EGI central banning setup for NGI_IT sites

The purpose of deploying the central banning over sites is to implement the EGI CSIRT central emergency suspension policy .

In brief, EGI CSIRT can centrally ban suspected or compromised user and robot certificates whenever they can be used to submit jobs.

In case a certificate has undergone suspension procedure NGIs and sites security contact will be promptly informed.

The solution is based on the Argus service able to deal with ban policy for certificate DNs. A three level hierachy for Argus (EGI, NGI and site levels) allows to centrally (EGI level) define banning policy inherited by both NGI and site levels.

To take into account sites without Argus, the central banning setup considers the two scenarios Site with Argus, Site without Argus.

Site with Argus

Enabling site Argus to read NGI Argus policy

In order to download the ban policy from the NGI Argus you have to ask to the NGI granting read access for your Argus's DN. Please submit a ticket to the **Central Support** support unit using the following template

Assign To	Central Support
Subject	Enable Argus server for "YOUR_SITE_NAME"
Description	Please add the following Argus DN: "DN of your Argus server"

Once your Argus is granted with the proper privileges, sites can add the NGI_IT Argus as a remote Policy Administration Point (PAP).

NGI_IT Argus endpoint	argus-it.cnaf.infn.it
NGI_IT Argus DN	/C=IT/O=INFN/OU=Host/L=CNAF/CN=argus-it.cnaf.infn.it

Using pap-admin utility to add NGI_IT PAP to your Argus

Add NGI_IT PAP (aka ngi_it)

```
pap-admin add-pap ngi_it argus-it.cnaf.infn.it
"/C=IT/O=INFN/OU=Host/L=CNAF/CN=argus-it.cnaf.infn.it"
```

Enable new NGI_IT PAP (aka ngi_it)

```
pap-admin enable-pap ngi_it
```

Make the new ngi_it PAP as the default one

```
pap-admin set-paps-order ngi_it default
```

Set polling interval to 10 minutes **(Please carefully consider this operation since could influence your Argus performances)**

```
pap-admin set-polling-interval 600
```

Reload policy and clear cache

```
/etc/init.d/argus-pdp reloadpolicy
/etc/init.d/argus-pepd clearcache
```

Verify new remote policy by using --all option with pap-admin client

```
pap-admin lp --all
```

Preventing yaim overwrites for added PAPs

Yaim is unable to configure and add new PAPs (no yaim variables provided) so running yaim on the Argus server can potentially remove added PAPs. To avoid such situation sites should perform the procedure to add NGI_IT PAP everytime they run yaim on the Argus server. You can script the procedure or use a configuration management tool like Puppet to automate such procedure.

Site without Argus

Site without Argus server can download the ban policy file publicly available here and integrate it with local site policy.

Such file will comprise the list of EGI and/or NGI banned DNs and needs to be stored in the CREAM CE ban file located at `/etc/lcas/ban_users.db` Sites can cron the download from their CEs to have it schedelued in the background.

The following snippet is a proof of concept that ignores local site policy previously defined:

```
cat /etc/cron.d/fetch-banlist

# Fetch ban list from central NGI repository
# and add DNs to ban_users.db file

0  *  *  *  *  root (sleep $(($RANDOM\%40+10))) && http_status=$(curl -sL -w '\%{http_code}' --co
```

Ask for support

For support requests, sites can open a ticket using our local ticketing system .

Please assign ticket to **Central Support** department and subject *Central ban YOUR_SITE_NAME*

This topic: SiteAdminCorner > NGI_ITCentralBanning
Topic revision: r9 - 2014-02-03 - GiuseppeMisurelli