
Introduction

Authentication in the Globus Toolkit is based on X.509 certificates. This document describes how to acquire and use the certificates that you will need to authenticate yourself to Globus services.
# Table of Contents

1. Usage scenarios ............................................................................................................................... 1
   1. Basic procedure for using GSI C ................................................................................................. 1
I. GSI Commands ................................................................................................................................ 2
   - grid-cert-diagnostics ..................................................................................................................... 3
   - grid-cert-info .............................................................................................................................. 5
   - grid-cert-request .......................................................................................................................... 7
   - grid-default-ca ........................................................................................................................... 10
   - grid-change-pass-phrase .............................................................................................................. 12
   - grid-proxy-init ........................................................................................................................... 13
   - grid-proxy-destroy ....................................................................................................................... 16
   - grid-proxy-info .......................................................................................................................... 17
   - grid-mapfile-add-entry ............................................................................................................... 19
   - grid-mapfile-check-consistency ................................................................................................. 20
   - grid-mapfile-delete-entry .......................................................................................................... 21
2. Troubleshooting ............................................................................................................................. 22
   1. Credential Troubleshooting ....................................................................................................... 22
   2. Grid map Troubleshooting ......................................................................................................... 25
Glossary ............................................................................................................................................... 26
List of Tables

1. Command line options ................................................................. 12
2. Command line options ................................................................. 14
3. Command line options ................................................................. 16
4. Command line options ................................................................. 17
5. Print options ............................................................................. 17
6. Validity options ......................................................................... 18
7. Command line options ................................................................. 19
8. Command line options ................................................................. 20
9. Command line options ................................................................. 21
2.1. Credential Errors ................................................................. 23
2.2. Gridmap Errors ................................................................. 25
Chapter 1. Usage scenarios

1. Basic procedure for using GSI C

In most cases, an individual will do the following:

- Acquire a *user certificate* from a certification authority (CA) with `grid-cert-request`. This certificate will typically be valid for a year or more and will be stored in a file in the individual's home directory.

  It is important to keep in mind when your cert will expire - after your user certificate expires, you may not be able to use secure services in GT!

- Use the end-user certificate to create a *proxy certificate* using `grid-proxy-init`. This will be used to authenticate the individual to grid services. Proxy certificates typically have a much shorter lifetime than end-user certificates (usually 12 hours). Once your proxy certificate expires, simply rerun `grid-proxy-init`.

GSI Commands
Name

grid-cert-diagnostics -- Print diagnostic information about certificates and keys

grid-cert-diagnostics [-h] [-p]

Description

The grid-cert-diagnostics command displays information about the current user's security environment, including information about security-related environment variables, security directory search path, personal key and certificates, and trusted certificates. It is intended to provide information to help diagnose problems using GSI security.

The full set of command-line options to grid-cert-diagnostics consists of:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Display a help message and exit</td>
</tr>
<tr>
<td>-p</td>
<td>Display information about the personal certificate and key that is the current user's default credential.</td>
</tr>
</tbody>
</table>

Examples

In this example, we see the default mode of checking the default security environment for the system, without processing the user's key and certificate. Note the user receives a warning about a cog.properties and about an expired CA certificate.

% grid-cert-diagnostics

Checking Environment Variables
================================
Checking if X509_CERT_DIR is set... no
Checking if X509_USER_CERT is set... no
Checking if X509_USER_KEY is set... no
Checking if X509_USER_PROXY is set... no

Checking Security Directories
============================
Determining trusted cert path... /etc/grid-security/certificates
Checking for cog.properties... found
    WARNING: If the cog.properties file contains security properties, Java apps will ignore the security paths described in the GSI documentation

Checking trusted certificates...
================================
Getting trusted certificate list...
Checking CA file /etc/grid-security/certificates/1c4f4c48.0... ok
Verifying certificate chain for "/etc/grid-security/certificates/1c3f2ca8.0"... ok
Checking CA file /etc/grid-security/certificates/9d8788eb.0... ok
Verifying certificate chain for "/etc/grid-security/certificates/9d8753eb.0"... failed
globus_credential: Error verifying credential: Failed to verify credential
globus_gsi_callback_module: Could not verify credential
globus_gsi_callback_module: The certificate has expired:
Credential with subject: /DC=org/DC=example/OU=grid/CN=CA has expired.

In this example, we show a user with a mismatched private key and certificate:

```
% grid-cert-diagnostics -p

Checking Environment Variables
==============================
Checking if X509_CERT_DIR is set... no
Checking if X509_USER_CERT is set... no
Checking if X509_USER_KEY is set... no
Checking if X509_USER_PROXY is set... no

Checking Security Directories
=======================
Determining trusted cert path... /etc/grid-security/certificates
Checking for cog.properties... not found

Checking Default Credentials
==============================
Determining certificate and key file names... ok
Certificate Path: "/home/juser/.globus/usercert.pem"
Key Path: "/home/juser/.globus/userkey.pem"
Reading certificate... ok
Reading private key... ok
Checking Certificate Subject... "/O=Grid/OU=Example/OU=User/CN=Joe User"
Checking cert... ok
Checking key... ok
Checking that certificate contains an RSA key... ok
Checking that private key is an RSA key... ok
Checking that public and private keys have the same modulus... failed
Private key modulus: D294849E37F048C3B5ACEEF2CCDF97D88B679C361E29D5CB5219C3E948F3E530CFC609489759E1D751F0ACFF0515A614276A0F4C11A57D92D7165BBAFA64E3140155DE448D45C182F4657DA13EDA288423F5B9D169DDF3822EFD81EB2E6403CE3CB4CCF96B65284D92592BB1673A18354DA241B9AFD7F494E54F63A93E15DCAE2
Public key modulus : C002C7B329B13BFA87BBAF214EACE3DC3D490165ACEB791790600708C544175D9193C9BAC5AE0D3B7CB49BB6A6D29B7E635FAC751E9A61CEA980226F1B63002902D6623A319E4682E7BFB0968DCE962CF218AD595AAAD6A0BA5C42AA9A9AF7FDD32B37C6E2BF0E311310AA55FFB9EAFDF5B995C7D9EEAD8D5D01F3531E0AE5
Certificate and and private key don't match
```
Name

grid-cert-info -- Display certificate information

grid-cert-info [-help] [-version] [-file CERTIFICATE-FI- 

Description

The grid-cert-info displays information from a user's credential, or from any X.509 certificate if the -file CERTIFICATE-FI- 
LENAME is used. By default, a text representation of the entire certificate is displayed. If more than one display option is present on the command line, the output is generated in the order the options occur on the command line.

The following search order is used to locate the default certificate:

- $X509_USER_CERT
- $HOME/.globus/usercert.pem
- $HOME/.globus/usercred.p12

If the certificate is encoded in pkcs12, grid-cert-info will prompt for the password used to protect the .p12 file.

The full set of command-line options to grid-cert-info is:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Print help information and exit</td>
</tr>
<tr>
<td>-version</td>
<td>Print version information and exit</td>
</tr>
</tbody>
</table>
| -file       | Read credential from CERTIFICATE-FI- 
LENAME instead of the default location. The file must have a .pem or .p12 extension. |
| -all        | Print all information from the certificate. This is the default unless any of the following options are given. |
| -subject    | Print the subject name of the certificate. |
| -issuer     | Print the subject name of the issuer of the certificate. This is the subject name of the Certificate Authority which signed the certificate. |
| -issuerhash | Print the hash of the name of the issuer of the certificate. This is the hash of the Certificate Authority which signed the certificate. |
| -startdate  | Print the date and time from which the certificate is valid |
| -enddate    | Print the date and time when the certificate expires. |

Examples

Print out the date range when a certificate is valid:

```sh
% grid-cert-info -startdate -enddate
Oct 29 13:09:42 2007 GMT
Oct 28 13:09:42 2008 GMT
```
Note that in this example, the start date is printed first, based on the order of the command-line options.

Limitations

The `–issuerhash` fails with some versions of OpenSSL.
Name

grid-cert-request -- Create a certificate request

[-commonname NAME] [-service SERVICE] [-host FQDN] [-interactive]
[-dir DIRECTORY] [-prefix PREFIX] [-ca HASH] [-nopw]

Description

grid-cert-request generates a public/private key pair an X.509 certificate request containing the public key and a subject name. By default, it generates a request for a user certificate for the invoking user. grid-cert-request can also be used to create host or service certificates based on command-line options. At least one Certificate Authority must be configured to use with the Globus Toolkit in order for this command to succeed.

Complete set of options to grid-cert-request is:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Print help information and exit</td>
</tr>
<tr>
<td>-version</td>
<td>Print version information and exit</td>
</tr>
<tr>
<td>-verbose</td>
<td>Don't clear screen after running OpenSSL</td>
</tr>
<tr>
<td>-force</td>
<td>Overwrite an existing certificate request if present.</td>
</tr>
<tr>
<td>-commonname NAME</td>
<td>Construct a subject name with NAME as the final name component. By default, the subject name is inferred from the output of the finger program. If that fails, grid-cert-request will prompt of a name.</td>
</tr>
<tr>
<td>-service SERVICE</td>
<td>Construct a subject name with the common name constructed from the SERVICE name and the hostname joined by the / character. The -service requires that the -host option also be used. The private key created for a service certificate request is not encrypted.</td>
</tr>
<tr>
<td>-host FQDN</td>
<td>Construct a subject name with FQDN as the name of the host. This must be a fully-qualified name in dotted string notation (e.g. grid.example.org). If no service is specified by the -service option, the subject name will be host/FQDN. The private key created for a host certificate request is not encrypted. By default the host certificate request and key are created in /etc/grid-security.</td>
</tr>
<tr>
<td>-interactive</td>
<td>Interactively prompt for the components of the certificate subject name.</td>
</tr>
<tr>
<td>-dir DIRECTORY</td>
<td>Write the certificate request and key to DIRECTORY, creating it if the directory does not exist. By default, the certificate request and key are placed in $HOME/.globus</td>
</tr>
<tr>
<td>-prefix PREFIX</td>
<td>Prepend the string PREFIX to the certificate, key, and request filenames. The default prefix is user for user certificates and host for host certificates.</td>
</tr>
<tr>
<td>-ca HASH</td>
<td>Choose a non-default Certificate Authority configuration to construct the certificate request. If HASH is present on the command line, then grid-cert-request will use that certificate authority's configuration. Otherwise, it will prompt the user for a CA to choose from the list of configured CAs.</td>
</tr>
<tr>
<td>-nopw</td>
<td>Create a private key without a password. This may be a security risk if the file permissions of the private key are not carefully maintained.</td>
</tr>
</tbody>
</table>
Examples

Request a user certificate:

% grid-cert-request

A certificate request and private key is being created. You will be asked to enter a PEM pass phrase. This pass phrase is akin to your account password, and is used to protect your key file. If you forget your pass phrase, you will need to obtain a new certificate.

Generating a 1024 bit RSA private key
               ................+++
               ........+++++
writing new private key to '/home/juser/.globus/userkey.pem'
Enter PEM pass phrase:

A private key and a certificate request have been generated with the subject:

/O=Grid/OU=Example/OU=User/CN=Joe User

If the CN=Joe User is not appropriate, rerun this script with the -force -cn "Common Name" options.

Your private key is stored in /home/juser/.globus/userkey.pem
Your request is stored in /home/juser/.globus/usercert_request.pem

Please e-mail the request to the Globus Certificate Service ca@grid.example.org
You may use a command similar to the following:

        cat /home/juser/.globus/usercert_request.pem | mail ca@grid.example.org

Only use the above if this machine can send AND receive e-mail. if not, please mail using some other method.

Your certificate will be mailed to you within two working days. If you receive no response, contact Globus Certificate Service at ca@grid.example.org

Request a host certificate, putting the request and key files in the $HOME/.globus/host directory.

% grid-cert-request -host grid.example.org -dir $HOME/.globus/host

A private host key and a certificate request have been generated with the subject:

/O=Grid/OU=Example/OU=User/CN=host/grid.example.org
The private key is stored in /tmp/examplegrid/hostkey.pem
The request is stored in /tmp/examplegrid/hostcert_request.pem

Please e-mail the request to the Globus Certificate Service ca@grid.example.org
You may use a command similar to the following:

    cat /tmp/examplegrid/hostcert_request.pem | mail ca@grid.example.org

Only use the above if this machine can send AND receive e-mail. if not, please mail using some other method.

Your certificate will be mailed to you within two working days.
If you receive no response, contact Globus Certificate Service at ca@grid.example.org

Limitations

Only supports PEM-encoded keys, certificates and certificate requests.
Name

grid-default-ca -- Set the default CA to use for certificate requests

grid-default-ca [-help] [-list] [-ca CA-HASH] [-dir SECURITY-DIRECTORY]

Description

The grid-default-ca program sets the default CA used by grid-cert-request. Based on the default CA choice, grid-cert-request will create a certificate request that matches the CA's naming policies.

If the -ca option is not provided on the command-line, grid-default-ca will display a list of available Certificate Authorities and prompt the user to choose one.

The full set of command-line options to grid-default-ca are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>Display a help message and exit</td>
</tr>
<tr>
<td>-list</td>
<td>List the available CAs but do not alter the default</td>
</tr>
<tr>
<td>-ca CA-HASH</td>
<td>Select the default CA whose subject name hash matches CA-HASH.</td>
</tr>
<tr>
<td>-dir SECURITY-DIRECTORY</td>
<td>Search SECURITY-DIRECTORY for additional CA certificates.</td>
</tr>
</tbody>
</table>

Examples

Show what certificate authorities are in the trusted cert directory:

% grid-default-ca -list

The available CA configurations installed on this host are:

Directory: /etc/grid-security/certificates

1) 1c3f2ca8 - /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
2) 3d8e6ce8 - /O=Grid/CN=Example CA
3) 6349a761 - /O=DOE Science Grid/OU=Certificate Authorities/CN=Certificate Manager
4) b38b4d8c - /C=US/O=Globus Alliance/CN=Globus Certificate Service

The default CA is: /C=US/O=Globus Alliance/CN=Globus Certificate Service
Location: /etc/grid-security/certificates/b38b4d8c.0

Change the default CA to be DOEGrids CA 1:

% grid-default-ca

The available CA configurations installed on this host are:

Directory: /etc/grid-security/certificates
1) 1c3f2ca8 - /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
2) 3d8e6ce8 - /O=Grid/CN=Example CA
3) 6349a761 - /O=DOE Science Grid/OU=Certificate Authorities/CN=Certificate Manager
4) b38b4d8c - /C=US/O=Globus Alliance/CN=Globus Certificate Service

The default CA is: /C=US/O=Globus Alliance/CN=Globus Certificate Service
Location: /etc/grid-security/certificates/b38b4d8c.0

Enter the index number of the CA to set as the default [q to quit]: 1

setting the default CA to: /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1

linking /etc/grid-security/certificates/grid-security.conf.1c3f2ca8 to
/etc/grid-security/grid-security.conf

linking /etc/grid-security/certificates/globus-host-ssl.conf.1c3f2ca8 to
/etc/grid-security/globus-host-ssl.conf

linking /etc/grid-security/certificates/globus-user-ssl.conf.1c3f2ca8 to
/etc/grid-security/globus-user-ssl.conf

...done.

Limitations

Displays all CAs in the output, even those where the globus-user-ssl.conf and globus-host-ssl.conf files are not installed in the trusted certificate directory. If one of those is chosen, grid-default-ca displays an error and exits.
Name
grid-change-pass-phrase -- Change the pass phrase on a private key
grid-change-pass-phrase

Tool description
grid-change-pass-phrase allows one to change the passphrase that protects the private key.

Command syntax
grid-change-pass-phrase [-help] [-version] [-file private_key_file]

Changes the passphrase that protects the private key. Note that this command will work even if the original key is not password protected. If the -file argument is not given, the default location of the file containing the private key is assumed:

- The location pointed to by X509_USER_KEY
- If X509_USER_KEY not set, $HOME/globus/userkey.pem

Options

Table 1. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-file location</td>
<td>Changes the passphrase on the key stored in the file at the non-standard location 'location'.</td>
</tr>
</tbody>
</table>

Limitations
Nothing applicable
Name

grid-proxy-init -- Generate a new proxy certificate

grid-proxy-init

Tool description

grid-proxy-init generates X.509 proxy certificates.

By default, this command generates RFC 3820\(^1\) Proxy Certificates.

There are also options available for generating other types of proxy certificates, including limited, independent and legacy. For more information about proxy certificate types and their compatibility in GT, see [http://dev.globus.org/wiki/Security/ProxyCertTypes](http://dev.globus.org/wiki/Security/ProxyCertTypes).

Command syntax

```
grid-proxy-init [-help][-pwstdin][-limited][-valid H:M] ...
```

\(^1\) [http://www.ietf.org/rfc/rfc3820.txt](http://www.ietf.org/rfc/rfc3820.txt)
Options

Table 2. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-debug</td>
<td>Enables extra debug output.</td>
</tr>
<tr>
<td>-q</td>
<td>Quiet mode, minimal output.</td>
</tr>
<tr>
<td>-verify</td>
<td>Verifies the certificate to make the proxy for.</td>
</tr>
<tr>
<td>-pwstdin</td>
<td>Allows passphrase from stdin.</td>
</tr>
<tr>
<td>-limited</td>
<td>Creates a limited globus proxy.</td>
</tr>
<tr>
<td>-independent</td>
<td>Creates an independent globus proxy.</td>
</tr>
<tr>
<td>-draft</td>
<td>Creates a draft (GSI-3) proxy.</td>
</tr>
<tr>
<td>-old</td>
<td>Creates a legacy globus proxy.</td>
</tr>
<tr>
<td>-valid &lt;h:m&gt;</td>
<td>Proxy is valid for ( h ) hours and ( m ) minutes (default:12:00).</td>
</tr>
<tr>
<td>-hours &lt;hours&gt;</td>
<td>Deprecated support of hours option.</td>
</tr>
<tr>
<td>-bits &lt;bits&gt;</td>
<td>Number of bits in key {512</td>
</tr>
<tr>
<td>-policy &lt;policyfile&gt;</td>
<td>File containing the policy to store in the ProxyCertInfo extension.</td>
</tr>
<tr>
<td>-pl &lt;oid&gt;, -policy-language &lt;oid&gt;</td>
<td>OID string for the policy language used in the policy file.</td>
</tr>
<tr>
<td>-path-length &lt;l&gt;</td>
<td>Allows a chain of at most ( l ) proxies to be generated from this one.</td>
</tr>
<tr>
<td>-cert &lt;certfile&gt;</td>
<td>Non-standard location of user certificate.</td>
</tr>
<tr>
<td>-key &lt;keyfile&gt;</td>
<td>Non-standard location of user key.</td>
</tr>
<tr>
<td>-certdir &lt;certdir&gt;</td>
<td>Non-standard location of trusted cert directory.</td>
</tr>
<tr>
<td>-out &lt;proxyfile&gt;</td>
<td>Non-standard location of new proxy cert.</td>
</tr>
</tbody>
</table>

Creating a Proxy Certificate

Proxies are certificates signed by the user, or by another proxy, that do not require a password to submit a job. They are intended for short-term use, when the user is submitting many jobs and cannot be troubled to repeat his password for every job.

The subject of a proxy certificate is the same as the subject of the certificate that signed it, with /CN=proxy added to the name. The gatekeeper will accept any job requests submitted by the user, as well as any proxies he has created.

Proxies provide a convenient alternative to constantly entering passwords, but are also less secure than the user's normal security credential. Therefore, they should always be user-readable only, and should be deleted after they are no longer needed (or after they expire).

To create a proxy with the default expiration (12 hours), run the grid-proxy-init program. For example:

```
% grid-proxy-init
```

The grid-proxy-init program can also take arguments to specify the expiration and proxy key length. For example:

```
% grid-proxy-init -hours 8 -bits 512
```
Limitations

Nothing applicable
Name

grid-proxy-destroy -- Destroy the current proxy certificate (previously created with grid-proxy-init)

grid-proxy-destroy

Tool description

grid-proxy-destroy removes X.509 proxy certificates.

Command syntax

grid-proxy-destroy [-help][-dryrun][-default][-all][--] [file1...]

Options

Table 3. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-debug</td>
<td>Displays debugging information.</td>
</tr>
<tr>
<td>-dryrun</td>
<td>Prints what files would have been destroyed.</td>
</tr>
<tr>
<td>-default</td>
<td>Destroys file at default proxy location.</td>
</tr>
<tr>
<td>-all</td>
<td>Destroys any user (default) and delegated proxies that are found.</td>
</tr>
<tr>
<td>--</td>
<td>Ends processing of options.</td>
</tr>
<tr>
<td>file1 file2</td>
<td>Destroys the files listed.</td>
</tr>
</tbody>
</table>

Limitations

Nothing applicable
Name

grid-proxy-info -- Display information obtained from a proxy certificate

grid-proxy-info

Tool description

grid-proxy-info extracts information from X.509 proxy certificates.

Command syntax

grid-proxy-info [-help][-f proxyfile][-subject][...][-e [-h H][-b B]]

Options

Table 4. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays usage.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-debug</td>
<td>Displays debugging output.</td>
</tr>
<tr>
<td>-file &lt;proxyfile&gt; (-f)</td>
<td>Non-standard location of proxy.</td>
</tr>
<tr>
<td>[printoptions]</td>
<td>See Table 5, “Print options”.</td>
</tr>
<tr>
<td>-exists [options] (-e)</td>
<td>Determine whether a valid proxy exists. options may contain any validation options described below. If a proxy exists, and meets any criteria defined by the validity options, then grid-proxy-info will terminate with the exit code 0. Otherwise, grid-proxy-info will terminate with the exit code 1. If no validity options are specified, the program will terminate with 0 if a currently-valid proxy file exists.</td>
</tr>
</tbody>
</table>

Table 5. Print options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-subject (-s)</td>
<td>Distinguished name (DN) of the subject.</td>
</tr>
<tr>
<td>-issuer (-i)</td>
<td>DN of the issuer (certificate signer).</td>
</tr>
<tr>
<td>-identity</td>
<td>DN of the identity represented by the proxy.</td>
</tr>
<tr>
<td>-type</td>
<td>Type of proxy (full or limited).</td>
</tr>
<tr>
<td>-timeleft</td>
<td>Time (in seconds) until proxy expires.</td>
</tr>
<tr>
<td>-strength</td>
<td>Key size (in bits).</td>
</tr>
<tr>
<td>-all</td>
<td>All above options in a human readable format.</td>
</tr>
<tr>
<td>-text</td>
<td>All of the certificate.</td>
</tr>
<tr>
<td>-path</td>
<td>Pathname of the proxy file.</td>
</tr>
</tbody>
</table>
Table 6. Validity options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-valid H:M (-v)</td>
<td>Time requirement for the proxy to be valid.</td>
</tr>
<tr>
<td>-hours H (-h)</td>
<td>Time requirement for the proxy to be valid (deprecated, use -valid instead).</td>
</tr>
<tr>
<td>-bits B (-b)</td>
<td>Strength requirement for the proxy to be valid.</td>
</tr>
</tbody>
</table>

Limitations

Nothing applicable
Name
grid-mapfile-add-entry -- Add an entry to a grid map file

grid-mapfile-add-entry

Tool description
grid-mapfile-add-entry adds entries to grid map files.

Command syntax
grid-mapfile-add-entry -dn DN -ln LN [-help] [-d] [-f mapfile FILE]

Options:

Table 7. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays help.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-dn DN</td>
<td>Distinguished Name (DN) to add. Remember to quote the DN if it contains spaces.</td>
</tr>
<tr>
<td>-ln LN1 [LN2...]</td>
<td>Local login name(s) to which the DN is mapped.</td>
</tr>
<tr>
<td>-dryrun, -d</td>
<td>Shows what would be done but will not add the entry.</td>
</tr>
<tr>
<td>-mapfile FILE, -f FILE</td>
<td>Path of the grid map file to be used.</td>
</tr>
</tbody>
</table>

Limitations
Nothing applicable.
**Name**

grid-mapfile-check-consistency -- Check the internal consistency of a grid map file

grid-mapfile-check-consistency

**Tool description**

`grid-mapfile-check-consistency` checks that the given grid map file conforms to the expected format as well as checking for common subject name problems.

**Command syntax**

`grid-mapfile-check-consistency [-help] [-mapfile FILE]`

**Options:**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays help.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-mapfile FILE, -f FILE</td>
<td>Path of the grid map file to be used.</td>
</tr>
</tbody>
</table>

**Limitations**

Nothing applicable
Name

grid-mapfile-delete-entry -- Delete an entry from a grid map file

grid-mapfile-delete-entry

Tool description

grid-mapfile-delete entry deletes a grid map file entry from the given file.

Command syntax


Options:

Table 9. Command line options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help, -usage</td>
<td>Displays help.</td>
</tr>
<tr>
<td>-version</td>
<td>Displays version.</td>
</tr>
<tr>
<td>-dn &lt;DN&gt;</td>
<td>Distinguished Name (DN) to delete.</td>
</tr>
<tr>
<td>-ln &lt;local name&gt;</td>
<td>Local Login Name (LN) to delete.</td>
</tr>
<tr>
<td>-dryrun, -d</td>
<td>Shows what would be done but will not delete the entry.</td>
</tr>
<tr>
<td>-mapfile, -f file</td>
<td>Path of the grid map file to be used.</td>
</tr>
</tbody>
</table>

Limitations

Nothing applicable.
Chapter 2. Troubleshooting

The following includes common errors for credentials and gridmap files. For information about system administrator logs, see Chapter 4, Debugging in the GSI C Admin Guide.

For a list of common errors in GT, see Error Codes.

1. Credential Troubleshooting

1.1. Credential Errors

The following are some common problems that may cause clients or servers to report that credentials are invalid:

For a list of common errors in GT, see Error Codes.
Table 2.1. Credential Errors

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Definition</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your proxy credential may have expired</td>
<td>Your proxy credential may have expired.</td>
<td>Use <code>grid-proxy-info</code> to check whether the proxy credential has actually expired. If it has, generate a new proxy with <code>grid-proxy-init</code>.</td>
</tr>
<tr>
<td>The system clock on either the local or remote system is wrong.</td>
<td>This may cause the server or client to conclude that a credential has expired.</td>
<td>Check the system clocks on the local and remote system.</td>
</tr>
<tr>
<td>Your end-user certificate may have expired</td>
<td>Your end-user certificate may have expired</td>
<td>Use <code>grid-cert-info</code> to check your certificate’s expiration date. If it has expired, follow your CA’s procedures to get a new one.</td>
</tr>
<tr>
<td>The permissions may be wrong on your proxy file</td>
<td>If the permissions on your proxy file are too lax (for example, if others can read your proxy file), Globus Toolkit clients will not use that file to authenticate.</td>
<td>You can “fix” this problem by changing the permissions on the file or by destroying it (with <code>grid-proxy-destroy</code>) and creating a new one (with <code>grid-proxy-init</code>). <strong>Important:</strong> However, it is still possible that someone else has made a copy of that file during the time that the permissions were wrong. In that case, they will be able to impersonate you until the proxy file expires or your permissions or end-user certificate are revoked, whichever happens first.</td>
</tr>
<tr>
<td>The permissions may be wrong on your private key file</td>
<td>If the permissions on your end user certificate private key file are too lax (for example, if others can read the file), <code>grid-proxy-init</code> will refuse to create a proxy certificate.</td>
<td>You can “fix” this by changing the permissions on the private key file. <strong>Important:</strong> However, you will still have a much more serious problem: it is possible that someone has made a copy of your private key file. Although this file is encrypted, it is possible that someone will be able to decrypt the private key, at which point they will be able to impersonate you as long as your end user certificate is valid. You should contact your CA to have your end-user certificate revoked and get a new one.</td>
</tr>
<tr>
<td>The remote system may not trust your CA</td>
<td>The remote system may not trust your CA</td>
<td>Verify that the remote system is configured to trust the CA that issued your end-entity certificate. See Installing GT 4.2.1 for details.</td>
</tr>
<tr>
<td>You may not trust the remote system’s CA</td>
<td>You may not trust the remote system’s CA</td>
<td>Verify that your system is configured to trust the remote CA (or that your environment is set up to trust the remote CA). See Installing GT 4.2.1 for details.</td>
</tr>
<tr>
<td>There may be something wrong with the remote service’s credentials</td>
<td>There may be something wrong with the remote service’s credentials</td>
<td>It is sometimes difficult to distinguish between errors reported by the remote service regarding your credentials and errors reported by the client interface regarding the remote service’s credentials. If you cannot find anything wrong with your credentials, check for the same conditions on the remote system (or ask a remote administrator to do so).</td>
</tr>
</tbody>
</table>
1.2. Some tools to validate certificate setup

1.2.1. grid-cert-diagnostics

The grid-cert-diagnostics program checks prints diagnostics about the user's certificates, and host security environment.

```
% grid-cert-diagnostics -p
```

1.2.2. Check that the user certificate is valid

openssl verify -CApath /etc/grid-security/certificates
  -purpose sslclient ~/.globus/usercert.pem

1.2.3. Connect to the server using s_client

openssl s_client -ssl3 -cert ~/.globus/usercert.pem -key ~/.globus/userkey.pem -CApath /etc/grid-security/certificates
  -connect <host:port>

Here <host:port> denotes the server and port you connect to.

If it prints an error and puts you back at the command prompt, then it typically means that the server has closed the connection, i.e. that the server was not happy with the client's certificate and verification. Check the SSL log on the server.

If the command "hangs" then it has actually opened a telnet style (but secure) socket, and you can "talk" to the server.

You should be able to scroll up and see the subject names of the server's verification chain:

```
depth=2 /DC=net/DC=ES/O=ESnet/OU=Certificate Authorities/CN=ESnet Root CA 1
verify return:1
depth=1 /DC=org/DC=DOEGrids/OU=Certificate Authorities/CN=DOEGrids CA 1
verify return:1
depth=0 /DC=org/DC=doegrids/OU=Services/CN=wiggum.mcs.anl.gov
verify return:1
```

In this case, there were no errors. Errors would give you an extra line next to the subject name of the certificate that caused the error.

1.2.4. Check that the server certificate is valid

Requires root login on server:

```
openssl verify -CApath /etc/grid-security/certificates -purpose sslserver
  /etc/grid-security/hostcert.pem
```
2. Grid map Troubleshooting

2.1. Grid map errors

The following are some common problems that may cause clients or servers to report that a user are not authorized:

For a list of common errors in GT, see Error Codes.

Table 2.2. Gridmap Errors

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Definition</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The content of the grid map file does not conform to the expected format</td>
<td>The content of the grid map file does not conform to the expected format.</td>
<td>Run <code>grid-mapfile-check-consistency</code> to make sure that your gridmap file conforms to the expected format.</td>
</tr>
<tr>
<td>The grid map file does not contain a entry for your DN</td>
<td>The grid map file does not contain a entry for your DN.</td>
<td>Use <code>grid-mapfile-add-entry</code> to add the relevant entry.</td>
</tr>
</tbody>
</table>
### Glossary

*Some terms not in the docs but wanted in glossary: scheduler*

**C**
- **Certificate Authority (CA)**: An entity that issues certificates. [fixme - flesh out]

**G**
- **grid map file**: A file containing entries mapping certificate subjects to local user names. This file can also serve as an access control list for GSI enabled services and is typically found in `/etc/grid-security/grid-mapfile`. For more information see the Gridmap section [here](#).

**P**
- **proxy certificate**: A short lived certificate issued using an EEC. A proxy certificate typically has the same effective subject as the EEC that issued it and can thus be used in its place. GSI uses proxy certificates for single sign on and delegation of rights to other entities.

For more information about types of proxy certificates and their compatibility in different versions of GT, see [http://dev.globus.org/wiki/Security/ProxyCertTypes](http://dev.globus.org/wiki/Security/ProxyCertTypes).

**S**
- **scheduler**: Term used to describe a job scheduler mechanism to which GRAM interfaces. It is a networked system for submitting, controlling, and monitoring the workload of batch jobs in one or more computers. The jobs or tasks are scheduled for execution at a time chosen by the subsystem according to an available policy and availability of resources. Popular job schedulers include Portable Batch System (PBS), Platform LSF, and IBM LoadLeveler.

**U**
- **user certificate**: A EEC belonging to a user. When using GSI, this certificate is typically stored in `$HOME/.globus/usercert.pem`. For more information on possible user certificate locations, see [this](#).