

GT 4.2.0 Component Guide to Public Interfaces: GSI-OpenSSH

DRAFT

GT 4.2.0 Component Guide to Public Interfaces: GSI-OpenSSH

DRAFT

Table of Contents

I. Command line tools	?
gsssh	6
gsscp	7
gssftp	8
1. Configuring	1
2. Environment variable interface	2
1. Environmental variables for GSI-OpenSSH	2
A. Errors	3
Glossary	4

DRAFT

List of Tables

A.1. GSI-OpenSSH Errors 3

DRAFT

Command line tools

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.

DRAFT

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]

DRAFT

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`

DRAFT

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[/]]]

DRAFT

Chapter 1. Configuring

The GSI-enabled OpenSSH software is installed with a default set of configuration files, described below. You may want to modify the `ssh_config` file before using the clients and the `sshd_config` file before using the server.

If the GSI-enabled OpenSSH install script finds existing SSH key pairs, it will create symbolic links to them rather than generating new key pairs. The SSH key pairs are not required for GSI authentication. However, if you wish to support other SSH authentication methods, make sure the `sshd` (running as root) can read the key pair files (i.e., beware of NFS mounts with `root_squash`). If running multiple `sshd`s on a system, we recommend configuring them so they all use the same key pairs (i.e., use symbolic links) to avoid client-side confusion.

- `$GLOBUS_LOCATION/etc/ssh/moduli`
`moduli` is a crypto parameter for generating keys.
- `$GLOBUS_LOCATION/etc/ssh/ssh_config`
`ssh_config` contains options that are read by `ssh`, `scp`, and `sftp` at run-time. The installed version is the default provided by OpenSSH, with `X11Forwarding` enabled. You may need to customize this file for compatibility with your system SSH installation (i.e., compare it with `/etc/ssh/ssh_config`).
- `$GLOBUS_LOCATION/etc/ssh/ssh_host_key[.pub]`
Your system's RSA public-/private-key pair for SSH protocol 1 communications.
- `$GLOBUS_LOCATION/etc/ssh/ssh_host_dsa[.pub]`
Your system's DSA public-/private-key pair for SSH protocol 2 communications.
- `$GLOBUS_LOCATION/etc/ssh/ssh_host_rsa[.pub]`
Your system's RSA public-/private-key pair for SSH protocol 2 communications.
- `$GLOBUS_LOCATION/etc/ssh/ssh_prng_cmds`
`ssh_prng_cmds` contains paths to a number of files that `ssh-keygen` may need to use if your system does not have a built-in entropy pool (like `/dev/random`).
- `$GLOBUS_LOCATION/etc/ssh/sshd_config`
`sshd_config` contains options that are read by `sshd` when it starts up. The installed version is the default provided by OpenSSH, with `X11Forwarding` enabled. You may need to customize this file for compatibility with your system SSH installation (i.e., compare it with `/etc/ssh/sshd_config`). For example, to enable PAM authentication, you will need to set "UsePAM yes" in this file.

Chapter 2. Environment variable interface

1. Environmental variables for GSI-OpenSSH

The GSI-enabled OpenSSH needs to be able to find certain files and directories in order to properly function.

The items that OpenSSH needs to be able to locate, their default location and the environment variable to override the default location are:

- *Host key*

Default location: /etc/grid-security/hostkey.pem

Override with X509_USER_KEY environment variable

- *Host certificate*

Default location: /etc/grid-security/hostcert.pem

Override with X509_USER_CERT environment variable

- *Grid map file*

Default location: /etc/grid-security/grid-mapfile

Override with GRIDMAP environment variable

- *Certificate directory*

Default location: /etc/grid-security/certificates

Override with X509_CERT_DIR environment variable

Appendix A. Errors

Table A.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 <code>gssissh</code> again.
...no proxy credentials...	Failing to run <code>grid-proxy-init</code> 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 <code>grid-proxy-init</code> .
...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 <code>grid-mapfile</code> 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 <code>[grid-mapfile fixme link]</code> .
...INTERNAL ERROR: authenticated invalid user xxx...	If the subject name given in the system's <code>grid-mapfile</code> 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 <code>grid-mapfile</code> .
...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 <code>gatekeeper</code>) 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 <code>grid-proxy-init</code> .

