OpenLDAP & Spocp
or how to use an external authorization system with OpenLDAP

Roland Hedberg
roland@catalogix.se
Short description of the Authz System

1. Policies & queries are expressed as restricted S-expressions
2. Anything not allowed is prohibited
3. Only positive rules exist
4. A query gets a positive answer if the query is a subset of one of the rules in the rule database
5. No ordering between rules
S-expression basics

• Is a list that can contain other lists and/or elements
  (resource (dn dc=se dc=catalogix))

• Adding another element at the end makes a list more specific
  (resource (dn dc=se dc=catalogix uid=roland))
So what can be done

1. Modify access_allowed() in acl.c
2. Add a slapd.conf option => changes in config.c
3. socket_pool => init.c
4. All the spocep handling is done in spocep.c
Access control based on what info?

\[
\text{Access\_allowed( Backend\ *} \ be,\ \text{Connection}\ *\ \text{conn,}\ 
\text{Entry}\ *\ e,\ \text{AttributeDescription}\ *\ \text{desc,}\ \text{struct}\ \text{berval}}\ 
\text{*val,\ \text{slap\_access\_t}\ access)}
\]

Presently using:
- userDN
- resourceDN
- attributename
- Attributevalue
- action
- tls\_ssf
A typical query

=> access_allowed: read access to "" "namingContexts" requested SPOCP access checking

=>QUERY

(5:spocp
 (8:resource(3:rdn1:-)(9:attribute(14:namingContexts)))
 (6:action1:4)
 (7:subject(3:sdn5:DC=SE6:DC=UMU10:CN=MANAGER1:-)(7:tls_ssf1:0)))

==>spocp returned 1

=> access_allowed: read access to "" "namingContexts" requested SPOCP access checking

=>QUERY

(5:spocp
 (8:resource(3:rdn1:-)(9:attribute(14:namingContexts)))
 (6:action1:4)
 (7:subject(3:sdn5:DC=SE6:DC=UMU10:CN=MANAGER1:-)(7:tls_ssf1:0)))

==>spocp returned 1
So what are the problems?

- Number of queries (how the AC evaluation is done)
- External AC
  - Requester == user DN (only knows what is present in the query)
  - Non LDAP updates of ACI
- Access control for one object is the union of all the rules that applies to that object. You can not block upstream rules!
- Tracking Changes in OpenLDAP
AuthzId API in OpenLDAP

- General ACI definition, best effort mapping??
- ACI in entries -> Authz backend must be told when things are changing
- Authz backend should be able to call data backends to get more info
- When to call the Authz backend