Table of Contents

LCG File Catalog

Functional description

See LFC General Description

Daemons running

- /opt/lcg/bin/lfc-dli
- /opt/lcg/bin/lfcdaemon

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

- /etc/init.d/lfc-dli {start|stop|status|restart|condrestart}
- /etc/init.d/lfcdaemon {start|stop|status|restart|condrestart}

Configuration files location with example or template

See LFC Configuration

- /opt/lcg/etc/NSCONFIG
- /opt/lcg/etc/lcg-dm-mapfile
- /etc/sysconfig/lfcdaemon
- /etc/sysconfig/lfc-dli
- /etc/shift.conf

Logfile locations (and management) and other useful

- /var/log/lfc/log
- /var/log/dli/log

Open ports

- LFC server daemon, the port 5010 has to allow incoming TCP connections from clients. (Usually from any site)
- If the LFC Data Location Interface (DLI) is deployed, the port 8085 also has to accept incoming TCP connection from clients.

Possible unit test of the service

UI , WN and itself

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

Cron jobs

None

Security information

Access control Mechanism description (authentication & authorization)

Concerning the LFC: LFC authentication uses an internal security layer which as deployed in WLCG usually* authenticates using globus's GSI GSS interface along with VOMS. Authentication is successful when a valid GSI handshake is performed and passes GSI's checks. If VOMS extensions are found they must be valid and not expired. (VOMS information is checked and extracted using the C glite-security-voms-api-cpp API).

Authorization is based on a numeric UID and a number of numeric GIDs. The UID is derived from the DN string. The first time a DN is encountered it is mapped to an unused UID. The GIDs are similarly mappings of VOMS FQANs which may be present in the user's certificate. If no VOMS FQANs are present a lookup is made using a flat file which is periodically rebuilt on the service machine (usually /opt/lcg/etc/lcgdm-mapfile). The file maps DN to a group name. If there is no mapping entry in the file and no VOMS FQANs authentication fails.

The access control follows a posix like model where the UID and GID(s) are checked on the entries in the LFC, which are presented in a similar way as files and directories in a posix filesystem.

Concerning the DLI: The DLI is a thin service in front of the LFC server which can accept SOAP queries, pass them to the LFC service, receive the reply and return a suitable SOAP reply to the client. The query is limited to a "replica lookup" query based on an LFN. The DLI service has no authentication and no authorization checks. The queries is passed to the backend LFC as a privileged query - if the entry exists the lookup is expected to succeed.

* a weaker form of authentication is available in some situations. Where a host (sometimes a vobox) is denoted as "trusted" in /etc/shift.conf there are two possibilities whereby the client can specify the name and group list to be mapped to numeric IDs within the LFC client-server protocol itself: (1) the client uses GSI but presents a host certificate which matches the name within the trusted entry in the server's /etc/shift.conf file and for which the client's reserve DNS matches, or (2) The client specified the "ID" protocol within the LFC client-server protocol and the client's forward confirmed hostname (i.e. found by a reverse followed by a forward lookup in which the forward lookup has to match the client's IP address) matches the trusted entry in /etc/shift.conf.

How to block/ban a user

The service provides no explicit mechanism to deny a user at the authentication or authorization stages.

Using the usual posix rules it may be possible to deny the user access to available directories within the catalog.

At the GSI layer authentication can be denied via the globus CRL mechanism. Users without VOMS extensions in their certificate can will also fail authentication if they have no entry in the mapping file.

Network Usage

Cf. Ganglia graphs, e.g.:
http://gridmon.fzk.de//gridka-adminserver/?r=hour&s=by%2520hostname&m=load_one&c=a01-008&h=lfc-2-fzk.gric

Firewall configuration

Due to the LFC server daemon, port 5010 is open, due to the LFC Data Location Interface (DLI), port 8085 is open.
There's also the connection between front-end(s) and database back-end. The database back-end may or may

not reside on the same machine(s) which run LFC servers. Supported database back-ends include mysql, Oracle and potentially postgreSQL (although as of writing postgresql is not deployed).

Security recommendations

Do not run the DLI service unless required.

Security incompatibilities

None known.

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

vdt_globus_essentials

Other security relevant comments

As usual for services using GSI and VOMS CA certificate files, signing policies, CRLs and VOMS server information have to be maintained on the service host, usually in /etc/grid-security/.

The LFC service requires a service certificate of type "host" (or without service name qualification, as is usual with globus GSI), to allow the client to authenticate the identity of the server using the globus GSI layer.

Utility scripts

None

Location of reference documentation for users

- See LFC General Description

Location of reference documentation for administrators

- See LFC Admin Guide

This topic: EGEE > GliteLFC
Topic revision: r12 - 2009-04-27 - DavidSmith