NetApp™

Go further, faster

draft-adamson-nfsv4-multi-domain-access

NFSv4 WG IETF 79, Beijing China
Andy Adamson
andros@netapp.com

Key Points Being Solved

- Multi domain NFSv4 access requires name resolution across domains
- There is no internet scale federated system for resolving names across domains
- Without facilities such a those described in the draft only read-only, public (world readable) documents can be shared safely across domains.

Key Points Being Solved

- Our draft describes name and authorization context resolution in a federated environment.
  - Principals, users and groups
- Provides standard methods for scalable cross-domain access to protected documents
  - Currently NFSv4 specific
- Independent of authentication methods

Potential Issues

- Ad hoc or proprietary methods for cross domain access might be enough
  - Still value in an INFORMATIVE draft
- Collisions with other work on federated namespaces
  - NFSv4 WG needs to continue be involved in federated work

Use Cases

- Corporate mergers
- Large corporations with multiple sites
- Universities that want to federate
- Businesses that want to federate with their suppliers
- Government sites with multiple security levels

Prototype

- 2002: Linux prototype uses two new LDAP attributes associated with rfc2307 posixAccount to implement multi-domain access between POSIX (32bit UID/GID) file systems.
  - umich_ldap libnfsid method is configurable
- Tested and used to some extent at the tri-labs
- Example of a government site with multiple security levels

Overlap with other proposals

- Simon Sorce's new KRB WG draft describes a general PAC for Kerberos
  - draft-sorce-krbwg-general-pac-00.txt
- The general PAC includes global identities applicable to cross realm resolution
- Co-author Nicolas Williams has brought our draft to the attention of the KRB WG
  - Some discussion of the two drafts on KRB WG mailing list

General PAC

- The general PAC is a Kerberos version of what we call the RPCSEC_GSS PAC
  - No name@domain considerations
- We describe what a server should do if a PAC is not available
- The two drafts complement each other

Overlap with Other Proposals

- The ABFAB WG; federated storage is one of the motivating use cases
- Initial focus is on describing a (GSS-API) federated identity mechanism
  - Includes resolution of federated attributes but no name resolution
- They are also aware of our draft

What's Next

- Broad NFSv4 WG review
  - Draft contains INFORMATIVE, NORMATIVE and REQUIRED features
  - Ensure we have the right mix for NFSv4
- Scope of draft needs to be broadened to federated storage
  - Stand alone draft
- Additional I-D content is needed

What's Next

- Authors need to track the general PAC
  - Ensure the drafts are usable together even if each piece can also be used independently
- ABFAB WG comments:
  - A lot of overlap, but not in their charter
  - Seek ABFAB review now and as we approach last call
- Authors need to consult the LDAP Directorate for all things LDAP

What's Next

- Draft needs a WG home
  - Both KRB and ABFAB WG vote for NFSv4 WG
- We request the draft be moved to an NFSv4 WG item
  - Directly applicable to NFSv4.x
  - Motivated by the FedFS work which also applies to multiple protocols

Questions?

Draft-adamson-nfsv4-multi-domain-access

Andy Adamson andros@netapp.com
Kevin Coffman kwc@citi.umich.edu
Nicolas Williams Nicolas.Williams@oracle.com