NORDUGRID-MANUAL-15
3/6/2010

User authorization in the ARC middleware.

Application notes.

Henrik Thostrup Jensen <htj@ndgf.org>, Aleksandr Konstantinov <aleks@fys.uio.no>

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. This configuration file is also read by servers like gridftpd to perform actual authorization. Generated grid-map files may be consequentially used for user authorization as well. This document covers one simplest scenario for setting 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 collected into grid-map files which in turn may be used used by services to authorize users. User-authorization is handled in intermediate entities called groups. These groups of users are defined by matching identity of user to defined rules among them lists fetch-able from http(s), ldap and files. It is also possible to match against VOMS attributes of connecting clients or to use user lists obtained from VOMS servers using nordugridmap utility. Although last option is widely in use one should use it with care because VOMS server may not necessary allow that. Nevertheless text below describes this option.

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 VOMS source url, and assigns every subject name the local unix account (`grid`). All such mapping pairs are stored in the file `/etc/grid-security/grid-mapfile`.

It is possible to also add users that should be allowed access (e.g., people at an institution, which are not in a VO). The following example shows how to do that by creating another `vo` block fetching list of locally allowed subject names from file `/etc/grid-security/local-grid-mapfile` and storing it to same output file.

```
[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. May be referred from other blocks.

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

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

mapped_unixid Local unix user to map the subjects to.

require_issuerdn Requires an issuerdn for the allowed users. Should be set to either "yes" or "no". Default is "no". This option 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 white-listing is done with: `filter="allow *lu.se*"`

For authorization to be applicable to be applicable one must create `group` blocks which are subsequently used in service-specific configuration parts to limit access to provided features. For information how to configure `group` blocks please refer to the document *CONFIGURATION AND AUTHORISATION OF ARC (NORDUGRID) SERVICES*. Service-specific configuration is described in the documents of corresponding services.

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 generate, and from which sources to read is specified in the `arc.conf` configuration file. For full description of the `arc.conf` settings see, the document *CONFIGURATION AND AUTHORISATION OF ARC (NORDUGRID) SERVICES* and previous section.

Invocation

To test the generation of the grid-map files it is possible to invoke `nordugridmap` command with `-t` (for test). This will make the program print out the generated 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 of ARC a grid-map file mapping the user subject name to a source is also generated. The file is stored at: `/etc/grid-security/grid-vo-mapfile`. A content 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 list 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 instead. 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 with all likelihood 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`