



EUROPEAN MIDDLEWARE INITIATIVE

PROXYRENEWAL 1.X – ADMINISTRATOR GUIDE

Document version:	1.0.0-1
EMI Component Version:	1.x
Date:	April 20, 2011

CONTENTS

1 INTRODUCTION	3
2 GLITE-PROXYRENEW COMMAND OVERVIEW	3
3 GLITE-PROXYRENEW COMMAND OVERVIEW	5

1 INTRODUCTION

The proxy renewal daemon runs as an internal component of the WMS node, which is responsible for keeping proxy certificates valid throughout all the lifetime of corresponding jobs. The daemon maintains a repository of proxy certificates that have been registered by the WMS for renewal. After successful registration of a proxy, the WMS refers to the repository file whenever it needs access the proxy of a particular job. When the finishes the WMS unregisters the proxy from the repository.

The proxy renewal daemon uses a simple text-based protocol to communicate with the clients (i.e., the WMS components). The communication is done over a local unix socket entirely. The renewal daemon do not expose any network interface. In order for the clients to be able to communicate over the socket and access the proxies from the repository, they have to run under the same unix id as the renewal daemon. By default, the glite user account is used as the common service user.

In order to keep the proxy certificates, the renewal daemon periodically contacts a MyProxy server and retrieves a fresh proxy. Therefore, for the renewal mechanism to be working, the users have to store their credentials in a MyProxy server first. When contacting the MyProxy server, the renewal daemon authenticates itself using an X.509 certificate and key (usually the WMS credentials). The configuration of the MyProxy server has to allow renewal requests done with these credentials.

When VOMS attributes are renewed the renewal daemon uses credentials of the user, thus the process resembles the common way how VOMS attributes are obtained and no special authorization is needed on the VOMS server side.

The renewals are attempted well before a proxy is about to expire. If an attempt fails, other ones are triggered until either one of them succeeds or the proxy expires. If a proxy cannot be renewed, its record is removed from the repository. Information about renewal attempts are logged via syslog, additional detailed information can be enabled using the `-d` switch.

The repository used by the proxy renewal daemon is a directory containing all registered proxy certificates along with some additional information. Names of the files always start with a hash computed from the X.509 subject name of the proxy. Besides the actual credentials, the daemon stores for each registered proxy also a list of job identifiers identifying jobs that were submitted with the related identity. In order to decrease the management overheads, the renewal daemon aggregates multiple proxy certificates of the same identity into a single proxy in the repository. Using this precaution decreases the number of renewal attempts and overall management operations.

2 GLITE-PROXYRENEW COMMAND OVERVIEW

NAME

glite-proxy-renew - simple client for the proxy renewal daemon.

SYNOPSIS

glite-proxy-renew -j <jobid> [options] command

DESCRIPTION

glite-proxy-renew communicates with the proxy renewal daemon and allows administrators to check its functions correctly. It is not meant to be used regularly.

COMMANDS

start Register a proxy with the renewal daemon to keep it renewed. The name of the file from the repository is returned as the result. The **-f FILE**, **--file FILE** option must be given.

stop Unregisters a proxy from the renewal repository. The proxy file will be removed.

get Lookup the renewal repository to find whether a proxy for the jobid is registered. If found, the command returns the filename from the repository.

OPTIONS

-f FILE, **--file FILE** Specifies the filename containing the proxy certificate that should be renewed.

-h, **--help** Display a list of valid options.

-j JOBID, **--jobid JOBID** Specifies the job id that is uniquely tied with the proxy. This option is obligatory and is required for all commands.

-p PORT, **--port PORT** Specifies port of the MyProxy server, which should be used to renew the proxy.

-s SERVER, **--server SERVER** Specifies the name of the MyProxy server, which should be used to renew the proxy.

-v, **--version** Display the version of the proxy renewal daemon.

FILES

/tmp/dgpr_renew_<uid> A unix socket used to talk to the daemon. It is created the daemon upon its start

ENVIRONMENT

GLITE_PR_TIMEOUT Sets the maximum number of seconds that the daemon is given to answer a request done over the unix socket. The default value is 120 seconds.

BUGS

Please

report all bugs to the gLite bug tracking system available at <https://gus.fzk.de>

SEE ALSO

glite-proxy-renewd(8)

AUTHOR

EU EGEE, EU EMI

3 GLITE-PROXYRENEW COMMAND OVERVIEW

NAME

glite-proxy-renewd - proxy renewal daemon

SYNOPSIS

glite-proxy-renewd [*options*]

DESCRIPTION

glite-proxy-renewd registers X.509 proxy certificates and periodically renews them using a MyProxy repository.

OPTIONS

- A DIR, --VOMSdir DIR** Renew also VOMS attributes if they are embeded in the renewed proxy. If the option is given, the renewal daemon will retrieve a fresh copy of the VOMS attributes and place it inside the new proxy.
- C DIR, --CAdir DIR** An alternative directory with trusted root anchors. This option overrides the **\$X509_USER_DIR** environment variable.
- c NUM, --condor-limit NUM** Specifies how many *NUM* seconds before expiration of a proxy should the renewal process be started. It defaults to 1800 seconds.
- d, --debug** Don't daemonize and start logging to stdout. Increased level of debugging is enabled, too.
- G FILE, --voms-config FILE** An alternative location of the VOMS configuration.
- h, --help** Display a list of valid options.
- k FILE, --key FILE** Get certificate from *FILE*. This option overrides the **\$X509_USER_CERT** environment variable.
- O, --order-attributes** Make sure that the order of renewed VOMS attributes is retained. Enabling this option may cause crashes of old VOMS servers (older than 1.8.12).
- r DIR, --repository DIR** All registered proxies and corresponding metadata will be stored in *repository*. The directory must exist and be writeable by the proxy renewal daemon.
- t FILE, --cert FILE** Get private key from *FILE*. This option overrides the **\$X509_USER_KEY** environment variable.

-V DIR, --VOMSdir DIR An alternative directory with trusted VOMS certificates

-v, --version Display the version of the proxy renewal daemon.

FILES

/tmp/dgpr_renew_<uid> A unix socket used to talk to the daemon. It is created the daemon upon its start

proxy repository A directory containing all the registered proxy certificates and additional meta-data.

There is no configuration file used the proxy renewal daemon.

ENVIRONMENT

GLITE_PR_TIMEOUT Sets the maximum number of seconds that the daemon can spend on serving the client over the unix socket. The default value is 120 seconds.

Also, standard globus variables are honoured:

X509_USER_KEY If **\$X509_USER_KEY** is set, it is used to locate the private key file.

X509_USER_CERT If **\$X509_USER_CERT** is set, it is used to locate the certificate file.

X509_CERT_DIR If **\$X509_CERT_DIR** is set, it is used to locate trusted CA's certificates and ca-signing-policy files.

BUGS

Please report all bugs to the gLite bug tracking system available at <https://gus.fzk.de>

SEE ALSO

glite-proxy-renew(1)

AUTHOR

EU EGEE, EU EMI