LDAP

The Lightweight Directory Access Protocol version 3 (LDAPv3) is specified by this set of eleven RFCs:

[RFC2251] Lightweight Directory Access Protocol (v3) [the specification of the LDAP on-the-wire protocol]

[RFC2252] Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions

[RFC2253] Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names

[RFC2254] The String Representation of LDAP Search Filters

[RFC2255] The LDAP URL Format

[RFC2256] A Summary of the X.500(96) User Schema for use with LDAPv3

[RFC2829] Authentication Methods for LDAP

[RFC2830] Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security

[RFC3771] The Lightweight Directory Access Protocol (LDAP) Intermediate Response Message (updates RFC2251)

[RFC3928] Lightweight Directory Access Protocol (LDAP) Client Update Protocol (LCUP)

[RFC3909] Lightweight Directory Access Protocol (LDAP) Cancel Operation

And, this document (RFC3377).

Informační model
- odvozen z X.500
- RFC 1777, RFC 2251
- Popisuje záznamy a atributy

Schema
- předloha (šablona) pro adresáře
- obsahuje seznam tříd a atributů, ze kterých jsou záznamy odvozeny
- aby mohly záznamy a atributy existovat v adresářovém stromu, musí odpovídat definicím, popsaným ve schématu
- schéma definuje dostupné třídy, definice typů atributů a syntaxi, ze které může být odvozen záznam

Třídy
- třída je kategorie objektů, které sdílí soubor společných charakteristik
- každý objekt v adresáři je instancí jedné nebo více tříd ve schématu

- v zásadě každý záznam obsahuje abstraktní třídu (top, alias), alespoň jednu strukturální třídu a může mít i pomocné třídy
- abstraktní třídy slouží jako vzory pro strukturální třídy
- strukturální třídy dědí všechny atributy, spojné s rodičovskou abstraktní třídou
- pomocné třídy dovolují položce dědit specifický soubor atributů
- obdoba vkládaných souborů

Atributy
- atributy jsou datové záznamy, použité k popisu tříd, definovaných ve schématu
- ve schématu jsou definovány odděleně od tříd, což dovoluje aplikovat jeden atribut do více tříd
- typ atributu je identifikován krátkým jménem a OID.
- Např. Common Name – CN (2.5.4.3)
- Organizational Unit – OU (2.5.4.11)
- ObjectClass (2.5.4.0)

Syntaxe
- definuje reprezentaci v paměti, pořadí slabik, pravidla pro porovnání typů vlastností
- hodnota atributu může být řetězec (string), číslo (number), časová jednotka, atd.
- syntaxe používaná v LDAP je pojmenovávaná pomocí OID
- Např. Distinguished Name (**1.3.6.1**.4.1.1466.115.121.1.12)
- UTC time (**1.3.6.1**.4.1.1466.115.121.1.53)
- Object Class Description (**1.3.6.1**.4.1.1466.115.121.1.37)

Položka (entry)
- položka je buď kontejner, nebo listový objekt specifické strukturální třídy
- položka je sestavena z různých atributů, definovaných ve schématu pro třídu, ze které je odvozen
- položky musí mít Relative Distinguished Name (RDN), které je unikátní vzhledem k sourozencům položky
- připojení RDN nebo Distinguished Name (DN) do adresářového informačního stromu musí být jednoznačné

Atributy
- kontejner i listový objekt mohou mít atributy
- atributy jsou definovány ve schématu a musí se řídit definicí schématu
- atributy se skládají ze jména, OID a hodnoty
- syntaxe atributu je definována ve schématu
- atributy jsou klasifikovány jako povinné nebo nepovinné

Model jmen
- jako primární klíče pro položky v adresáři jsou používány DN
- popsáno v RFC 1779 a RFC 2253

Distinguished Name (rozlišované jméno)
- položky jsou uspořádány v adresářovém informačním stromu podle jejich DN
- DN se skládá z posloupnosti RDN (Relative DN)

- DN představuje primární klíč pro přístup k objektu v adresářovém stromu
- Př. cn=jméno, dc=firma, dc=com
- cn=jméno,cn=doména, dc=com
- cn=CommonName, dc=DomainComponent

Relative Distinguished Name (relativní rozlišované jméno)
- RDN jsou součásti DN (DN se skládá z RDN)
- RDN je unikátní v kontejneru (totéž jako jméno souboru v adresáři)
- RDN obsahuje typ atributu a hodnotu
- Př. cn=jméno
- Ou=KIV
- Dc=uwb

Funkcionální model
- funkcionální model obsahuje devět operací ve třech oblastech
- ověřování (authentication) – klient dokazuje svoji identitu DSA (Directory Service Agent)
- dotazování (interrogation) – metody pro dotazování v adresářovém informčním stromě
- opravy (update) – mechanizmus, umožňující klientovi přidávat nebo modifikovat informaci v adresářovém informačním stromě

Ověřování
- open – vytváření a inicializace bloku propojení při otevření spojení s DSA
- bind – inicializace relace do DSA, po otevření relace je dohodnut způsob ověření mezi klientem a DSA
- unbind – ukončení relace mezi klientem a DSA

dotazování
- search – výběr položek ze specifikované oblasti adresářového informačního stromu, podle kritérií, daných filtrem prohledávání (search filter – RFC2254)
    - search base – DN objektu, definuje počátek prohledávání adresáře
    - search scope – definuje hloubku prohledávání (base or zero level – pouze objekt, one level – pouze objekty o úroveň níž, subtree – celý podstrom včetně základního objektu)
    - filter – odfiltrování některých objektů
    - selection – výběr atributů, které odpovídají kritériím ve filtru
    - optional control – ovlivnění postupu prohledávání
- compare – porovnání relačními operátory

LDAP Filter Operator	Description
=	Equal
~=	Approximately Equal
<=	Less than or equal to
>=	Greater than or equal to
&	AND
|	OR

!	NOT

- update – zahrnuje následující operace
    - add – vytvoření objektu klientem, objekt musí splňovat kritéria pro jeho vytvoření
    - modify – modifikace atributů položky, modifikace, vytváření a rušení atributů
    - modify RDN – přesun položky v adresářovém stromu
    - delete – vypuštění položky z adresářového stromu

bezpečnostní model
- specifikuje jak bezpečně přistupovat k informaci v adresáři
- Simple Authentication and Security Layer (SASL) – RFC 2222

Authentication Methods Supported by the LDAP API.

Authentication Method	Description	Credential
LDAP_AUTH_SIMPLE	Authentication with a simple clear-text password.	A string containing the user's password.
LDAP_AUTH_NTLM	Windows NT® LAN Manager	An array of strings containing the domain name, the user name, and the encrypted password.
LDAP_AUTH_DPA	Distributed password authentication (used by Microsoft Membership System)	
LDAP_AUTH_NEGOTIATE	Generic security services (GSS) (Snego). Does not provide any authentication services, instead chooses the most appropriate authentication method from a list of available services and passes all authentication information on to that service. Use with Windows® 2000	To log in as the current user, set the *dn* and *cred* parameters to NULL. To log in as another user, pass a pointer to a SEC_WINNT_AUTH_IDENTITY structure with the appropriate user name and password.
LDAP_AUTH_SSPI	This constant is obsolete and is included for backward compatibility only. Using this constant selects GSS (Snego) negotiation service.	

Další pojmy

Porty – klient se s DSA může propojit pomocí TCP nebo UDP

LDAP Connection End Points

Function	Port
LDAP	389
LDAP Secure Sockets Layer (SSL)	636
Global Catalog (GC)	3268
Global Catalog Secure Sockets Layer	3269

Metody importu a exportu – lze importovat i exportovat objekty

- LDAP Data Interchange Format (LDIF)
- Standard pro import a export do/ze souboru
- Řádkově orientované záznamy
- Možnost editovat objekty adresářového stromu v souboru

dn: CN=picturePath,CN=Schema,CN=Configuration,DC=reskit,DC=com
changetype: add
attributeID: 1.2.840.113556.1.4.7000.125.19
attributeSyntax: 2.5.5.9
cn: picturePath
isSingleValued: TRUE
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,
DC=reskit,DC=com
objectClass: attributeSchema
oMSyntax: 2

RootDSE – DSA-Specific Entry

- standardní atribut LDAP v3.0
- obsahuje informaci o adresářovém serveru včetně vlastností a konfigurace
- search BaseDN=null, filter ObjectClass=*
- vrací základní informace o serveru (RFC 2252, RFC 2251)