Documents Related to rfc5661bis
Status and Steps to Get This Done

David Noveck
First Post-107 Interim nfsv4wg Meeting
April 22, 2020
Motivation
Why this Needs to be Done (Slide One of Two)

• RFC5661 not right (i.e. contradicted by later RFCs) in too many areas:
  • Versioning approach is pre-RFC8178 (wrong and confusing 😞)
  • Confusion addressed by RFC8434 is not clarified
  • Changes in rfc5661sequi substantial
    • But we still need a single document explaining/defining NFSv4.1
• Internationalization section based on stringprep 😞 with no connection to NFS implementations.
Motivation
Why this Needs to be Done (Slide Two of Two)

• Treatment of security really needs updating/revision.
  • No threat analysis (vague security goal is stated but there is no clear definition or reason to believe it would be met, once understood).
  • Lack of attention to monitoring threats.
  • Use of AUTH_SYS (in the clear, with no client authentication) treated as optional ("MAY implement")!!!
  • Rpc-tls gives us ability to improve things, w/o changing v4.1 protocol.

• Accumulation of errata reports including some REJECTED ones with changes that the WG agrees are needed.
  • These changes not documented anywhere, except on the working group list 😞
Possibility
Why (I Believe) this Can and Will be Done.

• Lots of stuff already done:
  • Many changes already documented in existing RFCs.
  • In other cases, wg has made clear decisions that need to be explained.
  • Have a reasonable treatment of internationalization (in RFC7530)
  • Rpc-tls could be basis for a reasonable security approach.

• Need to come to terms with lingering post-RFC7530 trauma.
  • That effort was a drag, but we need to consider where we would be now if we hadn’t done it.
  • Working group needs to work together to address these issues, including serious review effort before submission
Overview

Multiple Documents to be Produced

• Some of the areas that need to be revised need to be addressed for all NFSv4 minor versions.
  • Internationalization:
    • RFC5661 was never fixed to be compatible with implementations.
  • Security:
    • Currently in bad shape for all minor versions.
    • Makes sense to provide an NFSv4-wide treatment.
• Revised NFSv4.1 spec also needed:
  • Based on RFC resulting from of draft-ietf-nfsv4-rfc5661sesqui-msns.
  • Will reference the above new documents.
  • Plus a bunch of other changes.

4/22/2020
Overview
Document Status Summary (Slide One of Two)

• Internationalization
  • Farthest along
  • Needs extensive review before WG adoption

• Security
  • Need to address existing weaknesses (for all minor versions)
  • RFC based on draft-ietf-nfsv4-rpc-tls expected to be of critical importance
  • Expect an Informational I-D, followed by adoption as an internal WG document.
  • That document, once the working group is satisfied with it, would be basis for Standards-track document
    • Then need to write and review a corresponding threat analysis.
Overview

Document Status Summary (Slide Two of Two)

• Addressing Rfc5661bis proper
  • Will start with a limited I-D.
    • Will use RFC resulting from draft-ietf-nfsv4-rfc5661sesqui-msns as a basis.
    • Will address a limited set of well-understood issues within the framework of the I-D.
  • Once working group adopts it as WG document:
    • Address replacement for RFC8434 and pNFS clarification in general.
    • Address other lingering problems with the document.
  • Will need a major review effort before submission
    • Many people will need to be involved.
Internationalization
For all minor versions

Work underway on I-D, with -01 just submitted
Will continue to work on producing draft-ietf-nfsv4-internationalization and an eventual RFC.
Internationalization

Just Propagate RFC7530 I18n 😊

• NFSv.0 implementations:
  • Did not match RFC3530 (really followed RFC3010).
  • But did match RFC7530

• RFC5661 matches RFC3530 😞
  • But NFSv4.1 implementations do match RFC7530
    • No internationalization changes made in NFSv4.1 or NFSv4.2.

• So, one could just apply the internationalization section of
  RFC7530 to NFSv4 as a whole.
  • Approach taken in draft-dnoveck-nfsv4-internationalization-00.
Internationalization
Fly (IDNA) in the Ointment 😞

• Handling of IDNA in RFC7530 is a problem
  • Valid when written to conform to IDNA2003
  • Now many of the things servers are to do (including SHOULDs) are in obsoleted documents.
  • Idnits flags these but allows submission to go through.
  • Not appropriate for new document even if IESG would accept it, which is kind of doubtful, anyway.

• Need to revise the IDNA handling to IDNA2008, while warning of (barely) possible compatibility issues.
  • Approach taken in draft-dnoveck-nfsv4-internationalization-01
Internationalization

Expected Path Going Forward

• Need to review the latest I-D.
  • Unfortunately, the set of working group members who might do that is kind of small.
  • May need to get input from internationalization experts outside the working group.
  • Also need input from implementers about how existing implementations deal with IDNA issues (if at all).

• Looking to get to a WG document.
  • Not sure how many iterations will be required.

• Time to pick a milestone: 12/2020 seems safe enough.
Security
For all minor versions

Informational I-D to be produced soon.
Will work toward a standards-track draft-ietf-nfsv4-security and an eventual RFC.
Security Problems 😞

Overview

• Document Problems
  • Lack of a threat analysis.
  • Goal is secure use on the internet.
    • Not made clear goal if has been realized.
    • Spoiler alert! It has not.

• Substantive Problems for implementations
  • Lack of encryption use.
  • Extensive use of AUTH_SYS
    • In the clear 😞
    • With **NO** authentication of clients 😞
Security Problems 😞
Presentation of Security Issues (Slide One of Two)

• Lack of Threat Analysis 😞
  • Once RFC3552 (BCP72) was approved, hard to justify a Security Considerations section without one.
    • Not clear how RFCs 3530, 5661 and 7530 slipped by with their existing Security Considerations sections.
  • Not clear what the Security Considerations section should/can say without a threat analysis.
  • In RFCs 7530 and 5661, it is a series of security-related observations.
Security Problems 😞
Presentation of Security Issues (Slide Two of Two)

• Without a threat analysis, many questions have no clear answers:
  • What are you protecting against, i.e. what does “Secure use on the internet’ mean?
  • If there are security choices, what is the effect of making such choices on security?
    • Use of AUTH_SYS treated as optional
    • Enforcing privacy is up to server – Cost is mentioned as a reason not to do it but there is no attention to the corresponding consequences.
  • What are the security consequences of insecure use other than on the internet?
    • Document seems to assume they are not important.
Security Problems 😞
Lack of Encryption Use

• Privacy treated in specs as an expensive add-on.
  • It is expensive
  • But it is required for secure use in most environments, including use on the internet which is an official NFSv4 goal.
  • Should not be treated as an optional add-on.

• Expense issue hard to address with current design.
  • Offloading the work is troublesome when each message is potentially sent with a different key.
  • As network speeds continue to increase, offloading becomes more necessary
Security Problems 😞
Use of AUTH_SYS (Slide One of Two)

• Officially, is an OPTIONAL means of authentication.
  • Officially OPTIONAL but it is not possible to ship a server which doesn’t support it, since almost nobody would use it
  • Without authentication of client, the client’s putative authentication of user cannot be trusted.
  • Reality: AUTH_SYS is an effectively MANDATORY (to implement) means of non-authentication which is OPTIONAL for attackers to use. Sigh!

• Situation needs to change
  • Interesting question is “How?”
Security Problems 😞
Use of AUTH_SYS (Slide Two of Two)

• Possibilities for change:
  • Get rid of it.
    • Might be a Security Directorate favorite, even though it is not possible.
  • Deprecate it in some way (e.g. saying “SHOULD NOT”)
    • Doesn’t prevent its use but at least warns people of the consequences.
    • Warning will probably not be effective.
  • Try to provide some way to reduce the problems
    • For example, provide a way to authenticate the client

• Need to select at least one of the above
  • May need to deprecate, or warn against the unimproved version, for example.
Opportunity to Fix Security Problems 😊

Take Advantage of Facilities Provided by Rpc-tls

• Facilities present in the base document seem tailor-made to address NFSv4 security issues.
  • That’s not an accident.
    • Thanks, Chuck and Trond 😊
    • These facilities need to be taken advantage of.
• Need to specify appropriate policies for rpc-tls use by NFSv4.
  • For encryption.
  • For client authentication.
• Many decisions to be made.
Framework for New Security Approach

Overview

• Needs to be based on a threat analysis
• Needs to deal with major security issues
  • Lack of encryption.
  • Execution of unauthenticated requests.
• Likely to be based on rpc-tls
  • Probably with some additional requirements
• Considerable complicating factors to deal with
  • General ones dealt with in Next Slide.
  • Others appear in background slides for particular issues
Framework for New Security Approach

Complicating Factors

• Possible need to change requirements applying to existing deployments.
  • Possible requirements to implement newer facilities (e.g. rpc-tls)
  • Need to adjust ill-advised requirements (e.g. AUTH_SYS being treated as optional)

• Care needed because:
  • Some changes might not be followed immediately or at all.
  • Changes can create inter-operability issues
Issues to be Decided

Threat Analysis Goals

• Need to protect against anything other than Byzantine attackers.
  • If there is a meaning to the goal “secure use on the internet”, this has to be it.

• Do we need to analyze a lower level of threat for isolated (e.g. within-company) networks?
  • Not clear what this would be, other than no security at all, which seemed to be a common assumption when RFC5661 was written
  • One interesting possibility is protecting against everything except denial-of-service attacks.
    • On within-company links, it is easy to identify attackers, providing deterrence
Issues to be Decided
Policies for Rpc-tls Encryptions (Background)

• Existing NFSv4 encryption polices have very limited use
  • Cost due to non-offloadable nature
  • General lack of interest in topic, including lack of attention in NFSv4 specification documents.

• Rpc-tls encryption is a good fit.

• Other existing and potential technologies.
  • Encryption provided by adapters in the RPC-over-RDMA case.
  • Possible use of TLS-equivalents such as Quic
Issues to be Decided

Policies for Encryption (Possible Approaches)

• Policies for rpc-tls implementation:
  • REQUIRED not viable at this point.
  • RECOMMENDED (for both server and client) seems reasonable.
    • Will need exceptions when TLS equivalents exist.
    • Consequences of not implementing should be clearly stated.

• Policies for use:
  • REQUIRED where implemented seems OK
    • But non-offloaded implementations pose a problem.
  • RECOMMENDED where implemented makes sense
    • Use of RPCSEC_GSS privacy is probably OK in non-internet environment.
    • Should be made clear that not providing encryption in some fashion has serious consequences.
Issues to be Decided
Policies for AUTH_SYS Use (First Background Slide).

• RFCs 7530 and 5661 treat is a valid choice, presumably for both implementation and use.
  • No real discussion of the possibility of unauthenticated requests being executed.
  • The word “OPTIONAL” is not used in RFC5661, although that is the impression given

• Some mention of techniques servers have used but:
  • No discussion of weaknesses of relying on source IP address or of root-squashing
  • No mandate to implement anything.
Issues to be Decided
Policies for AUTH_SYS Use (Second Background Slide).

• RFC 5531 Appendix A discusses AUTH_SYS as well:
  • “does not guarantee any security for the users or providers of a service, in itself”
  • Mentions use of privileged port convention, but
    • Nothing specified clearly enough it could actually be implemented.
    • Assumption made that every kernel client can be trusted.
    • Mentions that not every OS implements privileged ports but no consideration on the security consequences.

• Consequences of security weaknesses never discussed.
• Despite all these weaknesses, AUTH_SYS still used extensively
Issues to be Decided
Policies for AUTH_SYS Use (Possible Approaches).

• Basic choice to be made:
  • Elimination/Deprecation (e.g. “SHOULD NOT use AUTH_SYS).
  • Mitigation as provided for by Rpc-tls authentication of the client.
    • Should be combined with discussion of AUTH_SYS weaknesses (matches the dictionary definition of “deprecation”)

• I think we need to go with mitigation strategy.
  • Elimination will not be effective.
  • Rpc-tls provides authentication material
  • Need more work regarding how server is to use it.
Issues to be Decided
Policies for Client Authentication (Background)

• Main discussion of existing AUTH_SYS client checking is in Appendix A of RFC5531.
  • In implementation discussion
    • Doesn’t really reach the level of “guidance”
  • Focuses on privileged port indication
    • Makes the dubious assumption that all kernels can be trusted.

• Rpc-tls provides that client authentication information be provided.
  • Still need to address the question of how this information is to be used.
Issues to be Decided

Policies for Client Authentication (Issues to Look at)

• Where description is to appear:
  • Could appear in NFSv4 Security document
  • Could appear in correction to RFC5531.
  • RPC could establish framework with ULP responsible for details

• Nature of description:
  • Balance between normative text and implementation guidance needs to be decided.

• Substance of description not clear at this point:
  • Possible role, if any, of privileged port indication unclear
Issues to be Decided
V4.1 Session/state Protection (Background)

• RFC5661 provides three choices:
  • SP4_NONE most common (but provides no protection)
  • SP4_MACH_CRED not commonly used
  • SP4_SSV probably never implemented.

• Without session/state protection, clients exposed to DOS attacks
  • TLS encryption makes things more difficult for attacker but does not foreclose attacks.
Issues to be Decided

V4.1 Session Protection (Possible Approaches)

• With client authentication, can avoid need for SP4_MACHCRED
  • Only allow access to sessions established by same clients.
• Since this is a v4.1-only feature, will need changes in multiple documents:
  • Changes to description of state protection requirements will appear in rfc5661bis proper.
  • Security document will discuss, including lack of need for SP4_MACHCRED and SP4_SSV.
Security-related Documents

Document Progress Expectations.

• Informational Document
  • Expect -00 of I-D by 6/2020
  • Working group adoption targeted at 10/2020

• Standards-track document
  • Expect -00 of I-D by 3/2021
  • Working group adoption targeted at 9/2021

• Finally, we need a (doable) milestone.
  • Looking at 12/2021
Rfc5661bis
New NFSv4.1 Specification

Expect an I-D soon after rfc5661sesqui becomes an RFC
Will progress from there to a draft-ietf-nfsv4-rfc5661bis
and an eventual RFC.
rfc5661bis Proper
Areas To be Addressed (Slide One of Two)

• Internationalization (by ref-ing new document)
• Security (principally by ref-ing new document)
• Errata:
  • Dealing with ACCEPTED and HELD OVER reports should be routine.
  • Also need to address those formally REJECTED, where there was a working group consensus for change
rfc5661bis Proper
Areas to be Addressed (Slide Two of Two)

• Conformance with RFC8178
  • Eliminate last instance of idea that each minor version makes its own rules

• Better handling of requirements for pNFS mapping types.
  • Start with the work done in RFC8434
  • Need to look at overall organization of sections 12 and 13
rfc5661bis Proper

Other Areas that Probably Need Work

• Clarity issues with RFC2119 terms:
  • MUSTs that are commonly ignored.
    • E.g. Section 2.10.6.2 about waiting for reply before reusing slot.
  • Mysterious SHOULDs

• Clarify lock recovery
  • Current silo-d approach has led to confusion.
  • Need to deal better with recovery by presenting an overall client-centric introduction to addressing loss of session and clientid access
RFC5661bis Proper

Other Areas that Might Need Work

• Other issues that people are concerned about?
  • Questions one is asked because the spec isn’t clear
  • Would like wg discussion of potential issues as part of planning for standards-track document.
  • Any issues where document review results in disagreement about what spec says.
rfc5661bis Proper
Overall Document Plan (Slide One of Two)

• Will initially produce an I-D, to address some preliminary matters:
  • To be based on RFC based on draft-ietf-nfsv4-rfc5661sesqui-msns
  • Internationalization and security mainly addressed by referencing new v4-wide documents
  • Errata, including those formally REJECTED, where appropriate
  • Conformance with RFC8178
rfc5661bis Proper
Overall Document Plan (Slide Two of Two)

• Other matters to be addressed as part of WG document
  • Need a plan to address them at document promotion

• Issues to Consider:
  • Dubious uses of RFC2119 terms
  • Providing more clarity about recovery situations

• Need a plan for extensive review
  • Need to address our changes
  • Also clarity of existing text.