GT 5.2.4 Release Notes: GSI-OpenSSH

Table of Contents

1. Component Overview ........................................................................................................... 1
2. Feature summary .................................................................................................................. 1
3. Summary of Changes in GSI OpenSSH ............................................................................... 2
4. Fixed Bugs for GSI OpenSSH ............................................................................................ 2
5. Known Problems in GSI OpenSSH ..................................................................................... 2
6. Technology dependencies .................................................................................................... 2
7. Tested platforms .................................................................................................................. 2
8. Backward compatibility summary ....................................................................................... 2
9. Associated Standards .......................................................................................................... 3
10. For More Information ........................................................................................................ 3
Glossary .................................................................................................................................. 3

1. Component Overview

GSI-OpenSSH is a modified version of OpenSSH that adds support for X.509 *proxy certificate* authentication and delegation, providing a single sign-on remote login and file transfer service. GSI-OpenSSH can be used to login to remote systems and transfer files between systems without entering a password, relying instead on a valid *proxy credential* for authentication. GSI-OpenSSH forwards proxy credentials to the remote system on login, so commands requiring proxy credentials (including GSI-OpenSSH commands) can be used on the remote system without the need to manually create a new proxy credential on that system. For more information about GSI-OpenSSH, see the GSI-OpenSSH Home Page \(^1\).

2. Feature summary

Supported Features

- The `gsissh` command provides a secure remote login service with forwarding of X.509 *proxy credentials*.

- The `gsiscp` and `gsisftp` commands provide a secure file transfer service authenticated with X.509 proxy credentials, mimicking the `rcp/scp` and `ftp/sftp` commands.

- All standard OpenSSH features are supported, excluding Kerberos authentication. Kerberos authentication is *not* compatible with GSI-enabled OpenSSH.

- The GSI-OpenSSH server can replace the standard system SSH server in typical environments.

- If no username is given on the command-line, GSI-OpenSSH automatically determines the username that corresponds to the X.509 proxy *certificate subject* in the server’s `grid-map-file`.

Deprecated Features

- None

\(^1\) http://grid.ncsa.illinois.edu/ssh/
3. Summary of Changes in GSI OpenSSH

3.1. New Features: GSI OpenSSH
None.

3.2. Improvements: GSI OpenSSH
None.

4. Fixed Bugs for GSI OpenSSH
None.

5. Known Problems in GSI OpenSSH
None.

6. Technology dependencies
GSI-OpenSSH depends on the following GT components:

- GSI C

GSI-OpenSSH depends on the following 3rd party software:

- OpenSSH²

7. Tested platforms
Tested Platforms for GSI-OpenSSH

- Mac OS X 10.5
- x86/x86_64 GNU/Linux
- PPC AIX 5.3
- Sun4u Solaris 5.10

8. Backward compatibility summary
GSI-OpenSSH is backward compatible.

9. Associated Standards
Associated standards for GSI-OpenSSH:

² http://www.openssh.org/
• RFC 2743 GSSAPI
• RFC 2744 GSSAPI: C-bindings
• RFC 4462 GSSAPI Authentication and Key Exchange for the SSH Protocol

10. For More Information

See GSI-OpenSSH more information about this component.

Glossary

C
certificate subject An identifier for the certificate owner, e.g. "/DC=org/DC=doegrids/OU=People/CN=John Doe 123456". The subject is part of the information the CA binds to a public key when creating a certificate.

P
proxy certificate A short lived certificate issued using a 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/ProxyCertificateTypes.

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.

3 http://www.ietf.org/rfc/rfc2743.txt
4 http://www.ietf.org/rfc/rfc2744.txt
5 http://www.ietf.org/rfc/rfc4462.txt