Creación dun dominio en Linux

Sumario

- 1 Que é un dominio
- 2 OpenLDAP
  - 2.1 Instalar e configurar o servidor
  - 2.2 Crear o dominio
    - 2.2.1 Conexión co servidor
    - 2.2.2 Creación de unidades organizativas
  - 2.3 Instalar e configurar os clientes
    - 2.3.1 libnss-ldap
    - 2.3.2 libpam-ldap
  - 2.4 Perfís móbiles mediante NFS
- 3 Integración de servizos co OpenLDAP
  - 3.1 vsFTPd
  - 3.2 Apache

Que é un dominio

Os dominios permiten centralizar a xestión de usuarios e administrar os recursos dunha LAN de forma eficiente. En Linux existen diferentes tecnoloxías para crear dominios, tanto en redes homoxéneas como en redes heteroxéneas con Linux e MS-Windows.

Aquí veremos OpenLDAP (Open *Lightweight Directory Access Protocol* ou Protocolo Lixeiro de Acceso a Directorios libre) como mecanismo de creación de dominios para redes Linux e Windows. Existen outros métodos, como NIS (*Network Information System*) (ou NIS+) e que, de feito, son moito máis sinxelos de configurar, porén, son incompatibles con Windows.

OpenLDAP non só proporciona autentificación para os usuarios dentro do sistema, senón que centraliza esta autentificación para os distintos servizos dun sistema informático como poidan ser: unha Web, un Wiki, unha aula virtual, un servidor ftp, os servidores de correo, etc.

Se na nosa rede dispomos dun servidor LDAP e configuramos todos os equipos e todos os servizos para que se autentifiquen nel, bastará con crear as contas de usuario e grupos no servidor LDAP para que estes poidan facer uso do sistema e dos seus servizos dende calquera posto da rede. É, polo tanto, un servizo ideal para centralizar a administración de usuarios nun único lugar. Tamén será necesario configurar os equipos clientes da rede para que utilicen o servidor LDAP como servidor de autentificación.

Os pasos a realizar para crear o dominio con OpenLDAP son:

1. Instalar e configurar OpenLDAP.
2. Crear o dominio.
3. Configurar os equipos clientes para que se autentiquen contra o OpenLDAP.

OpenLDAP

Instalar e configurar o servidor

O servidor OpenLDAP está dispoñible no paquete slapd (Stand-alone LDAP Daemon). Tamén convén instalar o paquete ldap-utils que contén utilidades adicionais:

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

Durante a instalación, pediranos que introduzamos o contrasinal de administrador do servidor ldap. Podemos configurar calquera contrasinal, por exemplo 'abc123.'

Unha vez instalado hai que configuralo:

```
sudo dpkg-reconfigure slapd
```

Contestaremos ás preguntas que se nos van facendo. As respostas por defecto deberían funcionar para unha configuración básica. Se nalgún momento te equivocas introducindo os parámetros podes volver executar o asistente tecleando novamente o anterior comando.

Os ficheiros de configuración de OpenLDAP están en /etc/ldap/slapd.conf

Crear o dominio

Unha vez instalado e configurado o servidor LDAP, a seguinte tarefa é o deseño da estrutura e a introdución de datos no directorio. Posto que a finalidade do noso servidor LDAP é que sirva de almacén de usuarios e grupos para autentificación, deberemos crear unha estrutura que parta da **base do noso directorio**, para almacenar devandita información. Tal e como se explica máis abaixo, crearemos unha **unidade organizativa** (ou) chamada grupos, para almacenar os grupos de usuarios e crearemos outra unidade organizativa chamada usuarios para almacenar aos usuarios.

Para acceder ao directorio LDAP e poder crear e modificar elementos en devandito directorio convén ter un explorador de directorios LDAP (LDAP browser). Existen moitos exploradores LDAP tanto de pago como libres. Entre as aplicacións libres usaremos gq pero son bastante potentes phpldapadmin (aplicación web), JXplorer e LDAP Account Manager.

Para instalar gq, podemos utilizar apt-get. Unha vez instalada, para executar gq tan só debemos pulsar alt+f2 e escribir gq ou lanzala dende o menú gráfico:

```
sudo apt-get install gq
```

Conexión co servidor

A conexión co servidor LDAP podemos facela como usuario anónimo ou como usuario administrador. Se conectamos de forma anónima só poderemos visualizar os elementos pero non poderemos facer cambios; se conectamos como administrador, poderemos crear, modificar e eliminar elementos de calquera tipo.

Para conectar ao servidor LDAP como administrador necesitamos a seguinte información:

- Dirección IP do servidor LDAP
- Protocolo do servidor (LDAP v3 no noso caso)
- Base do directorio (dc=asim,dc=org no noso caso)
- Nome de usuario administrador (cn=admin,dc=asim,dc=org no noso caso)
- Contrasinal (abc123. no noso caso)

A base do directorio adóitase denominar en inglés **base DN** ou Nome Distinguido da base do directorio.

O nome do usuario co que nos conectamos adóitase denominar en inglés user DN ou tamén **bind** DN**.**

O nome de usuario administrador por defecto adoita ser admin e a miúdo hai que proporcionar nome e base do directorio: cn=admin,dc=asim,dc=org

Creación de unidades organizativas

O directorio estrutúrase en unidades organizativas (en inglés *organizational unit* - ou). No nosos caso, estas van almacenar usuarios e grupos polo que haberá que crealas mediante o gq.

No momento de crear unha ou aparecerá unha ventá de introdución de datos para o elemento que estamos a crear. Os elementos do OpenLDAP organízanse en objectClasses, ou **tipos de obxectos**. Como se trata dunha unidade organizativa debemos seleccionar o tipo organizationalUnit. Existen moitos tipos de obxectos que teñen distintos atributos, para dar cabida a diferentes configuracións.

Unha vez creadas as ou hai que crear os grupos propiamente ditos, os usuarios e asignar os usuarios aos seus grupos correspondentes:

- **Grupos**. Para crear os grupos dentro da unidade organizativa pódese usar o objectClass de tipo posixGroup, co cal observarás os atributos clásicos dun grupo POSIX. Podes introducir membros ao grupo, dentro deste tipo de obxecto, aínda que todavía non existan os usuarios.
- **Usuarios**. Para crear os usuarios dentro da unidade organizativa o tipo de obxecto pódese usar un usuario POSIX, polo tanto habería agregar o tipo posixAccount. Esta tipoloxía obríganos, pola xerarquía das clases do OpenLDAP, a que dependa dun objectClass de tipo Account, polo que habería que engadilo tamén.

Instalar e configurar os clientes

Unha vez que temos o servidor OpenLDAP funcionando, realizaranse as modificacións nos clientes Linux para que, no canto de utilizar os clásicos ficheiros do sistema /etc/passwd, /etc/group e /etc/shadow, autentiquen aos usuarios contra o servidor OpenLDAP. Para iso é necesario instalar e configurar o paquete **libnss-ldap** e **libpam-ldap**.

libnss-ldap

NSS (*Name System Switch*) permite acceder a fontes de datos no sistema para obter información como alias de correo, nomes de máquinas, claves de usuario, etc. O acceso a estas fontes de datos configúrase no ficheiro nsswitch.conf. No noso caso servirá para indicarlle ao cliente que teña tamén en conta a base de datos do OpenLDAP, para aquelas aplicacións que o precisen. Para máis información:

```
man nsswitch.conf
```

Para instalar o paquete:

```
sudo apt-get install libnss-ldap
```

Durante a instalación teremos que introducir información para indicarlle ao cliente quen é o servidor OpenLDAP contra o que se ten que autenticar. Pódese relanzar o asistente de configuración en caso de que se cometa un erro:

```
sudo dpkg-reconfigure ldap-auth-config
```

O ficheiro de configuración que alberga a información que se acaba de introducir é o /etc/ldap.conf, que pode editarse se se requiren opcións adicionais na configuración.

Para que o servidor LDAP actúe coma se se tratara dos ficheiros passwd, group e shadow debemos indicar no ficheiro /etc/nsswitch.conf que se utilice LDAP como alternativa para autentificar usuarios. Podemos editar o ficheiro a man ou exectuar o seguinte comando que o cambiará automaticamente:

```
sudo auth-client-config -t nss -p lac_ldap
```

As opcións teñen o seguinte significado:

- **-t**: modifica o ficheiro /etc/nsswitch.conf. Tamén se poderían modificar os ficheiros da librería libpam-ldap.
- **-p**: indica o perfil a habilitar, deshabilitar, etc.
- **lac_ldap**: é o nome do perfil que forma parte do paquete.

Para máis información pódense usar as páxinas de manual.

libpam-ldap

PAM (*Pluggable Authentication Modules*) é o sistema de autenticación modular de Linux. A libraría libpam-ldap permite que as aplicacións que utilizan PAM para a autenticación poidan facela mediante un servidor LDAP. Para que o sistema linux se autentique mediante un servidor LDAP é necesario instalar esta libraría xa que utiliza PAM. Hai outras aplicacións ou servizos que utilizan PAM para a autenticación e polo tanto tamén poderían autenticarse ante un servidor LDAP.

Ao instalar libnss-ldap xa se instala o paquete libpam-ldap. Para especificar o modo de autenticación de cada servizo é necesario configurar os ficheiros que se atopan no cartafol /etc/pam.d/. No noso caso abonda con exectuar o seguinte comando:

```
sudo pam-auth-update
```

No asistente de configuración hai que escoller LDAP e, se é o caso, outros mecanismos de autenticación.

Hai que modificar adicionalmente o ficheiro /etc/pam.d/common-session para que se cree automaticamente o home, se este non existe, cando o usuario inicie sesión. Engadirase a seguinte liña ao final:

```
session   optional      pam_mkhomedir.so skel=/etc/skel umask=077
```

Para que os usuarios poidan cambiar a súa clave hai que modificar o ficheiro /etc/pam.d/common-password comentando as liñas onde aparece pam_unix.so e pam_ldap.so. Ademais hai que incluír as dúas seguintes liñas:

```
password sufficient pam_ldap.so
password required pam_unix.so nullok obscure min=4 max=8 md5 use_first_pass
```

Os arquivos comúns que se atopan en /etc/pam.d son:

- **/etc/pam.d/common-auth** (para autenticarse)
- **/etc/pam.d/common-account** (para dispor dunha conta)
- **/etc/pam.d/common-session** (para poder iniciar sesión)
- **/etc/pam.d/common-password** (para poder cambiar a clave).

Estes ficheiros conteñen unha liña que fai referencia á libraría pam_unix.so que corresponde a autenticación contra os ficheiros Linux. Para que os servizos do noso sistema utilicen primeiro as librarías pam_ldap.so para autenticar ao usuario, o comando anterior engade a liña pam_ldap.so nos ficheiros common. Así, auntenticará primeiro contra o servidor LDAP, e se a autenticación falla, probará despois cos ficheiros Linux.

Para poder xestionar o dominio correctamente hai que configurar o servidor de dominio para que tamén se autentique contra o LDAP, polo que será necesario configurar tamén no servidor as librerías anteriores.

Perfís móbiles mediante NFS

Se queremos que os /home dos usuarios estean centralizados no servidor podemos usar unha solución simple: NFS. Deste xeito, o cartafol persoal do usuario montarase cada vez que este se autentique no sistema, independentemente da máquina que use.

Hai que configurar o servidor e o cliente para iso. No servidor hai que engadir ao ficheiro /etc/exports a seguinte liña (os parámetros de rede poden cambiar dependendo da configuración de rede da máquina):

```
/home           10.0.0.0/8(rw,sync,no_subtree_check,no_root_squash)
```

Para exportar o novo punto de montaxe:

```
exportfs -a
```

No cliente hai que engadir a seguinte liña ao ficheiro /etc/fstab:

```
10.0.0.50:/home         nfs defaults,sync
```

Suponse que o servidor é 10.0.0.50. Para montar o novo directorio sen ter que reiniciar o sistema pódese executar o seguinte comando:

```
mount -a
```

Integración de servizos co OpenLDAP

Xa se comentou a potencialidade que proporciona un servidor OpenLDAP nunha rede, xa que permite centralizar o servizo de autenticación para as aplicacións. Anteriormente, veuse como centralizar a autenticación dos usuarios contra o sistema. Agora, verase como "obrigar" ao servidor FTP e ao Apache a que utilicen o OpenLDAP como mecanismo de autenticación.

Normalmente, a configuración de cada servizo para que use os usarios dados de alta no OpenLDAP variará, polo que teremos que consultar a información correspondente para parametrizar correctamente a aplicación.

vsFTPd

No caso do vsFTPD a integración co OpenLDAP é inmediata xa que utiliza PAM como mecanismo de autenticación. No ficheiro de configuración do programa, en /etc/vsftpd, xa hai unha liña que indica que a autenticación se realiza mediante PAM:

```
pam_service_name=vsftpd
```

No cartafol de configuración de PAM en /etc/pam.d/ hai un ficheiro para o servizo vsftpd onde se inclúen os ficheiros common-account e common-session. Dado que o servidor xa o configuramos para que as aplicacións que usan PAM empreguen o OpenLDAP como sistema de autenticación, abonda con configurar o vsFTPd segundo as nosas necesidades, por exemplo:

```
#Deshabilitamos o acceso anónimo
anonoymou_enable=NO
```

```
#Habilitamos o acceso e a escritura para usuarios locais do sistema
local_enable=YES
write_enable=YES

#Engaiolamos aos usuarios no seu directorio /home
chroot_local_user=YES
```

Apache

O servidor Web Apache non usa PAM como sistema de autenticación, senón que emprega unha serie de directivas propias, tal e como se veu no tema dedicado a este servizo. As restricións de acceso realízanse, normalmente, sobre o contido de directorios. Por iso, existe unha directiva chamada Directory que á súa vez conterá outras directivas que afectarán ao acceso ao contido dese directorio.

Para que o Apache use o OpenLDAP como sistema de autenticación primeiro hai que habilitar o módulo authnz_ldap:

```
sudo a2enmod authnz_ldap
```

A continuación hai que configurar as directivas dentro de Directory:

```
<Directory ruta ao directorio afectado>
#Directivas de configuración que afectan ao directorio especificado
AuthBasicProvider ldap
AuthType        Basic                           #Tipo autentificación
AuthName        "Acceso restrinxido"    #Mensaxe informativa
AuthLDAPURL "ldap://127.0.0.1/ou=usuarios,dc=asim,dc=org"       #Ruta ao servidor
AuthLDAPBindDN "cn=admin,dc=asim,dc=org"
AuthLDAPBindPassword "abc123."
Require valid-user      # Todos os usuarios do OpenLDAP
# Require user nome_usuario     #Lista usuarios permitidos
</Directory>
```

--Arribi 11:28 8 may 2009 (BST)