gx-map, a system for maintaining grid-mapfiles

Keith Thompson <kst@sdsc.edu>
San Diego Supercomputer Center
January 20, 2004

grid-mapfile overview

- The Globus grid-mapfile is a plain text file mapping DNs (GSI distinguished names) to Unix user names.
- The default location is /etc/grid-security/
- Protecting the grid-mapfile from unauthorized updates is critical.
- Keeping it up to date can be tedious and time-consuming.

gx-map

- gx-map allows users to request grid-mapfile updates without administrative intervention. Updates are typically applied within a few minutes.
- Requests can be automatically propagated to multiple systems.
- The actual updates are performed from cron jobs running under a privileged account.

gx-map

- The system is implemented in about 2700 lines of Perl. It's currently deployed at SDSC and on the TeraGrid clusters.
- gx-map is a work in progress.
- Why the funny name? An earlier version was part of "globus-extras", a set of auxiliary tools for Globus users at SDSC. gx-map is the sole survivor.

The “gx-map” command

- This is the user’s interface to the gx-map system. It can be run with many confusing command-line options or in interactive mode.
- Just type “`gx-map -interactive`” and follow the prompts.
- The result is a plain text request file, written to a world-writable directory.

Sample request file

```
{
        comment             Just testing
        dn                  "/O=Earth/CN=Keith Thompson"
        email               kst@sdsc.edu
        hostname            uffda.sdsc.edu
        map_to_name         kst
        map_to_uid          500
        operation           add
        requested_by_name   kst
        requested_by_uid    500
        timestamp           1071007538 Tue 2003-12-09 22:05:38 UTC
}
```

gx-map and cacl

- Another cron job (not part of the gx-map system) checks for new certificates issued by “cacl” and automatically invokes the gx-map command.
- Thus a user can obtain a certificate and have the DN added to multiple grid-mapfiles, all without administrative intervention.

The “gx-check-requests” command

- The “gx-check-requests” command is run from a cron job under a privileged account (typically “root” or “globus”).
- It checks for new request files generated by gx-map.
- Each new request is validated, annotated, and logged.

Sample annotated request

```
{
        NAMESPACE           UFFDA
        OWNER_NAME          kst
        OWNER_UID           500
        PROCESSED           1071007620 Tue 2003-12-09 22:07:00 UTC
        REQUEST_FILE        1071007538-uffda.sdsc.edu-kst-16532.request
        comment             Just testing
        dn                  "/O=Earth/CN=Keith Thompson"
        email               kst@sdsc.edu
        hostname            uffda.sdsc.edu
        map_to_name         kst
        map_to_uid          500
        operation           add
        requested_by_name   kst
        requested_by_uid    500
        timestamp           1071007538 Tue 2003-12-09 22:05:38 UTC
}
```

The “gx-gen-mapfile” command

- The “gx-gen-mapfile” command is run from a cron job under a privileged account on each host that needs a grid-mapfile.
- If the request log has been updated, it reads it, sorts it by timestamp, and traverses it, generating a new grid-mapfile from scratch.
- Multiple request logs can be read via http or ftp.

Sample cron jobs

```
#
# Every 5 minutes, check for new requests
#
4,9,14,19,24,29,34,39,44,49,54,59 * * * * \
   /usr/local/apps/gx-map/sbin/gx-check-requests -namespace SDSC

#
# Every 5 minutes, update the grid-mapfile (if needed)
#
0,5,10,15,20,25,30,35,40,45,50,55 * * * * \
   /usr/local/apps/gx-map/sbin/gx-gen-mapfile \
        -req default \
        -req ftp://ftp.sdsc.edu/pub/sdsc/globus/software/gx-
   map/sdsc-data/requests.log \
        /users/globus/gx/grid-mapfile
# (/etc/grid-security/grid-mapfile is a symlink to
# /users/globus/gx/grid-mapfile)
```

Installation

- Unpack the tarball
- Run “./configure-gx-map foo.conf”
- Run “make install”
- Sample config file:

```
PERL            /usr/bin/perl
PATH            /bin:/usr/bin
NAMESPACE       SAMPLE
INSTALL_DIR     /usr/local/apps/gx-map-0.4beta
DATA_DIR        /var/gx-map-0.4beta
GLOBUS_ADMINS   globus
ADMIN_EMAIL     globus@sdsc.edu      # not currently used
```

Namespaces

- A gx-map “namespace” is a consistent mapping of Unix user names and numeric UIDs to people.
- There are hooks to allow mappings across different namespaces.
- The “John Smith” problem: How do I know whether “jsmith@site1” and “jsmith@site2” are the same person?
- gx-map supports a user map file specifying this relationship. Ideally this should be generated from a definitive user database. Work on this is in progress.

Security

- The worst-case scenario: Allowing you to map your DN to my Unix account.
- The gx-map command itself is unprivileged; anyone can easily create a fake request file.
- The gx-check-requests command validates the ownership of the request file. If the OS allows non-root users to use chown (as HP-UX does by default), this can break.
- Be careful out there.

Availability

- The gx-map home page is http://www.sdsc.edu/~kst/gx-map/.
- The current release is 0.3; expect 0.4 Real Soon Now.
- Any questions: contact me, Keith Thompson, <kst@sdsc.edu>.
- If you find a security hole, *please* let me know ASAP.
- Released as open source under a BSD-like license.