

LDAP: Det enkleste er det beste

Stoff om LDAP i tidligere utgaver av Mellvik-Rapporten:

- “LDAP: Lettvekter med ubegrenset appetitt” i nr. 44
- “Mens vi venter på Single Logon: RADIUS” i nr. 56.
- “LDAP: Vindu mot oversikt og kontroll” i nr. 57.

Universalspråk for katalogtjenester

LDAP synes å ha vært der i evigheter, men hvor er den, hvilken rolle spiller den og hva betyr den for oss som skal holde IT-maskineriet i gang uten at ‘verden der ute’ merker at vi finnes?

Alderen tatt i betraktning er LDAP – *Lightweight Directory Access Protocol* – befengt med forbausende mange misforståelser, selv i høyst oppgående IT-miljøer. Et godt eksempel kommer fra Alcatel, som for en tid siden publiserte en hvitbok om nettopp LDAP. Her står det å lese at “*LDAP is not designed to be a high-powered database engine*”. Det er vanskelig å oppfatte dette på annen måte enn at ‘LDAP er et database-system som ikke er laget for tunge anvendelser’.

Interessant nok er dette den mest alminnelige misforståelsen knyttet til LDAP, som slett ikke er et databasesystem, men en protokoll, en aksessmekanisme. Misforståelsen har sin opprinnelse i det faktum at det som vanligvis ligger bakenfor LDAP, og som LDAP er en aksessmekanisme til, er en database. Hvordan denne databasen er organisert eller implementert, er protokollen uvedkommende – og den praktiske spennvidden er tilsvarende stor: Fra flate filer, som er lite effektivt for store datamengder, til Oracle, Sybase eller DB2.

LDAP spesifiserer en enkel og effektiv mekanisme for overføring av data til og fra en slik database, og er – som navnet indikerer – tilpasset behov i tilknytning til katalogtjenester. Opprinnelsen går tilbake til 80-tallet og OSIs X.500-standard, utviklet av og for telecom-markedet, og uanvendelig i praksis.

Målsettingen med LDAP, som først så dagens lys i 1993 og for alvor ble interessant i en større sammenheng med versjon 3 i 1997, var den samme som for X.500: Å etablere standardiserte aksessmekanismer for oppslag i *on line* kataloger med informasjon om brukere og ressurser. På det tidspunkt var Novells NDS⁹ det eneste signifikante produkt i dette segmentet, med Netscape som nærmeste konkurrent. I bakgrunnen arbeidet Microsoft med Active Directory, en vesentlig komponent i det som siden skulle bli Windows 2000.

Verken Novell eller Microsoft viste særlig interesse for standardisering, men ble tvunget til å ta klare standpunkter av nykommeren Netscape, som hadde god vind i seilene og satset 100% på LDAP. Et annet press-element i samme retning var Open Source implementasjonen OpenLDAP fra University of Michigan.¹⁰ Mot slutten av 1997 annonserte

⁹ NDS – NOVELL DIRECTORY SERVICES – er siden blitt omdøpt til eDirectory.

¹⁰ Se Mellvik-Rapporten nr. 58.

Microsoft at Active Directory ville støtte LDAP. Senere kom Novell med tilsvarende proklamasjon. Deretter forsvant LDAP ut av mediebildet.

Drømmen om SINGLE SIGNON

Ute av syne var imidlertid ikke det samme som ute av bildet. Den viktigste årsaken til at LDAP forsvant fra radarskjermen var at teknologien hadde landet. Nødvendigheten av katalogtjenester var allment akseptert og LDAP hadde ingen andre konkurrenter enn de proprietære alternativene fra Novell og enkelte andre aktører.

Drivkraften var erkjennelsen av at uten effektive katalogtjenester ville den eksplosive utviklingen i kjølvannet av allesteds nærværende nettverk og universell konnektivitet, stoppe opp. Det er ikke mulig å vedlikeholde brukerdata-baser, printerdata-baser, oversikter over nettverksnoder og så videre i dagens dynamiske omgivelser uten effektive katalogtjenester. Videre må tjenestene være delbare, lett tilgjengelige over nettverket via standard aksessmekanismer, og sist men ikke minst sikre.

Svaret måtte bli LDAP, som i løpet av 5 år har brakt oss et vesentlig skritt i retning av reell dataharmonisering i forbindelse med IT-drift. At drømmen om *Single Signon* fortsatt ikke er en realitet for mange miljøer, skyldes ikke LDAP, men at vi for det første skyter på et bevegelig mål, og for det andre at IT-miljøer i sin alminnelighet sliter med altfor mye gammel historie som det koster ufattelige summer å vedlikeholde og tilpasse til dagens behov.

Likeledes har sikkerhets-problematikk vært en brems: Eksponering av brukerinformasjon mot åpne nettverk er på den ene siden risikabelt, mens det på den andre siden åpenbart er nødvendig for å kunne autentisere brukerne. Vår Internett-sentrerte og i voksende grad trådløse verden har helt andre karakteristika enn den som fantes da LDAP i sin tid ble skapt. Her har kombinasjonen RADIUS/LDAP kommet effektivt til unnsetning, og er blitt en obligatorisk ingrediens i nettverkskomponenter som befinner seg på grensen mellom åpne og interne nettverk.

Aktører og utfordringer

Det skal som kjent mer enn standarder til for å etablere funksjonelle, kompatible og effektive tjenester. Standardene kan sammenlignes med et sett tegninger. De skal tolkes av entreprenører og bygningsarbeidere som i sin tur gjør valg ut fra egen erfaringsbakgrunn på områder som ikke er nevnt i tegningene. For LDAP gikk denne tilpasningsprosessen relativt smertefritt fordi det fantes en implementasjonsmal: Open Source produktet OpenLDAP ble utviklet og testet i parallell med standardiseringsarbeidet.¹¹ OpenLDAP ble dermed mal og utgangspunkt for produktene som dukket opp, først fra Netscape, siden fra den ene leverandøren etter den andre.

¹¹ I henhold til alminnelig praksis for Internett-standarder måtte det demonstreres at LDAP kunne implementeres før standarden kunne aksepteres.

Virkelig stor utbredelse fikk LDAP og katalogtjenester i kjølvannet av Windows 2000 og Active Directory (AD). Produktet hadde imidlertid også betydelige svakheter, først og fremst høy kompleksitet, tett integrasjon med operativsystemet og det mange kaller 'et oppblåst selvbilde'. Riktignok støtter AD LDAP, men produktet var implementert på en måte som forutsatte at det selv var universets senter. Å være klient i forhold til en annen LDAP-tjener var komplisert og ikke alltid mulig.

Denne begrensningen forsinket innføringen av AD i mange miljøer, og ga andre leverandører en velkommen åpning i markedet. Ikke minst derfor har vi i dag en sunn leverandør- og produktmessig bredde i katalogtjener-markedet – med store aktører som Sun, Oracle og Novell i tillegg til Microsoft, og en flora av nisjeleverandører og -produkter. Situasjonen er ideell for et segment som for det første er kritisk for markedet og for det andre er meget attraktivt sett fra leverandørsiden. Katalogtjenestene er i en rivende utvikling, med et kontinuerlig behov for nye tilleggstjenester, mekanismer og protokoller. For eksempel representerer Web-tjenester en ny samling utfordringer – for autentisering av programmer og tjenester mot hverandre, i tillegg til bruker-autentisering. For å gjøre slike transaksjoner effektive, trengs ikke bare standard-protokoller, men også standard programmeringsgrensesnitt – et område som er under arbeid i IETF¹² i disse dager.

I forbindelse med Web-tjenester forsvinner de vante forestillingene om hvor brukeren er i forhold til tjenestene. Vi kan ha flere nivåer av tjenester mellom 'forespørre' og 'utførende tjeneste'. Enklere blir det ikke av at tjenestene kan komme fra et stort antall leverandører som alle skal autentiseres i forhold til hverandre, og dessuten ha informasjon om hvem som spør og hvem som skal betale. I samme forbindelse er sikring av selve transaksjonene et kritisk element. Som vi var inne på i artikkelen om Web-tjenester i forrige utgave, har Microsoft og IBM samarbeidet om nye standarder på nettopp dette området. Standardforslaget SAML, *Security Assertion Markup Language*, er ett av resultatene som nylig ble presentert.

Skalerbarhet: ADs akilleshæl

Beskjeden skalerbarhet har vært Active Directorys største hemsko i det voksende katalogtjenermarkedet. Mens hovedkonkurrentene Novell og Sun begge har demonstrert funksjonelle tjenester med over én milliard registrerte brukere, har Microsoft aldri kommet over 70 millioner.

Nå kan dette høres ut som et høyere tall enn de fleste trenger å bry seg om, men datamengdene i katalogene vokser eksplisivt – og 'brukere' er ikke det samme som 'mennesker' i denne sammenheng. Det kan like godt være nettverksnoder, programmer, eller andre objekter.

Derfor har det vært viktig for Microsoft å komme på banen med et selvstendig produkt.

AD: Hemmende integrasjon

Hensikten med den tette integrasjonen mellom operativsystemet og Active Directory var for det første å sikre at tjenesten ble tatt i bruk, og for det andre å fjerne eventuelle behov for andre katalogtjenester. I ettertid viser dette seg å ha vært en feilvurdering fra Microsofts side. Tallrike spennende og positive egenskaper til tross, er AD en tung, ineffektiv og krevende koloss – og den eneste i sitt slag med tette koblinger til et operativsystem. I løpet av sin eksistens har produktet riktignok gjennomgått justeringer som har gjort tjenestene enklere å ta i bruk og samspillet med omverden ryddigere, men de grunnleggende svakhetene er fortsatt de samme: Høy kompleksitet, manglende skalerbarhet og tett integrasjon med operativsystemet.

¹² INTERNET ENGINEERING TASK FORCE, som står bak standardiseringsarbeidet i Internett-sammenheng, inklusive LDAP og LDIF. Med hensyn til programmeringsgrensesnitt finnes det forslag til standarder for programmeringsspråkene C og Java.

Svakhetene har vært tilstrekkelig hemmende for selskapets posisjon i katalogmarkedet til å kvalifisere utviklingen av et selvstendig produkt som nylig ble annonsert. AD/AM – der AM står for *Application Mode* – forandrer styrkeforholdet i markedet for katalogtjenester, og tilfører ny spenning sammen med økt konkurranse.

Konklusjon

5 års erfaring med katalogtjenester har gitt markedet kunnskap som det er særdeles viktig å ta med seg videre – uansett hvor på skalaen fra småbedrift til internasjonal gigant vi måtte befinne oss. Den aller viktigste er at det ikke finnes noe sentrum i universet. Vår avhengighet av katalogtjenester er allerede total, og enkeltstående, isolerte tjenester er av svært begrenset verdi. De må kunne snakke sammen, enkelt, effektivt og uten andre restriksjoner enn de som måtte være nødvendige av sikkerhetsmessige årsaker.

Denne kunnskapen er egentlig ikke ny. Internettets navnekatalog, DNS, har alltid vært distribuert av natur, og har hatt de mekanismene vi nå vet at også generelle katalogtjenester må ha for å fungere. Sterk sentralisering av tjenestene har utelukkende negative bivirkninger – for eksempel høy sårbarhet og synkende effektivitet.

Likeledes viser erfaringene at relasjonsdatabaser ikke er optimale lagringsmekanismer for kataloger. De er for det første funksjonelt uegnet, fordi de er laget for helt andre oppgaver og er overlesset med funksjoner som er overflødige og bidrar til ineffektivitet. For det andre er høy grad av replisering en nødvendighet for katalogtjenester. Relasjonsdatabaser er notorisk krevende og kostbare å replisere. Enkle, indekserte filer har ikke disse problemene, og har dessuten den fordel at de i mange tilfeller kan manipuleres med standardverktøy.¹³

Om Web-tjenester for miljøer flest kan ligge et stykke inn i fremtiden, er behovet for og fordelene ved *single signon* større enn noen gang – og tilsvarende hyperaktuelt for miljøer flest. Slike tjenester er utenkelige uten tilgang til LDAP-baserte katalogtjenester, som nå inngår i autentiseringsløsninger fra samtlige leverandører på markedet. Å ha en effektiv, pålitelig og skalerbar katalogtjeneste i drift er med andre ord ikke lenger et valg. Valget som gjenstår har med teknologi og leverandør å gjøre, og det hersker ingen tvil om hvilken tankegang som gir best resultat: Det enkleste er det beste. Den eller de leverandørene som har forstått dette, er spennende kandidater. ■

¹³ LDIF-standarden (LDAP DATA INTERCHANGE FORMAT), som spesifiserer et tekstbasert utvekslingsformat for LDAP-baserte katalogtjenester, viser seg å være anvendelig til langt mer enn datautveksling.