U7-OpenLDAP

Introducció i instal · lació

Tomàs Ferrandis Moscardó

1 LDAP. Introducció

LDAP significa Lightweight Directory Access Protocol. Com el seu nom indica, és un protocol lleuger en mode client-servidor per accedir als serveis de directori, específicament basats en els serveis de directori X.500. S'executa sobre TCP/IP o altres protocols orientats a connexió. LDAP es defineix a l'estàndard RFC2251. S'utilitza comunament per a emmagatzemar informació sobre organitzacions, usuaris, xarxes, etc.

Un directori (no confondre amb un directori del nostre disc dur, ja que és una estructura molt més àmplia) és similar a una base de dades, però tendeix a contenir més informació descriptiva, basada en atributs (recordem els atributs típics d'un arxiu en un directori local: només lectura, invisible, data de creació, etc...). En un directori, normalment, la informació es llegeix més que no pas s'escriu. Els serveis de directori habitualment estan optimitzats per a donar una ràpida resposta en operacions de cerca o exploració. També poden tenir la capacitat de replicar (en diversos servidors físics) la informació continguda en un directori a fi i efecte de millorar la disponibilitat de les dades i la fiabilitat. Com que la replicació de dades pot generar inconsistències, temporalment es sincronitzen les dades per a evitar-ho.

Hi ha moltes maneres diferents de proporcionar un servei de directori. Els diferents mètodes permeten que diferents tipus d'informació s'emmagatzemen en el directori, establir requisits diferents per a la forma en què la informació es pot referenciar, consultar i actualitzar, la manera com està protegida d'accessos no autoritzats, etc. Alguns serveis de directori són locals, proporcionant serveis a un context restringit (per exemple, el servei de finger en una única màquina). Altres serveis són globals, proporcionant serveis a un context molt més ampli.

1.1 Com funciona LDAP?

El funcionament, com hem dit abans, està basat en un model client-servidor. Un client LDAP es connecta a un servidor LDAP i li fa una consulta. El servidor contesta amb la resposta, o amb un apuntador on el client pot obtenir més informació (típicament un altre servidor LDAP). Dèiem abans que poden haver molts servidors amb les dades replicades: per tant no és problema que un client es connecti amb un servidor o a un altre; el client veurà sempre la mateixa vista del directori. Aquesta és una característica molt important d'un servei global de directori com LDAP.

1.2 Avantatges en l'ús de LDAP

Un directori LDAP destaca sobre els altres tipus de bases de dades per les següents característiques:

- És molt ràpid en la lectura de registres.
- Permet replicar el servidor de forma molt senzilla i econòmica.
- Moltes aplicacions de tot tipus tenen interfícies de connexió a LDAP i es poden int
- Disposa d'un model de noms globals que assegura que totes les entrades són úniques.
- Utilitza un sistema jeràrquic d'emmagatzematge d'informació.
- Permet múltiples directoris independents
- Funciona sobre TCP/IP i SSL
- La majoria de servidors LDAP són fàcils d'instal·lar, mantenir i optimitzar.

1.2.1 Usos pràctics de LDAP

Donades les característiques de LDAP seus usos més comuns són:

- Directoris d'informació. Per exemple bases de dades d'empleats organitzats per depa
- Sistemes d'autenticació / autorització centralitzada. Grans sistemes on es guarda g
- Sistemes d'autenticació per a pàgines web, alguns dels gestors de continguts més co
- Sistemes de control d'entrades a edificis, oficines ....
- Sistemes de correu electrònic. Grans sistemes formats per més d'un servidor que acc
- Sistemes d'allotjament de pàgines web i FTP, amb el repositori de dades d'usuari co
- Grans sistemes d'autenticació basats en RADIUS, per al control d'accessos dels usua

- Servidors de certificats públics i claus de seguretat.
- Autenticació única o "single sign-on" per a la personalització d'aplicacions.
- Perfils d'usuaris centralitzats, per permetre itinerància o "Roaming"
- Llibretes d'adreces compartides.

Alguns exemples

Sistema de correu electrònic Cada usuari s'identifica per la seva adreça de correu electrònic, els atributs que es guarden de cada usuari són la seva contrasenya, el seu límit d'emmagatzematge (quota), la ruta del disc dur on s'emmagatzemen els missatges (bústia) i possiblement atributs addicionals per activar sistemes anti-spam o antivirus.

Com es pot veure aquest sistema LDAP rebrà centenars de consultes cada dia (una per cada correu electrònic rebut i una cada vegada que l'usuari es connecta mitjançant POP3 o webmail). No obstant el nombre de modificacions diàries és molt baix, ja que només es pot canviar la contrasenya o donar de baixa a l'usuari, operacions ambdues que no es realitzen de forma freqüent.

Sistema d'autenticació a una xarxa Cada usuari s'identifica per un nom d'usuari i els atributs assignats són la contrasenya, els permisos d'accés, els grups de treball als quals pertany, la data de caducitat de la contrasenya, etc...

Aquest sistema rebrà una consulta cada vegada que l'usuari accedeixi a la xarxa i una més cada vegada que accedeixi als recursos del grup de treball (directoris compartits, impressores ...) per comprovar els permisos de l'usuari. Enfront d'aquests centenars de consultes només unes poques vegades es canvia la contrasenya d'un usuari o se l'inclou en un nou grup de treball. 2 Estructura d'una base de dades/directori LDAP 2.1 Entrades, objectes i atributs Com hem dit abans, una base de dades LDAP té una estructura jeràrquica. Bàsicament totes les dades s'emmagatzemen en alguna part del directori LDAP, i a similitud dels directoris de fitxers, aquest directori s'organitza en arbre.

Veiem primer, el punt i final del directori, que és l'entrada o objecte. El model d'informació de LDAP està basat en entrades. Una entrada és una col · lecció d'atributs que tenen un Nom Distintiu o Distinguished Name (identificat com DN) únic i global. El DN s'utilitza per referir-se a una entrada sense ambigüitats. Cada atribut d'una entrada té un tipus i un o més valors i son els que contenen la informació associada a l'objecte. Els tipus són

normalment paraules mnemotècniques, com “cn” per common name, o “mail” per una adreça de correu.

En comparació amb una base de dades relacional, una entrada seria com un registre. L'atribut seria el camp.

2.2 Estructura de l'atribut DN i una breu introducció històrica

2.2.1 Introducció històrica

El nivell superior d'un directori LDAP és la base, conegut com el “DN base”. Un DN base, generalment, pren una de les tres formes llistades ací. Suposem que treballes o estudies a l'institut Maria Enriquez de Gandia, el qual està a Internet a iesmariaenriquez.es.

o = “IES Maria Enriquez”, c = ES (DN base en format X.500)

En aquest exemple, o = IES Maria Enriquez es refereix a l'organització, que en aquest context hauria de ser tractada com un sinònim del nom de l'empresa. c = ES indica que la localització general de l'empresa està a ES. Hi havia una vegada en què aquest va ser el mètode d'especificar la teva DN base. Els temps i les modes canvien, però, aquests dies, la majoria de les empreses estan (o planegen estar) a Internet. I amb la globalització d'Internet, utilitzar un codi de país a la base DN probablement faça les coses més confuses al final. Amb el temps, el format X.500 ha evolucionat a altres formats llistats més avall.

o = iesmariaenriquez.es (DN base derivat de la presència a Internet de l'empresa)

Aquest format és bastant senzill, utilitzant el nom de domini de l'empresa com a base. Una vegada has passat la porció o = (la qual ve de organization =), qualsevol a la teva empresa hauria de saber d'on ve la resta. Aquest va ser, fins fa poc, probablement el més comú dels formats usats actualment.

dc = iesmariaenriquez, dc = ES (DN base derivat dels components de domini DNS de l'empresa)

Com el format previ, aquest utilitza el nom de domini DNS com la seva base. Però on l'altre format deixa el nom de domini intacte (i així llegible per les persones), aquest format està separat en components de domini: iesmariaenriquez.es esdevé dc = iesmariaenriquez, dc = es. En teoria, això pot ser lleument més versàtil, encara que és una mica més dur de recordar per als usuaris finals.

Aquest és el format recomanable per a noves instal · lacions. Si estàs planejant utilitzar Active Directory, Microsoft ja ha decidit per tu que aquest és el format que necessites .

2.2.2 Com organitzar les teues dades en el teu arbre de directori

En un sistema de fitxers UNIX, el nivell més alt és l'arrel (/). Per sota de l'arrel tens molts fitxers i directoris. Com es comentava anteriorment els directoris LDAP estan configurats en gran part de la mateixa manera.

Sota la teva base de directori, voldràs crear contenidors que separin lògicament les teves dades. Per raons històriques (X.500), la majoria dels directoris configuren aquestes separacions lògiques com a entrades OU. OU ve de "Unitats organitzacionals" (Organizational Units, en anglès), que en X.500 eren utilitzades per indicar l'organització funcional dins de l'empresa: vendes, finances, etc. Actualment les implementacions de LDAP han mantingut la convenció del nom ou =, però separa les coses per categories àmplies com ou = gent (ou = people), ou = grups (ou = groups), ou = dispositius (ou = devices), i altres.

2.2.3 El DN d'una entrada LDAP

Totes les entrades emmagatzemades en un directori LDAP tenen un únic "Distinguished Name," o DN. El DN per a cada entrada està compost de dos parts: el Nom Relatiu Distingit (RDN per les seves sigles en anglès, Relative Distinguished Name) i la localització dins del directori LDAP on el registre resideix.

El RDN és la porció de la teva DN que no està relacionada amb l'estructura de l'arbre de directori. La majoria dels ítems que emmagatzemes en un directori LDAP tindrà un nom, i el nom és emmagatzemat freqüentment en l'atribut cn (Common Name). Ja que pràcticament tot té un nom, la majoria dels objectes que emmagatzemarà LDAP utilitzen el seu valor cn com a base per a la seva RDN. Si estic emmagatzemant un registre per la meva recepta preferida de menjar de civada, estaré utilitzant cn=MenjardeCivadaDeluxe com el RDN de la meva entrada.

- El DN base del meu directori és dc=iesmariaenriquez, dc=es
- El RDN d'un registre d'un grup cn=alumnes

Atès tot això, quin és el DN complet del registre LDAP per a aquesta grup? Recorda, es llegeix en ordre invers, cap a enrere - com els noms de màquina en els DNS.

cn = alumnes, ou = groups, dc = iesmariaenriquez, dc = es

Ara és el moment d'abordar el DN d'un membre del nostre institut. Per als comptes d'usuari, típicament veuràs un DN basat en el cn o al uid (ID de l'usuari). Per exemple, el DN del professor Armand Mata (nom de login: armandmata) pot semblar-se a un d'aquests dos formats:

uid = armandmata, ou = professorat, ou=people, dc = iesmariaenriquez, dc = es (basat en el login)

LDAP (i X.500) utilitzen uid per a indicar "ID de l'usuari", no s'ha de confondre amb el número uid de UNIX. La majoria de les empreses intenten donar a cadascun un nom de login, així aquesta aproximació fa que tinga sentit emmagatzemar informació sobre els empleats. No t'has de preocupar sobre què faràs quan entre un nou professor amb el mateix nom, o si el mateix professor decideix canviar-se el nom. No has de canviar el DN de l'entrada LDAP.

cn = ArmandMata, ou = professorat, ou=people, dc = iesmariaenriquez, dc = es (basat en el nom)

Aquí veiem l'entrada Nom Comú o CN (per les seves sigles en anglès, common name) utilitzada. En el cas d'un registre LDAP per a una persona, pensa en el nom comú com els seu nom complet. Un pot veure fàcilment l'efecte col · lateral d'aquesta forma: si el nom canvia, el registre LDAP ha de "moure" d'un DN a un altre. Com s'indica anteriorment, has d'evitar canviar en DN d'una entrada sempre que siga possible.