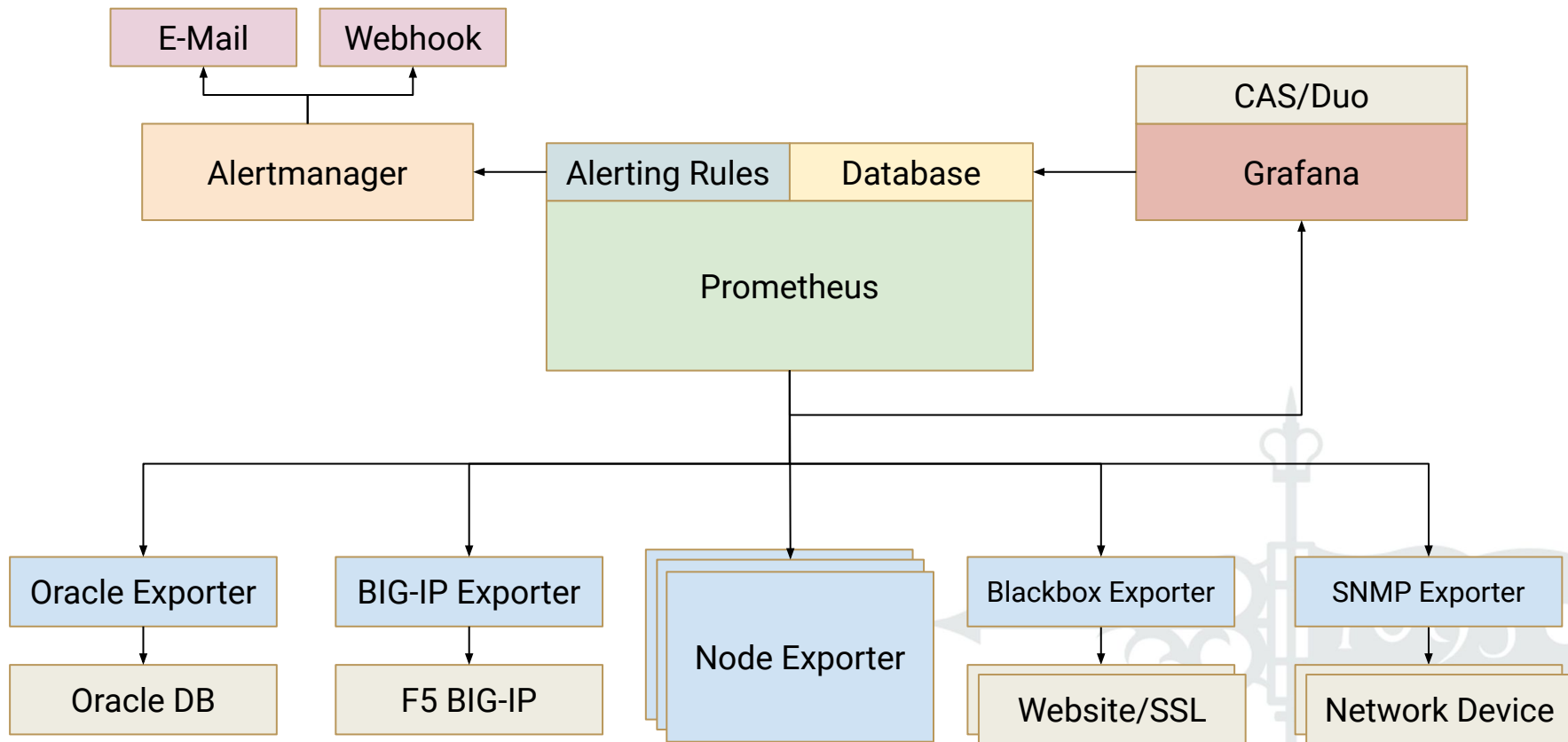
Alerting

- Alerts are just queries
- Alertmanager de-duplicates things and handles routing

```
alert: FilesystemToFillIn12Hours
expr:
predict_linear(node_filesystem_free_bytes{mountpoint!="/import",mountpoint!="/opt/scratch"}[
8h],
  12 * 3600) < 0
for: 5m
labels:
  filesystem: '{{ $labels.mountpoint }}'
  resource: storage
  severity: warning
```

Managing Configuration

- Configuration and Alerts kept in git
- Tested on push
  - If tests pass, put in to production

Resource Planning

- 250k+ metrics every 30s
- Retained locally for 45 days
- Roughly 65GB

But Why?

- Nagios
- Works in a modern way
- Need more than warnings and errors
- Incredibly Simple
- Large Community

Pain Points

- New query language
- Adjusting to data overload
- Rewriting alerts?

What Else?

- Additional tools for long term retention
- Federating Prometheis
- Incredibly easy to run in containers

Questions?

github.com/pcfens/vascan2019

pcfens@{wm.edu,Twitter,etc.}

WILLIAM & MARY

INFORMATION TECHNOLOGY