

GT 5.0.0 MyProxy: Developer's Guide

GT 5.0.0 MyProxy: Developer's Guide

Introduction

Please refer to the [MyProxy Developer's Guide](http://myproxy.ncsa.uiuc.edu/devguide.html)¹ on the MyProxy web site.

¹ <http://myproxy.ncsa.uiuc.edu/devguide.html>

Table of Contents

1. Before you begin	1
1. Feature summary	1
2. Tested platforms	1
3. Backward compatibility summary	1
4. Technology dependencies	2
5. MyProxy Security Considerations	2
2. Usage scenarios	3
3. Tutorials	4
4. Architecture and design overview	5
5. Troubleshooting	6
1. Common GT Errors	6
2. Errors	7
3. Additional MyProxy Troubleshooting	9
6. Related Documentation	10
Glossary	11

List of Tables

5.1. MyProxy Errors	8
---------------------------	---

Chapter 1. Before you begin

1. Feature summary

Supported Features

- Users can obtain certificates and trust roots from the MyProxy CA using **myproxy-logon**.
- Users can store and retrieve multiple X.509 *proxy credentials* using **myproxy-init** and **myproxy-logon**.
- Users can store and retrieve multiple X.509 end-entity credentials using **myproxy-store** and **myproxy-retrieve**.
- Users and administrators can manage trustroots (CA certificates and CRLs) using **myproxy-logon** and **myproxy-get-trustroots**.
- Administrators can load the repository with X.509 end-entity credentials on the users' behalf using **myproxy-admin-load-credential**.
- Administrators can use the **myproxy-admin-adduser** command to create *user credentials* and load them into the MyProxy repository.
- Administrators can use the **myproxy-admin-addservice** command to create *host credentials* and load them into the MyProxy repository.
- Users and administrators can set access control policies on the credentials in the repository.
- If allowed by policy, job managers (such as Condor-G) can renew credentials before they expire.
- The MyProxy server enforces local site passphrase policies using a configurable external call-out.

Deprecated Features

- None

2. Tested platforms

Tested Platforms for MyProxy:

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

3. Backward compatibility summary

All MyProxy versions are fully backwards compatible.

4. Technology dependencies

MyProxy depends on the following GT component:

- [GSIC](#)

5. MyProxy Security Considerations

You should choose a well-protected host to run the myproxy-server on. Consult with security-aware personnel at your site. You want a host that is secured to the level of a Kerberos KDC, that has limited user access, runs limited services, and is well monitored and maintained in terms of security patches.

For a typical myproxy-server installation, the host on which the myproxy-server is running must have `/etc/grid-security` created and a *host certificate* installed. In this case, the myproxy-server will run as root so it can access the host certificate and key.

Chapter 2. Usage scenarios

Please refer to the [MyProxy User Guide](#)¹ for MyProxy usage scenarios.

¹ <http://myproxy.ncsa.uiuc.edu/userguide.html>

Chapter 3. Tutorials

There are no tutorials available at this time.

Chapter 4. Architecture and design overview

The MyProxy system architecture and design is described in the following two publications:

- J. Basney, M. Humphrey, and V. Welch. The MyProxy Online Credential Repository¹. Software: Practice and Experience, 2005.
- J. Novotny, S. Tuecke, and V. Welch. An Online Credential Repository for the Grid: MyProxy². Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10), IEEE Press, August 2001.

¹ <http://www.ncsa.uiuc.edu/~jbasney/myproxy-spe.pdf>

² <http://www.globus.org/alliance/publications/papers/myproxy.pdf>

Chapter 5. Troubleshooting

1. Common GT Errors

For a list of common errors in GT, see [Error Codes](#).

2. Errors

Table 5.1. MyProxy Errors

Error Code	Definition	Possible Solutions
MyProxy server name does not match expected name	<p>This error appears as a mutual authentication failure or a server authentication failure, and the error message should list two names: the expected name of the MyProxy server and the actual authenticated name.</p> <p>By default, the MyProxy clients expect the MyProxy server to be running with a host certificate that matches the target hostname. This error can occur when running the MyProxy server under a non-host certificate or if the server is running on a machine with multiple hostnames.</p> <p>The MyProxy clients authenticate the identity of the MyProxy server to avoid sending passphrases and credentials to rogue servers.</p> <p>If the expected name contains an IP address, your system is unable to do a reverse lookup on that address to get the canonical hostname of the server, indicating either a problem with that machine's DNS record or a problem with the resolver on your system.</p>	<p>If the server name shown in the error message is acceptable, set the <code>MYPROXY_SERVER_DN</code> environment variable to that name to resolve the problem.</p>
Error in bind(): Address already in use	<p>This error indicates that the <code>myproxy-server</code> port (default: 7512) is in use by another process, probably another <code>myproxy-server</code> instance. You cannot run multiple instances of the <code>myproxy-server</code> on the same network port.</p>	<p>If you want to run multiple instances of the <code>myproxy-server</code> on a machine, you can specify different ports with the <code>-p</code> option, and then give the same <code>-p</code> option to the MyProxy commands to tell them to use the <code>myproxy-server</code> on that port.</p>
grid-proxy-init failed	<p>This error indicates that the <code>grid-proxy-init</code> command failed when <code>myproxy-init</code> attempted to run it, which implies a problem with the underlying Globus installation.</p>	<p>Run <code>grid-proxy-init -debug -verify</code> for more information.</p>
User not authorized	<p>An error from the <code>myproxy-server</code> saying you are "not authorized" to complete an operation typically indicates that the <code>myproxy-server.config</code> file settings are restricting your access to the <code>myproxy-server</code>. It is possible that the <code>myproxy-server</code> is running with the default <code>myproxy-server.config</code> file, which does not authorize any operations.</p>	<p>See Configuring MyProxy for more information.</p>

Error Code	Definition	Possible Solutions
Unable to verify remote side's credentials	An error saying "Unable to verify remote side's credentials," "Couldn't verify the remote certificate," or "alert bad certificate" often indicates that the client or server's certificate is signed by an untrusted Certification Authority (CA). The client must have a CA certificate and signing policy file installed in <code>/etc/grid-security/certificates</code> for the CA that signed the server's certificate. Likewise, the server must have a CA certificate and signing policy file installed in <code>/etc/grid-security/certificates</code> for the CA that signed the client's certificate.	See Configuring Certificates for more information.

3. Additional MyProxy Troubleshooting

For additional information, see the [MyProxy Troubleshooting Page](#)¹ at NCSA.

¹ <http://myproxy.ncsa.uiuc.edu/troubleshooting.html>

Chapter 6. Related Documentation

For additional information about MyProxy, see the [MyProxy Project Home Page](http://myproxy.ncsa.uiuc.edu/)¹ at NCSA.

¹ <http://myproxy.ncsa.uiuc.edu/>

Glossary

H

host certificate An EEC belonging to a host. When using GSI this certificate is typically stored in `/etc/grid-security/hostcert.pem`. For more information on possible host certificate locations see the [GSI C Developer's Guide](#).

host credentials The combination of a host certificate and its corresponding private key.

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 credentials The combination of a user certificate and its corresponding private key.