RPCSEC_GSSv3 I-D Update

Andy Adamson
andros@netapp.com
IETF 90, Toronto Canada
Presenter Title
Date

Topics

- Change the name "Compound Authentication"
  - IETF 89 comment
- Clarify use of new auth_stat enums

Compound Authentication

- IETF 89 comment:
  - The use of "compound" is too confusing, especially given it's use in NFSv4.x
- Considered AFS "combined" authentication
  - draft-wilkinson-afs3-rxgk-11 describes combining AFS tokens
  - Close, but GSS3 "compound" is different

Compound Authentication

- New term: **Multi-principal Authentication**
  - Two GSS3 contexts, parent and inner
  - Two principals
  - New terminology
- I submitted patches to the list to update draft-ietf-nfsv4-minorversion2-26

NetApp®

GSSv3 New auth_stat Enums

- Past drafts added four new auth_stat enums with no detail on their use or numeric value

- Draft 08 changed one of the new auth_stat names and provides details on their use and numeric values

- All auth_stat values are returned with:
  - Reply_status of MSG_DENIED
  - Reject state of AUTH_ERROR
  - Then the auth_stat value

NetApp®

Multi-principal Auth: new auth_stat

- Changed RPCSEC_GSS_COMPOUND_PROBLEM to RPCSEC_GSS_INNER_CREDPROBLEM

- Mirrors the RPCSEC_GSS_CREDPROBLEM which is the RFC 2203 defined auth_stat used for multi-principal parent and non-assertion GSS3 handles when:
  - No context corresponding to the GSS3 handle
  - Or context is found but MIC verification fails

Multi-principal Auth: new auth_stats

- RPCSEC_GSS_INNER_CREDPROBLEM is for multi-principal inner GSS3 context handle processing

- Two cases where this error can be returned on an RPCSEC_GSS_CREATE call with a multi-principal payload

  - If the server does not have a context corresponding to the inner context handle

  - The inner context is found but MIC verification fails

Structured Privilege: new auth_stats

- RPCSEC_GSS_UNKNOWN_MESSAGE
  - When the server receives an unrecognized structured privilege assertion in an RPCSEC_GSS_CREATE call

- RPCSEC_GSS_PRIVILEGE_PROBLEM
  - When the server fails the RPC application defined server verification for a structured privilege in an RPCSEC_GSS_CREATE call

Ready for WGLC?

- I've pinged Nico to get his explicit review of draft-ietf-nfsv4-rpcsec-gssv3-08

- Is the NFSv4 WG done reviewing? So far (AFAICS) these are the external reviewers:
  - Lars Eggert
  - Tom Haynes
  - Mike Eisler

- I spoke with Shawn Emery, the Kitten WG Chair, on Tuesday and he suggested we cross-post the draft to the kitten group for expert review.

Thank you