LDAP

Lightweight Directory Access Protocol の略。
ネットワーク上のユーザなどの資源情報を一元管理する仕組み。
Windows の AD も LDAP の機能を提供している。

Linux のコマンドによる LDAP

```
openldap-clients
```

が必要。

```
ldapsearch -h サーバ -D ユーザ -w パスワード -b サーチベース フィルタ
```

例：

```
ldapsearch -h ad_host -D test@vmware.local -w pass -b "DC=vmware,DC=local" "(sAMAccountName=hoge)"
ldapsearch -x -h ldap_server -b "DC=vmware,DC=local" "(uid=hoge)"
```

PHP による LDAP

PHP で Active Directory を用いた認証

Perl による LDAP

perl で Active Directory を用いた認証

リフェラル機能

http://software.fujitsu.com/jp/manual/manualfiles/M050000/B1WN4911/01/idmgr05/idmgr279.htm
リフェラル機能は、InfoDirectory サーバからリフェラル情報 (ldap-url) が通知された場合、その情報で指定された InfoDirectory サーバに対して同様の要求を行い情報を取得する機能です。

フィルタのサンプル

http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx

Query	LDAP Filter
All user objects	(&(objectCategory=person)(objectClass=user))
All user objects (Note 1)	(sAMAccountType=805306368)
All computer objects	(objectCategory=computer)
All contact objects	(objectClass=contact)
All group objects	(objectCategory=group)
All organizational unit objects	(objectCategory=organizationalUnit)
All container objects	(objectCategory=container)
All builtin container objects	(objectCategory=builtinDomain)
All domain objects	(objectCategory=domain)
Computer objects with no description	(&(objectCategory=computer)(!(description=*)))

Group objects with a description	(&(objectCategory=group)(description=*))
Users with cn starting with	(&(objectCategory=person)(objectClass=user)(cn=Joe*))
Object with description	(description=East\5CWest Sales)
Phone numbers in form (xxx) xxx-xxx	(telephoneNumber=(*)*-*)
Groups with cn starting with	(&(objectCategory=group)(|(cn=Test*)(cn=Admin*)))
All users with both a first and last name.	(&(objectCategory=person)(objectClass=user)(givenName=*)(sn=*
All users with direct reports but nomanager	(&(objectCategory=person)(objectClass=user)(directReports=*)(!(
All users with specified email address	(&(objectCategory=person)(objectClass=user)(|(proxyAddresses=*
Object with Common Name 'Jim * Smith'(Notes 3, 19)	(cn=Jim \2A Smith)
Objects with sAMAccountName that beginswith 'x', 'y', or 'z'	(sAMAccountName>=x)
Objects with sAMAccountName that beginswith	(&(sAMAccountName<=a)(!(sAMAccountName=$*)))
All users with	(&(objectCategory=person)(objectClass=user)(userAccountControl
All disabled user objects (Note 4)	(&(objectCategory=person)(objectClass=user)(userAccountControl
All enabled user objects (Note 4)	(&(objectCategory=person)(objectClass=user)(!(userAccountContr
All users not required to have a password(Note 4)	(&(objectCategory=person)(objectClass=user)(userAccountControl
All users with	(&(objectCategory=person)(objectClass=user)(userAccountControl
Users with accounts that do not expire(Note 5)	(&(objectCategory=person)(objectClass=user)(|(accountExpires=0)
Users with accounts that do expire (Note 5)	(&(objectCategory=person)(objectClass=user)(accountExpires>=1)
Accounts trusted for delegation(unconstrained delegation)	(userAccountControl:1.2.840.113556.1.4.803 :=524288)
Accounts that are sensitive and not trustedfor delegation	(userAccountControl:1.2.840.113556.1.4.803 :=1048574)
All distribution groups (Notes 4, 15)	(&(objectCategory=group)(!(groupType:1.2.840.113556.1.4.803:=2
All security groups (Notes 4, 19)	(groupType:1.2.840.113556.1.4.803:=2147483648)
All built-in groups (Notes 4, 16, 19)	(groupType:1.2.840.113556.1.4.803:=1)
All global groups (Notes 4, 19)	(groupType:1.2.840.113556.1.4.803:=2)
All domain local groups (Notes 4, 19)	(groupType:1.2.840.113556.1.4.803:=4)
All universal groups (Notes 4, 19)	(groupType:1.2.840.113556.1.4.803:=8)
All global security groups (Notes 17, 19)	(groupType=-2147483646)
All universal security groups (Notes 17, 19)	(groupType=-2147483640)
All domain local security groups(Notes 17, 19)	(groupType=-2147483644)
All global distribution groups (Note 19)	(groupType=2)

All objects with service principal name	(servicePrincipalName=*)
Users with	(&(objectCategory=person)(objectClass=user)(msNPAllowDialin=
Users with	(&(objectCategory=person)(objectClass=user)(!(msNPAllowDialin
All groups created after March 1, 2011	(&(objectCategory=group)(whenCreated>=20110301000000.0Z))
All users that must change their passwordat next logon	(&(objectCategory=person)(objectClass=user)(pwdLastSet=0))
All users that changed their password sinceApril 15, 2011 (CST) (Note 7)	(&(objectCategory=person)(objectClass=user)(pwdLastSet>=1294
All users with	(&(objectCategory=person)(objectClass=user)(!(primaryGroupID=
All computers with	(&(objectCategory=computer)(primaryGroupID=515))
Object with GUID	(objectGUID=\90\39\5F\19\1A\B5\1B\4A\9E\96\86 \C6\6C\B1\8D\11)
Object beginning with GUID	(objectGUID=\90\39\5F\19\1A\B5\1B\4A*)
Object with SID	(objectSID=S-1-5-21-73586283-152049171 -839522115-1111)
Object with SID	(objectSID=\01\05\00\00\00\00\00\05\15\00\00\00\6 B\D6\62\04\13\16\10\09\43\17\0A\32\57\04\00\00)
All computers that are notDomain Controllers (Note 4)	(&(objectCategory=computer)(!(userAccountControl:1.2.840.1135
All Domain Controllers (Note 4)	(&(objectCategory=computer)(userAccountControl:1.2.840.113556
All Domain Controllers (Notes 14, 19)	(primaryGroupID=516)
All servers	(&(objectCategory=computer)(operatingSystem=*server*))
All member servers (not DC's) (Note 4)	(&(objectCategory=computer)(operatingSystem=*server*)(!(userA
All direct members of specified group	(memberOf=cn=Test,ou=East,dc=Domain,dc=com)
All users not direct members ofa specified group	(&(objectCategory=person)(objectClass=user)(!(memberOf=cn=Te
All groups with specified direct member(Note 19)	(member=cn=Jim Smith,ou=West,dc=Domain,dc=com)
All members of specified group, includingdue to group nesting (Note 10)	(memberOf:1.2.840.113556.1.4.1941 :=cn=Test,ou=East,dc=Domain,dc=com)
All groups specified user belongs to,including due to group nesting (Notes 10, 19)	(member:1.2.840.113556.1.4.1941:=cn=Jim Smith,ou=West,dc=Domain,dc=com)
Objects with givenName 'Jim*' and sn 'Smith*', or with cn 'Jim Smith*' (Note 11)	(anr=Jim Smith)
All attributes in the Schema containerreplicated to the GC (Notes 6, 12)	(&(objectCategory=attributeSchema)(isMemberOfPartialAttributeS

All operational (constructed) attributes inthe Schema container (Notes 4, 12)	(&(objectCategory=attributeSchema)(systemFlags:1.2.840.113556.
All attributes in the Schema container notreplicated to other Domain Controllers(Notes 4, 12)	(&(objectCategory=attributeSchema)(systemFlags:1.2.840.113556.
All objects where deletion is not allowed(Notes 4)	(systemFlags:1.2.840.113556.1.4.803:=2147483648)
Attributes whose values are copied whenthe object is copied (Notes 4, 12)	(searchFlags:1.2.840.113556.1.4.803:=16)
Attributes preserved in tombstone objectwhen object deleted (Notes 4, 12)	(searchFlags:1.2.840.113556.1.4.803:=8)
Attributes in the Ambiguous NameResolution (ANR) set (Notes 4, 12)	(searchFlags:1.2.840.113556.1.4.803:=4)
Attributes in the Schema that areindexed (Notes 4, 12)	(searchFlags:1.2.840.113556.1.4.803:=1)
Attributes marked confidential inthe schema (Notes 4 , 12)	(searchFlags:1.2.840.113556.1.4.803:=128)
Attributes in the RODC filtered attributeset, or FAC (Notes 4, 12)	(searchFlags:1.2.840.113556.1.4.803:=512)
All site links in the Configurationcontainer (Note 13)	(objectClass=siteLink)
The nTDSDSA objects associated withall Global Catalogs. This will identify all DC'sthat are GC's. (Note 4)	(&(objectCategory=nTDSDSA)(options:1.2.840.113556.1.4.803:=
The nTDSDSA object associated with thePDC Emulator. This will identify the DCwith the PDC Emulator FSMO role (Note 18).	(&(objectClass=domainDNS)(fSMORoleOwner=*))
The nTDSDSA object associated with theRID Master. This will identify the DCwith the RID Master FSMO role (Note 18).	(&(objectClass=rIDManager)(fSMORoleOwner=*))
The nTDSDSA object associated with theInfrastructure Master. This will identify the DCwith this FSMO role (Note 18).	(&(objectClass=infrastructureUpdate)(fSMORoleOwner=*))
The nTDSDSA object associated with theSchema Master. This will identify the DC withthe Schema Master FSMO role (Note 18).	(&(objectClass=dMD)(fSMORoleOwner=*))
The nTDSDSA object associated with theDomain Naming Master. This will identify theDC with this FSMO role (Note 18).	(&(objectClass=crossRefContainer)(fSMORoleOwner=*))
All Exchange servers in the Configurationcontainer (Note 13)	(objectCategory=msExchExchangeServer)

All objects protected by AdminSDHolder	(adminCount=1)
All trusts established with a domain	(objectClass=trustedDomain)
All Group Policy objects	(objectCategory=groupPolicyContainer)
All service connection point objects	(objectClass=serviceConnectionPoint)
All Read-Only Domain Controllers(Notes 4, 19)	(userAccountControl:1.2.840.113556.1.4.803 :=67108864)