gx-map, a system for maintaining grid-mapfiles

Keith Thompson <kst@sdsc.edu>
San Diego Supercomputer Center
January 20, 2004
(Updated and expanded 2004-01-27; post-talk updates starting at slide 16)

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.
- Write a config file.
- 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.

Updated slides

- I gave this talk at GlobusWorld 2004.
- Here are a few more points that didn't make it into the original slides.

Security, Security, Security

- gx-map is a security-critical application.
- The author is not a security expert.
- Does this make you nervous? Good!
- gx-map has no known security bugs.
- Equivalently (and perhaps more accurately), all the security bugs are unknown ones.
- I think it's fairly robust, but there are no guarantees.

Paranoid mode

- The command-line arguments to gx-gen-mapfile allow you to specify the location of the grid-mapfile. This doesn't have to be "/etc/grid-security/grid-mapfile".
- If you don't quite trust gx-map, you can have it update a separate file; periodically, you can examine the separate file and manually copy it to /etc/grid-security if it looks ok.
- When/if you've decided to trust gx-map, you can modify the cron job so it writes directly to /etc/grid-security/grid-mapfile (or you can make /etc/grid-security/grid-mapfile a symlink).

Authentication by ownership

- gx-map depends on file ownership for authentication; it assumes that users can't use chown (see slide 14). HP-UX allows this by default; other Unix-like systems may be configurable to allow it.
- Open question: Does HP-UX allow non-root chowns across NFS?
- Three cases: HP-UX client, HP-UX server, HP-UX client *and* server.
- How else can the file ownership authentication model break?

Numeric UIDs?

- We assume that both user names and numeric UIDs are consistent within a namespace (typically a site or organization).
- Q: Why worry about UIDs? They don't appear in the grid-mapfile.
- A: The system on which gx-check-requests runs may not have all user accounts in /etc/passwd. In this case, gx-check-requests records the UID; it doesn't know the user name.

Numeric UIDs? (cont.)

- This is workable but ugly. Possible alternatives:
  - Assume/require that gx-check-requests runs on a system with all accounts, or make UID dependence configurable at installation time.
  - If a user doesn't have an account on the system running gx-check-requests, require administrative intervention.
  - Get username/UID information from somewhere other than /etc/passwd (system-specific).

User interface

- The first version of gx-map had only a command-line interface, with a dozen or so options. It all seemed perfectly clear to me (there's even a "-help" option) until I let someone else use it.
- The command-line interface is too complex, especially for a tool that most users will run only once.
- The command-line interface is still supported (mostly for use by automated tools), but the main user interface is now interactive, prompting the user for each required piece of information.

Command-line options

(See, I told you they were confusing)

```
% gx-map -long-help
Usage: gx-map [options]
Option names may be abbreviated.
    -help                 : Show a brief usage message and exit.
    -version              : Show version information and exit.
    -interactive          : Run interactively (recommended).
    -long-help            : Show this long usage message (recommended
                            only for Globus administrators and masochists).
    -add                  : Add the specified mapping.
    -remove               : Remove the specified mapping.
    -remove-dn            : Remove all mappings for the specified
                            distinguished name.  For use only by Globus
                            administrators.
    -remove-user          : Remove all mappings for the specified user.
    -update               : Request an update of all grid-mapfiles.
                            This normally isn't necessary, but it can be
                            useful if you already have a certificate and
                            get a new account on a machine.
Note: Exactly one of "-interactive", "-add", "-remove", "-remove-dn",
      "-remove-user", and "-update"
      (or "-help", "-usage", or -long-usage) must be specified.
-------------------------------------------------------------------------------
    -quiet                : Work silently.
                            Implies -force.
    -force                : Apply mapping without prompting.
                            Default is to ask for verification before
                            proceeding.
    -no-admin             : Assume the user is not a Globus administrator.
                            Intended for testing only; has no effect if
                            you're not already a Globus administrator.
    -dn "string"          : Distinguished name.
                            Default is extracted from ~/.globus/usercert.pem
    -certificate-file file  : Name of file from which to extract DN.
                            If neither "-dn" nor "-certificate-file" is
                            specified, extract DN from
                            $HOME/.globus/usercert.pem
    -force-dn             : Normally, gx-map (minimally) checks the DN for
                            proper syntax; this option overrides that check.
    -username name        : Unix user name to map.
                            This option is for use by Globus
                            administrators only.
    -directory dir        : Specify an alternate data directory.
                            This option is for use by Globus administrators
                            only.
                            The default data directory is
                            /usr/local/apps/gx-map-0.3/var .
    -email addr           : Your contact e-mail address.
                            This may be used to contact you if there's
                            a problem with your certificate.  If you
                            prefer not to submit your e-mail address,
                            you can use "-no-email".
    -no-email             : Don't submit an e-mail address.
    -comment "string"     : Comment to be added to request log (optional)
    -debugging            : Enable debugging output.
Note: If this help message has scrolled off the top of your screen, try
   gx-map -long-help | less
```


User interface (cont.)

- GUI? No.
- Web interface? No.
- Two reasons:
  1. I haven't had much practice implementing GUIs or web interfaces.
  2. I don't know how to integrate the gx-map security model into a fancy interface.
- gx-map runs only on Unix-like systems.

What's next?

- Future releases will have better support for propagating information among sites.
- If all systems using gx-map share an NFS-mounted file system, it's easy, but we have to deal with the hard case.
- I'll probably implement a central repository. Sites can upload their requests.log files to an ftp dropbox. A job running on the repository system checks for new uploads, merges everything together, and makes it all available by ftp or http.

What's next? (cont.)

- Uploaded requests.log files must be signed using a Globus proxy. If the repository doesn't recognize the certificate from which the proxy was generated, the upload is rejected.
- The merged log doesn't need to be signed; we assume that whatever is at the specified URL is authentic.
- Open questions: Should the merged log should be signed? Should uploaded logs be encrypted as well as signed? How private is this information?

What's next? (cont.)

- The grid-mapfile format allows multiple user names per DN; the next release will support this. (Not all Globus tools can use this.)
- `"/O=Foobar/CN=John Smith" user1,user2`
- (Multiple DNs per user name are already supported; each DN is on a separate line.)
- The gx-map client program will be able to extract a DN from a proxy certificate.

What's next? (cont.)

- In the next release, the grid-mapfile will automatically be checked into an RCS repository (this might be optional).
- It may also keep a log of all gx-map commands executed by users, as an aid to debugging and auditing.

What's next? (cont.)

- It would be possible to restrict gx-map so that a user can only map a certificate that he owns. (A user would need a valid proxy.)
- Is this necessary or desirable?
- Should a user be allowed to map somebody else's Globus certificate to his own account? (Such a mapping could be applied by an administrator if necessary.)

What's next? (cont.)

- Another possible feature: Automated maintenance of CRLs (Certificate Revocation Lists).
- A configuration file specifies which CAs (Certificate Authorities) are accepted and how to download the current CRL.
- A new tool, using gx-map's existing URL caching capability, keeps the CRLs up to date.
- Run the new tool from a cron job, perhaps once an hour. Details TBD.

What's next? (cont.)

- What else does gx-map need to do?
- Any suggestions are welcome; e-mail Keith Thompson <kst@sdsc.edu>.
- Security will always take precedence over bells and whistles.

gx-map 0.4.0

- As I write this, I'm just about to release gx-map 0.4.0.
- It includes support for automated maintenance of CRLs as discussed in slide 30, as well as multiple user names per DN in the grid-mapfile.
- It does not (yet) include support for cross-site updates (slides 25-26) beyond the existing ftp/http mechanism.