GT 5.0.3 GSI-OpenSSH: User's Guide

GT 5.0.3 GSI-OpenSSH: User's Guide

Introduction

This is a guide for using the GSI-enabled OpenSSH client. It assumes that you (or your system administrator) have already installed the GSI OpenSSH and that you have also acquired a _user certificate_ from an appropriate _Certificate Authority_.

Table of Contents

List of Tables

Chapter 1. Using GSI-OpenSSH

1. Creating a proxy

First, set the GLOBUS_LOCATION environment variable to the location of your GSI-enabled OpenSSH installation. It may already be set for you by your system administrator.

Then, create a *proxy credential* for GSI authentication by running the **grid-proxy-init** program. This is your single sign-on to the Grid. By default, **grid-proxy-init** will create a proxy credential good for 12 hours.

To create a proxy credential with a different lifetime, use the **-hours** option.

For example:

```
% grid-proxy-init -hours 8
```

2. Deleting a proxy

To delete a proxy that was previously create with grid-proxy-init, run:

```
% grid-proxy-destroy
```

3. Getting authorized to connect to a site

Before you can connect to a site, the site needs to know the identity in your certificate so that it can map that identity to your local account. At a minimum, the site will need to know your subject name from your certificate. You can get your subject name by running **grid-cert-info** with the **-subject** argument. For example:

```
% grid-cert-info -subject
```

Email your subject name to the administrator of the system you wish to connect to so that they can add your entry to the appropriate authorization files.

Once you have your proxy credential, all you should have to do is run gsissh, providing it with the hostname of the host you want to connect to. For example:

```
% gsissh myhost.somedomain.edu
```

You should then find yourself automatically logged into your account on the remote system. If something goes wrong, please see Chapter 2, Troubleshooting for assistance.

GSI-OpenSSH Commands

The gsissh(1), gsiscp(1), and gsisftp(1) commands provide the same interfaces as the standard OpenSSH *ssh*, *scp*, and *sftp* commands, respectively, with the added ability to perform X.509 *proxy credential* authentication and delegation.

Name

gsissh -- Secure remote login

`gsissh`

Tool description

Use the *gsissh* command to securely login to a remote machine.

Command syntax

gsissh [-l login_name] hostname | user@hostname [command]

Name

gsiscp -- Secure remote file copy

```
gsiscp
```

Tool description

Use the *gsiscp* command to securely copy files to or from a remote machine.

Command syntax

gsiscp [-P port] [[user@]host1:]file1 [...] [[user@]host2:]destfile

Name

gsisftp -- Secure file transfer

`gsisftp`

Tool description

The *gsisftp* command provides an interactive interface for transferring files to and from remote machines.

Command syntax

gsisftp [[user@]host[:dir[/]]]

Chapter 2. Troubleshooting

Some common errors are listed below. If you need additional assistance, please run gsissh with the '-vvv' argument (specifying verbose output) and send the output to your system administrator for assistance.

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

1. Errors

Table 2.1. GSI-OpenSSH Errors

Error Code	Definition	Possible Solutions
`GSS-API error Failure acquiring GSSAPI credentials: GSS_S_CREDENTIALS_EXPIRED`	This means that your proxy certificate has expired.	Run grid-proxy-init to acquire a new proxy certificate, then run `gsissh` again.
`...no proxy credentials...`	Failing to run grid-proxy-init to create a user proxy with which to connect will result in the client notifying you that no local credentials exist. Any attempt to authenticate using GSI will fail in this case.	Verify that your GSI proxy has been properly initialized via grid-proxy-info. If you need to initialize the proxy, use the command grid-proxy-init.
`...bad file system permissions on private key; key must only be readable by the user...`	The host key that the SSH server is using for GSI authentication must only be readable by the user which owns it. Any other permissions will cause this error.	Make sure that the host key's UNIX permissions are mode 400 (that is, it should only have mode readable for the user that owns the file, and no other mode bits should be set).
`...gssapi received empty username; failed to set username from gssapi context; Failed external-keyx for <user> from <host> <port>...`	If the server was passed an "implicit username" (i.e. requested to map the incoming connection to a username based on some contextual clues such as the certificate's subject), and no entry exists in the grid-mapfile for the incoming connection's certificate subject, the server should output a clue that states it is unable to set the username against which to authenticate.	Add an entry for the user to the Section 1.2, "Gridmap file".
`...INTERNAL ERROR: authenticated invalid user xxx...`	If the subject name given in the system's grid-mapfile points to a non-existent user, the server will give an internal error which is best caught when it is running in debugging mode.	Add a new account to the system matching the username pointed at by the user's subject in the grid-mapfile.
`...gssapi received empty username; no suitable client data; failed to set username from gssapi context; Failed external-keyx for <user> from <host> <port>...`	Should the user attempt to connect without first creating a proxy certificate, or if the user is connecting via a SSH client that does not support GSI authentication, the server will note that no GSSAPI data was sent to it. Verify that the client is able to connect through another GSI service (such as the gatekeeper) to make sure that the user's proxy has been created correctly.	Verify that you are using a GSI-enabled SSH client and that your GSI proxy has been properly initialized via grid-proxy-info. If you need to initialize this proxy, use the command grid-proxy-init.

2. The gsissh command prompts you for a pass phrase when you run it

This could mean that you don't have a proxy certificate; try running **grid-proxy-init** and then running gsissh again. It could also mean that the GSI authentication is failing for some reason and gsissh is falling back to a different authentication mechanism. Reasons that it might fail include:

- The host you are connecting to does not have a GSI-enabled OpenSSH server.

- You are not authorized to use GSI authentication to the host. Contact the administrator.

Chapter 3. Debugging

For information about sys admin debugging, see .

1. Specifying verbose output

If you need additional assistance, please run gsissh with the '-vvv' argument (specifying verbose output) and send the output to your system administrator for assistance.

Chapter 4. Usage statistics collection

1. GSI-OpenSSH usage statistics collection

By default, the GSI-OpenSSH server (sshd) will send a UDP packet containing usage information to usage-stats.cilogon.org:4810 after serving each request. See the <u>Privacy Policy</u>[1] for details. You can see the Globus Usage Statistics policy <u>here</u>[2].

---

[1] http://grid.ncsa.illinois.edu/ssh/privacy.html
[2] /toolkit/docs/latest-stable/Usage_Stats.html

Glossary

C

Certificate Authority (CA)   An entity that issues certificates.

P

proxy credentials   The combination of a proxy certificate and its corresponding private key. GSI typically stores proxy credentials in `/tmp/x509up_u<`*`uid`*`>` , where <uid> is the user id of the proxy owner.

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 <u>this</u>.