dCache and LDAP AuthN

Ron Trompert

SURFsara

A tiny Bit of History

- Number of systems
  - Own user administration system
  - Some users had access to more than one system
    - Multiple loginnames and passwds ☹
- Central User Administration (CUA)
  - Pam_ldap
  - Set of ldap servers
    - Redundant, failover, blablablabla
  - One loginname and one passwd
    - Select systems where the user should have access to

About dCache

- Uids and gids in CUA
- WebDAV with http basic authn
  - Uids and gids in CUA but passwd not
  - Need LDAP AuthN

JAAS

- AuthN and AuthZ
- Pluggable
- Now in dCache
  - kerberos

JAAS and Kerberos

- Jaas config file
  - default:
    `kerberos.jaas.config=/etc/dcache/jgss.conf`
  - jgss.conf:

```
com.sun.security.jgss.accept {
   com.sun.security.auth.module.Krb5LoginModule required
   doNotPrompt=true
   useKeyTab=true
   keyTab="${/}etc${/}dcache${/}krb5.keytab"
   debug=false
   storeKey=true
   principal="nfs/<your-server-fqan-host-name>.ifh.de@DCACHE.WORKSHOP";
};

Krb5Gplazma {
    com.sun.security.auth.module.Krb5LoginModule required debug=true
useTicketCache=false;
};
```

JAAS and Kerberos

- gplazma.conf:

```
auth       optional jaas gplazma.jaas.name=Krb5Gplazma
map        optional krb5
map        optional nsswitch
identity   optional nsswitch
session    optional nsswitch
```

JAAS and LDAP

- JAAS config file
  - dcache.conf:
    `kerberos.jaas.config=/etc/dcache/ldap.conf`
  - ldap.conf:

```
LdapGplazma {
    org.apache.activemq.jaas.LDAPLoginModule required
    debug=true
    initialContextFactory=com.sun.jndi.ldap.LdapCtxFactory
    connectionURL="ldaps://ldap.cua.sara.nl"
    connectionProtocol=""
    authentication=simple
    userBase="ou=Users,dc=hpcv,dc=sara,dc=nl"
    userSearchMatching="(uid={0})"
    userSearchSubtree=false
    roleBase="ou=Groups,dc=hpcv,dc=sara,dc=nl"
    roleSearchMatching="(cn={0})"
    roleSearchSubtree=false
    ;
};
```

JAAS and LDAP

- AuthN went fine, but……
  It did not work out of the box. Module produced principles which could not be handled by other gplazma modules for mapping
- Tigran wrote the mutator module, thanks !!!

JAAS and LDAP

- gplazma.conf:

```
auth    optional  x509
auth    optional  voms
auth    optional  kpwd
auth    optional  jaas gplazma.jaas.name=LdapGplazma
map     optional vorolemap
map     optional mutator gplazma.mutator.accept=org.apache.activemq.jaas.UserPrincipal gplazma.mutator.produce=org.dcache.auth.UserNamePrincipal
map     sufficient authzdb
map     sufficient kpwd
account requisite kpwd
session sufficient authzdb
session sufficient kpwd
```

Questions?????