PEC 1

Seguridad en Sistemas Operativos

Pablo Riutort Grande

9 de marzo de 2020

1. Linux

1.1.

	Comando	**Valor**
Versión del kernel	uname -r	4.19.0-8-amd64
Num. particiones del disco	df -h | grep ^/dev | wc -l	4
Memoria del sistema	head -1 /proc/meminfo	MemTotal: 4041712 kB
Servidor DNS configurado	cat /etc/resolv.conf | tail -1	nameserver 10.0.2.3
Gateway de la subred	ip -br route show | head -1	default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
Dirección IP	ip -br addr show | tail -1	10.0.2.15/24 fe80::a00:27ff:fe23:3552/64
Tipo de sistema en /	df -h / - -output=fstype | tail -1	ext4
Espacio utilizado en la /	df -h / - -output=used | tail -1	3.0G

1.2.

Creo que el sistema debería tener particiones para /var puesto que en este directorio se guardan los logs, emails y otros datos de sistemas de bases de datos. Un mejor esquema de pariticiones sería:

- /tmp
- /var
- /var/log
- /var/www
- /home
- /usr

1.3.

Primero crearía una partición de disco con el comando fdisk. Este comando listar las particiones en disco (fdisk -l) y añadir nuevas tablas de partición (fdisk /dev/<sd>) y guardarlas en disco. Este se consigue con las opciones "n" para crear una nueva partición y seleccionamos el tipo con "e" y "p" (extendida o primaria). Los siguientes pasos tienen que ver con la configuración de la partición en sí, como el espacio que tendrá asignado.
Una vez hecho esto, con el comando mkfs se crea un sistema de ficheros en la partición, en nuestro caso: "mkfs -t ext3 /dev/<sd>" dará formato a la partición y creará un sistema de journal tipo ext3.
Finalmente podemos montar el sistema de ficheros con el comando "mount" y hacerlo persistente en el sistema modificando el archivo /etc/fstab.
Alternativamente, se puede realizar el mismo proceso instalando herramientas gráficas de particionado como GParted.

1.4.

Para mover /home a una nueva partición podemos usar el comando fdisk. Con fdisk -l podemos listar las particiones y discos. Supongamos que el comando lista un disco /dev/sdb, los pasos a realizar serían los siguientes:

1. Creamos una partición nueva con fdisk /dev/sdb de tipo primaria (opción n y despúes p).

2. Confirmamos la partición con "w" que nos creará la partición con nombre similar a /dev/sdb1.
3. Creamos el sistema de ficheros en la nueva partición con mkfs -t ext4 /dev/sdb1.
4. Montamos el nuevo disco con mount /dev/sdb1 /mnt (siendo /mnt nuestro punto de montaje). Esto nos permite copiar datos en el nuevo disco.
5. Movemos (o copiamos) el directorio /home en el punto de montaje: mv /home/* /mnt
6. Ahora podemos crear un nuevo directorio /home en nuestra raíz que será el punto de montaje del disco (que ahora contiene /home): mkdir /home.
7. Finalmente, montamos el disco en /home: umount /dev/sdb1; mount /dev/sdv1 /home/

Mount the external partition onto a temporary Home location.
Copy the files from your current Home folder to this temporary Home folder.
Relocate the current Home folder
Mount the new Home folder.

1.5.

El siguiente comando crea un usuario con directorio propio en /home, fecha de expiración a 1/1/2018, bash como shell, perteneciente al grupo users y con nombre "alumno".

```
sudo useradd -m -e 2018-01-01 -s /bin/bash -G users alumno
```

Seteamos el password con el siguiente comando

```
sudo passwd alumno
```

E introducimos por terminal el password 12345.

1.6.

Creamos el usuario uoc perteneciente al grupo staff.

```
sudo useradd -G staff uoc
```

Para que tenga permisos sobre los ficheros de alumno, debemos añadir el directorio /home/alumno/ al grupo staff

```
sudo chgrp -R staff /home/alumno/
```

Y asignarle permisos de lectura al grupo

```
sudo chgrp g+r /home/alumno/
```

1.7.

Añadimos como propietario a uoc y al grupo staff el directorio.

```
sudo chown -hR uoc:staff /srv/uoc/
```

Añadimos permisos de escritura y quitamos los de ejecución al directorio para el grupo

```
sudo chmod g+w-x /srv/uoc
```

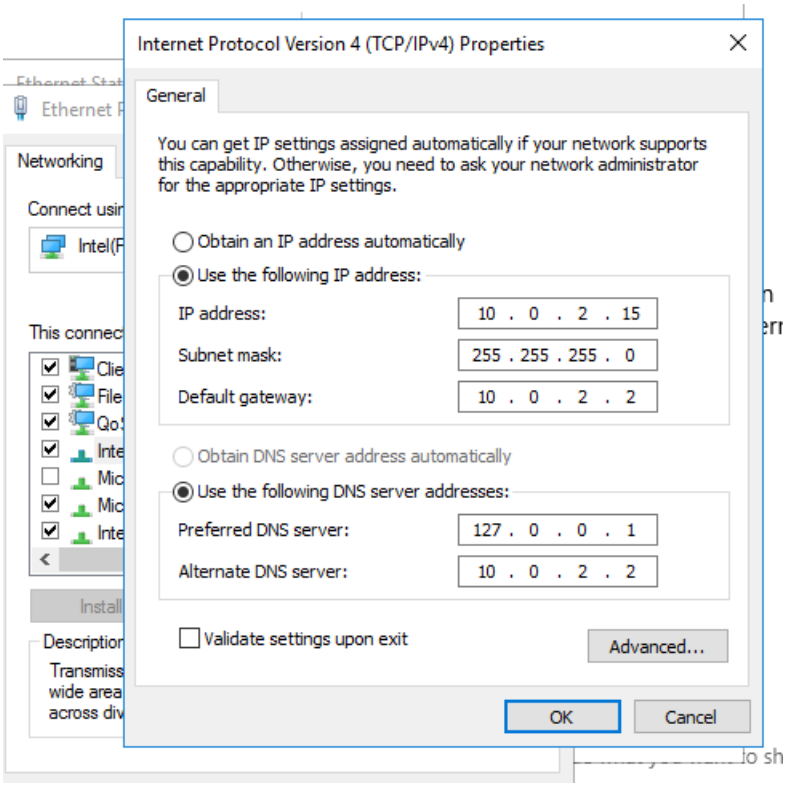
Por defecto, el directorio tiene permisos de lectura y ejecución para "others", este grupo se aplica a los demás usuarios del sistema, al cual pertenece el usuario "alumno".

```
$ ls -lh /srv/
total 4.0K
drwxrw-r-x 2 uoc staff 4.0K Mar  8 15:07 uoc
```

2. Windows

2.1.

Previamente al Active Directory se ha creado una máquina virtual de Windows Server 2016. Posteriormente a su creación se ha instalado la imágen Windows proporcionada y se ha creado una cuenta de admin con una contraseña alfanumérica de 9 caracteres con mayúsculas y minúsculas asociada al usuario administrator.
Posteriormente y para que el sistema funcione correctamente, se ha cambiado la configuración de red para utilizar IPs estáticas y el servidor DNS.



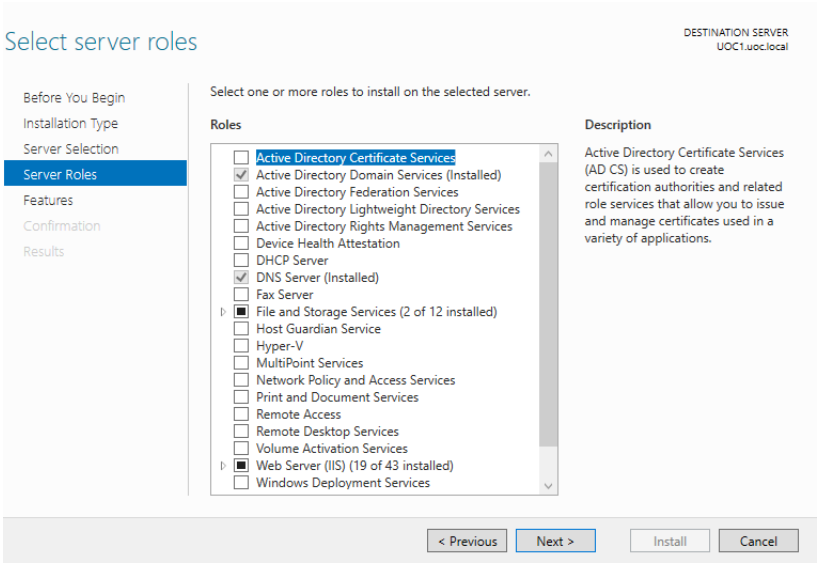
Después de esta configuración, mediante la herramienta de *Server Manager* se han realizado las siguientes tareas:

1. En el primer menú de *Configure this local server* se ha cambiado el nombre del servidor local a UOC1.

2. En el segundo menú se han instalado las aplicaciones mencionadas en la Figura 2.

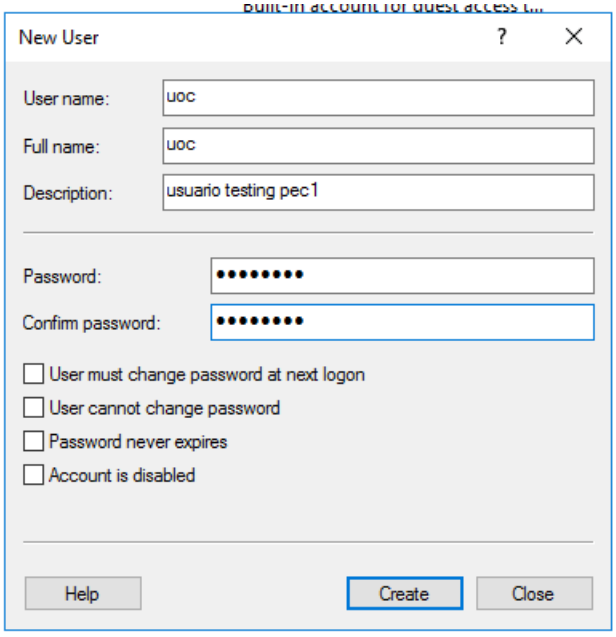
3. Una vez instalado el Active Directory, se puede crear un bosque llamado uoc.local con contraseña de mismas características que el administrador (9 carácteres, minúsculas, mayúsculas y algún número).

4. El sistema pide que se reinicie para la correcta configuración.

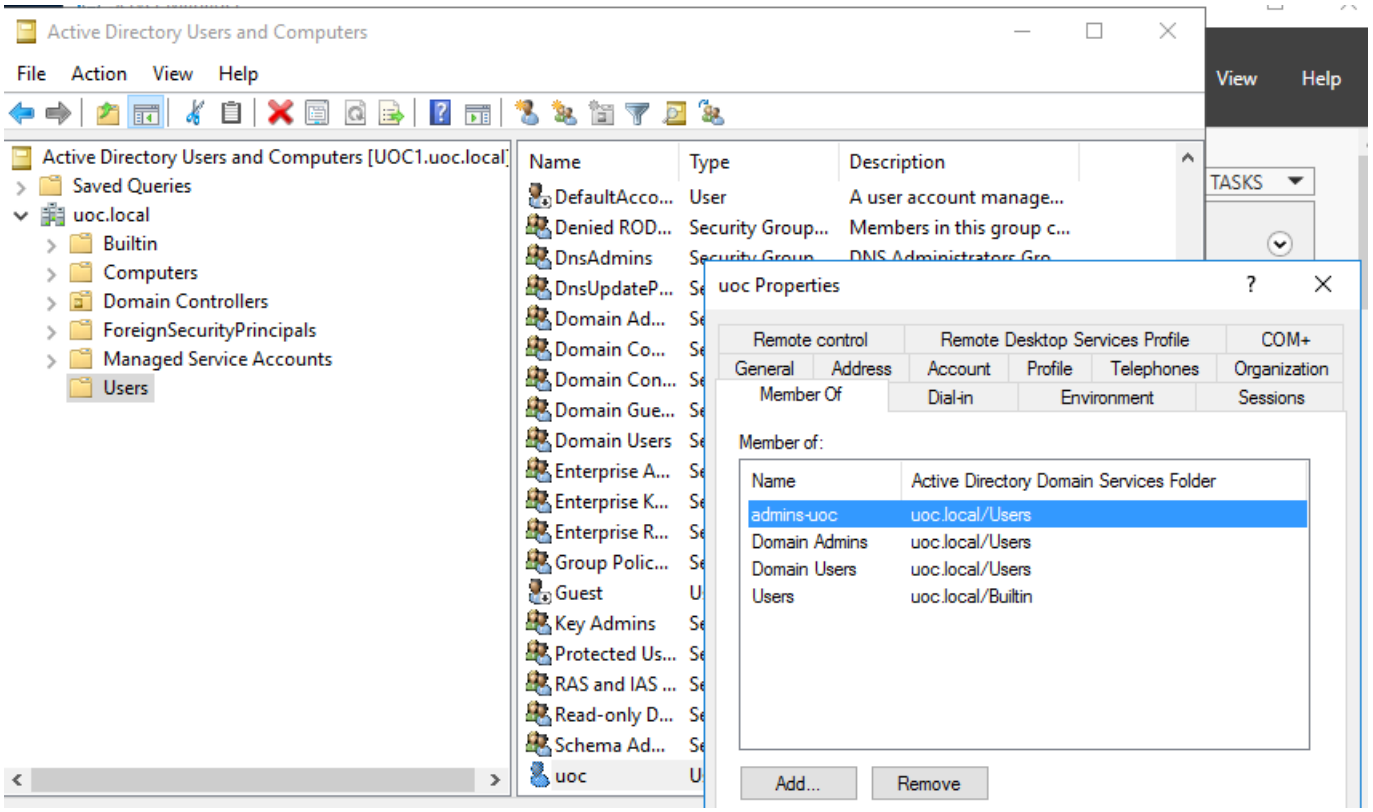


2.2.

Tanto el usuario como el grupo se han creado a través del método tradicional de gestión de usuarios de Windows: Computer Management / System Tools / Local Users and Groups / Users & Groups:



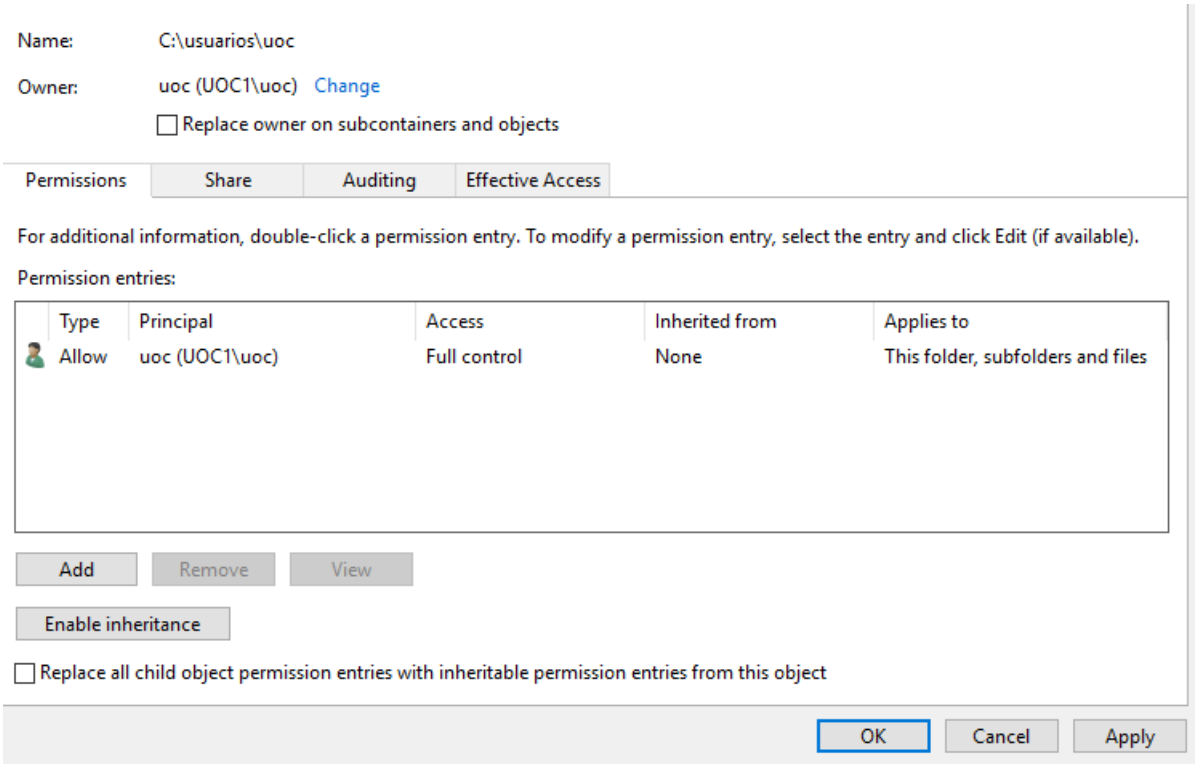
La contraseña sigue las mismas características que las del administrador.
Posteriormente se ha utilizado la herramienta de Active Directory Users and Computers para asociar el usuario al grupo:


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [UOC1.uoc.local]
Saved Queries
uoc.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name Type Description
DefaultAcco... User A user account manage...
Denied ROD... Security Group... Members in this group c...
DnsAdmins
DnsUpdateP...
Domain Ad...
Domain Co...
Domain Con...
Domain Gue...
Domain Users
Enterprise A...
Enterprise K...
Enterprise R...
Group Polic...
Guest
Key Admins
Protected Us...
RAS and IAS ...
Read-only D...
Schema Ad...
uoc
View Help
TASKS
uoc Properties
Remote control
Remote Desktop Services Profile
COM+
General Address Account Profile Telephones Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
admins-uoc uoc.local/Users
Domain Admins uoc.local/Users
Domain Users uoc.local/Users
Users uoc.local/Builtin
Add...
Remove

2.3.

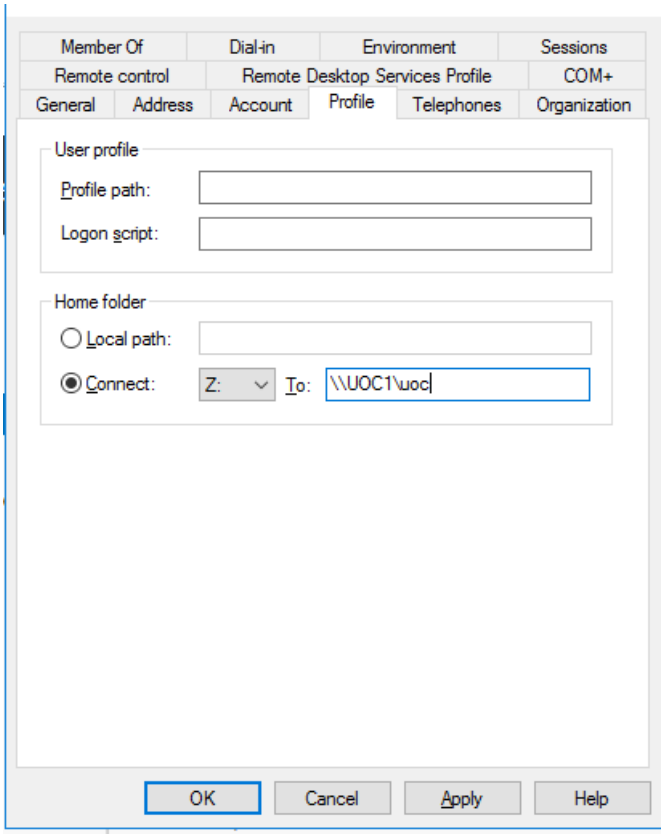
Para este apartado:

1. Se han creador los directorios usuarios cuyo contenido es uoc dentro de C:
2. En el apartado Properties de la carpeta se cambian los permsisos de acceso en los apartados de Security se conceden permisos al usuario uoc y se eliminan los de los demás
3. En Security también podemos deshabilitar la herencia de permisos para quitarle permisos a los demás usuarios que no sean uoc ni pertencezcan al grupo.



Ahora pasamos a usar la aplicación de Active Directory Users and Computers, donde seleccionamos nuevamente a nuestro usuario y en la lengüeta de Profile podemos seleccionar el directorio UOC1
uoc como unidad Z:

Si nos logueamos como UOC vemos que el directorio se encuentra en nuestro directorio raíz y que somos el único usuario que tiene acceso.


Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User profile
Profile path:
Logon script:
Home folder
Local path:
Connect:
Z:
To:
\\UOC1\uoc
OK
Cancel
Apply
Help