SLAC afs groups proposal

Proposed by Tom Glanzman - based on BABAR experience

The current situation with GLAST AFS disk permissions might be improved by creating a new group, e.g., g-glast-admin, owned by owner-g-glast. This group should then be added to *every* GLAST-owned AFS directory and given all seven permissions, "rwlidka". Further, the owner of g-glast should probably be changed from owner-g-glast to g-glast-admin. With such a scheme, one achieves a reasonable level of administrative control:

1. owner-g-glast -- owns g-glast-admin, but has no direct directory permissions of its own. Its sole function in life is to administer to the needs of g-glast* groups. This group would have very few members (as it now does). It is ultimately the "master key" to the whole scheme.

2. g-glast-admin -- has all privs on all GLAST volumes. This group might contains a smallish group of trusted people whom could take on such tasks as modifying directory/volume permissions, creating new mount points, etc.

3. g-glast -- remains as it is, the largest of the three groups (contains everyone?), giving r/w permission to many(most) GLAST AFS volumes, but not able to make structural changes to the AFS structure. This group would change its owner to g-glast-admin.

4. g-glast:* -- remain as special-purpose groups, however the owner of these groups would now be g-glast-admin (not g-glast nor owner-g-glast).

In this way, the this morning's situation would be avoided in the future. We devised a similar scheme for BABAR and it has been in heavy use for over 10 years now with minimal modification, or need to request special services from SCS. There may also be some desire to change -- or at least rethink -- the group access flags associated with the various groups.

One might also consider setting up "maintainer accounts" for membership in owner-g-glast and/or g-glast-admin. BABAR did this in order to reduce the likelihood of someone in such a group accidentally performing an operation with too much authority and clobbering something of value! I have such an account, "dragon-m", which I seldom use. By design.

- Tom