آشنایی با پروتکل LDAP

اشاره :

یکی از سرویس‌هایی که روی لینوکس ارائه می‌شود، امکان کار با پروتکل LDAP است. این سرویس که تا حدودی برای بسیاری از کاربران و مدیران شبکه ناآشنا است، در کنار سرویس سامبا (Samba) بستری برای ارتباط سکوی اپن‌سورس با دیگر سکوهای سیستم‌عاملی ایجاد می‌کند و موجب می‌شود بدون در نظرگیری استانداردها و پروتکل‌های سمت سرویس‌دهنده، با آن‌ها سازگاری و همسان‌سازی داشته باشد. در این مقاله خوانندگان و علاقمندان را با مفهوم این سرویس آشنا می‌کنیم. در ضمن به کارکرد آن نیز نگاهی می‌افکنیم. به دلیل آن‌که راه‌اندازی و پیکربندی این سرویس باید همراه با یک سرویس‌دهنده کامل باشد، آن را به زمان دیگری موکول می‌نماییم. برای کسب اطلاعات بیشتر و دریافت بسته‌های نصب LDAP نیز می‌توانید به سایت رسمی این پروژه به نشانیwww.OpenLDAP.org مراجعه نمایید.

سرویس دایرکتوری

دایرکتوری یا فهرست راهنما، یک سرویس ویژه در شبکه‌های کامپیوتری یا اینترنت است که برای بهبود کار با بانک‌های‌اطلاعاتی برای خواندن، جست‌وجو و مرور اطلاعات به کار می‌رود. با استفاده از سرویس دایرکتوری می‌توان محتویات بانک اطلاعاتی را دسته‌بندی نمود، برای آن‌ها ویژگی‌ها و ایندکس‌هایی تعریف کرد و بر این اساس فایل‌ها و اطلاعات شبکه را برای دسترسی سریع و آسان طبقه‌بندی نمود. برای مثال، در شبکه ممکن است یک بانک اطلاعاتی از فایل‌ها وجود داشته باشد. با استفاده از سرویس دایرکتوری می‌توان این فایل‌ها را طبقه‌بندی نمود، ویژگی‌های مختلفی به آن‌ها افزود و عملیات بروزرسانی و آپلود آن‌ها را انجام داد؛ به طوری که دسترسی به آن‌ها از روی شبکه برای کاربران ساده و راحت باشد.

هر سرویس دایرکتوری دارای ویژگی‌های اساسی زیر است:

- قابلیت بهینه‌سازی خواندن و دسترسی به فایل‌ها
- مدلی توزیع شده برای مدیریت و ذخیره اطلاعات
- افزایش و توسعه ویژگی‌ها و انواع اطلاعات ذخیره شده

- ایجاد یک ابزار جست‌وجوی پیشرفته روی شبکه

روش‌های مختلفی برای راه‌اندازی یک سرویس دایرکتوری وجود دارد. علاوه بر این، متدهای مختلفی برای مدیریت اطلاعات و ذخیره‌سازی آن‌ها براساس آپلودکردن آن‌ها روی بانک اطلاعاتی، نحوه دسترسی، چگونگی مرجع‌دهی آن‌ها برای یک سرویس دایرکتوری قابل استفاده است. برخی از سرویس‌های دایرکتوری محلی (Local) هستند و فقط روی یک شبکه محلی یا یک ماشین سرویس‌دهنده اجرا می‌شوند. برخی دیگر از دایرکتوری‌ها عمومی (Global) هستند و روی چندین شبکه محلی یا سرویس‌دهنده توزیع می‌شوند، و امکان مدیریت و دسترسی به اطلاعات روی شبکه را از این طریق فراهم می‌کنند. Domain Name System) DNS) یک مثال از سرویس دایرکتوری عمومی است.

پروتکل LDAP

Directory Access Protocol Lightweight یک پروتکل مبتنی بر شبکه و X500 برای دسترسی به سرویس‌های دایرکتوری روی شبکه است. این پروتکل دارای مستندات RFC2251 و RFC3377 است. به علت آن‌که دایرکتوری‌های موجود روی شبکه یکتا نیستند و هر یک ممکن است براساس یک سکوی سیستم‌عاملی و ساختار متفاوت باشند، پروتکل LDAP امکان برقراری ارتباط و مدیریت آن‌ها را فراهم می‌کند. در حقیقت LDAP ابزاری برای مدیریت اطلاعات شبکه، حساب‌های کاربری، ماشین‌های میزبان شبکه و منابع درون شبکه است. با استفاده از این استاندارد می‌توان یک مدیریت متمرکز و واحد را به کل پیکره شبکه اعمال نمود و با دسترسی به تمام سرویس‌های درون شبکه (سخت‌افزاری و نرم‌افزاری) امکان همسان‌سازی و پیکربندی آسان آن‌ها را فراهم کرد.

در حالت کلی پروتکل LDAP وظایف زیر را بر عهده دارد:

- ایجاد یک زبان مشترک دسترسی دایرکتوری (Directory Access) بین ماشین میزبان و سرویس‌دهنده در شبکه و امکان برقراری ارتباط و تبادل اطلاعات میان آن‌ها فارغ از سکوی سیستم‌عاملی و سخت‌افزاری.

- ایجاد قابلیت استفاده از متدهای ساده رمزنگاری در پروتکل TCP/IP برای تبادل اطلاعات کنترلی و مدیریتی مانند کنترل و مدیریت کاربران در شبکه.

- ایجاد یک استاندارد برای استفاده از دایرکتوری در شبکه.

این استاندارد قابلیت نصب و پیکربندی ساده و انعطاف‌پذیر سرویس دایرکتوری و سفارشی نمودن آن برای نیازهای گوناگون را روی شبکه فراهم می‌کند.

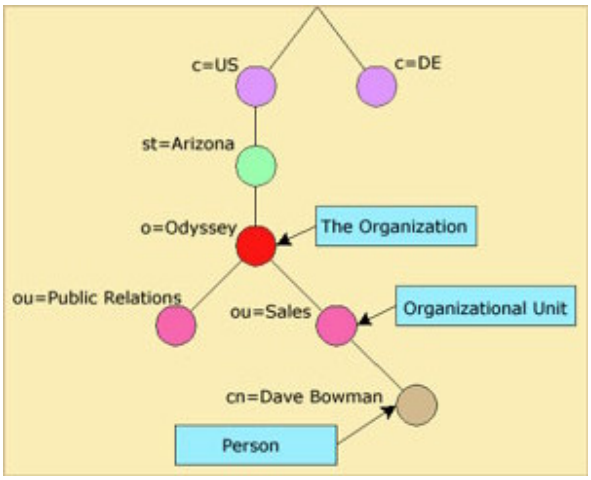
- **پشتیبانی توابع API**:

این پروتکل از C، Netscape's Java SDK، PerLDAP، SunSoft's JNDI و Microsoft's Active Directory Services Interface) ADSI) پشتیبانی می‌کند و با آن‌ها سازگار است. این ویژگی امکان مدیریت و کنترل دسترسی شبکه‌های گسترده را فراهم می‌کند که دارای چندین سکوی نرم‌افزاری/ سخت‌افزاری هستند.

- استفاده از یک استاندارد با نام LDIF (LDAP Data Interchange Format) برای توصیف و تشریح اطلاعات دایرکتوری. این استاندارد که توسط یک ابزار با همین نام به کار گرفته می‌شود، تحت خط فرمان است و امکان تنظیم مجموعه‌ای از دایرکتوری‌ها یا آپلودکردن آن‌ها برای استفاده در دایرکتوری را در اختیار مدیر شبکه قرار می‌دهد.

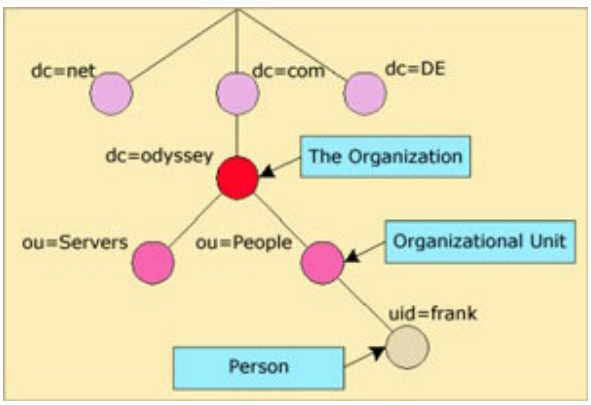
ساختار LDAP

اطلاعاتی که روی LDAP قرار می‌گیرد، اطلاعاتی ایندکس‌دار و مدخل‌مانند است. بدین معنی که اطلاعات به صورت مجموعه‌ای از ویژگی‌های توزیع شده قابل دسترسی هستند که از یکدیگر متمایزند و کاربران می‌توانند از طریق ایندکس‌های موجود، به اطلاعات دسترسی پیدا نمایند.



شکل 1

برای مثال، عبارت می‌تواند یک ایندکس برای اطلاعات دستوری و برای آدرس‌های ایمیل باشد. cn می‌تواند ارزش یک داده یا اطلاعات برای یک کاربر یا ماشین باشد (برای مثال Misagh و mail) آدرس ایمیل مرتبط با ارزش cn باشد (برای مثال misagh@example.com).



شکل 2

روی LDAP اطلاعات به صورت مدخل‌های دایرکتوری و سلسله مراتبی قرار می‌گیرند. این ساختار سلسله مراتبی انعکاسی از ساختار شبکه یا اینترنت و وضعیت جغرافیایی یا قرارگیری ماشین‌های کلاینت و سرویس‌دهنده است.

در شکل 1 و 2 دو ساختار سلسله مراتبی قرارگیری اطلاعات روی دایرکتوری برای دسترسی LDAP نشان داده شده است.

در شکل دو که گویای قرارگیری اطلاعات در دایرکتوری مبتنی بر اینترنت است، در بالاترین سطح از net،com و DE که یک پسوند دامنه اختصاصی است، تشکیل یافته است.

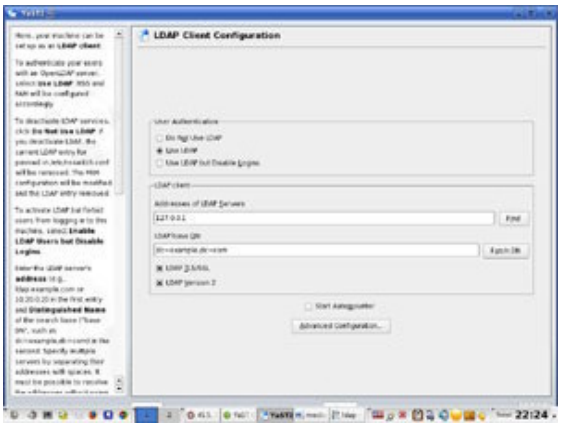
اگر شاخه com را پیگیری نمایید، به سطح odyssey می‌رسید که یک سرویس‌دهنده اختصاصی درون سازمانی است.

در ادامه سطح odyssey به دو شاخه server و people تقسیم می‌شود که روی هر یک می‌تواند اطلاعات مختلفی قرار گیرد و یک کاربر که امکان دسترسی به این فهرست راهنما برایش مهیا است، می‌تواند با شناسه ID اختصاصی خود به فایل‌ها و اطلاعات دسترسی داشته باشد.

این ساختار دسترسی به اطلاعات و کنترل مجوزها، همچنین مدیریت آن‌ها را برای سرویس‌دهنده اختصاصی سازمان و دیگر سرویس‌دهنده‌ها که امکان اتصال به دایرکتوری را دارند، ساده می‌نماید. LDAP ساز و کاری برای اتصال به این دایرکتوری و برقراری یک ارتباط مدیریتی در لینوکس برای مدیران شبکه فراهم می‌کند.

LDAP در لینوکس

LDAP خود یک پروتکل و استاندارد برای برقراری ارتباط با سرویس دایرکتوری‌های مختلف است، اما در لینوکس برای به کارگیری و مدیریت این پروتکل ابزار OpenLDAP ارائه شده است. OpenLDAP یکی از بنیادی‌ترین ابزارهای لینوکس است و به همین خاطر در غالب توزیع‌های لینوکس مشاهده می‌شود و امکان نصب و راه‌اندازی آن به راحتی وجود دارد. بنابراین نصب این سرویس کار چندان مشکلی نخواهد بود، اما پیکربندی LDAP برای دسترسی به دایرکتوری‌های تعریف شده و تنظیمات آن‌ها براساس مستندات شبکه، نیازمند دقت و تمرین است.



شکل 3

علاوه بر این، هر توزیع، ابزارهای متنوع مدیریتی برای کار با این سرویس ارائه نموده است. برای نمونه در توزیع SUSE، در بخش Network Service ابزار Client LDAP ارائه شده است که می‌توان با دادن آدرس سرویس‌دهنده LDAP و شماره DN اختصاصی تعریف شده برای کاربر، به این سرویس متصل شد (شکل 3).

برای تنظیمات مورد نیاز باید به سراغ پوشه etc/openldap/ رفت. در این پوشه فایل‌های پیکربندی ldap.conf و slapd قرار دارند. برای شروع و خاتمه سرویس LDAP نیز از دو دستور slapd start و slapd stop استفاده می‌شود. slapd نام دایمون ابزار OpenLDAP در لینوکس است.

نصب و پیکربندی LDAP روی دبیان سارژ

دبیان بزرگ‌ترین توزیع لینوکس است که قابلیت‌ها و ویژگی‌های آن موجب شده روی کامپیوترهای سرور و با هدف ایجاد سرویس‌دهنده به راحتی راه‌اندازی شود. سارژ یا دبیان 3/1 آخرین نسخه این توزیع است که شامل طیف گسترده‌ای از برنامه‌ها و ابزارهای موردنیاز برای یک سیستم سرور است. در ادامه نصب و پیکربندی سرویس‌دهنده پروتکل LDAP روی این توزیع مرور می‌شود. برای نصب LDAP، اگر در هنگام نصب دبیان نصب نشده است، باید از دستور زیر استفاده نمود:

```
apt-get install slapd ldap-utils
```

با اجرای دستور فوق ابزار OpenLDAP و ابزارهای دیگر وابسته به آن نصب می‌شوند. اکنون از مسیر etc/openldap/ فایل دایمون slapd.conf را توسط یک ویرایشگر متنی باز نمایید. دو گزینه برای دسترسی به سرویس‌دهنده LDAP و مدیریت آن و که نام دامنه سرویس LDAP است، در این فایل باید تنظیم شوند. برای مثال:

```
omit openLDAP server configuration? no
DNS domain name: example.org
Admin password: ldap
database backend to use: BDB
Do you want your database to be removed when slapd is purged? no
protocol? No2Allow LDAPv
```

پس از انجام دادن تنظیمات موردنیاز و اجرای سرویس LDAP، با استفاده از دستور

```
ldapsearch -x -b dc=example,dc=org
```

می‌توانید سرویس‌دهنده LDAP و صحت کارکرد آن را تست نمایید. سپس باید اطلاعات پایه‌ای اولیه سلسله‌مراتبی سرویس دایرکتوری شبکه یا نام دامنه مورد نظر برای OpenLDAP تعریف شوند. برای این منظور یک فایل متنی را باز کنید و نام آن را base.ldif قرار دهید. این فایل در همان پوشه openldap ذخیره می‌شود. همان‌طور که در ضمن مثالی در بالا اشاره شد، اطلاعات یک دایرکتوری ممکن است به صورت زیر باشند:

```
dn: ou= People, dc= example, dc=org
ou: People
objectClass: top
objectClass: organiationalUnitz
dn: ou= Group, dc= example, dc=org
ou: Group
objectClass: top
objectClass: organiationalUnitz
```

اکنون برای افزودن فایل اطلاعات به دایرکتوری LDAP و اجرای سرویس‌دهنده از فرمان زیر استفاده می‌شود:

```
ldapadd -x -D "cn=admin,dc=example,dc=org" -W -f base.ldif
```

در صورت اجرای دستور بالا و صحیح بودن کلمه عبور، خروجی مشاهده‌شده در ترمینال خط فرمان باید با عبارت . آغاز شده باشد که بیانگر آماده بودن سرویس‌دهنده LDAP برای وارد نمودن اطلاعات جدید یا مدیریت کاربران است. در گام بعد معمولاً مدیران شبکه یک گروه کاری را تعریف می‌کنند تا کاربرانی که می‌خواهند به اطلاعات روی سرویس دایرکتوری دسترسی داشته باشند عضو این گروه شوند. نام گروه می‌تواند group.ldap باشد. بدون این‌که بخواهیم درگیر جزئیات و پیچیدگی‌های راه‌اندازی یک گروه کاری روی LDAP شویم، می‌توان اینگونه عمل نمود:

```
dn: cn= ldapusers, ou= Group, dc= example, dc=org
objectClass: PosixGroup
ObjectClass: top
cn: ldapusers
userPassword: [crypt]x
gidNumber:9000
```

اکنون LDAP برای برقراری یک ارتباط و استفاده روی شبکه آماده است. البته می‌توان در ادامه سرویس‌هایی مانندIDIF را نیز برای کاربران و گروه کاری تعریف و تنظیم نمود.

نتیجه‌گیری

برخی از سرویس‌های ارائه‌شده روی لینوکس ویژگی‌های منحصربه‌فردی دارند که توانایی و امکانات مدیران شبکه را افزایش می‌دهند و موجب می‌شوند شبکه را آسان‌تر مدیریت کرد و سریع‌تر کارهای روزمره و عادی را پیگیری نمود.
LDAP پروتکلی است که امکان ارتباط با سرویس دایرکتوری و مدیریت اطلاعات و کاربران روی یک شبکه را فراهم می‌کند. این سرویس توسط ابزار OpenLDAP در لینوکس اجرا می‌شود و مخصوص سکوی نرم‌افزاری اپن‌سورس برای سازگاری با دیگر سکوها است. در صورت نبود این پروتکل در لینوکس، مدیران شبکه مجبور می‌شدند از ابزارهای شبیه‌سازی و مجازی‌سازی برای راه‌اندازی یک کلاستر جهت ارتباط با سرویس دایرکتوری سیستم‌عامل‌هایی مانند ویندوز استفاده نمایند