draft-dnoveck-nfsv4-security-00

Motivation, Status, Next steps

David Noveck

Nfsv4 wg meeting within IETF111

July 29-30, 2021
Motivation
Original Reasons

• State of existing security consideration sections
  • No threat analyses
  • No discussion of weaknesses of AUTH_SYS
  • No discussion of need for encryption.

• Need to address the opportunity provided by RPC-with-TLS

• Need to consolidate the discussion in a single NFSv4-wide document
Motivation

Recently Found Issues

• Lack of clarity regarding attributes owner and owner_group
  • Are these essentially REQUIRED?

• Sections on co-ordination of acl and mode needed a lot of work, so we need review of those changes
  • No clear reasons for many uses of SHOULD and MUST
  • Insistence that these attributes not conflict complicated by having multiple definitions of “conflict”

• Undue (in my view) solicitude, toward implementation of withdrawn Posix acl model, as opposed to the Nfsv4 acl model.
  • Is it now (long past) time to drop this?
Status
State of -00 (Slide one of two)

• Very preliminary -00
  • Rushed to get in by deadline
  • Main goal is to give the working group something to discuss
    • Has replaced security-needs, which will be allowed to expire
    • Instead of “this needs to be discussed” now have something to agree or disagree with.

• Really needed one more month
  • Has lots of typos
    • Please comment on mailing list
  • Lots of “[TBD in -01]” sections
Status
State of -00 (slide two of two)

• Does have material for WG to discuss
  • There are 23 paragraphs headed “[Working group discussion needed]:”
    • Many are easily addressed.
    • Some might be hard to resolve

• Major restructuring makes review-by-diff impossible
  • Please read the document and comment about issues you see.
Status
Expectations for-01

- Expect to submit in about a month.
- Minimal payload:
  - Address typos.
  - Fill in TBD sections.
- Aspirational:
  - Resolve as many contentious issues as we can
  - Come closer to full agreement on others.
Further Steps

Potentially Contentious Issues (Slide one of two)

• Status of owner and owner-group attributes
  • They are essentially REQUIRED
  • Might have difficulty saying that out loud.

• Dealing with alternative approaches to computing mode:
  • Current RFC8881 uses an “intentional” “SHOULD” which reads, to me like a “MAY”
  • “MUST” seems what is needed to me but we need consensus on this point.
  • Compromise could be a real “SHOULD with valid reasons to do otherwise (‘Implementer does not want to’ is not OK here.)
Further Steps
Potentially Contentious Issues (Slide two of two)

• Document makes major new recommendations.
• Need to reach agreement on.
  • Peer authentication recommendations.
  • Encryption recommendations
  • What constitutes valid reasons to do otherwise.
  • Expect some disagreement on performance/overhead issues that we need to work through.

• Discussion of future security needs.
  • Don’t need agreement (right now on what we will do
  • But do need to agree on what document will say.
Further Steps

Discussion of Security Gaps

• Following items mentioned:
  • Security for data at rest
  • Content signing
  • Revision/extension for Labelled Nfs
  • Encrypted RDMA protocols.

• Anything on this list that shouldn’t be?
• Does anything need to be added?
Further Steps
Expected path to WGLC

• Hope to get a lot of issues resolved in the -01,
• But not sure exactly how much will be left.
• Expect most issues to resolved on the mailing list
  • But might need to schedule design calls on some issues.
• Not sure how many iterations it will take.
• Feel December 2021 is a reasonable target for WGLC