Do The Right Thing!

How LDAP servers should help LDAP clients

Michael Ströder <michael@stroeder.com>

Paris, 2013-11-19

Who?

Michael Ströder <michael@stroeder.com>

Freelancer : LDAP and PKI consulting

Active open source projects:

- http://web2ldap.de
- http://python-ldap.org

Not a UI expert

Old-fashioned

Concerned about insecurity by complexity

Why?

```
Kurt Zeilenga wrote:
> It might be interesting to discuss how/where web2ldap is
> able to support its users using vendor-inspecific codes,
> where you need to use vendor-specific codes, where LDAP's
> discovery mechanisms help, where they don't, what you do
> when they don't, etc.
```

How to guide human users using as much server-side information as possible ?

How much client-side knowledge is needed?

What?

Guiding vs. enforcing, notes about users

Introduction to available server information

Example use-cases with web2ldap using server information

Recommendations

Open issues to be solved

Guiding... (1)

Mantra:
Guiding is not *enforcing*!

Avoid user frustration, reducing false attempts to reach use-case goal in normal situation

Try to use server-side extensions to improve client behaviour without bothering user

Don't stop a skilled user to do something unusual

Guiding... (2)

Meaningful input forms:

- searchable naming contexts (rootDSE)
- available attributes and editable input values (subschema, access control, constraints)
- Information about affected LDAP entries (count)

Gracefully handle user's input values (normalize)

Optional use of : DIT content/structure rules, name forms, LDAPv3 ext. controls and ext. operations

Enforcing... (1)

Recommendation: Let only the server enforce...

- schema
- access control
- constraints (values, uniqueness, references)

Avoid client enforcing of schema and constraints because users could circumvent rules
=> data integrity risks

Avoid client-side access control because users could circumvent rules
=> security risks

Enforcing... (2)

Client-side access control requires powerful proxy user accounts which in real life gets (ab)used later for other purposes (yuck!)

More meaningful logging possible by using end user's identity for LDAP operations

Server can check constraints within one transaction

Enforcing... (3)

Things to enforce at client side based on client configuration or user's input:

- StartTLS
- bind method

Local security configuration in web2ldap is gateway security policy

Users...

Some personal observations:

- Users are not dumb
- Users are pretty good in ignoring unneeded things
- Users appreciate additional information if something went wrong and will report it to you
- Secretary with usual office skills provides better data than IT guy with technical LDAP skills
- Speaking with end users helps

personal observations are the opposite of mainstream UI opinions of IT guys...

Server-side information (1)

LDAP result information (often overlooked)

- result code
- diagnostic message

rootDSE (obvious)

- naming contexts, default search root
- features (extended controls/operations)
- vendor-specific information (server roles etc.)

subschema subentry (most promising)

Server-side information (2)

extended controls

extended operations

number of entries/values (entry count)

operational attributes (modifyTimestamp, *numSubordinates* etc.)

special count extensions

audit / change log databases (for restoring?)

server-side access control and constraints

Rather not generic

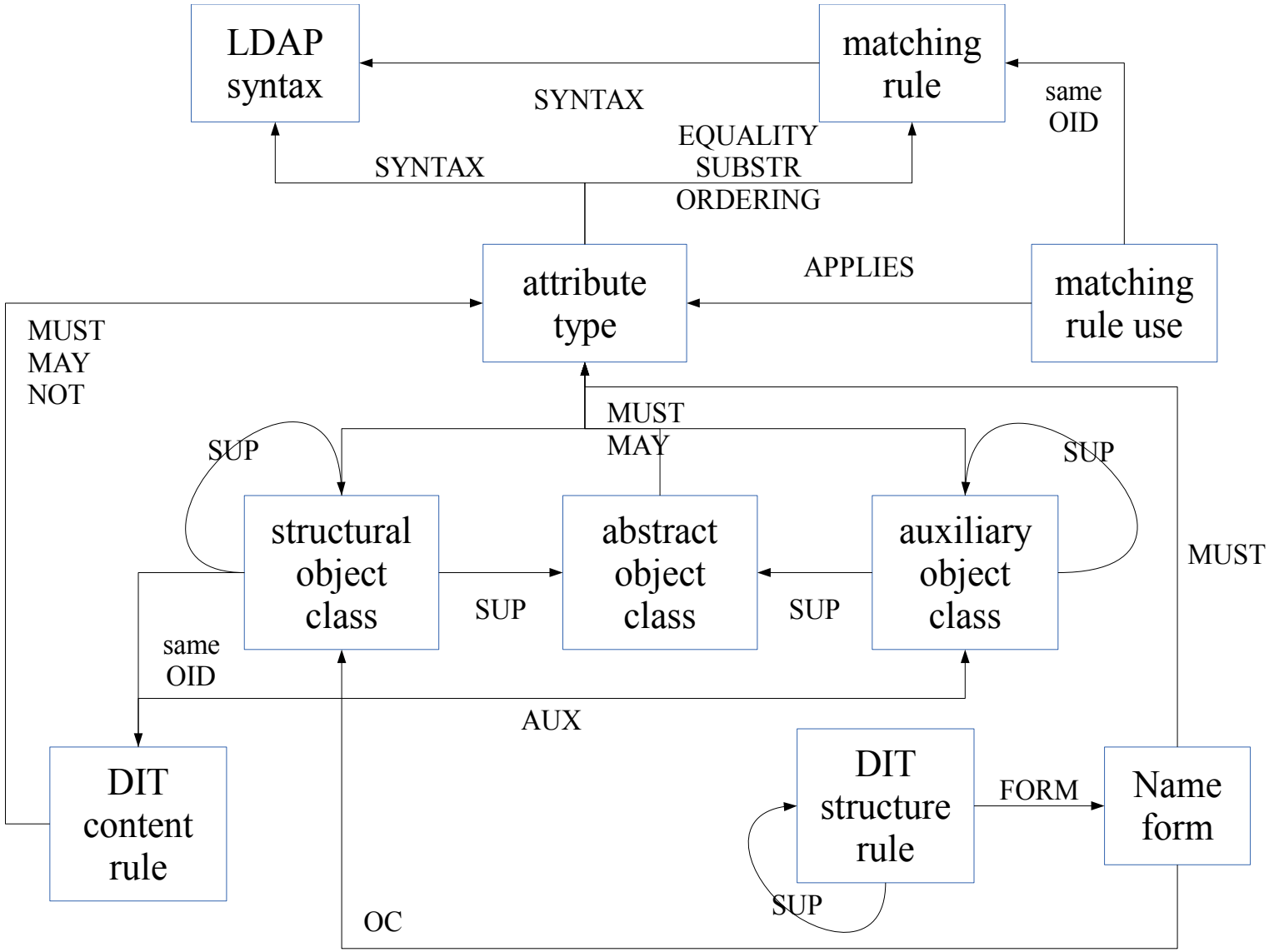
/web2ldap/passwd
Set password with various methods
(RFC 3062 ext.op., client-side hashed, MS AD, Samba3 hashes)

/web2ldap/groupadm
Add/remove entry to/from groups

/web2ldap/dds
Refresh operation for dynamic entries
(implemented for Dieter)

Still subschema used almost everywhere.

Subschema subentry (1)



Subschema subentry (2)

Query attribute *subschemaSubentry* in current entry

Read and parse the referenced subschema subentry

Fall-back needed due to access restrictions

Each part of the DIT could have separate subschema (rarely in practice)

Not unusual to have big subschema subentry ~200..400kB => caching needed!

Demos

Any special interests ?

Diffing with matching rules

Goal:
Fine-grained delete-by-value to provoke collisions in case of concurrent write access (e.g. two admins working at the same ticket)

web2ldap uses *EQUALITY* matching rule information to determine whether it's possible to delete a certain attribute value

Matching rules are inherited !

It's not sufficient to only look at the *AttributeTypeDescription*...

DIT structure rules & name forms

Enforce tree structure, web2ldap guides

Ideal if server sets *governingStructureRule*

If not you have to find nearest “subschema administrative point”

Real X.500 servers might provide attribute *administrativeRole* with a value of *subschemaAdminSpecificArea*
=> rather exotic in the pure LDAP field
=> fall-back to best matching naming context

Thanks to S. Legg for this private lesson :-)

Interop issues (1)

Domino/LDAP tested up to 7.x (not sure whether fixed in 8.x):

- single null-byte in attribute *namingContexts*
- returns diagnosticMessage in ISO-8859-1
- many attributes not found in subschema

web2ldap has work-arounds

otherwise users would blame web2ldap not to work with Domino/LDAP

BTW : It was funny to see Domino/LDAP 5.x crash because of tab character sent in a password ;-) (fixed)

Interop issues (2)

Assertion control sent with modify request to detect concurrent write access

Leads to interop issues with *slapo-constraint*

Had to disable this completely forever even if it gets fixed because vendor version not available in rootDSE

Users would blame web2ldap not to work with OpenLDAP

Interop issues (3)

Basically it's good when LDAP server enforces access control - also on use of extended controls

But overzealous checks are not good !

OpenDJ disallowed post read entry control even in case the user was allowed to read entry

At least a non-critical controls should not result in error code being returned

Users would blame web2ldap not to work with OpenDJ

Interop issues (4)

ApacheDS returned invalid ASN.1 encoding for password policy response control

=> raising ASN.1 exception was disabled in python-ldap in case of invalid but non-critical response controls

Otherwise users would blame web2ldap not to work with ApacheDS

Interop issues (5)

OpenLDAP returned invalid ASN.1 encoding for read entry response control

Immediately fixed by Pierangelo within hours

But decoding work-around added to web2ldap

Otherwise users would blame web2ldap not to work with OpenLDAP

or I'd have to disable the feature forever.

Interop issues (6)

non-ASCII chars in MS AD's are a bad idea

SASL/DIGEST-MD5 does not work even though you can see UTF-8 mentioned in SASL messages

impossible to work around this

I don't expect this to be ever fixed because of AD's own backward compability commitment

Recommendation to client developers

Don't implement an advance LDAP client, it's waste of your spare time

Prefer RAD to meet customer's requirements

Still crazy enough?

Still interested in implementing advanced LDAP features ?

Mantra : testing, testing, testing, testing, ...

Otherwise people will complain about your client and will prefer dumb LDAP clients

Interop testing with servers

OpenLDAP 2.x
OpenDJ 2.4.x
MS Active Directory W2K3..W2K12
CA eTrust Directory 8.1 and 12.0
Novell eDirectory 8.7.x and 8.8.x
Lotus Domino LDAP R5.x, R6.x and R7.0.x
389/Fedora Directory Server (fairly recent)
iPlanet/SunONE Directory Server 5.x and 6.x
Siemens DirX 6.x
Innosoft Distributed Directory Server (IDDS)
IBM Directory Server 5.1
Apache DS 1.5 and 2.0M7
OpenDS 1.0 and 2.0RC
Isode's M-Vault LDAP/X.500 Directory Server R14
eB2Bcom's ViewDS (formerly View500) 6.0e11
Critical Path InJoin and Directory Server 4.2
Syntegra (historic)
Netscape Directory Server 4.x (historic)

Recommendation to server developers

Meaningful *diagnosticMessage* helps ! Don't write it just to the server's log.

Invite client developers to do interop testing of more advanced features (test drive licenses)

Fix bugs reported to you ;-)

Add *vendorName/vendorVersion* to rootDSE

Document proprietary schema and extensions

don't hide experimental schema (.666)

Recommendation to IT admins

Don't set overrestrictive access control on

- rootDSE
- subschema subentry
- operational attributes

Try to find interop issues and report them to client and server developers if appropriate

Mantra : Logging helps...

Access control

Goal : Disable input fields if no write access

Parsing proprietary ACLs / ACIs not an option

Get Effective Rights control :
different variants with the same control OID !

web2ldap uses *allowedAttributesEffective*
(available in MS AD and *slapo-allowed*)

Value-based access control is an issue

Rather a permissive write access interpretation is recommended

Failed attributes control

The *diagnosticMessage* is useful but not machine-readable, user has to read and correctly interpret it.

How about a response control listing what went wrong for which attribute?

Would be useful to point the user directly to input fields with false data.

Attribute constraints (1)

New schema definition *attributeConstraints* (suggested on *ietf-ldapext* back in 2008)

- REGEX
- VALUES
- LDAPURI
- OPTIONS
- NUMBER <min>..<max>
- MAXBYTELEN / MAXCHARLEN

Would partially directly fit HTML5 browser-side checking

Attribute constraints (2)

Attribute type 'jpegPhoto' with restricted size and limited to a single value:

```
attributeConstraints
( 0.9.2342.19200300.100.1.60
    MAXNUMBER 1
    MAXBYTELEN 4000 )
```

Attribute 'gender' restricted to values in ISO-5801:

```
attributeConstraints
( 1.3.6.1.4.1.5427.1.389.4.7
    VALUES ( '0' $ '1' $ '2' $ '9' ) )
```

Attribute constraints (3)

Search URIs

```
( <attribute type OID>

  LDAPURI <search URI> )
```

Value of attribute o in any org. entry :

```
ldap:///ou=dc=example,dc=com?o??
(objectClass=organization)
```

DN of manager's person entry :

```
ldap:///dc=example,dc=com???
(&(objectClass=inetOrgPerson)
(title=Manager))
```

Thanks !

Any questions?

Any suggestions?

Still so crazy to develop advanced clients?

Improve «dead» LDAP together?

Have fun!