NORDUGRID-MANUAL-15
28/5/2010

User authorization in the ARC middleware

Henrik Thostrup Jensen <htj@ndgf.org>

1 User authorization

Authorization of users is configured in the `arc.conf` configuration file, which is read by nordugridmap in order to generate a list of allowed users in one or more files, typically grid-map files. These grid-map files are then (typically) used for user authorization. This document covers the settings in the `arc.conf` file, and the nordugridmap utility.

1.1 arc.conf

By defining a VO blocks in `arc.conf` it is configured which users will get authorized (by producing grid-map files which are in turn used by services to authorize users). User-authorization is handled in groups, as handling the user lists manually is major hazzle. These groups of users can be fetched from http(s), ldap, files, and from VOMS servers, with the last being the typical.

Following is an example of how to allow the `bio.ndgf.org` VO:

```
[vo]
id="vo_ndgf_biogrid"
vo="ndgf_biogrid"
file="/etc/grid-security/grid-mapfile"
source="vomss://voms.ndgf.org:8443/voms/bio.ndgf.org"
mapped_unixid="grid"
```

This will fetch a list of users from the source url, and create a mapping from the user subject names to the mapped unix (`grid`) in the file `/etc/grid-security/grid-mapfile`.

It is possible to keep a local file of users that should be allowed access (e.g., people at an insitution, which are not in a VO). The following example shows this:

```
[vo]
id="users"
name="users"
file="/etc/grid-security/grid-mapfile"
source="file:///etc/grid-security/local-grid-mapfile"
```

The `local-grid-map` file, should be of the format:

```
‘‘UserSN’’ unixuser
```

Description of the possible entries in a VO block:

id An identifier for the VO block.

vo A name for the VO block.

file File to write the UserSN -¿ unixuser mapping to.

source Where to fetch the user subject list from. It possible to have multiple source entries in a VO block.

mapped_unixid Local unix user to map the subjects to.

require_issuerdn Require an issuerdn the allowed users. Should be set to either “yes” or “no”. Default is “no”. The options is typically left out.

filter Filter in or out certain users. E.g., blacklisting is done with:
`filter="deny /O=Grid/O=NorduGrid/OU=bad.site/CN=Bad User"`
and whitelisting is done with: `filter="allow *lu.se*"`

1.2 Nordugridmap

To generate the grid-map files, nordugridmap can retrieve user lists from both local files and several kinds of remote servers. Which files to generated, and from which sources to read is specified in the `arc.conf` configuration file. For a description of the `arc.conf` settings see, the document *CONFIGURATION AND AUTHORISATION OF ARC (NORDUGRID) SERVICES*

Invocation

To test the generation of the grid-mapf files it is possible to invoke `nordugridmap` with `-t` (for test). This will make the program print out the grid-map files for inspection (files will not be written / created).

It is possible to specify an alternative configuration file by using `-c CONFIG_FILE`.

Finally it is possible to print help and options for the program using the `-h` switch.

User-VO map

From version 0.8.1 ARC a grid-map file mapping the user subject name to a VO source is also generated. The file is stored at: `/etc/grid-security/grid-vo-mapfile`. A line could look like this:

```
"/O=Grid/O=NorduGrid/OU=ndgf.org/CN=Henrik Thostrup Jensen" "vomss://voms.ndgf.org:8443/voms/bio.ndgf.org"
```

If a user happens to be in several VOs, the first entry found is used.

Caching

Once a list of user subjects have been retrieved the lists is saved (cached) in the `/var/spool/nordugrid/gridmapcache` directory. If the `nordugridmap` utility fails to retrieve a user list, the cached entry will be used insted. Currently this mechanism is only enabled on VOMS servers.

Note: This feature is of writing not yet committed, but might appear in ARC 0.8.1, and will all likelyhood in ARC 0.8.2.

cron

To ensure that grid-map files are updated, `nordugridmap` should be executed regularly and automatically. Once a day should be the minimum, but 4-6 times a day is better in order to get user addition more quickly propagated. We recommend you use CRON or similar. To run `nordugridmap` every four hours, use the following crontab entry:

```
0 */4 * * * /opt/nordugrid/libexec/nordugridmap
```

Make sure the change the path, if ARC is installed elsewhere than `/opt/nordugrid`