GT 5.0.1 MyProxy: Developer's Guide

Introduction

Please refer to the MyProxy Developer's Guide\(^1\) 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:

- GSI C

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:


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

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Definition</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MyProxy server name does not match expected name</strong></td>
<td>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. 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. The MyProxy clients authenticate the identity of the MyProxy server to avoid sending pass-phrases and credentials to rogue servers. 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.</td>
<td>If the server name shown in the error message is acceptable, set the MYPARTY_SERVER_DN environment variable to that name to resolve the problem.</td>
</tr>
<tr>
<td><strong>Error in bind(): Address already in use</strong></td>
<td>This error indicates that the myproxy-server port (default: 7512) is in use by another process, probably another myproxy-server instance. You cannot run multiple instances of the myproxy-server on the same network port.</td>
<td>If you want to run multiple instances of the myproxy-server on a machine, you can specify different ports with the -p option, and then give the same -p option to the MyProxy commands to tell them to use the myproxy-server on that port.</td>
</tr>
<tr>
<td><strong>grid-proxy-init failed</strong></td>
<td>This error indicates that the grid-proxy-init command failed when myproxy-init attempted to run it, which implies a problem with the underlying Globus installation.</td>
<td>Run grid-proxy-init -debug -verify for more information.</td>
</tr>
<tr>
<td><strong>User not authorized</strong></td>
<td>An error from the myproxy-server saying you are &quot;not authorized&quot; to complete an operation typically indicates that the myproxy-server.config file settings are restricting your access to the myproxy-server. It is possible that the myproxy-server is running with the default myproxy-server.config file, which does not authorize any operations.</td>
<td>See Configuring MyProxy for more information.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Definition</td>
<td>Possible Solutions</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unable to verify remote side's credentials</td>
<td>An error saying &quot;Unable to verify remote side's credentials,&quot; &quot;Couldn't verify the remote certificate,&quot; or &quot;alert bad certificate&quot; 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 /etc/grid-security/certificates for the CA that signed the server's certificate. Likewise, the server must have a CA certificate and signing policy file installed in /etc/grid-security/certificates for the CA that signed the client's certificate.</td>
<td>See Configuring Certificates for more information.</td>
</tr>
</tbody>
</table>

### 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\footnote{http://myproxy.ncsa.uiuc.edu/} at NCSA.
# Glossary

## H

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host certificate</td>
<td>An EEC belonging to a host. When using GSI this certificate is typically stored in <code>/etc/grid-security/hostcert.pem</code>. For more information on possible host certificate locations see the <a href="#">GSI C Developer's Guide</a>.</td>
</tr>
<tr>
<td>host credentials</td>
<td>The combination of a host certificate and its corresponding private key.</td>
</tr>
</tbody>
</table>

## P

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy credentials</td>
<td>The combination of a proxy certificate and its corresponding private key. GSI typically stores proxy credentials in <code>/tmp/x509up_u&lt;uid&gt;</code>, where <code>&lt;uid&gt;</code> is the user id of the proxy owner.</td>
</tr>
</tbody>
</table>

## U

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user credentials</td>
<td>The combination of a user certificate and its corresponding private key.</td>
</tr>
</tbody>
</table>