Self-Provisioning NFSv4 Identity Mapping

Chuck Lever <chuck.lever@oracle.com>
Consulting Member of Technical Staff

NFSv4 Identity Mapping

- Interoperate with POSIX and non-POSIX filesystems and security models
- Users and file ownership are typically represented internally by integers or data structures
  - POSIX UID and GID
  - Windows security identifier
  - Kerberos PAC
- Externally (on the wire) they can be represented by a generic string
  - Converted by receiver into local internal representation

NFSv4 ID Domain Name

- Part of a UTF-8 string that externally represents a file's owner and group
  - `user@domain-name`

- Represents an administrative namespace where local identity values always represent the same entity

- Same syntax rules as a DNS domain label

NFSv4 ID Domain Name

- NFSv4 ID domain name is not necessarily the same as a host's DNS domain name
  - Host may reside in multiple DNS domains
  - Identity administration realms may not coincide with DNS domain hierarchy
  - NAT and WAN often assign DNS domain name that does not match NFSv4 domain name
  - Organizational transition, such as merger

Provisioning Identity Mapping

- Automatic
  - Host's DNS domain name
  - DNS TXT record (implemented in Solaris)

- Explicit
  - Config file
  - Administrative command

- Handled by plug-in
  - LDAP
  - nsswitch

Problem Statement

- Understanding and enabling ID mapping is a frequent inhibitor of NFSv4 adoption
- Stringified UIDs are not sufficient in mixed environments
- Let's enable and standardize a mechanism to self-provision identity mapping

The Common Case

- Many more file access clients than servers
- Mobile clients come and go frequently
- Organization may have one user identity authority, but decentralized management of DNS

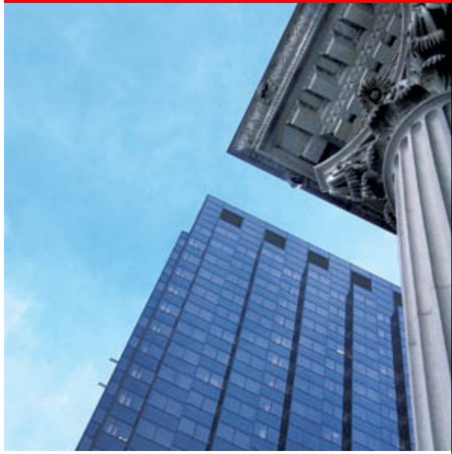
Design Considerations

- Is a single DNS record type enough for an 80% solution?

- Security considerations for distributing ID mapping configuration information?

- Could a new DHCP option be used instead? How about mDNS or DNS-SD?

- What mechanism is currently preferred by the IETF?



Questions/Discussion