

BNL Site-AAA requirements for OSG-0 (February 2005)

Version 0.1 (newer versions posted at <http://grid.racf.bnl.gov/siteAAA/publications/>)

Gabriele Carcassi, Shigeki Misawa, Razvan Popescu, Jason Smith, Tom Throwe, Dantong Yu, Xin Zhao

Preamble

We are not trying to address here the final solution for Grid authorization: this is meant as an intermediate system which is a step forward from what we currently have on Grid3. This set of requirements applies to the system we would like to see in production at BNL by February 2005 and for the next year. The fall-back solution is what is currently used in Grid3.

This document doesn't address the VO services provided by BNL.

Use cases

Centralized grid identity mapping of grid resources for BNL

Allow a resource administrator to set a site wide policy for mapping certificate to local accounts.

An XML policy will be used by GUMS to decide how to implement the mapping. The mapping will be propagated to the gatekeepers either through a grid-mapfile or through a callout.

Provide accountability for grid jobs.

An administrator can examine a job and determine with which certificate it was submitted.

It will be implemented by assigning an account to each Grid identity. The only exception might be some special role accounts (i.e. production leader) that come in with role based authentication. The gatekeeper logs will maintain the past mappings between the Grid identity and the local identity for auditing purposes.

Use a static pool of accounts for generic grid access

A generic grid user will be assigned a precreated account. Every time the user will come back to the site, the same account will be used. Only that user will be using that account.

GUMS will be given the set of usernames that are in the pool. GUMS will assign them to the users either at the grid-mapfile generation or, if using the callout, at the user's first access to the site.

The accounts won't be recycled, that is the account lease will be indefinite: cleaning an account has several issues, both at site and application levels, which we don't expect to resolve by February. Account cleaning will be crucial to handle a high volume of users. The current number of grid3 users is 138 which, even assuming an explosive growth of 1000% in a year, is still manageable. After this new set of requirements will be in production we will concentrate on the problem of account cleanup.

To avoid running out of accounts, GUMS will have to monitor when the pool usage has reached 90% and contact the administrator.

Allow people who have an account at BNL to use it instead of the generic grid access one

Some users do have a user account at BNL and they should be allowed to use it for grid jobs. As a default, they will be mapped to an account from the pool, but they will be able to request to be mapped to their user account. The mapping will be changed by the resource admin (i.e. the user won't be able to select from generic grid or personal account through any mechanism such as role authentication).

The user will simply send an e-mail to the resource administrator, which will manually change the setting in GUMS.

Role based authentication

The user will be able to create an extended proxy that contains information about which role he is going to take. The user will then be provided special privileges associated to that role. The details of which privileges to give need to be worked out with the experiments.

As part of the privilege project, there will be a callout module for the CE which will contact GUMS to retrieve the account mapping based on the extended proxy. GUMS will allow to map the user either to a different account (either specific to the user and role, or common to all users using that role) or to the same account with a different group. The exact mechanism still needs to be identify, and will be probably driven by what application can support.

Provide BNL cyber security department with site access control to Grid resources

A cyber security official can flag a user to be allowed/denied on site and all gatekeepers should abide by that decision.

SAZ is going to be site access authorization. All BNL gatekeepers will contact SAZ to determine whether the user has site access.

Notes and other issues to be resolved:

- For storage we plan to have a group account for each vo. This means that in many cases the local credentials for the CE will be different for the SE. The job will use its proxy to authenticate to the SE.
- For the shared storage, such as NFS, the authentication is the uid and gid set by the gatekeeper. One way to allow shared access between users would be for GUMS to assign the gid. If the account comes from a pool, though, the gid can't be pre-assigned. This needs investigation.
- When a user comes in with a specific role, we have different options. We can assign all users coming to a role to a common account. We are not sure whether this will satisfy DOE requirements in the long run. However, the whole set of

changing we are proposing move us a lot closer to DOE requirements. It might be feasible as a short term solution.

- Another way to assign different roles would be to change gid. This has the same problem as mentioned before: the accounts from the pool are preregistered. We can also envision creating ad-hoc accounts for those users who are going to use group accounts. It very much depends on the use the experiments are going to do with them.

Dictionary

GUMS: Grid User Management System, a service developed at BNL to maintain a site-wide certificate-to-local-user mapping policy. It allows to say: `aftpexp*.bnl.gov` should be accessible to all members of USATLAS mapped to the group account 'usatlas1', while `rftpexp*.rhic.bnl.gov` should be accessible to all members of STAR and PHENIX mapped to their respective BNL personal accounts.

SAZ: Site AuthoriZation, a service developed at Fermilab to maintain site-wide security policies.

CE: Computing Element, i.e. the GRAM gatekeeper

SE: Storage Element, i.e. gridFTP, SRM, HRM, dCache. Doesn't include NFS.

BNL: Brookhaven National Laboratory