Table of Contents

AMGA Service Reference Card

Functional description

AMGA is the ARDA Metadata Grid Application, the metadata catalog service of EMI. It can be used to store metadata about different types of data, e.g files and job properties.

A metadata is a list of attributes associated with entries. An attribute is a key/value pair with a type (SQL type) associated to it. A schema is a set of attributes. A collection is a set of entries associated with a schema. Schemas can be modified at runtime. Metadata are organised in a filesystem-like hierarchy: collection (directory) and entry (file). The catalog can be queried with an SQL-like language or a navite SQL language. AMGA has been designed specifically for being multipurpose, scalable and fault tolerant (through DB replication).

C++, Shell, Python and Java API are provided as well as an interactive console where commands can be issued like in a DB console.

Services running

- /usr/bin/amgad
- /usr/bin/mdrepdaemon

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

- /etc/init.d/mdservice

Configuration files location with example or template

- AMGA Server : /etc/amgad.config
- AMGA Client : /etc/mdclient.config

Logfile locations (and management) and other useful audit information

- /var/log/amgad.log

Open ports

- 8822, Connections from AMGA clients

Possible unit test of the service

- N/A. However, the source tar ball includes some functionality test sets at the test directory

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

The service state is held in the RDBMS.

Security information

Access control Mechanism description (authentication & authorization)

Authentication & Authorization

Authentication can be done via a certificate or a password. After the authenticity of a user is established in the handshaking of the client with the server, the client needs to be authorized to use the role of a certain user. Authorization is optional, if authorization is not enabled for the server, any authenticated user can assume any role he wishes. Authorization is controlled via the amgad.config configuration.

Authorization can be done via certificates or passwords, both must be explicitly enabled. For authentication via certificates to work, both the server and the client must have SSL enabled. Four ways are foreseen to accessing the necessary information to match user names with their credentials, one or more must be enabled for Authorization to work:

- A grid-map file mapping certificate subjects that is distinguished names to users. This is a static setup and no new users can be added at runtime. No password authorization is possible via a grid map file.
- A user database using the database backend. This allows creation of users and the management of their credential at runtime. This is the only option which allows password based login.
- Authorization using a VOMS. All users registered with a VO will be assigned to the user specified here. You can give several VOMS-URL user pairs here.
- Authorization via VOMS certificates. All users connecting with a VO information-enriched certificate obtained via voms-proxy-init will be assigned to specific AMGA users depending on the role within the VO.

Note that only the DB based user management module is able to make changes to the user setup. If you have several user management modules activated at the same time, then listing users and checking their credentials for authorization will go through the users in all of the modules. A user is authorized as soon as he has been found in any of the modules.

Access Control Lists

ACLs (Access Control Lists) can be assigned to any directory.

The following commands exist to manipulate ACLs of a directory;

- acl_add directory group rights
- acl_remove directory group: You can use the to remove all ACLs of a directory
- acl_show directory

Permission Handling

- whoami : Prints out the name of the current user. Note that this command does not need any connections of the AMGA server and can thus be also used to do a test on whether an AMGA server is alive and what response time it has.
- chown entry/dir new_owner: Changes the owner of a directory or entry. Only the owner of an entry is allowed to execute this, or the root-user. chown does not check whether the user exists, since user management is considered to be handled outside of AMGA.
- chmod entry/dir new_permissions: Changes the access permissions of an entry or directory. Entries have owner and group-permissions, while directories have owner permissions and group permissions are handled via ACLs. Group permissions for entries allow you to remove privileges granted for all entries in a directory via the directories ACLs. The format of new_permissions is rwxrwx for entries and rwx for directories where "-"-signs can be substituted for the letters if you do not want to give a certain privilege. The permissions for entries are the concatenation of first the user and then the group rights. The x-Flag allows a user to enter a directory or respectively list an entry. r-and w-flags allow

users to read/write metadata while the w-flag for directories allows users to create or delete entries in the given directory. Users cannot list directories for which they don't have read permissions. The command works also for patterns and uses a transaction.

How to block/ban a user

For gridmapfile based authentication, you can do as explained in: How to ban/blacklist user on CE and SE

Network Usage

Nothing reported.

Firewall configuration

Here are informations on glite related traffic that should be authorized: link

Security recommendations

To ease the security monitoring and the expansion of attacks, it's strongly recommended to run the server in a dedicated machine (virtualization technology can help there).

If the server is deployed for grid users, it's recommended to use only certificates for authentication.

Security incompatibilities

Nothing reported.

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

Nothing reported.

Other security relevant comments

Nothing reported.

Location of reference documentation for users

- AMGA Home page

Location of reference documentation for administrators

- AMGA Home page

This topic: EMI > AMGAreference
Topic revision: r1 - 2011-04-20 - unknown