CodeX: Rekommendationer för drift och strukturering av katalogsystem

Leif Johansson, Stockholms universitet <leifj@it.su.se>

Dett dokument beskriver rekommendationer för drift och strukturering av katalogsystem vid Svenska högskolor och universitet.

Table of Contents

Vem bör läsa detta dokument?

Detta dokument bör läsas av ansvariga för planering och drift av katalogsystem vid Svenska universitet och högskolor. Dokumentet kan också fungera som en ledning för externa intressenter som vill veta hur katalogsystem är organiserade inom högskoleområdet i Sverige. Dokumentet kan tjäna som stöd vid upphandling av katalogsystem och kunsulttjänster.

Namngivning

Vid namngivning av entryn som representerar grupper och användare (personer) skall sk *DC-naming* användas. DC-naming betyder att domännamnet example.com assoceras med dc=example,dc=com och objekten som representerar dessa objekt (ex dc=example,dc=com) har strukturell typ domain:

```
dn: dc=example,dc=com
dc: example
objectClass: domain
objectClass: top
```

RDN för användare skall vara unikt inom varje administrativt kontext mao server eller grupp av refererande servrar. RDN för användare bör vara uid. RDN för grupper skall också vara unikt inom ett administrativt kontext och bör använda commonName (cn).

Schema för persondata

Entryn som representerar användare skall använda norEduPerson (som ärver av eduPerson) med en profilering som beskrivs i detta avsnitt. I eduPerson är samtliga attribut frivilliga (MAY), detta dokument profilerar schemat genom att kräva att följande attribut alltid finns på entryn med **objectClass=norEduPerson**:

1. eduPersonPrincipalName
2. norEduPersonNIN
3. eduPersonOrgUnitDN
4. eduPersonOrgDN
5. eduPersonAffiliation

Attributet eduPersonPrincipalName har syntax directoryString och skall innehålla en domän-baserad principal som skall följa denna ABNF:

```
edupersonprincipalname-principal   = uid-rdn-value "@" domainpart
uid-rdn-value                      = 1*( ALPHA / DIGIT )
domainpart                         = 1*( VCHAR )
```

Produktionen uid-rdn-value skall innehålla värdet av attributet uid som dessutom bör vara RDN för entryt enligt ovan. Vidare skall norEduPersonNIN innehålla ett av RSV utfärdat personnummer eller ett av myndigheten eller LADOK utfärdat temporärt personnummer som skall vara unikt inom landet respektive myndigheten. Attributen eduPersonOrgUnitDN och eduPersonOrgDN skall innehåll referenser (directoryName) till entryn som uppfyller de krav som detta dokument ställer på organisationsobjekt.

Attributet eduPersonAffiliation skall innehålla en eller flera värden ur mängden member, student, alumni, employee eller affiliate. Om employee eller student finns bland värdena så skall även member finnas bland värdena.

Schema för grupper

Grupper som kan komma att refereras till från annan högskola eller 3:e part skall använda schemat groupOfUniqueNames och skall använd directoryString-formen av uniqueMenber. Med andra ord får inte uniqueMember innehålla ett värde på formen "#" bitstring och skall alltså alltid innehålla ett distinguishedName som refererar till samma administrativa kontext som entryt ligger i.

Schema för organisationsdata

Nota Bene

Attributen norEduOrgIdentifier och norEduOrgUnitIdentifier finns inte i norEduOrg idag men är rekommendationer som CodeX LDAP-arbetsgrupp har framfört till Uninett.

Organisationer och organisationsdelar (institutioner, forskargrupper mm) skall använda organization resp. organizationalUnit som strukturella objektklasser samt norEduOrg resp norEduOrgUnit som auxiliära objektklass med följande profilering:

Förutom de attribut som måste finnas enligt schemat skall följande attribut finnas med på en organisation (norEduOrg):

1. norEduOrgIdentifier

Förutom de attribut som måste finnas enligt schemat skall följande attribut finnas med på en organisationsdel (norEduOrgUnit):

1. norEduOrgUnitIdentifier

Schema för rollinformation

Roller representeras i katalogen som objekt av typen organizationalRole och är associerade med den container där objekten återfinns.

Indexering och sökprestanda

Vissa katalogservrar tillåter administratören att ha kontroll över vilka attribut som indexeras för hög sökprestanda. Eftersom upprätthållade av sådana index tär på resurser vid skrivoperationer är det viktigt att välja ut vilka attribut som skall indexeras. Applikationer som används mellan myndigheter och som skall följa eller använda denna BCP BÖR endast utföra likhetsjämförelser. Andra index än sk equality-index specificeras alltså inte här. Följande attribut SKALL alltid indexeras:

- objectClass
- eduPersonOrgUnitDN
- eduPersonOrgDN
- eduPersonPrincipalName
- eduPersonAffiliation
- norEduPersonNIN
- uniqueMember
- roleOccupant

G

Uppslagning av användare

Givet en katalog som uppfyller ovanstående egenskaper finns det en enkel metod att hitta det katalogentry som är associerat med en eduPersonPrincipalName.

1. Parsa värdet localpart@domainpart av eduPersonPrincipalName enligt ABNF (RFC 2234).
2. Slå upp en SRV-post för _ldap._tcp för domainpart i dns.
3. Kontakta LDAP-servern och sök under det DN som motsvarar domainpart enligt DC-namingstandard med filter **eduPersonPrincipalName=localpart@domainpart**