
draft-eisler-nfsv4-impid-00.txt
draft-adamson-nfsv4-spkm3-00.txt

IETF-64
2005-11-08

Mike Eisler
email2mre-ietf@yahoo.com

# draft-eisler-nfsv4-impid-00.txt

- Problem: “NFSv4.0 has no method for allowing clients and servers to provide to each other their implementation identities”
- Why is this a problem?
  - Interoperability will continue to be an ongoing problem
  - Modern operating environments automate collection of customer problem report data
    - collecting this data manually is error prone
  - Even if interoperability is not problem, understanding what customers are using helps
  - The number of client operating environments is declining, but the rate of change among remaining clients between revisions is high:
    - AIX 5.2 versus 5.3, Linux 2.4 versus 2.6, Solaris 9 versus 10
  - The number NFS server implementations is growing
    - 11 different implementers submitted SPEC SFS 97 results from 1997-2001
    - 20 different implementers submitted SPEC SFS 97 R1 results from 2001-2005

# draft-eisler-nfsv4-impid-00.txt

- Solution: new operation for exchanging IMPID strings between client and server
- Objections:
  - Use “signature” approaches:
    - This could be harder than implementing NFSv4
    - Not as simple as performing an md5 on arguments
  - Collecting field data to decide which implementations to test against can obscure importance of different applications
    - That’s why statisticians, accountants, and actuaries exist

# draft-eisler-nfsv4-impid-00.txt: Objections (continued)

- SSH has IMPIDs and implementers have abused them (complex matrices exist in SSH clients and servers for tailoring behaviors)
  - SSH asked for this problem. From draft-ietf-secsh-transport-24.txt:
    - "The 'softwareversion' string is primarily used to trigger compatibility extensions and to indicate the capabilities of an implementation."
  - Compare this to draft-eisler-nfsv4-impid-00.txt:
    - "An NFSv4 client or server MUST NOT interpret the implementation identity information … Because it is likely some implementations will violate the protocol specification … Implementations MUST allow:
      - the EXCH_IMPL_IDENTS4 operation to be disabled.
      - … users … to set the contents of … [the] nfs_impl_id structure to any value"

# draft-adamson-nfsv4-spkm3-00.txt

- RFC 2025 – Defined GSS mechanisms, SPKM-1, and -2
  - Assumed an enterprise-wide PKI with certificates stored in a directory service
- RFC 2847 – Defined SPKM-3
  - Like TLS, does not require an enterprise or global directory for storing certificates
  - RFC 2847 also added LIPKEY a simple GSS mechanism for sending a username/password over an encrypted channel

# What's in draft-adamson-nfsv4-spkm3-00.txt?

- Major Changes
  - Explicitly call out mutual authentication so that clients can use X.509 credentials
  - Resolution of issues:
    - Mapping of X.509 Distinguished Names to GSS name types
    - Key size specifications
    - ASN.1 encoding ambiguities
- Where do Andy and Olga want to go with it?
  - NFSv4 should be capable of leveraging existing Grid X.509 infrastructure current in use by Globus GSI
  - Provide open source code to implement it

# Objections to draft-adamson-nfsv4-spkm3-00.txt

- We've not seen many NFS v4 over SPKM implementations
  - If we don't get two independent interoperable implementations, then SPKM-3 will be dropped from the NFSv4 spec once it advanced to Draft
- DTLS
  - This looks promising, but no one has volunteered specify and implement it
  - By comparison there has been two SPKM-3s and have been two SPKM-[12]s implemented, so the proof of concept exists
    - Adamson and Kornievskaia are implementing SPKM