Remote Name Mapping for Linux NFSv4

Andy Adamson
Center For Information Technology Integration
University of Michigan
NFSv4 Administrative Domain

- NFSv4 domain = unique UID/GID space

- Multiple Security Realms
  - Kerberos, PKI Certificate Authorities (SPKM3)

- Multiple DNS - NIS domains

- Pick one DNS domain to be the NFSv4 Domain Name
  <user@nfsv4domain>

  - ACL 'who' and GETTATTR owner and owner_group
Local NFSv4 Domain: Name to ID

- One to one correspondence between UID and NFSv4 domain name
  - joe@arbitrary.domain.org
- GSS Principal name will differ from NFSv4 domain name
  - Kerberos V: joe@ARBITRARY.DOMAIN.ORG
  - PKI: OU=US, OU=State, OU=Arbitrary Inc, CN = Joe User Email= joe@arbitrary.domain.org
Local Mount: Kerberos V

v4 Domain: arbitrary.domain.org
K5 Realm: TANGENT.REALM
DNS Domain: citi.umich.edu

NFSv4 Client

GSSD
/etc/krb5.keytab

NFSv4 Server

LDAP

Secure LDAP Call FAILS

nfs/host.citi.umich.edu@TANGENT.REALM

GSSD
If machine name, map to nobody

nfs/host.citi.umich.edu@TANGENT.REALM

gss context call succeeds

gss context creation
Local Mount: Kerberos V Issues

- Distribution of client keytabs? Linux: yes
  - With no keytab:
    - Allow AUTH_SYS for SETCLIENTIDID and mount of Kerberos export
    - User Kerberos credentials
  - Server: maps machine credentials to nobody (mount)
  - Client root user: UID 0?
    - Map to machine principal (no password)
    - Map to per server root principal (with password)
Local Principal: Kerberos V

- New Linux kernel keyring service enables kernel Kerberos credential storage, and PAG-like behaviour
- NSS ID mapping
  - `getpwid` on principal portion assumes UNIX name `(posixAccount uid) == K5 principal`
- UMICH LDAP ID mapping
  - `GSSAuthName` attribute added to LDAP `posixAccount` to associate with `uidNumber`
- Server GSSD principal mapping failure = context creation failure
Local Principal: Kerberos V

v4 Domain: arbitrary.domain.org
K5 Realm: TANGENT.REALM
DNS Domain: citi.umich.edu

% kinit joe@TANGENT.REALM

GSSD
/tmp/krb5cc_UID

NFSv4 Client

joe@TANGENT.REALM

LDAP
GSSAuthName:joe@TANGENT.REALM
uidNumber: 10098
gidNumber: 10

GSSD
secure LDAP call

NFSv4 Server

gss context creation succeeds

gss context creation
Local User: Set ACL

v4 Domain: arbitrary.domain.org
K5 Realm: TANGENT.REALM
DNS Domain: citi.umich.edu

10098

joe

% setfacl -m u:joe:rw /tmp/x.c

NFSv4 Name: joe@arbitrary.domain.org
uidNumber: 10098  uid: joe

joe@arbitrary.domain.org

NFSv4 Client

joe@arbitrary.domain.org

NFSv4 Server

joe@arbitrary.domain.org

IDMAPD

IDMAPD

SETATTR

/tmp/x.c

10098:rw
Local User: Set ACL issues

- setfacl POSIX interface uses UID/GID across kernel boundary
  - two name mapping calls
  - local posixAccount name (no @nfsv4domain)
  - NFSv4Name attribute added to LDAP posixAccount to associate full nfsv4 name with uidNumber
- Linux nfs4_setfacl interface passes string names across kernel boundary
  - no local name needed
Local User: Get ACL

v4 Domain: arbitrary.domain.org
K5 Realm: TANGENT.REALM
DNS Domain: citi.umich.edu

% getfacl /tmp/x.c

NFSv4 Name: joe@arbitrary.domain.org
uidNumber: 10098  uid: joe

LDAP

IDMAPD

NFSv4 Server

IDMAPD

GETATTR

NFSv4 Client

joe@arbitrary.domain.org

joe@arbitrary.domain.org

joe@arbitrary.domain.org

joe@arbitrary.domain.org

10098

10098

10098:rw

joe

10098
Local User: Get ACL issues

- getfacl POSIX interface uses UID/GID across kernel boundary
  - LDAP posixAccount: uid is displayed
  - two name mapping calls
- LINUX nfs4_getfacl interface passes string names across kernel boundary
Kerberos V X-Realm and Linux NFSv4

- X-realm GSS context initialization just works
- GSSAuthName and NFSv4Name can hold remote user names.
- Need to add posix account with GSSAuthName for UID/GID mapping of remote user
- Set posixAccount shell to /dev/null for NFSv4 remote access without local machine access
- Secure LDAP communication required
Remote Kerberos V Principal

v4 Domain: citi.umich.edu
K5 Realm: CITI.UMICH.EDU
DNS Domain: citi.umich.edu

v4 Domain: arbitrary.domain.org
K5 Realm: TANGENT.REALM
DNS Domain: citi.umich.edu

% kinit andros@CITI.UMICH.EDU

GSSD
/tmp/krb5cc_UID
NFSv4 Client

[LDAP] GSSAuthName: andros@CITI.UMICH.EDU
uidNumber: 10075
gidNumber: 10

andros@CITI.UMICH.EDU
GSSD secure LDAP call
NFSv4 Server

andros@CITI.UMICH.EDU
gss context creation succeeds

gss context creation
Remote User: Set ACL

v4 Domain: citi.umich.edu
K5 Realm: CITI.UMICH.EDU
DNS Domain: citi.umich.edu

v4 Domain: arbitrary.domain.org
K5 Realm: TANGENT.REALM
DNS Domain: citi.umich.edu

% setfacl -m u:andros:rwx /tmp/x.c

LDAP
NFSv4Name: andros@citi.umich.edu
uidNumber: 23975  uid: andros

NFSv4 Server
andros@citi.umich.edu
/tmp/x.c
10075:rw

IDMAPD

NFSv4 Client
andros@citi.umich.edu
SETATTR
Remote User: Set ACL

- Remote realm: associate NFSv4Name with uidNumber, gidNumber, and GSSAuthName
  - NFSv4RemoteUser schema available
  - NFSv4domain name always used
- Secure LDAP communication required
Remote User: Get ACL

- v4 Domain: citi.umich.edu
- K5 Realm: CITI.UMICH.EDU
- DNS Domain: citi.umich.edu

**LDAP**

NFSv4Name: andros@citi.umich.edu
uidNumber: 23975  uid: joe

% getfacl /tmp/x.c

NFSv4 Client

**LDAP**

NFSv4Name: andros@citi.umich.edu
uidNumber: 10075

10075:

**IDMAPD**

NFSv4 Server

/gettmp/x.c

10075:rw

GETATTR

NFSv4 Client
Remote User: Get ACL

- LDAP mappings required only for POSIX getfacl
  - NFSv4Name and uidNumber for remote user
  - uid (local user name) for remote user
- nfsv4_getfacl simply displays the on-the-wire ACL name
- Secure LDAP not required
Any Questions?

http://www.citi.umich.edu/projects