POSIX draft ACL attribute extension to NFSv4.2

Rick Macklem FreeBSD project

Some NFSv4.2 server implement POSIX draft ACLs as their “true form”
For those server's, the acl/dacl attribute can only provide an approximation of the “true form” ACL

This draft proposes new attributes that allow an NFSv4.2 client to manipulate a POSIX draft ACL directly

- An ACL's true form is the model of ACL actually stored for the file object and used to determine access permissions on the object
- The acl_trueform attribute is a read-only attribute that indicates the true form
- Set to ACL_MODEL_NFS4, ACL_MODEL_POSIX_DRAFT or ACL_MODEL_NONE

- The acl_trueform_scope attribute is a read-only attribute that describes the scope of acl_trueform
- The acl_trueform_scope can be ACL_SCOPE_FILE_SERVER, ACL_SCOPE_FILE_SYSTEM or ACL_SCOPE_FILE_OBJECT

- The posix_default_acl and posix_access_acl are read/write attributes for the POSIX draft ACLs
- Each consists of
  - an ACE count
  - the ACEs
    - tag (user_obj, user, group_obj,..)
    - perm (read/write/execute)
    - who string (owner->uid, owner_group->gid)

VERIFY/NVERIFY

- Problematic because there is no definition of “same”

  - For example, ACE ordering does not affect semantics...

    --> Are two ACLs with the same ACEs, but in a different order the “same”?

- There is also a problem with the who strings, where different strings can refer to the same uid/gid.

Multiple mode attributes

- This was brought up during discussion on the email list, but I'll admit I did not understand the need for separate mode attributes?

Prototype implementations

- I had done prototype implementations of these attributes for both FreeBSD and Linux
- With the exception of VERIFY/NVERIFY, they appear to function and interoperate well

I hope that these implementations will receive testing at the next Bakeathon