Quelques pistes pour le déploiement effectif de l'accréditation différenciée à l'aide de VOMS.

David Weissenbach

Institut Pierre-Simon Laplace, CNRS, Paris

22 mars 2007 — CC–IN2P3

Quelques scénarios

Scénarios véritables pour la VO ESR:

- Les utilisateurs du soft MIMOSA ont accès à des données confidentielles qui doivent être stockées sur SE.
- Il serait appréciable que le programme de détermination des CMT de gros tremblements de terre puisse avoir accès à des queues prioritaires et/ou à des CPU habituellement non accessibles aux autres utilisateurs de la VO.
- Certains des utilisateurs de SpecFEM3D peuvent avoir accès à des plugins ou au code source, avec des mainteneurs.

Hypothétiques ou pour d'autres VOs:

- EGEODE prévoit d'avoir des utilisateurs gratuits et des utilisateurs payants.
- L'IPSL bouffe tout mon espace disque si je ne leur colle pas un quota serré.
- Je voudrais que les utilisateurs de /dteam/france en qui j'ai confiance puissent tuer des processus qui traîneraient sur mes WNs.

Beaucoup de flou

Plusieurs mois après le passage a gLite (et donc normalement à VOMS), de nombreux soucis restent d'actualité :

- la diffusion des certificats des serveurs voms;
- beaucoup de sites utilisent encore le grid–mapfile comme mécanisme d'autorisation;
- le peu d'empressement des utilisateurs –mal formés– à initier des proxys VOMS complets;
- les formations d'utilisateurs prévoient rarement des TP étendus sur VOMS : leur mise en place nécessite encore d'avantage de temps et de préparations;
- intégration dans un certain nombre de services : myproxy, LFC, ...

Mais surtout, NA1, NA4, les VOs, JRA1, SA1, chaque site, ..., tous ont des attentes où des conceptions différentes des services rendus par VOMS.

Et on va encore sous peu enrichir ces proxys VOMS de "General Attributes" ...

Service minimum

La configuration par défaut de gLite ne prévoit que 3 cas particuliers au sein de chaque VO : le **software manager**, le **production manager**, le **VO admin**.
Les VOs en traduisent le plus souvent certains en Rôles VOMS (en groupes pour lhcb). Mais elles définissent également de temps en temps leurs propres rôles (ex : opérator pour dteam) ou groupes.

Quant aux groupes internes aux VOs, rien n'est imposé mais rien n'est proposé non plus. La série de variables yaim `VO_XXX_VOMS_EXTRA_MAPS` a fait long feu, remplacée par le fichier `groups.conf` qui permet plus de détails et qui constitue la base pour yaim de la configuration de LCMAPS.

La configuration des mappings par LCMAPS est contenue dans `$EDG_HOME/etc/lcmaps/gridmapfile` et `$EDG_HOME/etc/lcmaps/groupmapfile`.

le proxy VOMS

```
[weissenb@amundsen Simple]$ voms-proxy-init --voms dteam
Your identity: /O=GRID-FR/C=FR/O=CNRS/OU=IPSL/CN=David Weissenbach Dteam
Enter GRID pass phrase:
Creating temporary proxy ............................ Done
Contacting  lcg-voms.cern.ch:15004 [/C=CH/O=CERN/OU=GRID/CN=host/lcg-voms.cern.ch] "dteam" Done
Creating proxy ..................................................... Done
Your proxy is valid until Thu Mar 15 02:47:24 2007


[weissenb@amundsen Simple]$ voms-proxy-info --all
subject   : /O=GRID-FR/C=FR/O=CNRS/OU=IPSL/CN=David Weissenbach Dteam/CN=proxy
issuer    : /O=GRID-FR/C=FR/O=CNRS/OU=IPSL/CN=David Weissenbach Dteam
identity  : /O=GRID-FR/C=FR/O=CNRS/OU=IPSL/CN=David Weissenbach Dteam
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u501
timeleft  : 11:59:55
VO        : dteam
subject   : /O=GRID-FR/C=FR/O=CNRS/OU=IPSL/CN=David Weissenbach Dteam
issuer    : /C=CH/O=CERN/OU=GRID/CN=host/lcg-voms.cern.ch
attribute : /dteam/Role=NULL/Capability=NULL
attribute : /dteam/ce/Role=NULL/Capability=NULL
attribute : /dteam/france/Role=NULL/Capability=NULL
attribute : /dteam/france/IPSL-IPGP-LCG2/Role=NULL/Capability=NULL
timeleft  : 11:59:56
```

Comment vérifier sous quelle identité on échoue :

- CE : `globus-job-run $CE /usr/bin/id`
- SE Classic : `globus-url-copy file:$fic gsiftp://$SE/path/to/VO/fic` ; `edg-gridftp-ls -v gsiftp://$SE/path/to/VO` (**donne des UIDs/GIDs**).

Deux tentatives

Comment vais-je être vu si je teste mon appartenance au groupe /dteam/ce par rapport à l'ensemble de la VO dteam ?

	lcg–CE	glite–CE	Classic SE	DPM
/dteam	dteam032:dteam	dteam032:dteam	dteam055:dteam	?:dteam
/dteam/ce	dteam032:dteam	GRAM error 7	dteam055:dteam	perm. denied

La situation apparaissant en rouge est bien sur particulièrement dangereuse si je pensais mettre mes fichiers à l'abri...

Et pour ESR au RC IPSL-IPGP ?

	lcg–CE	Classic SE
/esr	esr007:esr	esr014:esr
/esr/specfem SE	esrfem01:esrfem	esrfem01:esrfem

Les petits plus

Qu'a-t-il fallu en plus ? Une configuration adéquate de lcmaps et bien sur des comptes et groupes pour différencier ces utilisateurs :

- un groupe : esrfem
- un pool d'utilisateurs : esrfem01, esrfem02, ...
- et un mapping adéquat :
  groupmapfile:
  "/VO=esr/GROUP=/esr/specfem/Role=NULL/Capability=NULL" esrfem
  "/VO=esr/GROUP=/esr/specfem" esrfem
  gridmapfile:
  "/VO=esr/GROUP=/esr/specfem/Role=NULL/Capability=NULL" .esrfem
  "/VO=esr/GROUP=/esr/specfem" .esrfem
- Sur le Classic SE : un répertoire avec les propriétés et permissions adéquates.

NB :

- Les noms des groupes et utilisateurs doivent être formés en ajoutant un suffixe au nom du sur-groupe.
- L'ordre des lignes dans la configuration de lcmaps n'est pas significative.

De plous en plous diffichile

Si l'implémentation des groupes VOMS semble assez évidente et que le consensus dessus se fait naturellement, il n'en va pas de même pour celle des rôles.

- Doit on les "mapper" vers des pools, des comptes individuels ? Au fond, comment peut on interpréter cette notion de rôle ?
- La définition des groupes s'effectue au niveau de la VO entière, mais leur constitution peut se différencier en fonction des sous–groupes.

Quant aux capacités, il y a unanimité pour ne pas les utiliser dans un premier temps.

Reprenons de la hauteur

Au final, la gestion des mappings est une affaire délicate.

- Sous quelle forme les VOs doivent elles indiquer leur choix ? Et à qui ? Peuvent–elles tabler sur 1 ss–gpe VOMS $\Longrightarrow$ 1 mapping ?
- Les sites sont ils tenus d'appliquer ces mappings ou peuvent–ils opérer leur propre sélection ?
- Il faudrait incorporer à SAM et FCR des tests exhaustifs de validité des groupes/rôles. Il faudrait donc un certificat test dédié pour chaque VO.
- Peu de (aucune?) règles de bonnes conduite ont été édictées.
  - Les VOs ne doivent pas continuellement changer leur organisation.
  - ...

Dernière difficulté : pensez à sauver vos configs LCMAPS avant de lancer `configure_node`.[1]

[1] ticket GGUS à suivre...

Mais...

Observons le cas particulier de D Weissenbach dans ESR. Il est membre d'à peu près tous les groupes de la VO. Il a crée sur ses SE et CE des groupes et comptes pour traduire ces groupes VOMS.

```
[esrsgm@amundsen esrsgm]$ voms-proxy-init --voms esr:/esr
Your identity: /O=GRID-FR/C= [ ... ]
.............. Done
Your proxy is valid until Thu Mar 15 05:46:22 2007

[esrsgm@amundsen esrsgm]$ globus-job-run hudson.datagrid.jussieu.fr \
 /usr/bin/id  -Gn
esr esreowf esreo esrfem
```

Aïe, il appartient à tous ces groupes!! En effet son proxy contient tous les attributs auxquels il peut prétendre, seul leur ordre et donc le groupe de base de la "session" diffère.

... il y a un "mais"

D. Weissenbach peut donc *à son insu?* saboter les affaires de /esr/eobs avec un proxy quelconque.

```
[root@barentz root]# ls -l /storage/esr
total 20
drwxrwx---    2 root     esreowf      4096 Feb 14 17:51 ecmwf
drwxrwx---    3 root     esreo        4096 Feb  9 11:00 eobs
drwxrwx---  211 esr001   esr          8192 Mar 13 10:52 generated
drwxrwx---    2 esrprd   esgoce       4096 Jan 12  2006 goce

[esrsgm@amundsen esrsgm]$ globus-url-copy file:$PWD/glite_wms.conf \
gsiftp://barentz.datagrid.jussieu.fr/storage/esr/eobs/arg

[root@barentz root]# ls -l /storage/esr/eobs
total 4
-rw-rw-r--    1 esr014   esr           322 Mar 14 18:08 arg
```

NB : Sur un worker node, on est membre d'un unique groupe, mais on peut se servir du proxy tout pareil!!

Cohérent ? Oui. Consistant ?

Au total cette multi appartenance n'est en fait qu'un raccourci un peu rapide :

```
[moguilny@amundsen ~]$ grid-proxy-init
Your identity: /O=GRID-FR/C=FR/O=CNRS/OU=IPGP/CN=Genevieve Moguilny
Enter GRID pass phrase for this identity:
Creating proxy ............................... Done
Your proxy is valid until: Fri Mar 16 02:39:27 2007
[moguilny@amundsen ~]$ globus-job-run hudson.datagrid.jussieu.fr /usr/bin/id
uid=4012(esr012) gid=2026(esr)

[moguilny@amundsen ~]$ voms-proxy-init \
 -cert $X509_USER_PROXY -key $X509_USER_PROXY --voms esr:/esr/specfem
Your identity: /O=GRID-FR/C=FR/O=CNRS/OU=IPGP/CN=Genevieve Moguilny/CN=proxy
Creating temporary proxy ..................... Done
Contacting  mu4.matrix.sara.nl:30001 [/O=dutchgrid/O=hosts/OU=sara.nl/CN=mu4.ma
Creating proxy ............................................ Done
Warning: your certificate and proxy will expire Fri Mar 16 02:39:27 2007
which is within the requested lifetime of the proxy
[moguilny@amundsen ~]$ globus-job-run hudson.datagrid.jussieu.fr /usr/bin/id
uid=4101(esrfem01) gid=2024(esrfem) groups=2026(esr)
```

Documents utilisés

- Integration of VOMS + LCAS/LCMAPS : http://grid-it.cnaf.infn.it/fileadmin/sysadm/voms-integration/voms-integration.html/
- Guide to LCMAPS : http://www.dutchgrid.nl/DataGrid/wp4/jr/lcmaps/
- VOMS Guide : https://edms.cern.ch/document/571991
- L'interface web d'administration de votre serveur voms préféré : https://server.domain:8443/voms/vo/webui/admin