Table of Contents

glite-PX

Functional description

The gLite distribution of the MyProxy server.

MyProxy is a standalone server which manages proxy renewal to avoid the need for long lived proxies.

Daemons running

- /opt/globus/sbin/myproxy-server -c /etc/myproxy-server.config --verbose

Init scripts and options (start|stop|restart|...)

- /etc/init.d/myproxy (start|stop|status)

Configuration files location with example or template

- /opt/globus/share/myproxy/myproxy-server.config

Logfile locations (and management) and other useful

MyProxy logs to syslog with the **LOG_DAEMON** facility.

Messages from myproxy-server are prefixed with the string 'myproxy-server' (configurable).

Open ports

- http://jra1mw.cvs.cern.ch:8180/cgi-bin/jra1mw.cgi/org.glite.site-info.ports/doc/?only_with_tag=HEAD

Possible unit test of the service

myproxy-init from a UI;

- $ myproxy-init -s my.proxy.server -d -n

Where is service state held (and can it be rebuilt)

Proxies and meta-data are stored in

- /var/myproxy

Cron jobs

- /etc/cron.daily/myproxy.cron

Security information

Access control Mechanism description (authentication & authorization)

Access is controlled by a single configuration file (/etc/myproxy-server.config). Detailed information can be found at (http://grid.ncsa.uiuc.edu/myproxy/authorization.html)

Who can store credentials?

The acccept_credentials policy sets the policy for who can store credentials based on the clients SSL/TLS authenticated identity.

Who can modify or get information about stored credentials?

Only the credential owner can overwrite, remove or get information about stored credentials. The authenticated SSL/TLS identity must match the identity of the stored credentials

Who can retrieve a delegated credential?

For more details, please check again http://grid.ncsa.uiuc.edu/myproxy/authorization.html.

The access is controlled by a concatenation of administrator's set of policies (myproxy-server.config) and credential's owner policies (defined by myproxy-init/myproxy-store parameters). The client must satisfy one of the following:

- Client's identity matches the myproxy-server.config authorized_retreivers policy AND the possibly owner's defined one or (if none was set but owner) the myproxy-server.config default_retrievers policy
- Client's identity matches the myproxy-server.config authorized_renewers policy and the owner's defined one or (if none was set by the owner) the myproxy-server.config default_renewers policy
- Client's identity matches the myproxy-server.config trusted_retrievers and authorized_retrievers policies and the owner's set defined one's (or the default policies at myproxy-server.config)

Who can directly retrieve a credential?

The client's identity must satisfy the policies for delegated retrieval AND also match the myproxy-server.config authorized_key_retrievers policy. If the owner has defined a authorized_key_retrievers policy the client's identity must also satisfy it.

How to block/ban a user

The MyProxy accepted_credentials_mapapp call-out is passed the certificate subject and username of a credential to be stored and may return zero to allow and nonzero to deny the request. To block a user from storing credentials, define an accepted_credentials_mapapp call out program that consults a banned user list and returns nonzero to deny requests by banned users.

For the case where a banned user has already stored credentials and you want to deny access to the credentials, myproxy-admin-query enables the administrator to find the credentials and either remove them or "lock" them.

Network Usage

Two services are running that need network access on this node-type.

- the MyProxy server service. The server binds to the 7512/tcp port.
- the Resources BDII service. As (almost) all gLite services MyProxy has a resource BDII to advertise its endpoint and its capabilities. The resource BDII binds to the 2170/tcp port.

Firewall configuration

The proposed firewall configuration is to deny access to anyhost/anyport and allow:

- 7512/tcp incoming traffic from the subnets that this server is servicing (probably anyhost)
- 2170/tcp from the local site-BDII service
- Any other administration required port for the administration subnet/interface (i.e. 22/tcp (ssh))

Security recommendations

No stipulation

Security incompatibilities

No stipulation

List of externals (packages are NOT maintained by Red Hat or by gLite)

The following packages from the Scientific Linux CERN repository are included to the MyProxy RPM list:

- openldap-servers
- perl-Convert-ASN1
- perl-URI
- perl-libwww-perl

The following packages from the DAG repository are included to the MyProxy RPM list:

- perl-HTML-Parser
- perl-HTML-Tagset
- perl-IO-Socket-SSL
- perl-LDAP
- perl-Net-SSLeay
- perl-XML-NamespaceSupport
- perl-XML-SAX

Other security relevant comments

As MyProxy service is usually hosting valid credentials it is required that logs, network activities and local (physical) access are monitored.

Utility scripts

The config file /etc/myproxy-server.config is actually generated from $EDG_LOCATION/etc/edg-myproxy.conf in the following way;

- /etc/rc.d/init.d/myproxy-generate-config.pl $CERTDIR $X509_USER_CERT $EDG_LOCATION/etc/edg-myproxy.conf $CONFIG

Location of reference documentation for users

Troubleshooting advice is available here;

- http://grid.ncsa.uiuc.edu/myproxy/troubleshooting.html

Location of reference documentation for administrators

- http://grid.ncsa.uiuc.edu/myproxy/

This topic: EGEE > GlitePX
Topic revision: r12 - 2009-06-30 - GianniPucciani