GGF8 Authorization Report and Issues

Andrew McNab, University of Manchester

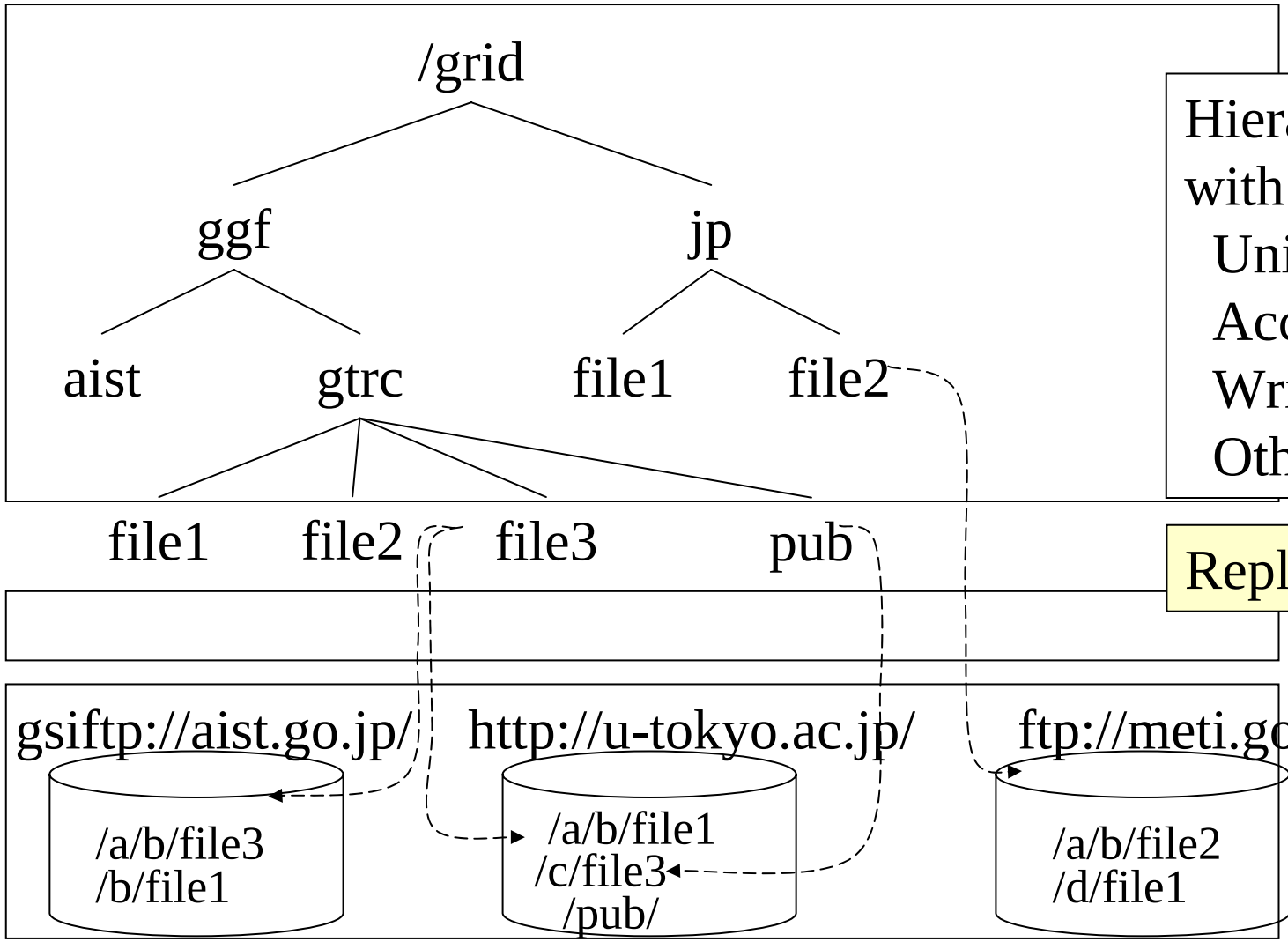
mcnab@hep.man.ac.uk

Outline

- Grid Filesystems BOF
- Authorization Working Group
- OGSA Working Group BOF
- Further OGSA Authz discussion
- XACML

Grid Filesystems BOF

- BOF led by Osamu Tatebe <o.tateba@aist.go.jp>



Virtual Filesystem Directory Service

Hierarchical namespace with filesystem metadata
- Unique path name
- Access control
- Write lock
- Other metadata

Replica Location Service

File Transport Service

Grid Filesystems RG proposed charter

- "Grid File System Research Group explores issues related to file system data in grid computing environment. We are interested in the possibility of federating namespace of existing physical file system, and individual files, and managing files through the application of service oriented architecture for file system infrastructure and objects. The objective of the group is to provide a forum for discussing approaches to facilitate file sharing and to promote the use of common services provided by other working groups.
- Initially, the proposed research group aims to identify the requirements and functionalities for Grid file systems. To achieve this goal, we undertake the following tasks:
- Survey research projects and products related to the Grid and wide-area filesystems.
- Organize and document requirements of Grid filesystems from application's perspective."

Authorization Working Group

- Nearing completion of Authorization Framework document
- This presents a general way of describing and classifying authorization systems
- Includes some examples
- and application of framework to existing authorization systems
- Makes it possible to describe key features of a system in a couple of sentences
- "EDG is moving to a Push Model system, based on group Attribute Authorities (VOMS) and Authorization Decision Servers/Functions at each site (LCAS plugins.)"
- Further work on standardisation probably as part of OGSA Authz WG.

OGSA Authorization WG BOF

- The objective of the OGSA Authorization WG is define the specifications needed to allow for interoperability and pluggability of authorization components in OGSI services. This will include the following documents:
- An OGSI authorization requirements document discussing what scenarios need to be addressed and what the requirements of those scenarios are. This document should build off of the work done by the Authorization Frameworks and Mechanisms group.
- A specification for an OGSA authorization service which can render authorization decisions on actions regarding OGSI services. This should include at least one profile of how such a service would be implemented with a standard mechanisms (e.g., SAML).
- A specification for an OGSA authorization language. While implementations of various servics may use internal representations of policy, this specificaiton will define at least one language for exchange of authorization policy based on a existing standard (e.g., XACML).

OGSA Authorization further discussion

- 1) Decision Callout Protocol/Interface (Authz Query and Reply) Where called from? What is included? Conditions, Obligations Format of Authorization Decisions
- 2) Attribute assertion format (and Roles?), SAML<->other representations
- 3) Policy Statements/Language Format, Identifying authorities for attribute requests, (G)ACL formats, SAML<->XACML transformations
- 4) External repositories for attribute assertions
- 5) Authorization information privacy and confidentiality requirements
- 6) OGSA Authorization Scenarios

XACML

- "eXtensible Access Control Markup Language"
- OASIS standard as of Feb 2003
- Allows for many types of complicated policy, but supporting it all probably too much for what we need.
- So agree GACL-like subset instead?
- "Son of GACL", SACML? ("Simple ACML"), GACML? ("Grid ACML")
- Do this within OGSA Authz context?