Motivation

Provide a unified user interface to deal with ACLs on Linux & Windows EOS mounts.

ACL Model Comparison

<table>
<thead>
<tr>
<th>POSIX ACLs</th>
<th>Rich ACLs</th>
<th>EOS ACLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>POSIX 1003.1e</td>
<td>similar to NFSv4 / Windows style ACLs</td>
<td>directory level ACLs (like AFS)</td>
</tr>
<tr>
<td>widely supported e.g. XFS, Ext4, CephFS supported in FUSE filesystems, kernel support - stored as ext. attributes</td>
<td>implemented for XFS, Ext4, but no generic support in standard kernel or in FUSE filesystems - stored as ext. attributes</td>
<td>supported for all EOS access protocols split into system and user ACLs stored as two ext. attributes.</td>
</tr>
<tr>
<td>numerical IDs, require Linux user &amp; groups e.g. not possible to use CERN EGroups</td>
<td>numerical IDs and textual unmanaged IDs (map to EGroups)</td>
<td>numerical IDs and textual unmanaged IDs (map to EGroups)</td>
</tr>
<tr>
<td>coarse permissions</td>
<td>inheritance/propagation/deny/write/append/ delete/deleteChild entries</td>
<td>concise notation: u:rtb:rx!w,g:c3:rwx,z:rx</td>
</tr>
</tbody>
</table>

Example of an EOS ACL

dir user:10763:rw+d,
egroup:atlas-comp-cern-storage-support:rw+d

dir user:10763:rw+d,
egroup:atlas-comp-cern-storage-support:rw+d

dir user:10763:rw+d,
egroup:atlas-comp-cern-storage-support:rw+d

dir user:10763:rw+d,
egroup:atlas-comp-cern-storage-support:rw+d

Outlook

extend EOS ACL system to natively provide CERNBOX share setting and have single source of access control

Example of an EOS Rich ACL

- accessible via eosxd mount client
- reasonable set of permissions
- textual and numeric subject IDs, textual group IDs treated as CERN EGroup
- EOS ACL enhancements
  - ACLs for plain files
  - "deny" type entries e.g. no deletion ID

- back/forward translation of EOS ACLs on the fly
- enabling EOS usage as DFS drop-in solution via HA Samba gateways

Example of Linux mode bits

dir user:10763:rw+d,
egroup:atlas-comp-cern-storage-support:rw+d

dir user:10763:rw+d,
egroup:atlas-comp-cern-storage-support:rw+d

dir user:10763:rw+d,
egroup:atlas-comp-cern-storage-support:rw+d