



Transition timeline from VOMS-Admin to IAM

Ops Coordination meeting, March 7, 2024

Maarten Litmaath

v1.0

Introduction

- Since almost 20 years, the experiments have relied on **VOMS-Admin** services for managing VO memberships, groups and roles
- Support of VOMS-Admin ends with the CentOS 7 EOL: **June 30**
- The replacement service is already being used by each experiment: (INDIGO-) **IAM**
 - Regularly importing users, groups and roles from VOMS-Admin
 - Providing a 3rd VOMS service for each experiment, to create proxies
 - The only *critical* use of those services today is in the provisioning of *tokens* for submitting pilot jobs to CEs
 - Such tokens are given lifetimes of a few days to mitigate service downtimes etc.
- We now are looking into when to **stop** depending on VOMS-Admin
 - Not too soon yet, because of concerns about the IAM service level today
 - Some weeks before June 30, to allow us to gain experience with the new situation and still have a temporary fall-back option, should it be needed

A second migration

- The IAM instances for the LHC experiments currently are hosted on the CERN *OpenShift* service for containers
 - That looked a reasonable decision a few years ago
- In the end, however, we want to have all IAM instances on the *Kubernetes* service instead, to profit from improvements in:
 - Logging
 - Monitoring
 - Load-balancing
 - GitOps
- Unfortunately, we **cannot** keep the same hostnames for the IAM instances
- We will thus have to run a campaign for sites to **add** those new names to the configurations of their services
 - VOMS LSC files
 - Token issuers

Draft timeline (1/3)

- Week of March 11
 - Launch campaign for sites to support the future IAM services on K8s
- March
 - Investigate HA options for the short vs. medium term
 - VO management **training** information!
- March-April
 - Get the most urgent issues fixed in the IAM code and configurations
 - Also taking into account lessons learned from DC24, though we do **not** need to be ready for using tokens *at scale* in the next months!

Draft timeline (2/3)

- April
 - Create IAM instances on K8s and start testing them
 - Ad-hoc and/or SAM tests
- April 29
 - Remove legacy VOMS servers from “vomses” files
 - Each experiment will come to rely on its IAM VOMS endpoint on OpenShift
- May 6
 - VOMS-Admin switched off for the first VO
 - No such service is deleted yet
- June 3
 - VOMS-Admin switched off for the last VO
- June 30
 - VOMS-Admin EOL

Draft timeline (3/3)

- Still to be decided in the coming months, per experiment:
 - When to start **using** the IAM instances on K8s in production
 - When to consider switching **off** the OpenShift instances
- Hopefully the experiments can use their OpenShift and K8s instances concurrently!
 - Helps with our HA options
 - The DB is shared between them
- Discussion...