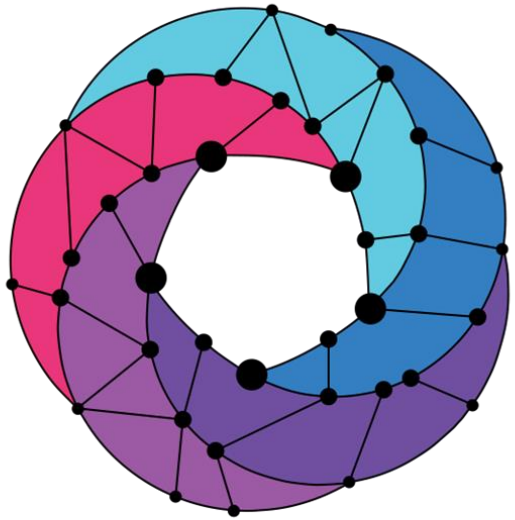


Open Source
MANO

OSM-MR#9 Hackfest

OSM in Production

Alex Chalkias, Eduardo Sousa, Mark Beierl (Canonical)
Fabián Bravo (Whitestack)

ETSI

Session goals

- Clarify the current state of the art
- Understand any new issues from the field
- Discuss further enhancements within the OSM community

Production considerations for OSM

Open Source MANO

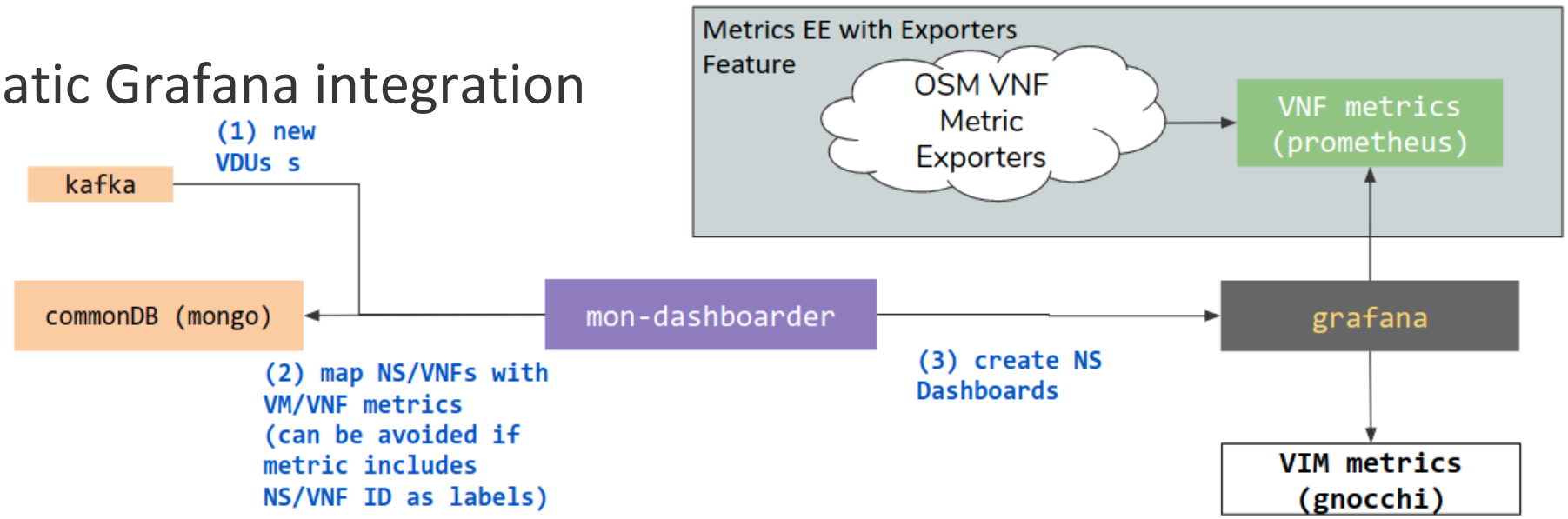
- Availability
  - OSM components - NBI, LCM, RO, VCA, MON, POL
  - HA, geo-redundancy, backups and disaster recovery
- Integrations - authentication, monitoring, ext. systems
- Deployment - K8s substrates, proxy/air-gap
- Operations
  - Capacity - sizing, planning, scaling
  - Upgrades and patches
- Security - ETSI NFV-SEC, CIS, NCSC, NIST
  - Secret storage

NBI, LCM, RO, POL

- Stateless services on Kubernetes - except for RO
- High availability is supported
- Data stores are Mongo and MySQL with standard HA
- Shared files provided by Mongo

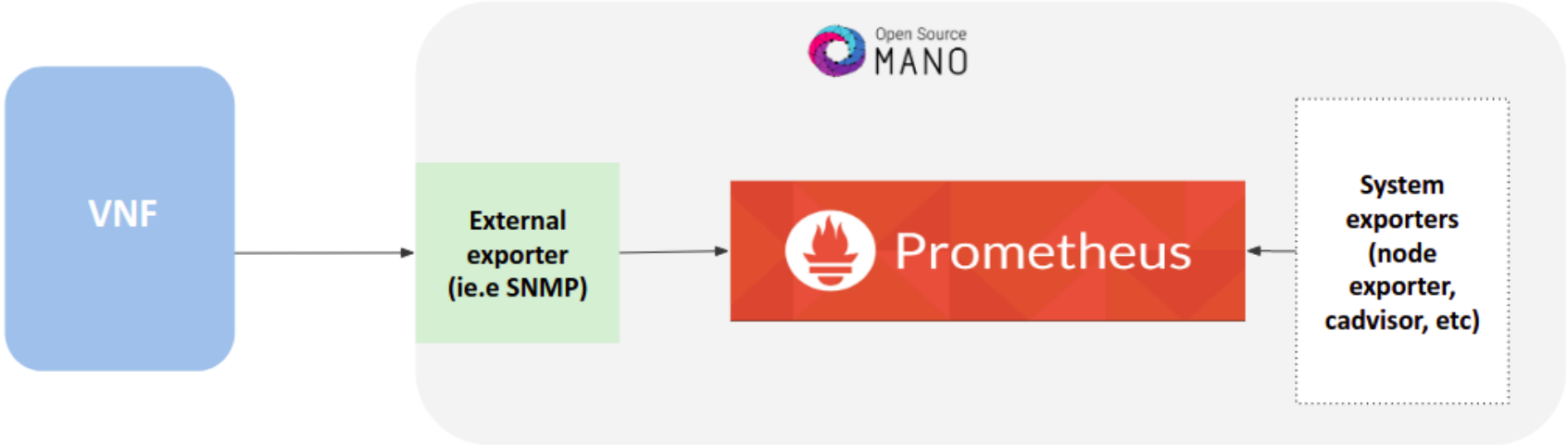
MON

- Currently not scalable, so collection is migrating to a new architecture, where VIM metrics are not re-collected by OSM
- High availability supported
- Uses MongoDB to store alarms
- Next step: automatic Grafana integration



MON

- No framework for complex VNF monitoring
  - New - SNMP support through Prometheus exporters
  - Add exporters for each VIM/VNF use case, separate type for every VIM
  - Use MongoDB streams reacting to changes instead of busy-waiting strategy



VCA

- Juju controller
  - High availability with 3 clustered Juju instances
  - Handles thousands of charms on modest capacity (32GB RAM, 4 cores)
  - Automatic failover handling
- LXD
  - High availability with 3 clustered LXD nodes
  - Juju already handles failover automatically
- Proxy Charms
  - Control of scaling to 2+ units
  - Initial guidelines for HA Charms [1][2] - Proxy charms should be stateless
  - Future improvement: HA Kubernetes proxy charms

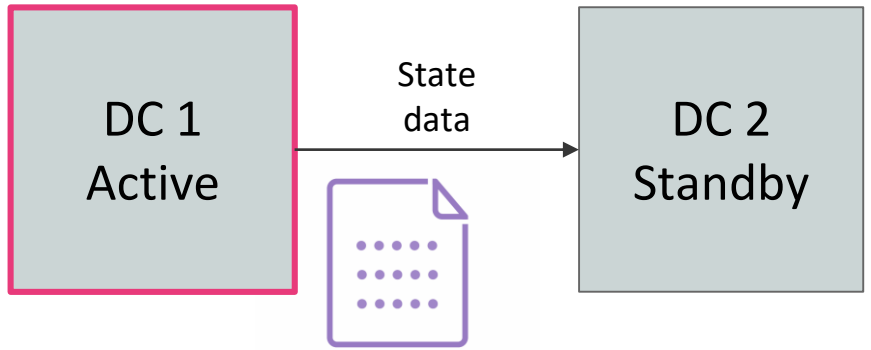
Backup

- Databases - well and widely understood
  - Mongodb
  - MySQL
  - Prometheus internal db
- VCA
  - Juju controller has built-in backup/restore capability
  - Proxy charm containers snapshot via LXD or underlying filesystem
  - Could standardise backup primitives, e.g

```
juju run-action magma-o/leader osm-backup
```

Geo-redundancy and disaster recovery

- Active/Standby strategy
- Active stack is running normally
- OSM state data stored in persistent block device
- Storage replication across sites
- Transition from standby to active made by the operations team



Integration

- Authentication
- External systems through NBI
  - RBAC policy definition
  - Compliance with SOL005 for OSS/BSS integration
  - Subscription and notification for NS lifecycle events
- MON & LMA:
  - OSM cluster + substrate monitoring
  - VNF workloads
- Export events to external systems (SNMP, Syslog, Prometheus, Graylog, Elastic, etc)

Deployment

- Openstack cloud
  - Load balancing
  - Block storage backend
  - Pre-created K8s and VNF flavors
- Bare metal machines
  - Machine provisioning (e.g. MAAS)
  - Load balancing (e.g. MetalLB, F5)
- Networking
  - Access to external systems (e.g. LDAP, OSS/BSS, Monitoring)
- Proxied & air-gapped environments

Operations

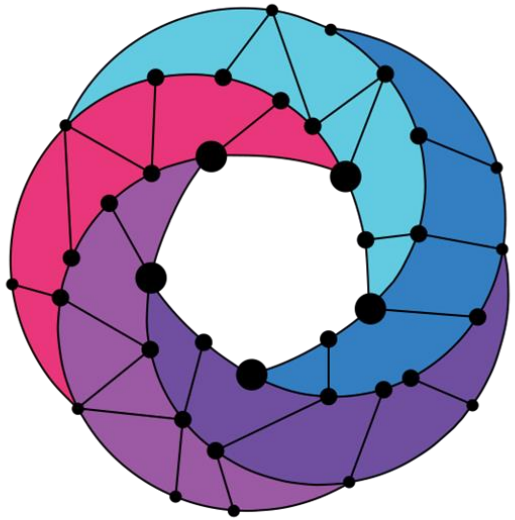
- Capacity planning
  - Sizing
  - Scaling
- Resource monitoring
  - LXD
  - K8s cluster
  - OSM components including MySQL, MongoDB, Kafka, etc.
- Cluster scale-out
  - Is my capacity planning correct? How to address alerts?
- Upgrades and patching
  - Any issue that needs urgent fixing? How to enable new feature <foo>?

Security

- FIPS / CIS hardening for the substrate
- Monitoring of dependencies for vulnerabilities
- CVE patching of upstream OSM container images
- ETSI NFV-SEC? NCSC? NIST? Which are important?
- Kubernetes security
  - Authorization Mode: AlwaysAllow or stricter, e.g. RBAC?
  - Resource quota per pod
  - Security contexts

Secrets storage

- Different secrets in use:
  - Database/message queue/external systems credentials
  - SSL certificates
  - Encryption keys
- Currently OSM does not have a coherent approach for secret storage:
  - Some stored in mongodb, others shared in docker environments
- New mechanism for certs/private keys
  - Vault



Open Source MANO

Find us at:

osm.etsi.org
osm.etsi.org/wikipub