OpenLDAP

O OpenLDAP é uma implementação open source do protocolo LDAP. Existem versões do OpenLDAP para os mais variados sistemas operacionais como: Linux, BSD, AIX, HP-UX, MacOS, Solaris, Microsoft Windows e z/OS. O pacote do OpenLDAP está disponível na maioria dos repositórios das distribuições Linux e seu código-fonte pode ser obtido através do endereço http://www.openldap.org.

Principais características do OpenLDAP:

- Suporte a IPV4 e IPV6
- Controle de acesso
- Suporte a vários tipos de bancos de dados
- Replicação da base
- Suporte a criptografia - SSL e TLS

Composição do pacote OpenLDAP:

- Servidor LDAP - daemon slapd
- Bibliotecas que implementam o protocolo LDAP
- Utilitários, ferramentas e clientes de exemplo

Instalação

Conforme mencionamos anteriormente o OpenLDAP possui pacotes compilados para a maioria das distribuições Linux, mas a instalação também pode ser feita a partir do código-fonte. Dentro do contexto no nosso curso vamos utilizar a instalação a partir do repositório da distribuição.

Debian/Ubuntu

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

Além da instalação do pacote slapd é recomendado instalar também o pacote ldap-utils que contém uma série ferramentas que auxiliam na administração do diretório. Durante a instalação um assistente será iniciado para auxiliá-lo na configuração inicial do serviço, serão feitas algumas perguntas e ao final será criada a raiz da árvore do LDAP. Por padrão o domínio configurado no servidor será utilizado como raiz da árvore, ou seja, se nossa máquina está configurada com o domínio **empresa.com.br** a base da nossa árvore será criada como dc=empresa,dc=com,dc=br, portanto certifique-se de que os arquivos /etc/hosts e /etc/hostname estão com os valores FQDN corretos. Após a instalação os arquivos referentes ao serviço do OpenLDAP serão armazenados no diretório /etc/ldap.

Caso seja necessário modificar a estrutura criada na instalação podemos utilizar o comando dpkg-reconfigure para executar novamente o assistente de configuração e realizar a mudanças desejadas na base de dados.

Reconfigurando o pacote slapd.

```
# dpkg-reconfigure slapd
```

Ao final da instalação os schemas core, cosine, nis e inetorgperson serão carregados no servidor LDAP, será criada a raiz da árvore do diretório (exemplo: dc=empresa,dc=com,dc=br), o usuário administrador será cn=admin,dc=empresa,dc=com,dc=br e a senha será informada durante a execução o assistente.

Gerenciando o serviço

Iniciando o daemon slapd:

```
# service slapd start
```

Parando o daemon slapd:

```
# service slapd stop
```

RedHat/CentOS/Fedora

```
# yum install openldap openldap-servers openldap-clients
```

Assim como fizemos para as versões baseadas em Debian/Ubuntu, recomendamos a instalação dos pacotes openldap-client e openldap que possuem, além do cliente, uma série de bibliotecas e ferramentas para auxiliar a administração do servidor. A instalação em distribuições baseadas em RedHat não possui um assistente de configuração, deixando a cargo do administrador realizar toda a configuração após a instalação do pacote, dessa forma, ao final da instalação o administrador deverá criar os arquivos LDIF necessários para carregar todos os schemas e construir a árvore do diretório. Após finalizar a instalação os arquivos serão armazenados no diretório /etc/openldap.

Iniciando o serviço:

```
# systemctl start slapd
```

Habilitar a inicialização automática do serviço:

```
# systemctl enable slapd
```

O servidor OpenLDAP será instalado com o schema core e serão criados apenas a raiz cn=config e o usuário administrador cn=Manager,dc=my-domain,dc=com.

Como as distribuições baseadas em Debian/Ubuntu possuem um assistente de configuração, vamos descrever os passos necessários para configurarmos a base das distribuições baseadas em RedHat/CentOS manualmente, assim teremos ambas as bases com as configurações muito semelhantes. Vamos precisar criar alguns arquivos LDIF com atributos que ainda não mencionamos, entretanto comentaremos sobre estes parâmetros mais à frente.

Adicionar os schemas *cosine*, *nis* e *inetorgperson*. O instalador disponibiliza os principais schemas no diretório /etc/openldap/schema, basta carregar os schemas desejados.

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

Crie uma senha para o usuário administrador e anote o hash que será gerado.

```
# slappasswd
New password:
Re-enter new password:
{SSHA}ngoCZqT9QjMNM9pRvSSnPYa6a3JvWIk2
```

Crie o arquivo config.ldif com o conteúdo abaixo.

```
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by
  dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
  read by dn.base="cn=admin,dc=empresa,dc=com,dc=br" read by * none
```

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=empresa,dc=com,dc=br
```

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=empresa,dc=com,dc=br
```

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}ngoCZqT9QjMNM9pRvSSnPYa6a3JvWIk2
```

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=admin,dc=empresa,dc=com,dc=br" write by anonymous auth by self write by *
none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=admin,dc=empresa,dc=com,dc=br" write by * read
```

Adicione as informações do arquivo a base

```
# ldapmodify  -Y  EXTERNAL  -H  ldapi:///  -f  config.ldif
```

Crie o arquivo base.ldif com a raiz do diretório (dc=empresa,dc=com,dc=br)

```
dn: dc=empresa,dc=com,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: Empresa
dc: Empresa
```

Adicione as informações à base

```
# ldapadd -x -D cn=admin,dc=empresa,dc=com,dc=br -W -f base.ldif
```

Configuração

Versões mais antigas do OpenLDAP possuíam todas as configurações em um arquivo de texto – slapd.conf, entretanto nas versões mais recentes as configurações passaram a ser armazenadas dentro da própria base do LDAP, esse novo formato é conhecido como RTC – Run-Time Configuration, com este método as alterações no servidor são feitas em tempo real, qualquer modificação feita na base do OpenLDAP é refletida imediatamente no servidor não sendo mais necessária a reinicialização do serviço. Esse método cria uma nova raiz na base do OpenLDAP chamada cn=config, dentro desta raiz ficam armazenadas todas as configurações do servidor. Para realizar qualquer alteração na configuração será necessário criar um arquivo LDIF com as mudanças desejadas e em seguida carregá-lo no OpenLDAP.

Migrando do slapd.conf para o cn=config

A migração do arquivo de configuração slapd.conf para o formato cn=config pode ser feita utilizando o aplicativo slaptest, ele irá ler o arquivo de configuração e irá gerar a base do LDAP compatível com o formato cn=config.

```
# slaptest -f /etc/ldap/slapd.conf -F /etc/ldap/slapd.d
```

- **-f :** especifica o arquivo de configuração slapd.conf
- **-F:** informa o diretório onde será criada a base no formato cn=config

Para iniciar o servidor utilizando o novo formato certifique-se de que o OpenLDAP irá ler as informações a partir do diretório informando como saída no comando slaptest, você pode utilizar o atributo -F do daemon slapd.

Detalhes da árvore de configuração

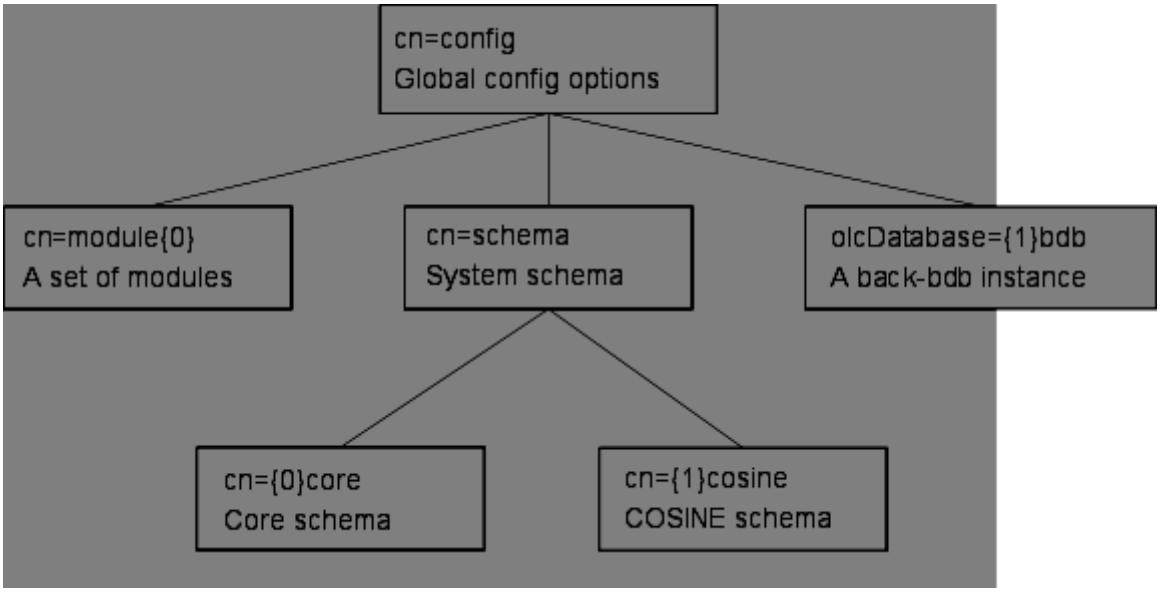

Figura 1: DIT cn=config

cn=config	Raiz da árvore de configuração que contém os atributos globais de configuração do servidor slapd.
cn=module{0}	Possui a lista dos módulos que são dinamicamente carregados pelo servidor.
cn=schema	Possui a lista dos schemas que estão carregados no servidor, cada galho representa um schema com suas respectivas configurações.
cn={0}core cn={1}cosine	Schemas que estão carregados no servidor. O número entre chaves representa a ordem com que os schemas serão lidos pelo servidor OpenLDAP.
olcDatabase={1}bdb olcDatabase={indice}tipo	Os registros do tipo olcDatabase contém as configurações referentes a base do LDAP, o valor entre chaves é um índice que determina a ordem de leitura das informações seguido pelo tipo de base à qual as configurações são pertinentes.

Tipo	Descrição
bdb	Berkeley DB transactional backend
config	Slapd configuration backend
dnssrv	DNS SRV backend
hdb	Hierarchical variant of bdb backend
ldap	Lightweight Directory Access Protocol (Proxy) backend
ldif	Lightweight Data Interchange Format backend
meta	Meta Directory backend
monitor	Monitor backend
passwd	Provides read-only access to passwd(5)
perl	Perl Programmable backend
shell	Shell (extern program) backend
sql	SQL Programmable backend

Tabela 1 – Tipos de backend

Populando a base do LDAP

Com o servidor devidamente instalado e a nossa DIT criada, podemos inserir os registros no nosso serviço de diretório. É muito comum encontrarmos empresas que já possuem uma base de usuários independente para a maioria dos serviços e quando a administração de todas essas bases começa a gerar problemas o LDAP surge como uma possível solução. Planejar a infraestrutura dos serviços é uma tarefa muito importante de um administrador de sistemas, mesmo que sua empresa ou instituição seja de pequeno porte o custo de se manter um serviço de autenticação centralizado deve ser muito bem avaliado pois poderá poupar muito trabalho no futuro.

Migration Tools

Conforme vimos no início do capítulo para inserirmos um registro na base do LDAP precisaremos criar um arquivo LDIF com as informações necessárias para caracterizar o objeto na base de dados, agora imagine que sua instituição possui 1000 usuários e 500 grupos diferentes e você precisa popular a base do servidor com essas informações, o mais obvio seria criar um script que percorresse os arquivo /etc/passwd, /etc/shadow e

/etc/group, gerasse os arquivos LDIF correspondentes aos usuários e grupos do sistema e em seguida incluísse essas informações na base. O pacote Migration Tools faz exatamente isso, ele é formado por um conjunto de scripts Perl que auxiliam na migração de contas de usuários, grupos, aliases, hosts, netgroups e etc para a base do LDAP. O projeto é mantido pela empresa PADL Software Pty Ltd e pode ser obtido através do site oficial da empresa ou através dos repositórios da maioria das distribuições Linux.

Instalação

Debian/Ubuntu

```
# apt-get install migrationtools
```

RedHat/CentOS

```
# yum install migrationtools
```

Configuração

Os scripts serão instalados no diretório /usr/share/migrationtools. Para distribuições baseadas em Debian/Ubuntu apenas o arquivo migrate_common.ph será armazenado no diretório /etc/migrationtools os demais scripts permanecerão no diretório /usr/share/migrationtools.

Edite o arquivo migrate_common.ph e configure as opções desejadas para a criação dos arquivos LDIF, vamos comentar as opções mais comuns.

Parâmetro	Descrição
NAMINGCONTEXT{'key'}	Determina o nome do galho da nossa DIT ao qual o script deverá relacionar o conteúdo que será migrado. O script é identificado pelo atributo key.
DEFAUL_MAIL_DOMAIN	Nome do domínio que será utilizado para o atributo mail.
DEFAULT_BASE	Base da nossa árvore do LDAP, será usado como sufixo para compor o atributo DN dos elementos da base.
EXTENDED_SCHEMA	Adiciona as classes de objetos organizationlPerson, inetOrgPerson entre outras.

Tabela 2 – Atributos de configuração do arquivo migrate_common.ph

Altere os atributos do arquivo migrate_common.ph conforme abaixo:

```
...
} else {
...
$NAMINGCONTEXT{'passwd'} = "ou=usuarios";
$NAMINGCONTEXT{'group'} = "ou=grupos";
$NAMINGCONTEXT{'hosts'} = "ou=maquinas";
…
$DEFAULT_MAIL_DOMAIN = "empresa.com.br";
$DEFAULT_BASE = "dc=empresa,dc=com,dc=br";
$EXTENDED_SCHEMA = 0;
```

Gerando o arquivo LDIF com a base da árvore do diretório:

```
# cd /usr/share/migrationtools
# ./migrate_base.pl > /tmp/base.ldif
```

O script migrate_base.pl que é responsável por criar o arquivo LDIF referente a DIT do nosso diretório, entretanto ele não é muito flexível e vai criar a base de acordo com os valores configurados nos atributos NAMINGCONTEXT{} do arquivo migrate_common.ph. Será necessário editar o conteúdo do arquivo /tmp/base.ldif para que ele possa representar a nossa DIT de maneira correta.

Gerando o arquivo LDIF dos usuários

```
# ./migrate_passwd.pl /etc/passwd /tmp/usuarios.ldif
```

Gerando o arquivo LDIF dos grupos

```
# ./migrate_group.pl /etc/group /tmp/grupos.ldif
```

Todos os usuários do arquivo /etc/passwd e grupos do arquivo /etc/group serão migrados para os respectivos arquivos *.ldif*, isso quer dizer que usuários e grupos do sistema como bin, sys, mail e outros também serão migradas. É recomendado editar os arquivos ldif gerados e deixar apenas os usuários e grupos válidos.

> A implementação do pacote migrationtools para Debian/Ubuntu possui as diretivas de configuração IGNORE (UID|GID) BELOW e IGNORE (UID|GID)_ABOVE que permitem especificar um intervalo de UIDs e GIDs que serão considerados na migração das contas, esse recurso é interessante para evitar que contas de usuários do sistema sejam adicionadas a base.

Inserindo as informações na base do LDAP

```
# ldapadd -x -W -D "cn=admin,dc=empresa,dc=com,dc=br" -f /tmp/base.ldif
# ldapadd -x -W -D "cn=admin,dc=empresa,dc=com,dc=br" -f /tmp/grupos.ldif
# ldapadd -x -W -D "cn=admin,dc=empresa,dc=com,dc=br" -f /tmp/usuarios.ldif
```

Podemos utilizar o comando slapcat para realizar o dump da base e verificarmos se as informações foram inseridas corretamente.

```
# slapcat
```