



# NFSv4 WG - IETF 67 Access Control Issues

Mike Eisler (channeling Dave  
Noveck, Bruce Fields)

[email2mre-ietf AT  
yahoo.com](mailto:email2mre-ietf@yahoo.com)

- ▶ **Issue121: SETATTR of mode to provide setting of non-permission bits**
- ▶ **Issue112: ACL inheritance changes**
- ▶ **Issue136: ACL: Allow separate setting of audit and allow/deny ACE**

- ▶ **Motivation: Allow setting of sticky, setuid, setgid, without incurring any changes to ACL**
- ▶ **Proposal: Add a SETATTR-only attribute that includes a mask and mode**
- ▶ **If a bit is set in the mask, then the corresponding bit in the mode is changed**

- ▶ **Two Windows ACL semantics are missing from NFSv4:**
  - A bit that indicates whether an ACL was inherited
  - A bit that indicates whether a dynamic inheritance utility should propagate an ACL to a particular file object
- ▶ **Bruce fields has proposed a new NFSv4.1 ACL type that puts these two semantics as flags separate from the array of ACEs**

- ▶ **In Windows the Discretionary ACL (list of ALLOW/DENY ACEs) can be set separately from the Security ACL (list of AUDIT/ALARM ACEs)**
- ▶ **This is important. A change to ALLOW/DEY or mode shouldn't destroy an AUDIT ACE**
- ▶ **Bruce Fields has proposed separate DACL and SACL attributes that use the new type proposed for issue 112**