Linux Network Servers

OpenLDAP

A cada dia que surgem novos sistemas nas empresas a fim de resolver diversos tipos de problemas, logo cresce a necessidade de ter um maior controle e melhores mecanismos de busca de informação. Segurança e controle de dados são imprescindíveis em qualquer empresa. Umas das vantagens do OpenLdap é a possibilidade de que vários sistemas possam compartilhar de base de dados de usuários e senhas de forma centralizada e integrada.

O projeto OpenLdap é um serviço de diretório, que utiliza o protoloco LDAP (Lightweight Directory Access Protocol – Protocolo Leve de Acesso a Diretórios), baseado no protocolo X.500. O OpenLdap utiliza o trafego de dados via TCP-IP podendo ser implementado em diversas plataformas em redes IPV4 e IPV6, possibilitando autenticação, mecanismos de segurança no uso de certificados e criptografia, podendo ser configurado para restringir acesso a socket layer, ter multipla instâncias de banco de dados, múltiplas Threads, permite replicação e configuração do serviço de acordo com a sua necessidade através de Schema.

Características de um sistema de diretórios

- Centraliza e organiza informações;
- Evita redundância;
- É otimizado para fazer pesquisas, pois utiliza algoritmos de busca sofisticados;
- Podem ser distribuídos, isto é, não precisam necessariamente armazenar suas informações em um mesmo local.

Estrutura do LDAP

A organização da estrutura de dados do OpenLdap é hierárquica, sendo referenciada a forma de Árvore, com conceito de orientação de objetos. A árvore de informações do LDAP possui um elemento raiz, onde começa a busca das informações. Sendo assim, o sistema percorre os nós filhos até encontrar o elemento desejado. A raiz e seus ramos são diretórios. Por exemplo: temos um diretório raiz, depois temos a rede da empresa, o departamento (diretoria, secretaria, financeiro etc) e o funcionário. Logo, um diretório pode ter seus sub-diretórios que são chamados de entradas. Cada entrada possui um ou mais atributos (características). Os diretórios representam a raiz e os ramos, as entradas representam as folhas.

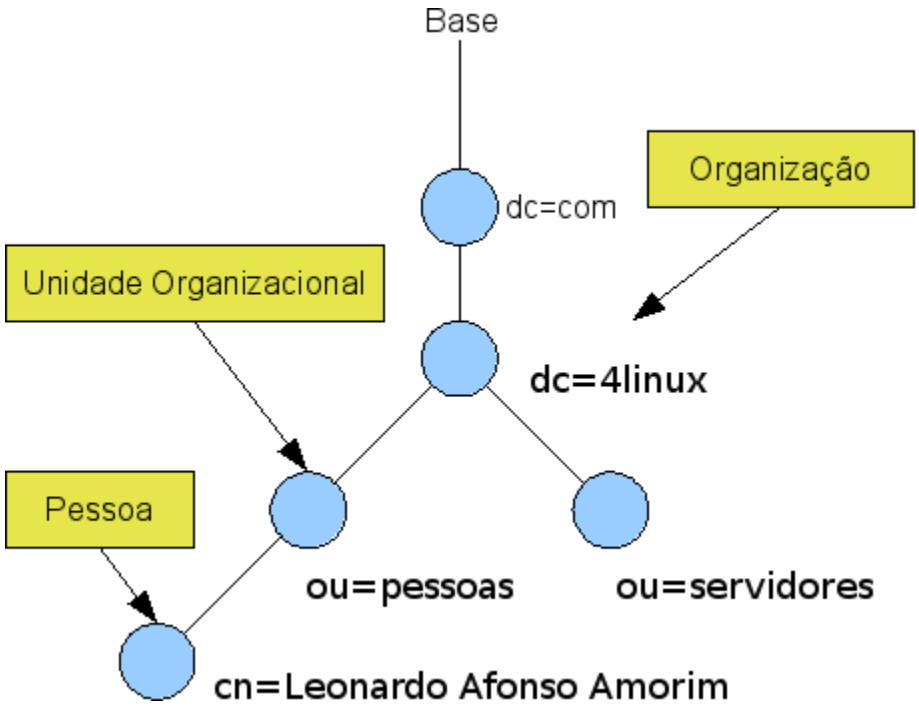
Atributos de diretórios:

Atributo	Descrição
c	Representa país (country)
o	Representa uma ornanização como uma empresa (organization)
ou	Representa um departamento (organization unit)

Linux Network Servers

Atributos de entradas:

Atributo	Descrição
cn	Representa um nome (common name)
uid	Representa a identidade de um usuário (user ID)
gn	Representa o nome próprio de uma pessoa (given name)
sn	Representa o sobrenome de uma pessoa (surname)



OpenLdap constitui-se de:

slapd - serviço openldap;
slurpd - serviço para replicação e atualização openldap;
libraries - são bibliotecas para implementação do OpenLdap, com utilitários e ferramentas;

Linux Network Servers

Instalação do OpenLDAP

Para instalar o servidor OpenLdap, com as ferramentas e bibliotecas necessárias, execute:

```
# aptitude install libldap2 ldap-utils slapd
```

Após a instalação, execute o comando que irá reconfigurar a base OpenLDAP para as nossas necessidades:

```
# dpkg-reconfigure slapd
```

O comando dpkg-reconfigure pode ser aplicado a qualquer pacote Debian.
Use-o quando omitir ou precisar reconfigurar aplicativos.

Este comando fará uma série de perguntas, e elas devem ser respondidas corretamente para que não haja problemas posteriores de configuração:

```
Omitir configuração do servidor OpenLDAP: NÃO
Informe o nome de domínio DNS para construir a base dn: seunome.com.br
Informe nome da organização: 4linux
Digite senha: 123456
Escolha base de dados: BDB
Remoção da base de dados quando o pacote slapd for expurgado: NÃO
Mover base antiga de dados em /var/lib/ldap: SIM
Permitir protocolo LDAPv2: SIM
```

Após realizar as configurações, inicie o daemon slapd:

```
# invoke-rc.d slapd start
```

Como verificar se o serviço está disponível para a rede?

Verifique se o serviço está disponível para a rede na porta 389:

```
# netstat -putan | grep 389
```

Linux Network Servers

O arquivo de configuração do servidor slapd está localizado em /etc/ldap/slapd.conf e, a não exige nenhum tipo de configuração adicional a não ser que o administrador saiba o que está fazendo, porém, há dois parâmetros extremamente relevantes para o administrador de sistemas.

O primeiro é o campo de schemas:

```
# Definições de Schema e objectClass
include/etc/ldap/schema/core.schema
include/etc/ldap/schema/cosine.schema
include/etc/ldap/schema/nis.schema
include/etc/ldap/schema/inetorgperson.schema
```

O que é um schema?

Um schema é um componente responsável por definir a sintaxe de regras e atributos de um objeto OpenLDAP, ou, basicamente, estes arquivos são responsáveis por decodificar e permitir a integração de ferramentas por parte do servidor.

Ao integrar ferramentas como o servidor de e-mails Postfix ou o sudo ao LDAP, esses pacotes já trazem um schema para realizar a integração.

O segundo parâmetro são as ACL's, que especificam quem pode efetuar escrita dentro do OpenLDAP.:

```
access to attrs=userPassword,shadowLastChange
by dn="cn=admin,dc=seu-nome,dc=br" write
by uid=”syadmin,dc=seunome,dc=com,dc=br” write
by anonymous auth
by self write
by * none
access to dn.base="" by * read
```

Cuidado com as ACL's de escrita no OpenLDAP.

No caso acima, tanto o usuário sysadmin quanto o usuário admin tem acesso de escrita na base.

Como testar a sintaxe do arquivo?

Faça o teste de sintaxe do arquivo com o comando slaptest:

```
# slaptest
```

Linux Network Servers

Uma dúvida muito comum de quem está iniciando em OpenLDAP é: Como migrar uma base local para uma base LDAP?

Para isso, existe a ferramenta migrationtools, uma série de scripts em perl que podem auxiliar neste processo.

Para instalar estes scripts, execute:

```
# aptitude install migrationtools
```

Este script possui algumas configurações padrão que precisam ser ajustadas, caso contrário, a migração pode ir por agua abaixo.

Abra o arquivo /usr/share/migrate_common.ph e edite as linhas abaixo:

```
$DEFAULT_MAIL_DOMAIN="seunome.com.br";
$DEFAULT_BASE="dc=seunome,dc=com,dc=br";
```

Após realizar esta configuração, precisamos gerar três arquivos, um contendo a raiz da arvore, outro contendo os grupos e o ultimo contendo os usuários:

```
# cd /usr/share/migrationtools
# ./migrate_passwd.pl /etc/passwd /etc/ldap/users.ldif
```

Após realizar este processo, abra o arquivo /etc/ldap/users.ldif. O mesmo deve apresentar várias entradas semelhantes a entrada abaixo.

O que é o LDIF?

Este formado é o LDIF (LDAP Data Interchange Format), e é desta maneira que os dados devem ser incluidos no sistema LDAP quando não temos nenhuma ferramenta de administração.

Cada sintaxe abaixo é definida por um atribto dentro de um “schema”.

A 4Linux possui um curso de OpenLDAP básico e avançado, aonde pode ser visto desde a integração de um servidor de correio até a definição e criação de um schema para LDAP.

Linux Network Servers

Este é um arquivo LDIF que define uma conta padrão Unix:

```
dn: uid=root,ou=People,dc=seunome,dc=com,dc=br
uid: root
cn:: cm9vdA==
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$1$dL7nEggA$P6Ib/H9QBkdd/sTcUBW1z1
shadowLastChange: 12495
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 0
gidNumber: 0
homeDirectory: /root
gecos: root
```

Agora vamos migrar a base de grupos do sistema e gerar a nossa base:

```
# ./migrate_group.pl /etc/group /etc/ldap/groups.ldif
# ./migrate_base.pl > /etc/ldap/base.ldif
```

Após gerar o arquivo base.ldif, remova as 9 primeiras linhas que definem o topo da arvore, pois eles já foram inclusos no OpenLDAP durante o comando "dpkg-reconfigure slapd".

Após criar os arquivos, adicione primeiramente o arquivo base.ldif com o comando abaixo:

```
# ldapadd -x -D cn=admin,dc=seunome,dc=com,dc=br -f /etc/ldap/base.ldif -W
```

Faça o mesmo para o arquivo groups.ldif:

```
# ldapadd -x -D cn=admin,dc=seunome,dc=com,dc=br -f /etc/ldap/groups.ldif -W
```

E por último, faça o mesmo para arquivo users.ldif:

```
# ldapadd -x -D cn=admin,dc=seu-nome,dc=com,dc=br -f /etc/ldap/users.ldif -W
```

Linux Network Servers

Administração via linha de comando

A suíte OpenLDAP possui alguns comandos para administração do servidor. Aprender a lidar com estes comandos é fundamental para qualquer administrador de redes.

O primeiro comando que devemos aprender a utilizar é o comando ldapsearch, pois é com ele que iremos efetuar buscas dentro da nossa arvore.

Para procurar o usuário aluno, execute:

```
# ldapsearch -x -b dc=seunome,dc=com,dc=br uid=aluno
```

O administrador pode buscar qualquer elemento dentro da arvore manipulando o parametro de busca. Experimente o seguinte comando:

```
# ldapserch -x -b dc=seunome,dc=com,dc=br uidNumber=1000
```

Outro comando importante é o ldapmodify. Com ele, é possível alterar, incluir ou remover praticamente qualquer campo da arvore de forma rápida, pratica e simples.

Vamos alterar o campo loginShell do usuário aluno. Para isso, crie um ldif com o seguinte conteúdo:

```
# vim /root/loginShell.ldif
dn: uid=aluno,ou=People,dc=seunome,dc=com,dc=br
changetype: modify
replace: loginShell
loginShell: /bin/false
```

Agora, vamos alterar o parametro loginShell com o comando:

```
# ldapmodify -x -D cn=admin,dc=seunome,dc=com,dc=br -f /root/loginShell -W
```

Linux Network Servers

Operações de Backup

Uma aula de OpenLDAP não estaria completa sem ao menos mencionar uma técnica de Backup/Restore de um servidor OpenLDAP.

Iremos, nesta seção, aprender a usar duas ferramentas do próprio projeto OpenLDAP, a ferramenta slapcat, para realizar o backup, e a ferramenta slapadd, para realizar o restore.

Para realizar o backup, simplesmente realize o seguinte comando:

```
# slapcat –l /root/backup.ldif
```

Gerando uma cópia de segurança:

```
# cp /root/backup.ldif /root/backup_copia.ldif
```

Para ter certeza que o seu backup é seguro, é importante realizá-lo em um periodo livre de gravações, ou com o servidor slapd desligado.

Após realizar o backup, vamos remover desligar o servidor slapd e remover sua base de dados inteira:

```
# ldapdelete -x -D cn=admin,dc=seunome,dc=com,dc=br -w secret -r
dc=seunome,dc=com,dc=br

# invoke-rc.d slapd stop
```

Como podemos nos certificar que a base realmente foi removida?

Para nos certificar-mos de que a base realmente foi removida, execute o comando slapcat novamente, mas tenha certeza de que você não está sobrescrevendo o seu backup:

```
# slapcat
```

E como restaurar a base usando o comando slapadd?

Vamos restaurar a nossa base, utilzando o comando slapadd:

```
# slapadd -l backup.ldif
```

Note que a arvore continua com os elementos que descrevem a base LDAP.

Abra o arquivo de backup e remova as linhas de 1 a 13. ;)

Linux Network Servers

Execute o comando slapcat novamente, para termos certeza que o backup foi restaurado:

```
# slapcat
```

Atenção: Os comandos slapcat, slapadd, ldapsearch e ldapadd poderão cair na prova de certificação.

Realize os backups de acordo com a política de sua empresa, e:
Execute testes de RESTORE periodicamente!

Configurando a autenticação dos clientes

Para que os nossos computadores possam autenticar-se como clientes LDAP, é necessário que modifiquemos uma série de arquivos do PAM e também é necessária a instalação de alguns pacotes.

Instalando os pacotes necessários e configure-os: de acordo com o instrutor:

```
#aptitude install libnss-ldap libpam-ldap
```

Qual a função do arquivo nsswitch.conf ?

O arquivo /etc/nsswitch.conf é o responsável por indicar aos programas e aplicativos aonde buscar o usuário e senha.

Modificando este arquivo, estamos mantendo a busca nos arquivos /etc/passwd e /etc/shadow, e ampliando as opções dizendo que o sistema também pode consultar uma base LDAP:

```
# vim /etc/nsswitch.conf
passwd:compat ldap
group: compat ldap
shadow:compat ldap
```

Agora vamos configurar o arquivo /etc/libnss-ldap.conf

```
# vim /etc/libnss-ldap.conf
nss_base_passwd ou=People,dc=seunome,dc=com,dc=br
nss_base_shadow ou=People,dc=seunome,dc=com,dc=br
```

Agora vamos configurar o arquivo /etc/pam_ldap.conf

```
#vim /etc/pam_ldap.conf
nss_base_passwd ou=People,dc=seunome,dc=com,dc=br
nss_base_shadow ou=People,dc=seunome,dc=com,dc=br
```

Linux Network Servers

Por último, iremos configurar o PAM para que ele busque os usuários na base LDAP.

Atenção: Muito cuidado, faça cópia dos originais e mantenha mais dois terminais de root abertos ;)

Configure o arquivo /etc/pam.d/common-auth

```
# vim /etc/pam.d/common-auth
```

Remova as opções existentes e acrescente estas:

```
auth sufficient pam_ldap.so
auth required pam_unix.so nullok_secure try_first_pass
```

Configure também o arquivo /etc/pam.d/common-account:

```
# vim /etc/pam.d/common-account
```

Remova as opções existentes e acrescente estas:

```
account sufficient pam_ldap.so
account required pam_unix.so
session required pam_mkhomedir.so skel=/etc/skel umask=0077
```

Agora configure o arquivo /etc/pam.d/common-password

```
# vim /etc/pam.d/common-password
```

Remova as opções existentes e acrescente estas:

```
password sufficientpam_unix.so nullok obscure min=4 max=8 md5
password required pam_ldap.so try_first_pass
```

Edite também o arquivo /etc/pam.d/common-session:

```
# vim /etc/pam.d/common-session
```

Remova as opções existentes e acrescente estas:

```
session sufficient pam_ldap.so
session required pam_unix.so
```

Linux Network Servers

A partir deste momento, qualquer usuário incluído no OpenLDAP estará apto a logar neste computador.

Existe uma interface administrativa para o OpenLDAP para facilitar nossa vida de administrador?

Qual?

Instalando uma interface administrativa

Como vimos até aqui, administrar um servidor OpenLDAP "na unha" pode ser uma tarefa extremamente cansativa, dependendo o tamanho da sua estrutura.

Para facilitar um pouco a nossa vida, iremos instalar uma ferramenta baseada em plataforma Web para realizar a administração do nosso servidor.

Para isso, instale o pacote phpldaadmin junto com suas ferramentas:

```
# aptitude install php-pear php5-ldap phpldapadmin
```

Abra o seu browser e digite no campo URL:

```
http://127.0.0.1/phpldapadmin/index.php
```

Para efetuar login, utilize o formato do próprio LDAP para especificar usuários:

```
cn=admin,dc=seunome,dc=com,dc=br
```

Configure o https para que a senha do admin não trafegue em texto claro pela rede. Além disso, é interessante colocar o OpenLDAP para trabalhar com OpenSSL:

```
http://www.bayour.com/LDAPv3-HOWTO.html#4.1.OpenSSL|outline
```

Autenticando o Squid na base de usuários LDAP

Para completar a nossa aula, que tal realizar a configuração do squid para que ele fique integrado ao nosso servidor OpenLDAP.

Para isso, abra o arquivo de configuração do squid que foi visto na aula já dada, e então configure-o:

```
# vim /etc/squid/squid.conf
auth_param basic program /usr/lib/squid/ldap_auth -b dc=seu-nome,dc=com,dc=br -f uid=
%s 192.168.200.1
```