

# Open Source: Autentisering, RADIUS og LDAP

Artikler om LDAP, RADIUS og autentisering i tidligere utgaver av Mellvik-Rapporten:

- "LDAP: Lettvekter med ubegrenset appetitt" – nr. 44
- "LDAP: Vindu mot oversikt – og kontroll" – nr. 57
- "LDAP: Det enkleste er det beste" – nr. 111
- "Mens vi venter på single signon" (RADIUS) – nr. 56
- "Identity management: Ingen vei utenom" – nr. 117
- "Identity management: Produkter og utfordringer" – nr. 118
- "God sikkerhet krever 802.1X" – nr. 121
- "802.1X: The inside story" – nr. 122

*Det handler om samspill, forenkling, sikkerhet og identity management. Og ikke minst dårlig samvittighet. Riktignok har andelen av IT-miljøer som har tatt i bruk LDAP-baserte katalogtjenester, vokst kraftig de siste 3 årene. En viktig drivkraft bak forandringen er Windows 2003 Server, som nærmest tvinger frem bruken av Active Directory – dersom hele systemets funksjonelle og sikkerhetsmessige register skal bli tilgjengelig.*

Dette er forklaringen på at Active Directory i løpet av relativt kort tid ble den mest utbredte LDAP-katalog på markedet, helt i tråd med Microsofts intensjon. Forholdet til LDAP-standarden og åpenhet/kompatibilitet overfor katalogtjenere fra andre leverandører, kan riktignok diskuteres, men er blitt bedre over tid. Denne praktiske kompatibiliteten går flere veier. Når Microsoft ikke vil følge standardene, har konkurrentene ingen annen vei til målet enn å tilpasse seg til Microsoft.

## Integrasjon og samspill

Poenget i denne sammenhengen er imidlertid ikke Active Directory og dens kvaliteter, men integrasjon. Uansett hvilke produkter som benyttes, er LDAP omsider – og på overtid – blitt et sentralt element i enhver systemarkitektur, både av sikkerhetsmessige og praktiske årsaker. Katalogens rolle spenner langt videre enn som brukerdatabase. Eksempler på andre informasjonstyper som havner under kontroll på denne måten, er data fra nettnavn-katalogen (DNS), fra adressetildelingstjenesten (DHCP), fra utstyrsregisteret og fra nettverket (policy- og statusinformasjon).

Samtidig med at katalogen er blitt selve nøkkelen i forbindelse med sikkerhet, autentisering og andre driftsoppgaver, består en typisk IT-infrastruktur av plattformer og produkter fra ulike leverandører. Dermed blir mulighetene for effektivt samspill produktene imellom – og ikke minst mellom produktene og katalogen, en kritisk faktor. Nettopp dette forholdet er årsaken til at LDAP-standarden, som blant annet karakteriseres ved sin relative enkelhet og effektivitet, har fått en slik sentral rolle. Avledet av den omfattende og komplekse X.500-standarden, kom LDAP inn på scenen på et perfekt tidspunkt med de riktige kvalifikasjonene tidlig på 90-tallet.

## Integrerte identitets-tjenester

Før vi ser på mulighetene for samspill på tvers av plattformer og produkter, er det hensiktsmessig med en kort repetisjon av hvilke elementer som inngår i en moderne autentiserings-løsning.

802.1X-standarden er selve grunnsteinen i forbindelse med moderne nettverks-autentisering. Vi gjennomgikk denne teknologien i Mellvik-

Rapporten nr. 121 og 122, og observerte i den forbindelse at ved siden av LDAP-katalogen, er RADIUS-tjeneren et vesentlig element. Oversiktsbildet ser med andre ord slik ut:

- ✓ Infrastruktur som støtter 802.1X
- ✓ Radius-tjener
- ✓ Katalogtjener

Videre bør, som vi var inne på ovenfor, følgende tjenester bringes inn under samme tak:

- ✓ DHCP
- ✓ DNS
- ✓ Eventuelt PKI

Til sammen utgjør disse tjenestene det vi kan kalle 'integreerte identitets-tjenester', og må alltid sees i sammenheng. Dette er en relativt overkommelig oppgave så lenge forholdene er små, oversiktlige og begrenset til én enkelt plattform, for eksempel Windows, Sun/Solaris eller Apple Mac.<sup>4</sup> Virkeligheten er som regel en ganske annen, hvilket gjør det interessant å se nærmere på hva som skjer når vi blander korene, for eksempel med katalogtjener fra Novell, Radius-tjener på Windows og DNS/DHCP på Linux. Er standardiseringen god nok til at vi kan blande hummer og kanari på denne måten?

Dessuten, i og med at vår avhengighet av autentiserings- og katalogtjenesten blir total, kan vi etablere redundante tjenester på tvers av plattformer, og derigjennom oppnå høy tilgjengelighet? Og sist, men ikke minst: Linux er markedets raskest voksende tjener-plattform, hvordan er det med slike produkter og tjenester på nettopp Linux?

### Samspill og komplikasjoner

Det korte svaret på spørsmålene om samspill er 'ja' – det meste lar seg gjøre, og kompleksiteten er overkommelig om enn høyst variabel. En gjennomgang av hva som fungerer hvor godt i hvilke sammenhenger, hører hjemme i en annen sammenheng, men fremskrittet de to siste årene har vært signifikant. Ikke minst har de fleste leverandører og produkter lært seg å leve med Active Directorys særegenheter, hvilket er en forutsetning for generelle løsninger i de fleste miljøer.

Ved siden av Microsofts implisitte rolle på Windows, er Novell et uunn-gåelig navn i sammenhenger der katalogtjenere diskuteres. Som pionér i katalogtjener-markedet med NDS, Novell Directory Services, midt på 90-tallet, er selskapet fortsatt en av lederne i segmentet. Novells 'en gros konvertering' til Linux har naturligvis også omfattet katalog-produktene, og *Identity Management* på Linux-plattformen kan ikke evalueres uten å ta med Novells produkter i prosessen.

<sup>4</sup> Artikkelen om IDM i Mellvik-Rapporten nr. 118 gir flere pekere med hensyn til produkter og leverandører.

### En finger over alt

Mens vi som regel forbinder autentisering kun med brukernes pålogging, er realiteten at autentiseringer foregår nærmest kontinuerlig – i en lang rekke sammenhenger. Derfor blir katalogtjenesten og IDM-løsningen en så kritisk og sentral komponent i vår IT-infrastruktur.

Autentisering skjer for eksempel hver gang epost-klienten ser etter nye meldinger, hver gang vi aksesserer sikrede sider på web-tjeneren, når vi arkiverer eller sender epost, når vi aksesserer filer og periferiutstyr via nettverket og så videre.

En viktig del av et moderne IDM-system er å kunne gi brukeren privilegier avhengig av hvor innloggingen kommer fra. Når Hansen logger inn fra hotellet i Washington er det neppe lurt at hun får fri adgang til interne utskriftsenheter hjemme, og kanskje ei heller høyt gradert informasjon. Autentisering er ikke det samme som autorisasjon.

## Open Source

Like interessant er det å se nærmere på hvilke Open Source-alternativer som finnes. Etter å ha brakt på det rene at operativsystemer, databaser<sup>5</sup> og Office-pakker<sup>6</sup> med Open Source-opprinnelse kan konkurrere i kvalitet og funksjonalitet med kommersielle produkter, er det rimelig å anta at også *Identity Management* er å finne i denne gruppen. Det faktum at både DNS- og DHCP-tjenester<sup>7</sup> til alle tider har vært vesentlig bedre i Open Source-innpakning enn fra kommersielle aktører, bidrar til å heve interessen ytterligere. Lar det seg gjøre å etablere en integrert *Identity Management*-løsning – med funksjonelt grensesnitt mot Active Directory basert på Open Source-komponenter?

Svaret kommer raskt og fra en overraskende kant: Apples Mac OS X Server er i vesentlig grad basert på Open Source, og har en *Identity Management*-løsning som med unntak av det administrative grensesnittet er basert på Open Source-komponenter. Open Directory 2, som produktet kalles, tar utgangspunkt i OpenLDAP som kombineres med andre Open Source-komponenter som Berkeley DB, Kerberos og SASL. Open Directory spiller en sentral rolle i Mac OS X Server, og har fått et elegant administrativt brukergrensesnitt og mekanismer som gjør samspill med Active Directory og andre LDAP-kataloger til en overkommelig affære.

Valget av Berkeley DB (BDB), som til tross for sin relative anonymitet er verdens mest utbredte databasesystem, er interessant i denne sammenhengen. BDB er en såkalt indeks-sekvensiell database (i motsetning til relasjonsdatabase) og støtter ikke SQL, hvilket gjør den uegnet i enkelte sammenhenger og perfekt i andre. Den er berømt for høy effektivitet og minimalt ressurskonsum, og passer som hånd i hanske i katalogtjener-sammenheng hvor en relasjonsdatabase er *overkill* og unødig komplikasjon. Dermed blir kombinasjonen nok et eksempel på fordelene med å velge oppgavetilpassede verktøy i stedet for kompliserende og ineffektive universalverktøy.

## Fakta

Rammen på neste side gjennomgår en del nøkkelparametre for OpenLDAP og FreeRADIUS, som sammen med OpenIX, Kerberos og administrasjonsgrensesnittet Webmin utgjør grunnstammen i Open Source-baserte autentiserings-løsninger.

Vi skal i løpet av 2005 komme tilbake til eksempler på praktisk bruk av disse komponentene – på egen hånd og i kryssplattform-situasjoner. Har du kommentarer, erfaringer eller ønsker i den forbindelse, hører vi gjerne fra deg. ■

5 Se Mellvik-Rapporten nr. 116, "Open Source databaser: Modne for nye oppgaver?".

6 Se for eksempel Mellvik-Rapporten nr. 118, "Open Office: Klar for manndomsprøven?".

7 Andre nærliggende eksempler i samme åndedrag er Web-tjenere, med Apache i spissen, og epost-agenter – som Postfix, Qmail og Sendmail.

### OpenLDAP

- Prosjektet ble opprinnelig startet ved University of Michigan i 1995, siden overtatt og videreutviklet av The OpenLDAP Foundation.
- Støtter LDAP til og med versjon 3.
- Kan kjøres på alle tenkelige plattformer, inklusive Windows.
- Kan kjøres mot nærmest hva som helst av databaser, Berkeley DB er standard og det enkleste.
- Transaksjonssikring via SSL/TLD, Kerberos eller SASL.
- Kan administreres via Web-verktøyet Webmin.
- [www.openldap.org](http://www.openldap.org)

### FreeRADIUS

- Implementerer en RADIUS autentiserings-tjener ihht. spesifikasjonene i RFC2865, 2868, 3575.
- Kan kjøres uten videre på alle Linux/Unix-plattformer og distribusjoner (og er inkludert med mange av dem), samt på Windows under Cygwin eller Windows Services for Unix.
- Tilleggsmoduler for autentisering fra PAM, Apache 1.3 og 2.0.
- Kan autentisere mot MySQL, PostgreSQL, Oracle i tillegg til LDAP.
- Støtter samtlige varianter av EAP, inkl. Cisco LEAP.
- Mer enn 50 leverandørspesifikke utvidelser.
- Er blant de 5 mest utbredte RADIUS-tjenerne i verden.
- Inkluderer mekanismer for høy tilgjengelighet (HA), med automatisk *failover*.
- Skalerer fra embedded (industrielle systemer) til systemer med millioner av brukere.
- Inkluderer et eget Web-basert (php) admin-verktøy.
- [www.freeradius.org](http://www.freeradius.org)