Forschungszentrum Karlsruhe
in der Helmholtz-Gemeinschaft

On VO Box SLAs

Forschungszentrum Karlsruhe
Institute for Scientific Computing

Holger Marten

The GridKa VO box SLA ("SLA" in the following)

- is *one* generic SLA for all VOs

  based on two additional documents
  - the generic *"LCG VO Box Recommendations and Questionnaire" (S.Traylen)* ***[1]***
  - the generic *"VO Box Security Recommendations and Questionnaire" (D.Groep)* ***[2]***
- can thus be re-used for other, non-LHC VOs as well
- contains not only a description of service levels
- but also a detailed workflow
  - e.g.: due to the split responsibilities, two persons, one from the site ***and*** another from the VO must work together to setup the services after a hardware failure. How do these people come together?
- i.e., there are responsibilities for both, the site *and* the VO
- has been sent to the GridKa TAB for comments

Karlsruhe Institute of Technology

Observation: Rather complicated workflow and several obscurities in the whole context.

(Too?) many people involved

Site admins

- role and function is clear

[1] appoints a *“VO maintainer”*

- his / her function in [1] is vague: *“By submitting this questionnaire or by using… any VO box service, the VO maintainer agree that their personal information will be shared among all sites …”*
- e.g. ATLAS interprets: *“The VO box is maintained by ATLAS site contacts and ATLAS operations team. The questionnaire has been answered by: …”*

We (currently) *defined* and *require* that:

- the VO maintainer is *exactly one* named VO (contact) person who
- summarizes and writes down the VO box requirements in [1]
- is owner of and responsible for any activities on the local account <vo>sgm
  Anonymous (sgm-) accounts are prohibited at FZK.

***CMS (Germany) suggests:* use *VO manager* instead of *VO maintainer* for this.**

Karlsruhe Institute of Technology

(Too?) many people involved

[2] additionally appoints a *“VO security responsible”*

- their functions are better defined in [2]: “*… both (the VO maintainer and the sec. responsible) take responsibility for all services running on the VO box under the VO’s systems credentials, and for all actions, events and incidents resulting directly or indirectly running on the VO box under the VO’s user and group system identity*”

What is the difference in responsibility between both people?

Do VOs expect to be informed about security incidents through their security responsible? – that’s not in line with EGEE procedures.

VO security responsible could / should register to sec. response team. – but this likely doesn’t scale for dozens of VOs.

We (currently) *defined* that:

- the VO maintainer is *exactly one* named VO (contact) person… (see previous slide)
- security incidents will be handled according to EGEE incident handling procedures by our local Site Security Officer

According to these procedures, the Grid Security Officer decides about confidentiality of security incidents (together with the incident handl. response team)

(Too?) many people involved

[1] defines a *"VO service intervention contact"*

- depending on the VO, this is a person, group of persons or several groups of persons to be informed in case of service interventions

Why this? – we'd have to implement several workflow additionally to EGEE broadcast ("scheduled / unscheduled downtime")

Suggestion: can't these people or groups simply register for receiving broadcasts?

However, we accepted this workflow for the time being.

Karlsruhe Institute of Technology

(Too?) many people involved

[2] mentions *“VO administrators”*

- and defines their access
- but no VO specified this person or group of persons

Acc. To our current understanding we split this into *“A. VO software managers”* and *“B. VO admins”*, but this might be GridKa specific.

Karlsruhe Institute of Technology

(Too?) many people involved

“A. VO software managers”

- sometimes also referred to as “sgms” = “software grid managers”
- are responsible for installing VO specific software and services on the VO box through remote grid procedures *in user space (!)*
- are (currently) all mapped to one local account <vo>sgm (which - according to our local policies – *must* be owned by a single person (currently the VO maintainer; see previous slides)

Depending on the VO, these are currently 7-30 people that can modify whatever they find on account <vo>sgm.

- **Is this what the experiments want and what the VO maintainer signs to be responsible for?**
- **For sites, their availability and communication paths this is horrible – if allowed at all.**

Karlsruhe Institute of Technology

We accepted this for the time being, but it urgently calls for single accounts and clear responsibilities through groups & roles.

(Too?) many people involved

“B. VO admins”

- are people working either locally or through remote access to help debugging experiment specific problems in close collaboration with site admins
- these people are defined by the GridKa TAB
- they must be personally known to GridKa admins at all time

Let’s hope that they always know and understand what the VO software managers are doing…

Karlsruhe Institute of Technology

An example work flow

If a site detects a hardware failure of a VO box…

A site operator must

- announce an unscheduled downtime through EGEE broadcast
- inform the **VO service intervention contact**
- appoint a **site admin** for the reparation process

The VO service intervention contact (remember it's a group of people!) must

- appoint a **VO software admin** to the above appointed site admin

The site admin(s) must **(could be more than one – for hardware, OS, mw, backup,…)**

- install new hardware and recover the OS
- send a "go ahead" to the VO software admin

The VO software admin must

- recover the VO services
- test and iterate with the site admin
- agree with the site admin about readiness of the new system

A site operator must

- announce the end of the unscheduled downtime through EGEE broadcast
- inform the VO service intervention contact about the success

Summary I

Procedures for operating VO boxes are extremely complicated and communication intensive due to

- split responsibilities between sites and VOs
- many (groups of) people involved
- complicated, error prone workflow
- writing of sophisticated SLAs ;-)
- …

… and the problem multiplies with the number of VOs and different software solutions and organisations thereof.

See reminder on the next slide !

Karlsruhe Institute of Technology

Summary II

The WLCG OB concluded in its meeting on March 20, 2006:

The OB endorses the GDB proposals regarding VO boxes as follows:

- ***The experiments must not enhance their usage of VO-specific services until the VO box working group has drawn its conclusions.***
- ***After the final report of this group, decisions will have to be made and a timetable established for the implementation of these services in the general middleware.***
- ***Until that is done, the Tier-1 centres are requested to allow the deployment of VO-specific services so that the experiments can fully participate in SC4.***
- ***It is left for the individual Tier-2 centres to decide if they can provide these services or not.***
- ***Ultimately the OB wishes to see all deployments of VO-specific services replaced by generic middleware.***

The overall message is that the OB strongly supports the line of doing things in common and does not support the line of experiment-specific implementations.

… and the VO box working group identified class 1 and class 2 services ...

Can we get an overview of where we are with this?