Globus Toolkit Error FAQ

The purpose of this document is to outline common errors encountered after the installation and setup of the Globus Toolkit.

1. `GRAM Job Submission failed because the connection to the server failed (check host and port) (error code 12)`
2. `error in loading shared libraries`
3. `ERROR: no valid proxy, or lifetime to small (one hour)`
4. `GRAM Job submission failed because authentication with the remote server failed (error code 7)`
5. `GRAM Job submission failed bacause authentication failed: remote certificate not yet valid (error code 7)`
6. `GRAM Job submission failed bacause authentication failed: remote certificate has expired (error code 7)`
7. `GRAM Job submission failed because data transfer to the server failed (error code 10)`
8. `GRAM Job submission failed because authentication failed: Expected target subject name="/CN=host/hostname" Target returned subject name="/O=Grid/O=Globus/CN=hostname.domain.edu" (error code 7)`
9. `Problem with local credentials no proxy credentials: run grid-proxy-init or wgpi first`
10. `GRAM Job submission failed because authentication failed: remote side did not like my creds for unknown reason`
11. `GRAM Job submission failed because the job manager failed to open stdout (error code 73)`

    or

    `GRAM Job submission failed because the job manager failed to open stderr (error code 74)`
12. `GRAM Job submission failed because the provided RSL string includes variables that could not be identified (error code 39)`
13. 530 Login incorrect / FTP LOGIN REFUSED (shell not in /etc/shells)
14. globus_i_gsi_gss_utils.c:866: globus_i_gsi_gss_handshake: Unable to verify remote side's credentials: Couldn't verify the remote certificate OpenSSL Error: s3_pkt.c:1031: in library: SSL routines, function SSL3_READ_BYTES: sslv3 alert bad certificate (error code 7)
15. globus_gsi_callback.c:438: globus_i_gsi_callback_cred_verify: Could not verify credential: self signed certificate in certificate chain (error code 7)

    or

    globus_gsi_callback.c:424: globus_i_gsi_callback_cred_verify: Can't get the local trusted CA certificate: Cannot find issuer certificate for local credential (error code 7)
16. SSL3_GET_CLIENT_CERTIFICATE: no certificate returned
17. undefined symbol: lutil_sasl_interact followed by a failure to load a module. /usr/local/globus-2.4.2/etc/grid-info-slapd.conf: line 23: failed to load or initialize module libback_giis.la

---

1. `GRAM Job Submission failed because the connection to the server failed (check host and port) (error code 12)`

Diagnosis

Your client is unable to contact the gatekeeper specified. Possible causes include:

- The gatekeeper is not running
- The host is not reachable.
- The gatekeeper is on a non-standard port

Solution

Make sure the gatekeeper is being launched by inetd or xinetd. Review the Install Guide if you do not know how to do this. Check to make sure that ordinary TCP/IP connections are possible; can you ssh to the host, or ping it? If you cannot, then you probably can't submit jobs either. Check for typos in the hostname.

Try telnetting to port 2119. If you see a "Unable to load shared library", the gatekeeper was not built statically, and does not have an appropriate LD_LIBRARY_PATH set. If that is the case, either rebuild it statically, or set the environment variable for the gatekeeper. In inetd, use /usr/bin/env to wrap the launch of the gatekeeper, or in xinetd, use the "env=" option.

Check the $GLOBUS_LOCATION/var/globus-gatekeeper.log if it exists. It may tell you that the private key is insecure, so it refuses to start. In that case, fix the permissions of the key to be read only by the owner.

If the gatekeeper is on a non-standard port, be sure to use a contact string of host:port.

Back to top

---

2. `error in loading shared libraries`

Diagnosis

`LD_LIBRARY_PATH` is not set.

Solution

If you receive this as a client, make sure to read in either $GLOBUS_LOCATION/etc/globus-user-env.sh (if you are using a Bourne-like shell) or $GLOBUS_LOCATION/etc/globus-user-env.csh (if you are using a C-like shell)

Back to top

---

3. `ERROR: no valid proxy, or lifetime to small (one hour)`

Diagnosis

You are running `globus-personal-gatekeeper` as root, or did not run `grid-proxy-init`.

Solution

Don't run `globus-personal-gatekeeper` as root. `globus-personal-gatekeeper` is designed to allow an ordinary user to establish a gatekeeper using a proxy from their personal certificate. If you are root, you should setup a gatekeeper using inetd or xinetd, and using your host certificates. If you are not root, make sure to run `grid-proxy-init` before starting the personal gatekeeper.

Back to top

---

4. `GRAM Job submission failed because authentication with the remote server failed (error code 7)`

Diagnosis

Check the $GLOBUS_LOCATION/var/globus-gatekeeper.log on the remote server. You will probably see something like:

```
Authenticated globus user: /O=Grid/O=Globus/OU=your.domain/OU=Your Name
Failure: globus_gss_assist_gridmap() failed authorization. rc =1
```

Solution

This indicates that your account is not in the grid-mapfile. Create the grid-mapfile in /etc/grid-security (or wherever the -gridmap flag in $GLOBUS_LOCATION/etc/globus-gatekeeper.conf points to) with an entry pairing your subject name to your user name. Review the Install Guide if you do not know how to do this. If you see "rc = 7", you may have bad permissions on the /etc/grid-security/. It needs to be readable so that users can see the certificates/ subdirectory.

Back to top

---

5. `GRAM Job submission failed bacause authentication failed: remote certificate not yet valid (error code 7)`

Diagnosis

This indicates that the remote host has a date set greater than five minutes in the future relative to the remote host.

Try typing "date -u" on both systems at the same time to verify this. (The "-u" specifies that the time should be displayed in universal time, also known as UTC or GMT.)

Solution

Ultimately, synchronize the hosts using NTP. Otherwise, unless you are willing to set the client host date back, you will have to wait until your system believes that the remote certificate is valid. Also, be sure to check your shell environment to see if you have any time zone variables set.

Back to top

---

6. `GRAM Job submission failed bacause authentication failed: remote certificate has expired (error code 7)`

Diagnosis

This indicates that the remote host has an expired certificate.

To double-check, you can use grid-cert-info or grid-proxy-info. Use grid-cert-info on /etc/grid-security/hostcert.pem if you are dealing with a system level gatekeeper. Use grid-proxy-info if you are dealing with a personal gatekeeper.

Solution

If the host certificate has expired, use grid-cert-renew to get a renewal. If your proxy has expired, create a new one with grid-proxy-init.

Back to top

---

7. `GRAM Job submission failed because data transfer to the server failed (error code 10)`

Diagnosis

Check the $GLOBUS_LOCATION/var/globus-gatekeeper.log on the remote server. You will probably see something like:

```
Authenticated globus user: /O=Grid/O=Globus/OU=your.domain/OU=Your Name
Failure: globus_gss_assist_gridmap() failed authorization. rc =1
```

Solution

This indicates that your account is not in the grid-mapfile. Create the grid-mapfile in /etc/grid-security (or wherever the -gridmap flag in $GLOBUS_LOCATION/etc/globus-gatekeeper.conf points to) with an entry pairing your subject name to your user name. Review the Install Guide if you do not know how to do this.

Back to top

---

8. `GRAM Job submission failed because authentication failed: Expected target subject name="/CN=host/hostname" Target returned subject name="/O=Grid/O=Globus/CN=hostname.domain.edu" (error code 7)`

Diagnosis

New installations will often see errors like the above where the expected target subject name has just the unqualified hostname but the target returned subject name has the fully qualified domain name (e.g. expected is "hostname" but returned is "hostname.domain.edu").

This is usually becuase the client looks up the target host's IP address in /etc/hosts and only gets the simple hostname back.

Solution

The solution is to edit the /etc/hosts file so that it returns the fully qualified domain name. To do this find the line in /etc/hosts that has the target host listed and make sure it looks like:

```
xx.xx.xx.xx hostname.domain.edu hostname
```

Where "xx.xx.xx.xx" should be the numeric IP address of the host and hostname.domain.edu should be replaced with the actual hostname in question. The trick is to make sure the full name (hostname.domain.edu) is listed before the nickname (hostname).

If this only happens with your own host, see the explanation of the failed to open stdout error, specifically about how to set the `GLOBUS_HOSTNAME` for your host.

Back to top

---

9. `Problem with local credentials no proxy credentials: run grid-proxy-init or wgpi first`

Diagnosis

You do not have a valid proxy.

Solution

Run grid-proxy-init

Back to top

---

10. `GRAM Job submission failed because authentication failed: remote side did not like my creds for unknown reason`

Diagnosis

Check the $GLOBUS_LOCATION/var/globus-gatekeeper.log on the remote host. It probably says "remote certificate not yet valid". This indicates that the client host has a date set greater than five minutes in the future relative to the remote host.

Try typing "date -u" on both systems at the same time to verify this. (The "-u" specifies that the time should be displayed in universal time, also known as UTC or GMT.)

Solution

Ultimately, synchronize the hosts using NTP. Otherwise, unless you are willing to set the client host date back, you will have to wait until the remote server believes that your proxy is valid. Also, be sure to check your shell environment to see if you have any time zone variables set.

Back to top

---

11. `GRAM Job submission failed because the job manager failed to open stdout (error code 73)`

Or

`GRAM Job submission failed because the job manager failed to open stderr (error code 74)`

Diagnosis

The remote job manager is unable to open a connection back to your client host. Possible causes include:

- Bad results from globus-hostname. Try running globus-hostname on your client. It should output the fully qualified domain name of your host. This is the information which the GRAM client tools use to let the jobmanager on the remote server know who to open a connection to. If it does not give a fully qualified domain name, the remote host may be unable to open a connection back to your host.
- A firewall. If a firewall blocks the jobmanager's attempted connection back to your host, this error will result.
- Troubles in the ~/.globus/.gass_cache on the remote host. This is the least frequent cause of this error. It could relate to NFS or AFS issues on the remote host.
- It is also possible that the CA that issued your Globus certificate is not trusted by your local host. Running 'grid-proxy-init -verify' should detect this situation.

Solution

Depending on the cause from above, try the following solutions:

- Fix the result of 'hostname' itself. You can accomplish this by editing /etc/hosts and adding the fully qualified domain name of your host to this file. See how to do this in the explanation of the expected target subject error. If you cannot do this, or do not want to do this, you can set the `GLOBUS_HOSTNAME` environment variable to override the result of globus-hostname. Set `GLOBUS_HOSTNAME` to the fully qualified domain name of your host.
- To cope with a firewall, use the `GLOBUS_TCP_PORT_RANGE` environment variable. If your host is behind a firewall, set `GLOBUS_TCP_PORT_RANGE` to the allowable incoming connections on your firewall. If the firewall is in front of the remote server, you will need the remote site to set `GLOBUS_TCP_PORT_RANGE` in the gatekeeper's environment to the allowable incoming range of the firewall in front of the remote server. If there are firewalls on both sides, perform both of the above steps. Note that the allowable ranges do not need to coincide on the two firewalls; it is, however, necessary that the `GLOBUS_TCP_PORT_RANGE` be valid for both incoming and outgoing connections of the firewall it is set for.
- If you are working with AFS, you will want the .gass_cache directory to be a link to a local filesystem. If you are having NFS trouble, you will need to fix it, which is beyond the scope of this document.
- Install the trusted CA for your certificate on the local system.

Back to top

---

12. `GRAM Job submission failed because the provided RSL string includes variables that could not be identified (error code 39)`

Diagnosis

You submitted a job which specifies an RSL substitution which the remote jobmanager does not recognize. The most common case is using a 2.0 version of globus-job-get-output with a 1.1.x gatekeeper/jobmanager.

Solution

Currently, globus-job-get-output will not work between a 2.0 client and a 1.1.x gatekeeper. Work is in progress to ensure interoperability by the final release. In the meantime, you should be able to modify the globus-job-get-output script to use $(GLOBUS_INSTALL_PATH) instead of $(GLOBUS_LOCATION).

Back to top

---

13. `530 Login incorrect / FTP LOGIN REFUSED (shell not in /etc/shells)`

Diagnosis

The 530 Login incorrect usually indicates that your account is not in the grid-mapfile, or that your shell is not in /etc/shells.

Solution

If your account is not in the grid-mapfile, make sure to get it added. If it is in the grid-mapfile, check the syslog on the machine, and you may see the /etc/shells message. If that is the case, make sure that your shell (as listed in finger or chsh) is in the list of approved shells in /etc/shells.

Back to top

---

14. `globus_i_gsi_gss_utils.c:866: globus_i_gsi_gss_handshake: Unable to verify remote side's credentials: Couldn't verify the remote certificate`
`OpenSSL Error: s3_pkt.c:1031: in library: SSL routines, function SSL3_READ_BYTES: sslv3 alert bad certificate (error code 7)`

Diagnosis

This error message usually indicates that the server you are connecting to doesn't trust the Certificate Authority (CA) that issued your Globus certificate.

Solution

Either use a certificate from a different CA or contact the administer of the resource you are connecting to and request that they install the CA certificate in their trusted certificates directory.

---

15. `globus_gsi_callback.c:438: globus_i_gsi_callback_cred_verify: Could not verify credential: self signed certificate in certificate chain (error code 7)`

Or

`globus_gsi_callback.c:424: globus_i_gsi_callback_cred_verify: Can't get the local trusted CA certificate: Cannot find issuer certificate for local credential (error code 7)`

Diagnosis

This error message indicates that your local system doesn't trust the certificate authority (CA) that issued the certificate on the resource you are connecting to.

Solution

You need to ask the resource administrator which CA issued their certificate and install the CA certificate in the local trusted certificates directory.

---

16. `SSL3_GET_CLIENT_CERTIFICATE: no certificate returned`

Diagnosis

This error message indicates that the name in the certificate for the remote party is not legal according local signing_policy file for that CA.

Solution

You need to verify you have the correct signing policy file installed for the CA by comparing it with the one distributed by the CA.

---

17. `undefined symbol: lutil_sasl_interact`

Diagnosis

Globus replica catalog was installed along with MDS/Information Services.

Solution

Do not install the replica bundle into a GLOBUS_LOCATION containing other Information Services. The Replica Catalog is also deprecated - use RLS instead.

Back to top

Charles Bacon
Last modified: Tue Apr 23 10:21 CST 2002