NFS e Kerberos

Sumario

- 1 **ANTES DE COMEZAR** Antes de comezar con esta sección é imprescindible que a configuración descrita nos pasos anteriores do material funcione correctamente. En concreto, para poder comezas os pasos que se indican, **débese comprobar que**:
    - O cliente está configurado para autenticarse contra o servidor LDAP usando o protocolo seguro **LDAPS** (Apartado Autenticación segura contra o LDAP. Uso de TLS/SSL)
    - O cliente é capaz de montar carpetas do servidor por NFSv3 (Apartado Configuración do cliente NFS)
    - O cliente de kerberos está cofigurado correctamente para adquirir os tickets de kerberos no inicio de sesión dos usuarios (Apartado Configuración do cliente kerberos)

  Se algo disto non funcionase, debe solucionarse antes de seguir.
- 2 Requisitos previos para kerberizar o NFS
    - 2.1 Sincronizar a hora do cliente e servidor
    - 2.2 Crear no servidor de DNS unha entrada para a máquina cliente
    - 2.3 Configurar o cliente NFS tanto no cliente como no servidor
    - 2.4 Modificar o nome local dos equipos cliente e servidor
- 3 Creación dos *principals* e credenciais para o cliente e o servidor
- 4 Modificacións na configuración de kerberos
- 5 Modificacións na configuración do servidor e cliente NFS
    - 5.1 Modificacións no servidor NFS
    - 5.2 Modificacións no cliente NFS
- 6 Exportar a carpeta no servidor
    - 6.1 Eliminar as exportacións por NFS sen autenticación kerberos
    - 6.2 Crear as exportación por NFS con autenticación kerberos
- 7 * Crea o directorio para o pseudofilesystem (*/export*): **sudo mkdir /export**
    - Crea dentro deste directorio un directorio co nome da carpeta que lle indicamos que hai que exportar (ollo, directamente a carpeta, pero non a ruta completa:

  sudo mkdir /export/iescalquera
    - Crea unha montaxe de *loopback* para que esta carpeta enlace coa carpeta que queremos exportar (podemos vela co comando *mount*). Se visualizamos o ficheiro */etc/fstab*, atoparemos a seguinte liña que é a que fai esta montaxe:

  /home/iescalquera /export/iescalquera bind bind 0
    - No ficheiro de configuración de NFS (*/etc/exports*) crea dúas liñas, unha para definir o pseudofilesystem (levará sempre a opción *fsid*) e outra para definir a carpeta exportada dentro del:

  /export gss/krb5(no_subtree_check,rw,nohide,fsid=0) /export/iescalquera gss/krb5(no_subtree_check,rw,nohide)
- 8 Montar a carpeta no equipo cliente
- 9 Inicio de sesión no cliente en modo gráfico

ANTES DE COMEZAR

Antes de comezar con esta sección é imprescindible que a configuración descrita nos pasos anteriores do material funcione correctamente. En concreto, para poder comezas os pasos que se indican, **débese comprobar que**:

- O cliente está configurado para autenticarse contra o servidor LDAP usando o protocolo seguro **LDAPS** (Apartado Autenticación segura contra o LDAP. Uso de TLS/SSL)
- O cliente é capaz de montar carpetas do servidor por NFSv3 (Apartado Configuración do cliente NFS)
- O cliente de kerberos está cofigurado correctamente para adquirir os tickets de kerberos no inicio de sesión dos usuarios (Apartado Configuración do cliente kerberos)

Se algo disto non funcionase, debe solucionarse antes de seguir.

Unha vez configurados o servidor e cliente kerberos, neste apartado imos ver os pasos necesarios para *kerberizar* o servizo NFS, e que faga uso do ticket emitido polo servidor kerberos para autenticar os usuarios. Isto é o máis complexo de todo o proceso, así que recoméndase que se faga con calma e paciencia, revisando ben cada un dos pasos.

Requisitos previos para kerberizar o NFS

Neste primeiro apartado imos realizar unha serie de configuracións previas necesarias para poder utilizar NFS con autenticación kerberos:

Sincronizar a hora do cliente e servidor

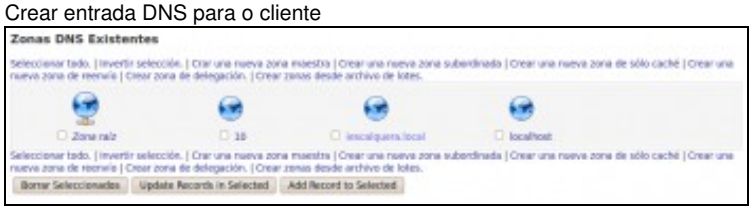
Como xa se comentou anteriormente, kerberos require para a emisión dos tickets unha sincronización da hora entre o cliente e o servidor, xa que unha diferenza de máis de cinco minutos entre elas fará que o protocolo non funcione correctamente.

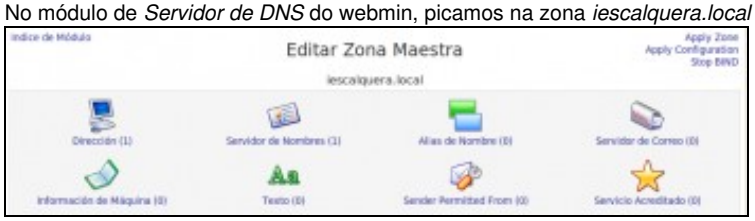
Polo tanto, é conveniente comprobar de novo que realmente a hora do equipo cliente e o servidor coinciden (podemos usar o comando *date* para ver a hora do sistema). Hai que ter moito coidado neste sentido sobre todo se se están utilizando máquinas virtuais, xa que ao gardar e restaurar o estado as horas moi probablemente se desincronizarán (Isto fará bastante latoso a configuración de nfs con kerberos con máquinas virtuais, xa que cada vez que restauremos o estado gardado probablemente kerberos deixará de funcionar correctamente ata que non resincronicemos as horas). Recórdese que se pode sincronizar a hora con un servidor de tempo co comando:

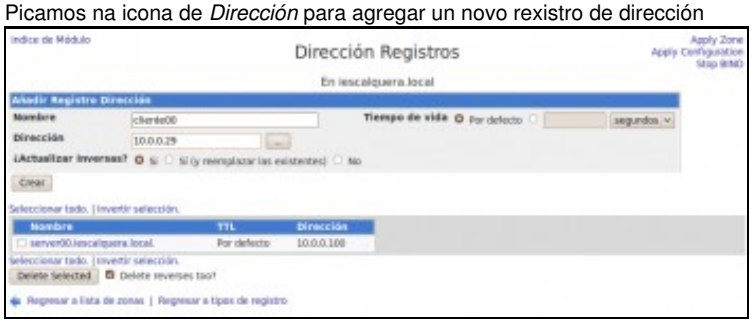
```
sudo ntpdate es.pool.ntp.org
```

Crear no servidor de DNS unha entrada para a máquina cliente

De momento na zona DNS asociada ao noso dominio (*iescalquera.local*) só introducimos un rexistro para a máquina servidor, no que lle asignamos o nome *server00.iescalquera.local*. Para que NFS funcione con kerberos, o servidor ten que poder resolver por DNS a dirección IP do equipo cliente e tamén ten que poder realizar a consulta inversa (é dicir, poder resolver o nome do equipo cliente a partir da súa dirección IP), así que os dous equipos deberán ter configurado como servidor de DNS o servidor e agregaremos un novo rexistro na zona para o equipo cliente, activando tamén a creación do rexistro de dirección inversa:

- Crear entrada DNS para o cliente
- 

No módulo de *Servidor de DNS* do webmin, picamos na zona *iescalquera.local*
- 

Picamos na icona de *Dirección* para agregar un novo rexistro de dirección
- 

Introducimos o nome e a dirección IP do rexistro

- 

Vemos o rexistro creado, e picamos no enlace *Apply Zone* para aplicar os cambios e activar o novo rexistro

Configurar o cliente NFS tanto no cliente como no servidor

Tanto o cliente como o servidor teñen que utilizar como servidor de DNS o servidor local, para poder resolver correctamente os nomes dos equipos do dominio (*cliente00.iescalquera.local*, *server00.iescalquera.local*, etc.). Así que configuraremos nos dous casos o ficheiro /etc/resolv.conf introducindo como servidor de DNS a dirección IP do servidor:

```
nameserver 10.0.0.100
```

(**NOTA:** Debemos ter moito coidado de que nin o cliente nin o servidor tomen o servidor de DNS por DHCP, xa que entón cada vez que adquiran unha dirección cambiarase a configuración do servidor de DNS) Tamén pode ser Ollo que non teñan a IP por DHCP, xa que pode establecer de novo o servidor DNS con outro servidor.

Modificar o nome local dos equipos cliente e servidor

Para que o servidor NFS poida arrancar correctamente cando introduzamos exportacións con autenticación kerberos, o nome local da máquina debe corresponderse co nome que ten asignada no servidor DNS (no noso caso, *server00.iescalquera.local*). Así que modificaremos o nome do equipo co comando **hostname**:

```
sudo hostname server00.iescalquera.local
```

Pero este cambio de nome non é permanente, e se reiniciamos o equipo veremos que ten de novo o nome antigo. Para que o cambio de nome perdure, temos que editar o ficheiro **/etc/hostname** e modificar aí o nome do equipo. Simplemente borraremos o nome anterior e escribiremos, no noso caso, *server00.iescalquera.local*

Podemos comprobar en calquera momento o nome local do equipo con:

```
sudo hostname
```

Creación dos *principals* e credenciais para o cliente e o servidor

Para que a autenticación por kerberos funcione nas exportacións de NFS, tanto o cliente como o servidor teñen que ser *principals* na base de datos de kerberos, así que creamos os *principals* en kerberos para o cliente e o servidor. Executamos **no servidor** os seguintes comandos:

- Autentificámonos en kerberos co usuario admin (teremos que introducir o contrasinal de *admin* (*admin*)):

```
sudo kinit admin/admin
```

- Usamos o comando *kadmin.local* que permite administrar a base de datos de kerberos dende o propio servidor, para engadir os *principals*:

```
sudo kadmin.local -q "addprinc -randkey nfs/server00.iescalquera.local"
sudo kadmin.local -q "addprinc -randkey nfs/cliente00.iescalquera.local"
```

- Engadimos no servidor as credenciais do *principal* no ficheiro */etc/krb5.keytab*. Executamos o seguinte comando no servidor:

```
sudo kadmin.local -q "ktadd nfs/server00.iescalquera.local"
```

- O mesmo pero **no equipo cliente**. Executamos o seguinte comando **no cliente** (agora usamos o comando *kadmin* que permite xestionar a base de datos de kerberos de forma remota):

```
sudo kadmin -p admin/admin -q "ktadd nfs/cliente00.iescalquera.local"
```

Modificacións na configuración de kerberos

Dende a versión 10.04 de Ubuntu Server, o protocolo de cifrado que ten que usar kerberos que funcionar con NFS non está permitido por defecto, así que para que permita o seu uso teremos que editar o ficheiro /**etc**/**krb5.conf** tanto no **cliente como no servidor** introducindo dentro da sección **[libdefaults]** a seguinte liña:

```
 allow_weak_crypto = true
```

No servidor, despois deste cambio deberemos reiniciar os servizos de kerberos:

```
sudo /etc/init.d/krb5-admin-server restart
sudo /etc/init.d/krb5-kdc restart
```

Modificacións na configuración do servidor e cliente NFS

Tamén teremos que facer uns cambios na configuración do servidor NFS e cliente NFS para que funcione correctamente a versión 4 e poidamos usar kerberos:

Modificacións no servidor NFS

- Editamos o ficheiro /**etc**/**default**/**nfs-kernel-server** para poñer:

```
NEED_SVCGSSD=yes
```

- No ficheiro /**etc**/**default**/**nfs-common**:

```
NEED_IDMAPD=yes
NEED_GSSD=yes
```

- E por último, no ficheiro /**etc**/**idmapd.conf**:

```
Domain = iescalquera.local
```

- Reiniciamos o servidor nfs para activar os cambios, e lanzamos os servizos *idmapd* e *gssd*:

```
sudo service gssd start
sudo service idmapd start
sudo /etc/init.d/nfs-kernel-server restart
```

Modificacións no cliente NFS

- Editamos o ficheiro /**etc**/**default**/**nfs-common** para poñer:

```
NEED_IDMAPD=yes
NEED_GSSD=yes
```

- Modificamos tamén o ficheiro /**etc/idmapd.conf** co mesmo valor que no servidor:

```
Domain = iescalquera.local
```

- Lanzamos os servizos *idmapd* e *gssd*:

```
sudo service gssd start
sudo service idmapd start
```

Exportar a carpeta no servidor

Eliminar as exportacións por NFS sen autenticación kerberos

Por algún problema na versión de NFS que utiliza Ubuntu 10.10, non poderemos ter exportadas no servidor carpetas por NFS con autenticación de sistema (*sys*) e kerberos (*krb5*). Se o facemos, o cliente quedarase colgado ao intentar montar a carpeta por NFS. Así que é moi importante que antes de exportar e montar as carpetas con autenticación kerberos, eliminemos ou deshabilitemos as que están exportadas con autenticación *sys*:

- En primeiro lugar, debemos desmontar as carpetas no equipo cliente, por exemplo:

```
sudo umount /home/iescalquera
```

- Tamén teremos que eliminalas do ficheiro */etc/fstab* se é o caso.

- No servidor, usando o webmin ou editando o ficheiro de configuración */etc/exports*, eliminamos ou deshabilitamos (no ficheiro de configuración equivalería a comentalas) as exportacións que haxa de carpetas que haxa activas.

Crear as exportación por NFS con autenticación kerberos

Imos agora a crear as exportacións pero usando autenticación con kerberos. Usamos o webmin para crear unha exportación, neste caso das carpetas persoais dos usuarios, por NFSv4, activando a autenticación por kerberos:

Indice de Módulo
Ayuda..

Crear Exportación

Detalles de Exportación

NFS Version (•) 4 ( ) 3 (or lower)

NFSv4 Pseudofilesystem to export /export ...

Directorio a exportar /home/iescalquera ... in /export/iescalquera

¿Activo? (•) Si ( ) No

Exportar a... (with or without Authentication)

( ) sys
- (•) Todo el mundo
- ( ) Máquina(s)
- ( ) Clientes WebNFS
- ( ) Grupo de Red
- ( ) IPv4 Red — Máscara de Red
- ( ) IPv6 Address /

(•) krb5
( ) lipkey
( ) spkm-3

Security level (•) Ninguno ( ) Integrity ( ) Privacy (including Integrity)

Exportar seguridad

Sólo lectura ( ) Si (•) No

¿Los clientes deben de estar en puerto seguro? (•) Si ( ) No

Disable subtree checking? (•) Si ( ) No

Hide the filesystem? ( ) Si (•) No

Immediately sync all writes? ( ) Si ( ) No (•) Defecto

Confiar en usuarios remotos ( ) Todo el mundo (•) Todo el mundo excepto root ( ) Nadie

Tratar usuarios no fiables como (•) Por defecto ( ) ...

Tratar grupos no fiables como (•) Por defecto ( ) ...

NFSv2-specific options

¿Hacer enlaces simbólicos relativos? ( ) Si (•) No

¿Denegar acceso al directorio? ( ) Si (•) No

No confiar en UIDs (•) Ninguno ( )

No confiar en GIDs (•) Ninguno ( )

Crear

Regresar a lista de exportaciones

Os parámetros máis importantes da exportación son os seguintes:

- **Versión de NFS**: Seleccionamos versión 4, xa que é a que permite autenticación por kerberos.
- **Método de autenticación**: krb5 (Kerberos 5).
- **Só lectura**: Non, xa que os usuarios deben poder realizar modificacións sobre as súas carpetas persoais.
- **Deshabilitar *subtree checking***: Polos motivos xa explicados no apartado de instalación do NFS.
- **Hide the filesystem**: Non. Este parámetro permite que, cando nunha exportación se pasa dun sistema de ficheiros a outro (como é o noso caso, xa que */home* reside nunha partición aparte), se mostre por NFS o contido dese outro sistema de ficheiros.
- No parámetro de **Security level** temos a opción de seleccionar **Integrity** (integridade) ou **Privacity**. Estas opcións engaden mecanismos para garantir a integridade (no primeiro caso) e incluso a privacidade (no segundo caso, cifrando todas as comunicacións) das conexións NFS, pero haberá que ter en conta que se activamos algunha destas opcións suporá un degradamento considerable do rendemento do protocolo NFS.
- Por último, imos ver que significa iso de exportar a carpeta nun pseudo-sistema de ficheiros (*pseudofilesystem*). Ao exportar a carpeta dentro do pseudofilesystem */export*, o webmin fai automaticamente unha serie de operacións que poderíamos tamén facer manualmente, e que son as seguintes:

- Crea o directorio para o pseudofilesystem (*/export*):

sudo mkdir /export

- Crea dentro deste directorio un directorio co nome da carpeta que lle indicamos que hai que exportar (ollo, directamente a carpeta, pero non a ruta completa:

sudo mkdir /export/iescalquera

- Crea unha montaxe de *loopback* para que esta carpeta enlace coa carpeta que queremos exportar (podemos vela co comando *mount*). Se visualizamos o ficheiro */etc/fstab*, atoparemos a seguinte liña que é a que fai esta montaxe:

/home/iescalquera /export/iescalquera bind bind 0

- No ficheiro de configuración de NFS (*/etc/exports*) crea dúas liñas, unha para definir o pseudofilesystem (levará sempre a opción *fsid*) e outra para definir a carpeta exportada dentro del:

/export gss/krb5(no_subtree_check,rw,nohide,fsid=0)
/export/iescalquera gss/krb5(no_subtree_check,rw,nohide)

Con isto, conseguimos exportar unha carpeta por NFS independentemente da súa localización no disco, e a filosofía sería que as demais carpetas que exportásemos por NFS neste equipo as definíramos tamén dentro deste *pseudofilesystem*. Dende os equipos clientes, accederán as carpeta introducindo só o seu nome, e non a ruta na que se atopa cada carpeta no servidor.

Montar a carpeta no equipo cliente

Por último, quédanos montar a carpeta no equipo cliente. Podemos utilizar o comando *mount* para facer a montaxe::

```
sudo mount -t nfs4 -o sec=krb5 server00.iescalquera.local:/iescalquera /home/iescalquera
```

A carpeta montada coa opción de seguridade de kerberos será accesible para os usuarios que obteñan o ticket correspondente do servidor kerberos. Podemos iniciar sesión no cliente con un usuario que non teña creado un *principal* en kerberos para comprobar que non pode acceder á súa carpeta persoal, mentres que os usuarios que sexan *principals* de kerberos poderán acceder sen problemas.

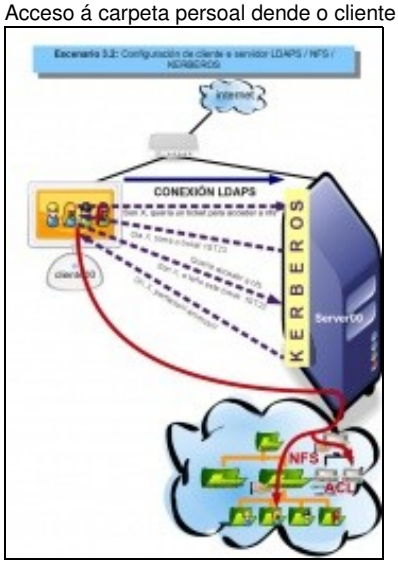
Se queremos montar a carpeta automaticamente cada vez que se arranca o equipo, podemos facer a montaxe no ficheiro */etc/fstab*, introducindo a liña:

```
server00.iescalquera.local:/iescalquera    /home/iescalquera   nfs4   sec=krb5   0   0
```

Inicio de sesión no cliente en modo gráfico

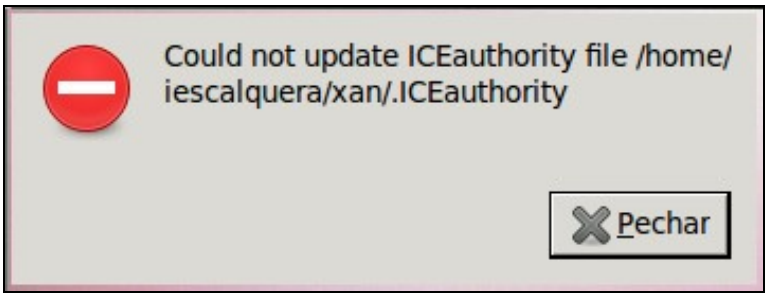
Coa unidade montada por NFSv4, podemos iniciar sesión no cliente en modo gráfico con un usuario que estea definido como *principal* de kerberos, e accederá a súa carpeta persoal utilizando o ticket que o obtén no inicio de sesión. Con isto xa acadamos o obxectivo fixado no escenario 3.2:

- Dominio co carpetas compartidas por NFS con kerberos
- 

  Acceso á carpeta persoal dende o cliente con un usuario do dominio
- 

  Escenario 3.2

Debido a algún *bug* na montaxe por NFSv4, aparecerá unha mensaxe de erro no inicio de sesión (poden atoparse en Internet moitas referencias a este erro, pero ata o momento non atopamos ningunha solución ao asunto):



-- Antonio de Andrés Lema e Carlos Carrión Álvarez