

Integración de FreeNAS nun dominio LDAP

- Neste apartado veremos os pasos necesarios para integrar o equipo FreeNAS dentro do dominio, de forma que poidamos acceder a el cos usuarios do mesmo.
- Antes de nada, debemos crear unha instantánea na máquina FreeNAS, co nome **Recén instalada**
- E restaurar as máquinas *dserver00* e *uclient01* á instantánea:
 - ♦ **Escenario 2.A - NFS**, se se vai facer o escenario 7.A ([Compartición de recursos por NFS nun dominio con LDAP](#))
 - ♦ **Escenario 3.B - Samba3 - Clientes Linux**, se se vai facer o escenario 7.B ([Compartición de recursos por CIFS nun dominio con LDAP e Samba3](#)). Neste caso, tamén restauraremos *wclient01* á instantánea **Escenario 3.A - Samba3 - Clientes Windows**

Sumario

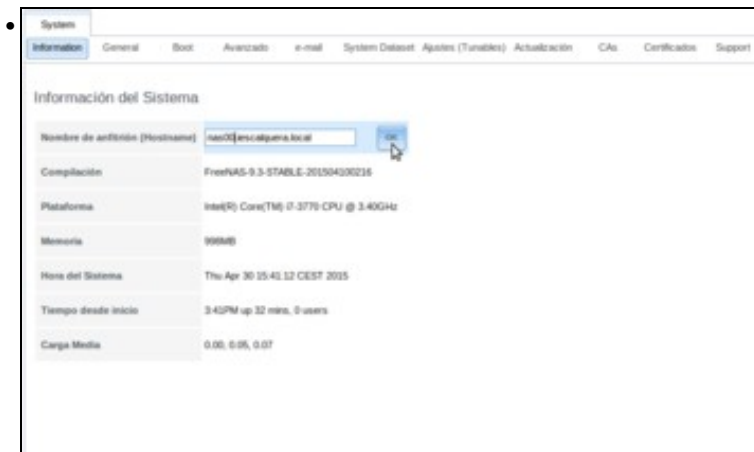
- 1 Cambiar o nome da máquina
- 2 Crear pool zfs e configuralo como pool do sistema
- 3 Integrar o equipo no dominio
 - ♦ 3.1 Integración nun dominio con LDAP e NFS
 - ♦ 3.2 Integración nun dominio con LDAP e samba3
- 4 Comprobación dos usuarios do dominio
- 5 Crear o esqueleto de carpetas
- 6 Configurar os permisos
- 7 Creación das carpetas persoais dos usuarios (home)

Cambiar o nome da máquina

- Este paso non é imprescindible, pero imos cambiar o nome da máquina para poñer o que se corresponde co escenario.
- Cambiar o nome da máquina



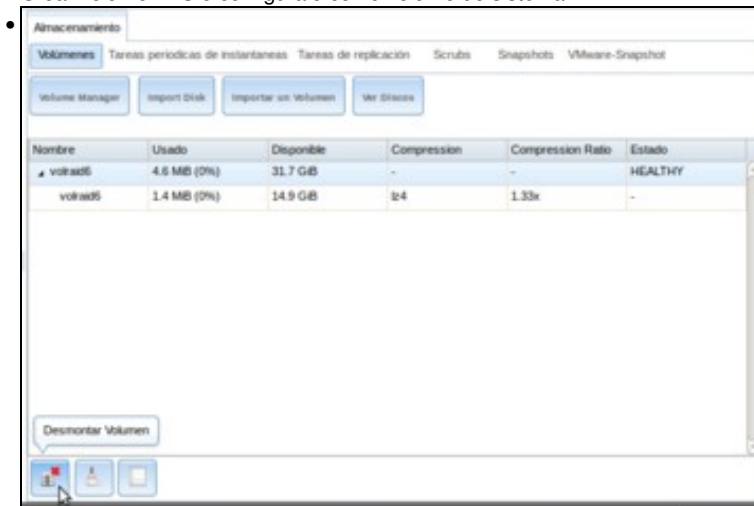
Se picamos na opción de **Información del sistema** na ferramenta de administración de FreeNAS, veremos que por defecto ten como nome *freenas*. Este nome non ten ningún inconveniente, pero nós seguindo o noso esquema queremos que o nome do equipo sexa *nas00.iescalquera.local*. Picamos no botón de **Edit** para cambiar o nome.



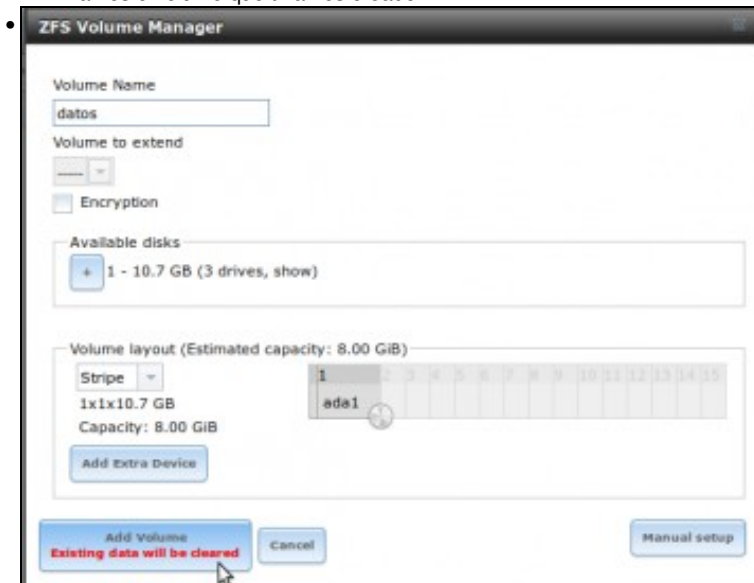
Introducimos o novo nome (**nas00.iescalquera.local**) e picamos en **Ok**.

Crear pool zfs e configuralo como pool do sistema

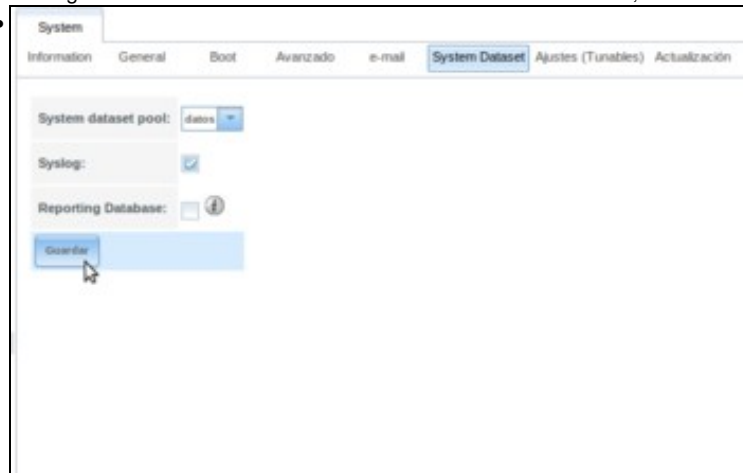
- Para integrar o equipo FreeNAS no dominio non habería por que ter ningún volume definido, pero nas últimas versións FreeNAS precisa ter configurado algún volume como *volume do sistema*, xa que aí garda certa información de configuración. Esta información é necesaria para poder iniciar algúns servizos como SMB.
- Crear volume ZFS e configuralo como volume do sistema



Eliminamos o volume que tiñamos creado.



Abrimos o xestor de volumes ZFS para crear un volume co nome *datos*. Podemos facer un volume en RAID con varios discos, pero tendo en conta que traballamos con unha máquina virtual na que os discos residen en realidade en ficheiros dun mesmo disco duro físico non imos conseguir un mellor rendemento senón todo o contrario. Por tanto, imos coller un único disco para o volume, e picamos en **Add Volume**.



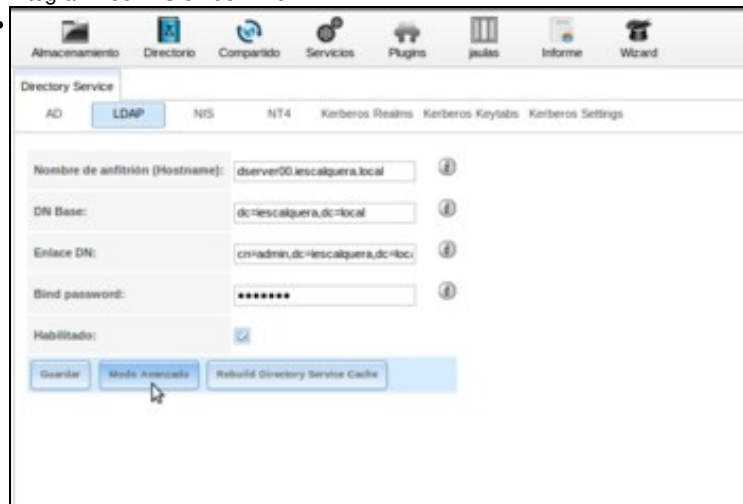
Unha vez creado o volume (en realidade, o pool) ZFS, imos á lapela de **Conxunto de datos do sistema** do apartado **Sistema** e comprobamos que ese volume xa está seleccionado na opción de **System dataset pool**.

Integrar o equipo no dominio

- Imos xa coa integración da máquina FreeNAS dentro do dominio para que recoñeza os usuarios e grupos do servidor LDAP. Aquí a configuración será diferente se estamos traballando nun dominio con samba3 e CIFS ou tan só co LDAP e NFS.

Integración nun dominio con LDAP e NFS

- Integrar FreeNAS en dominio LDAP



Picamos no botón de **Directorio** e imos ao apartado de **LDAP**. Introducimos:

- * O equipo que executa o servizo LDAP, **dserver00.iescalquera.local**
- * Como **DN Base** a rama base das buscas no LDAP: **dc=iescalquera,dc=local**
- * A DN do usuario administrador: **cn=admin,dc=iescalquera,dc=local**
- * O contrasinal dese usuario no LDAP
- * Activamos a opción de **Habilitado**.

Picamos no botón de **Modo Avanzado** para cambiar algún parámetro máis.

[illegible]

Cubrimos o sufixo das OUS dos usuarios, grupos e máquinas no LDAP e xa podemos gardar os cambios.

Directory Service

AD **LDAP** NIS NT4 Kerberos Realms Kerberos Keytabs Kerberos Settings

Notice: samba extensions not detected. CIFS authentication to LDAP disabled.

Nombre de anfitrión (Hostname): ⓘ

DN Base: ⓘ

Enlace DN: ⓘ

Contraseña de enlace:

Habilitado: ☒

Veremos unha advertencia indicando que a autenticación con CIFS estará desactivada xa que LDAP non ten as extensións de Samba.

Integración nun dominio con LDAP e samba3

- Integrar FreeNAS en dominio LDAP e samba3

The screenshot shows the 'Servicios' (Services) tab in the Windows Server configuration console. The list of services includes:

- AFP: OFF (locked)
- Controlador de Dominio: OFF (locked)
- DNS Dinamica: OFF (locked)
- FTP: OFF (locked)
- iSCSI: OFF (locked)
- LLDP: OFF (locked)
- NFS: OFF (locked)
- Rsync: OFF (locked)
- S.M.A.R.T.: ON (locked)
- SMB: OFF (locked)** (highlighted)
- SNMP: OFF (locked)
- SSH: ON (locked)

A tooltip labeled 'Configuración SMB' is visible over the lock icon of the SMB service.

En primeiro lugar, imos configurar o servizo de SMB (tamén chamado *CIFS*) para que o equipo se introduza correctamente no dominio samba3. Picamos no botón de **Servizos** e logo na chave asociada ao servizo de **SMB**.

Configuración SMB

Nombre de NetBIOS:	nas00
NetBIOS alias:	
Grupo de Trabajo:	IESCALQUERA
Descripción:	FreeNAS Server
Juego de caracteres DOS:	CP437
Juego de caracteres UNIX:	UTF-8
Nivel de registro:	Windows
Use syslog only:	☐
Maestro Local:	☐
Inicios de sesión de dominio:	☐
Servidor de Hora para el Dominio:	☐
Cuenta de invitado:	nobody
Máscara de permisos de Archivo:	
Máscara de permisos de Directorio:	
Permitir Contraseña vacía:	☐
Parámetros auxiliares:	

Introducimos o nome do dominio no **grupo de traballo**, e desmarcamos as opcións de **Maestro local** e **Servidor de hora para o dominio** se estivesen marcadas, xa que este equipo non vai ser controlador do dominio.

Permitir Contraseña vacía: ☐

Parámetros auxiliares: ldap:trusted = no

Extensiones Unix: ☒

Descubrir automáticamente compartidos con Zeroconf: ☒

Búsquedas de Hostnames: ☒

Server minimum protocol: SMB1

Server maximum protocol: SMB1

Permite ejecutar siempre: ☒

Obey pam restrictions: ☒

Dirección IPv4 enlazada: 172.16.5.12

Idmap Range Low: 90,000,000

Idmap Range High: 100,000,000

OK Cancelar

Nos **parámetros auxiliares**, engadimos o parámetro **Idapsam:trusted = no** para que logo o servizo de SMB autentique os usuarios correctamente contra o servidor LDAP. Activamos as **extensiones de Unix** e aceptamos.

Directory Service

AD LDAP NIS NT4 Kerberos Realms Kerberos Keytabs Kerberos Settings

Nombre de Dominio (DNS/Nombre Real):

Cuenta de Nombre de dominio:

Password de cuenta de dominio:

Habilitado:

Guardar Modo Avanzado Rebuild Directory Service Cache

Agora picamos no botón de **Directorio** para ir ao apartado de **LDAP**.

Directory Service

AD LDAP NIS NT4 Kerberos Realms Kerberos Keytabs Kerberos Settings

Nombre de anfitrión (Hostname): dserver00.iescalquera.local

DN Base: dc=iescalquera,dc=local

Enlace DN: cn=admin,dc=iescalquera,dc=local

Bind password: *****

Habilitado: ☒

Guardar Modo Avanzado Rebuild Directory Service Cache

Introducimos:

- * O equipo que executa o servizo LDAP, **dserver00.iescalquera.local**
- * Como **DN Base** a rama base das buscas no LDAP: **dc=iescalquera,dc=local**
- * A DN do usuario administrador: **cn=admin,dc=iescalquera,dc=local**
- * O contrasinal dese usuario no LDAP
- * Activamos a opción de **Habilitado**.

Picamos no botón de **Modo Avanzado** para cambiar algún parámetro máis.

Directory Service

AD LDAP NIS NT4 Kerberos Realms Kerberos Keytabs Kerberos Settings

Bind password: *****

Permitir enlaces anónimos: ☐

Sufijo de usuarios: iescalquera

Sufijo de grupos: iescalquera

Sufijo de computadores: iescalquera

Sufijo de máquinas: iescalquera

UUID sufixo: iescalquera

Redes habilitadas: ie802

Anfitrión de habilitados: iescalquera

Método de Encriptación: Argon2

Certificado: iescalquera

Tiempo de espera LDAP agotado: 30

Tiempo de espera DNS agotado: 30

Método de envío: ie802

Exigencias de seguridad: ie802

Parámetros auxiliares:

Sufijo: iescalquera

Habilitado: ☒

Guardar Modo Avanzado Rebuild Directory Service Cache

Cubrimos o sufixo das OUS dos usuarios, grupos e máquinas no LDAP, activamos o **Esquema Samba** para indicar que o LDAP que utilizamos inclúe este esquema, e xa podemos gardar os cambios.

Comprobación dos usuarios do dominio

- Unha vez integrado o equipo FreeNAS no dominio, usando unha das dúas opcións explicadas nos apartados anteriores, podemos comprobar que os usuarios e grupos do dominio están xa dispoñibles no sistema:

- Comprobación dos usuarios do dominio

```
[root@nas00] ~# getent passwd
root::565ntC5pa35x1QamLjy56eHw/yN/pCFqkcU6YtgAGxxQwAzLo5R3L04uP1vvTND6tLIVkxQXqtFVT4cVb
TaPXnpzvdz4NLUcMSLe5Bl0:0:0:root:/root:/bin/csh
daemon::1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator::2:5:System &:/usr/sbin/nologin
bin::13:7:Binaries Commands and Source:/usr/sbin/nologin
tty::4:65533:Tty Sandbox:/usr/sbin/nologin
kmem::5:2:KMem Sandbox:/usr/sbin/nologin
games::7:13:Games pseudo-user:/usr/sbin/nologin
news::8:8:News Subsystem:/usr/sbin/nologin
man::9:9:Master Man Pages:/usr/share/man:/usr/sbin/nologin
sshd::22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp::25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull::26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind::53:53:Bind Sandbox:/usr/sbin/nologin
proxy::62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
pflogd::64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
dhcpd::65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp::66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop::68:68:Post Office Owner:/nonexistent:/usr/sbin/nologin
www::80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
nobody::65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
avahi::200:200:avahi user:/nonexistent:/usr/sbin/nologin
messagebus::201:201:messagebus user:/nonexistent:/usr/sbin/nologin
ftp::14:14:/nonexistent:/bin/csh
auditd::78:77:Auditd unprivileged user:/var/empty:/usr/sbin/nologin
hast::845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
sol::10000:10000:Profe - Sol Lua:/home/tescalquera/profes/sol:/bin/sh
noe::10001:10000:Profe - Noe Ras:/home/tescalquera/profes/noe:/bin/sh
```

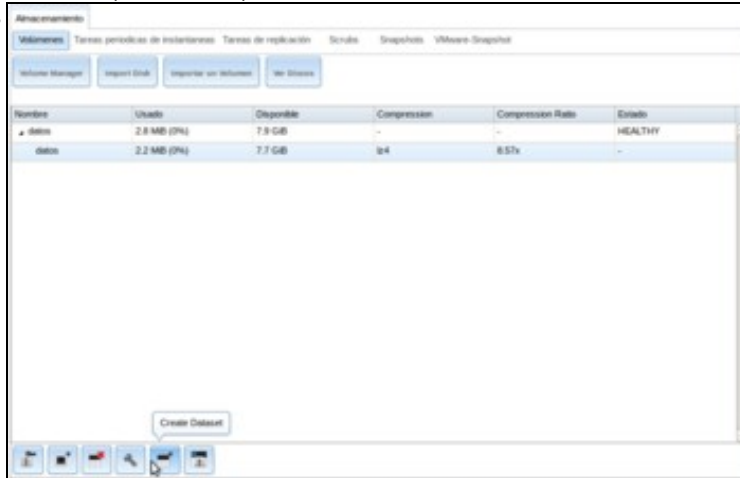
Podemos ver os usuarios do dominio con **getent passwd**.

```
[root@nas00] ~# getent group
wheel::8
daemon::1
kmem::2
sys::3
tty::4
operator::5:uucp
mail::6
bin::7
news::8
man::9
games::13
ftp::14
staff::20
sshd::22
smmsp::25
mailnull::26
guest::31
bind::53
proxy::62
authpf::63
pflogd::64
dhcpd::65
uucp::66
dialer::68
network::69
audit::77
www::80
nogroup::65533
nobody::65534
avahi::200
messagebus::201
hast::845
ladvd::78
webdav::666
media::8675309
g-dam1-profes::10002:sol
g-dam2-profes::10003:sol,noe
g-dam1-alum::10004:mon,tom
g-dam2-alum::10006:pia
g-usuarios::10000
g-profes::10001:sol,noe
g-alum::10005:mon,tom,pia
```

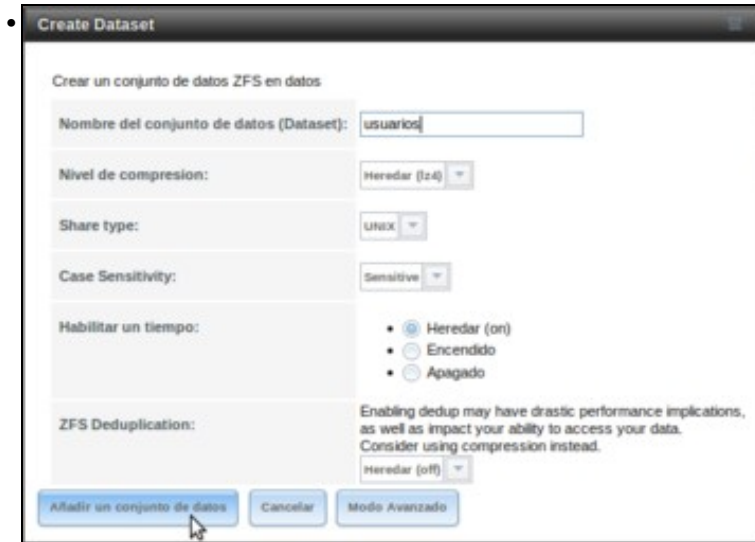
E os grupo con **getent group**.

Crear o esqueleto de carpetas

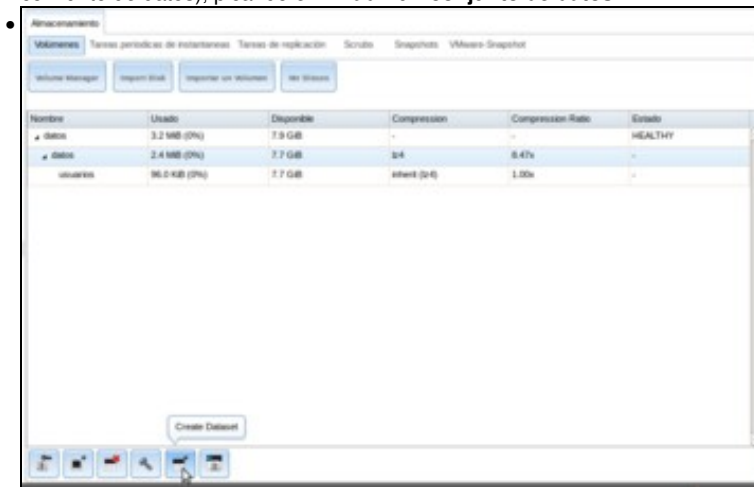
- Comezaremos creando o esqueleto de carpetas, que será moi similar ao que tiñamos en *dserver00* na [Parte III](#), así que poderemos reutilizar os mesmos scripts cambiando as carpetas base.
- Definiremos en FreeNAS dous conxuntos de datos (*datasets*) dentro do volume ZFS *datos*; para as carpetas dos usuarios e a carpeta común respectivamente. Desta forma podemos usar configuracións independentes para cada un deles, como cotas de disco, nivel de compresión, etc.
- Crear o esqueleto de carpetas



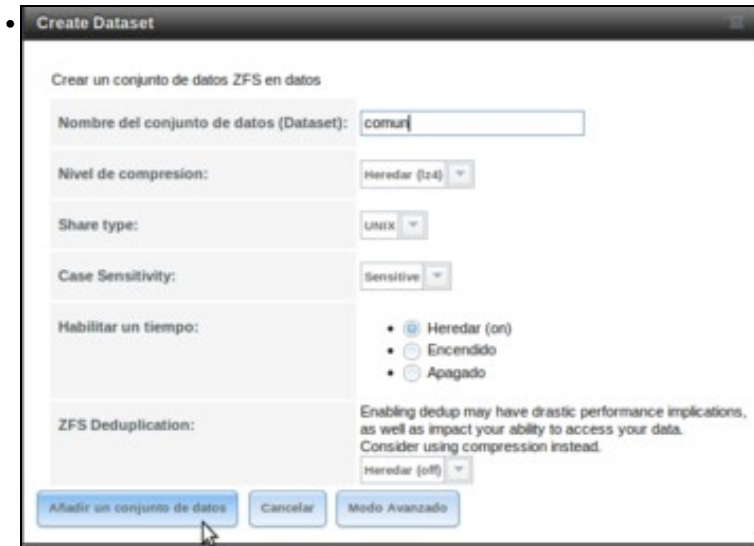
No apartado de **Volumes Activos** dentro da lapela de **Almacenamiento**, seleccionamos o volume *datos* e picamos no botón para **Crear un conxunto de datos ZFS**.



Poñemos como nome **usuarios** e deixamos o resto de opcións por defecto (poderíamos asignar se quixéramos un tamaño máximo para este conxunto de datos), picando en **Añadir un conxunto de datos**.



Vemos o conxunto de datos creado. Picamos sobre o volume ZFS **datos** e creamos outro...



coas mesmas opcións, pero co nome de **comun**.

- Na máquina FreeNAS, creamos no volume ZFS unha carpeta para crear os scripts para a creación do esqueleto de carpetas:

```
cd /mnt/datos
mkdir scripts
cd scripts
```

- Seguindo a mesma filosofía que na [Parte III](#), creamos un ficheiro de texto para almacenar todos os cursos que temos.

• FICHEIRO DE CURSOS: f00_cursos.txt

```
dam1
dam2
```

- O seguinte script establece o valor das variables que almacenan as rutas ás carpetas base do esqueleto, que neste caso cambian con respecto á parte III:

• SCRIPT DE VARIABLES GLOBAIS: 00_variables.sh

```
#!/bin/bash

# Define variable globais que van usar os demais scripts

#Variables
DIR_USUARIOS=/mnt/datos/usuarios
DIR_COMUN=/mnt/datos/comun
```

```
# Exportar variables
# Nos scripts que se van usar a continuación non faría falla que se exportasen as variables.
# Pero quedan exportadas por se a posteriori calquera dos scripts que vai importar
# o contido deste ficheiro precisase chamar a outros scripts que precisasen usar estas variables
export DIR_USUARIOS
export DIR_COMUN
```

- E por último, o seguinte script é exactamente o mesmo que o da parte III. O que fai é crear todas as carpetas do esqueleto.

• SCRIPT: 01_crear_esqueleto.sh

```
#!/bin/bash

#Chamar ao script de variables, temos varias opcións:

. ./00_variables.sh # Tamén podería ser: source ./00_variables.sh

#Crear esqueleto profes
#Por se executamos o script varias veces, comprobamos se xa existe o directorio
test -d $DIR_USUARIOS/profes || mkdir -p $DIR_USUARIOS/profes

#Crear esqueleto alumnos e comun
#Lemos o ficheiro cursos e procesamos cada curso
for CURSO in $(cat f00_cursos.txt)
do
    test -d $DIR_USUARIOS/alumnos/$CURSO || mkdir -p $DIR_USUARIOS/alumnos/$CURSO
    test -d $DIR_COMUN/$CURSO || mkdir -p $DIR_COMUN/$CURSO
done

#Crear en comun a carpeta para os departamentos
test -d $DIR_COMUN/departamentos || mkdir -p $DIR_COMUN/departamentos
```

- Executamos o script para crear o esqueleto de carpetas:

```
sh 01_crear_esqueleto.sh
```

- Comprobamos a súa execución, visualizando co comando **ls -R** o contido de */mnt/datos/usuarios* e */mnt/datos/comun*.

Configurar os permisos

- Este script é tamén idéntico ao que usamos na Parte III.

• SCRIPT: 02_axustar_permisos_esqueleto.sh

```
#!/bin/bash

#Chamar ao script de variables
. ./00_variables.sh # Tamén podería ser: source ./00_variables.sh

#Cartafol /home/iescalquera
chown root:g-usuarios $DIR_USUARIOS# Cambiar grupo propietario
chmod 750 $DIR_USUARIOS# Axustar permisos

#Cartafol profes
chown root:g-profes $DIR_USUARIOS/profes
chmod 750 $DIR_USUARIOS/profes

#Cartafol alumnos
chown root:g-usuarios $DIR_USUARIOS/alumnos
chmod 750 $DIR_USUARIOS/alumnos

#Cartafol cursos
for CURSO in $(cat f00_cursos.txt)
do
    chown root:g-usuarios $DIR_USUARIOS/alumnos/$CURSO
    chmod 750 $DIR_USUARIOS/alumnos/$CURSO
done
```

```
#Cartafol comun
chown root:g-usuarios $DIR_COMUN
chmod 750 $DIR_COMUN

#Subcartafol departamentos

chown root:g-profes $DIR_COMUN/departamentos
chmod 770 $DIR_COMUN/departamentos

#Subcartafoles cursos
# O participante no curso á vista do esquema de permisos
# e do exemplo de arriba debe ser quen de axustar
# os permisos de /comun/cursos
# Ollo!!!! nas subcarpetas co grupo others.
# Unha pista para o grupo propietario dos cursos: g-"$CURSO"-profes
#
#IMPORTANTE: o que se lle engada ao script, debe valer para futuros crecementos en curso: asir1, asir2, etc.
#Con só dar de alta no ficheiro f00_cursos.txt os cursos non deberamos tocar nada no presente script.
```

- Executamos o script

```
sh 02_axustar_permisos_esqueleto.sh
```

- Comprobamos resultados, por exemplo na carpeta /mnt/datos/usuarios:

```
[root@nas00] /mnt/datos/scripts# ls -la /mnt/datos/usuarios/
total 34
drwxr-x--- 4 root g-usuarios 4 May 24 07:05 ./
drwxr-xr-x 6 root wheel 6 May 24 07:03 ../
drwxr-x--- 4 root g-usuarios 4 May 24 07:05 alumnos/
drwxr-x--- 2 root g-profes 2 May 24 07:05 profes/
```

Creación das carpetas persoais dos usuarios (home)

- De novo, imos seguir a mesma estratexia que na parte III do curso para **crear as carpetas persoais dos usuarios**.
- Traemos para a carpeta scripts o contido de /etc/skel de *uclient01*.

```
[root@nas00] /mnt/datos/scripts# scp -r uadmin@uclient01:/etc/skel .
Could not create directory '/root/.ssh'.
The authenticity of host 'uclient01.iescalquera.local (172.16.5.20)' can't be established.
ECDSA key fingerprint is 08:66:4b:b7:0b:2c:ac:f0:c7:20:19:2a:0a:5d:dd:2c.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/root/.ssh/known_hosts).
uadmin@uclient01.iescalquera.local's password:
.bashrc 100% 3637 3.6KB/s 00:00
.bash_logout 100% 220 0.2KB/s 00:00
examples.desktop 100% 8980 8.8KB/s 00:00
.profile 100% 675 0.7KB/s 00:00
```

- Agora renomeamos a carpeta que se trouxo de Ubuntu, para evitar confusións.

```
[root@nas00] /mnt/datos/scripts# mv skel skel_ubuntu
[root@nas00] /mnt/datos/scripts# ls
./ 00_variables.sh 02_axustar_permisos_esqueleto.sh skel_ubuntu/
../ 01_crear_esqueleto.sh f00_cursos.txt
```

- Para finalizar, o script que crea as carpetas persoais dos usuarios e axusta os seus permisos teremos que modificalo un pouco, xa que en lugar de crear as carpetas dos usuarios en */home/iescalquera*, que é a ruta que indican os datos dos usuarios no LDAP, haberá que crealas na carpeta */mnt/datos/usuarios* (que está configurada no script de variables na variable *\$DIR_USUARIOS*).
- Faremos esta substitución utilizando o mesmo comando *awk*.

• SCRIPT: 03_crear_home_usuarios_axustar_permisos.sh

```
#!/bin/bash

#Chamar ao script de variables
. ./00_variables.sh

#Lembrar que cada usuario ten o seguinte formato
# Un/unha profe -> sol:x:10000:10000:Profe - Sol Lua:/home/iescalquera/profes/sol:/bin/bash
# Un/unha alumna -> mon:x:10002:10000:DAM1 Mon Mon:/home/iescalquera/alumnos/daml/mon:/bin/bash

# Observar que posición ocupan os campos e que están separados por :

# Imos extraer con awk dos usuarios con ID (campo 3) entre 10000 e 60000 os campos
# Usuario (campo 1) e home (campo 6)
# Deste último campo (home) imos extraer o grupo ao que pertence o usuario
# Neste caso o separador de campos é /, e o grupo está no 4º campo.

#Volcamos tódolos usuarios (locais e ldap) do sistema a un ficheiro
getent passwd>usuarios.txt

#Extraemos os campos anteriores
for USUARIO in $( awk -F: '$3>=10000 && $3<60000 {print $1":"$6}' usuarios.txt )
do
#USUARIO vai ter o seguinte formato
# sol:/home/iescalquera/profes/sol

NOME_USUARIO=$( echo $USUARIO | awk -F: '{print $1}')
HOME_USUARIO_LDAP=$( echo $USUARIO | awk -F: '{print $2}')
HOME_USUARIO=$( echo $USUARIO | awk -v DIR=$DIR_USUARIOS -F: '{gsub("/home/iescalquera",DIR,$2);print $2}')
GRUPO_GLOBAL_USUARIO=$( echo $HOME_USUARIO_LDAP | awk -F/ '{print $4}')

#Creamos a carpeta persoal do usuario/a
test -d $HOME_USUARIO || mkdir -p $HOME_USUARIO

#Copiamos o contido de skel_ubuntu (ocultos incluídos, -a) á carpeta persoal do usuario/a
cp -a skel_ubuntu $HOME_USUARIO

#Comprobamos se o usuario/a é un profe
if [ $GRUPO_GLOBAL_USUARIO = "profes" ]
then
#Se é un profe deixamos entrar só a ese profe na súa carpeta persoal
$NOME_USUARIO+g-sudo $HOME_USUARIO
700 $HOME_USUARIO
else
#Se é un alumno o campo 5 do home coincide con parte do nome do grupo ao que pertence
GRUPO_ALUMNO=$( echo $HOME_USUARIO_LDAP |awk -F/ '{print $5}')

#Se é un alumno deixamos entrar en modo lectura execución aos profes dese curso
# en modo recursivo
$NOME_USUARIO+g-$GRUPO_ALUMNO"-profes $HOME_USUARIO
750 $HOME_USUARIO
fi
done

rm usuarios.txt
```

• Unha vez executado o script con:

```
sh 03_crear_home_usuarios_axustar_permisos.sh
```

• Podemos comprobar con *ls -la* sobre as carpetas dos usuarios o seu resultado.