

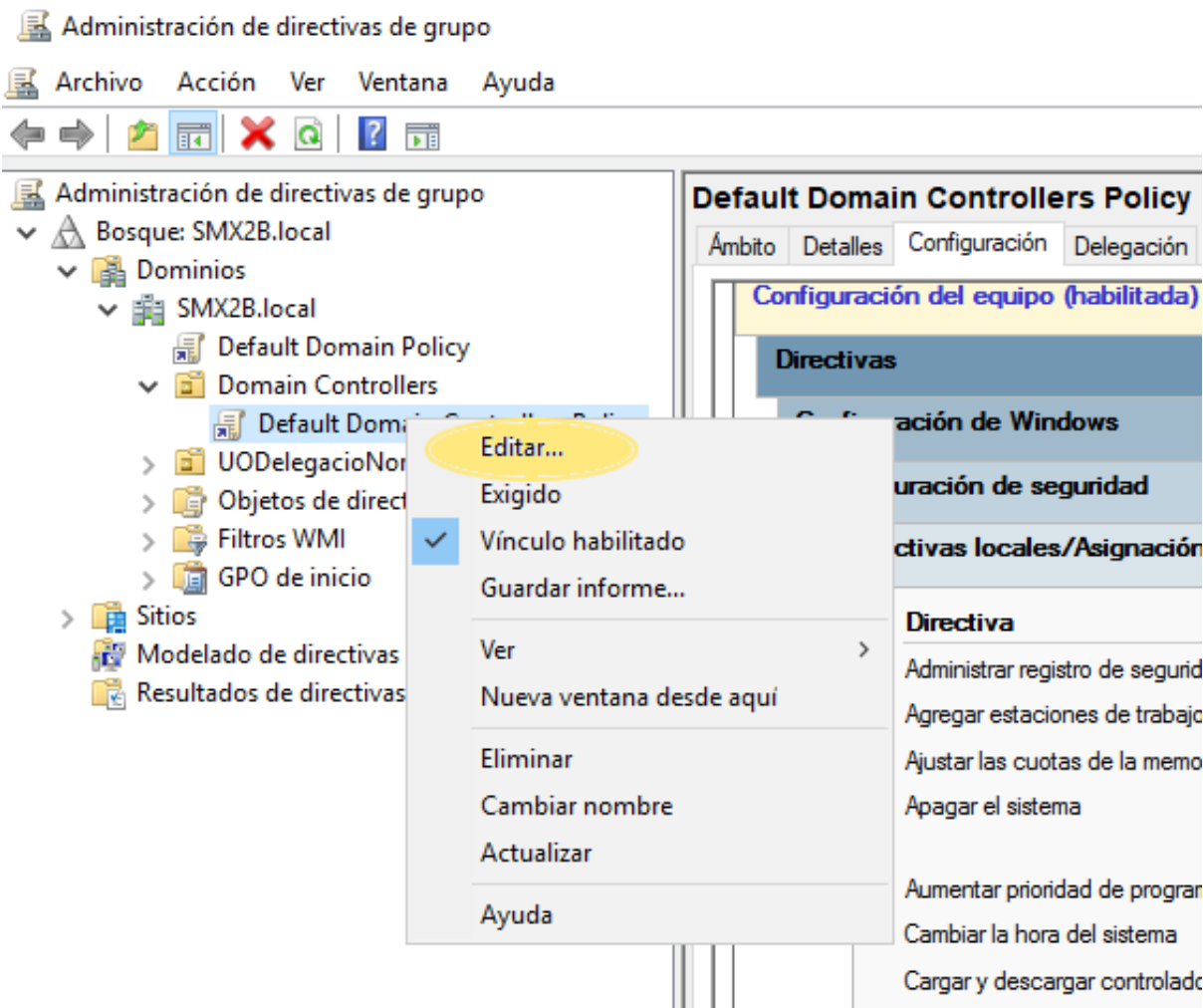
# U3. WINDOWS SERVER. ADMINISTRACIÓ I CONFIGURACIÓ (V)

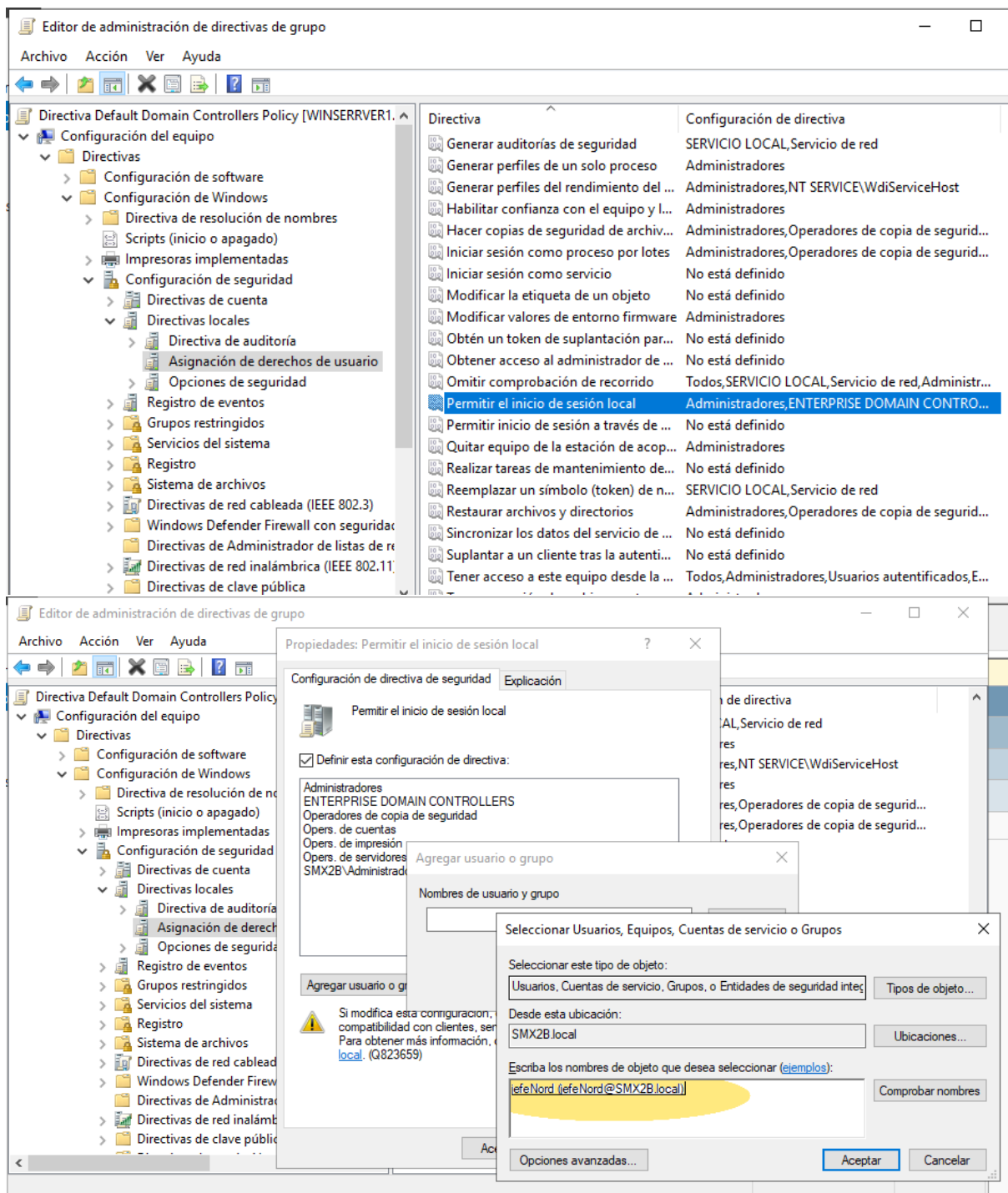
## GESTIÓ DE UO I AVANÇ DIRECTIVES LOCALS DE SEGURETAT

@tofermos 2024

### Índex

1 Les UO	8
Per a què es creen les UO?	8
La divisió del treball duu l'especialització	8
2 La delegació de control de la UO	8
2.1 Seleccionem l'usuari, usuaris o grups	8
2.2 Assignem drets	11
2.3 Habilem l'usuari per a iniciar sessió.	11





14

14

2.4 Comprovació de les accions que podem fer . . . . . 16

¿Quieres permitir que esta aplicación haga cambios en el dispositivo?



Server Manager

Editor comprobado: Microsoft Windows

[Mostrar más detalles](#)

Para continuar, escribe el nombre de usuario y la contraseña de un administrador.

jefeNord

●●●●●●●●●●

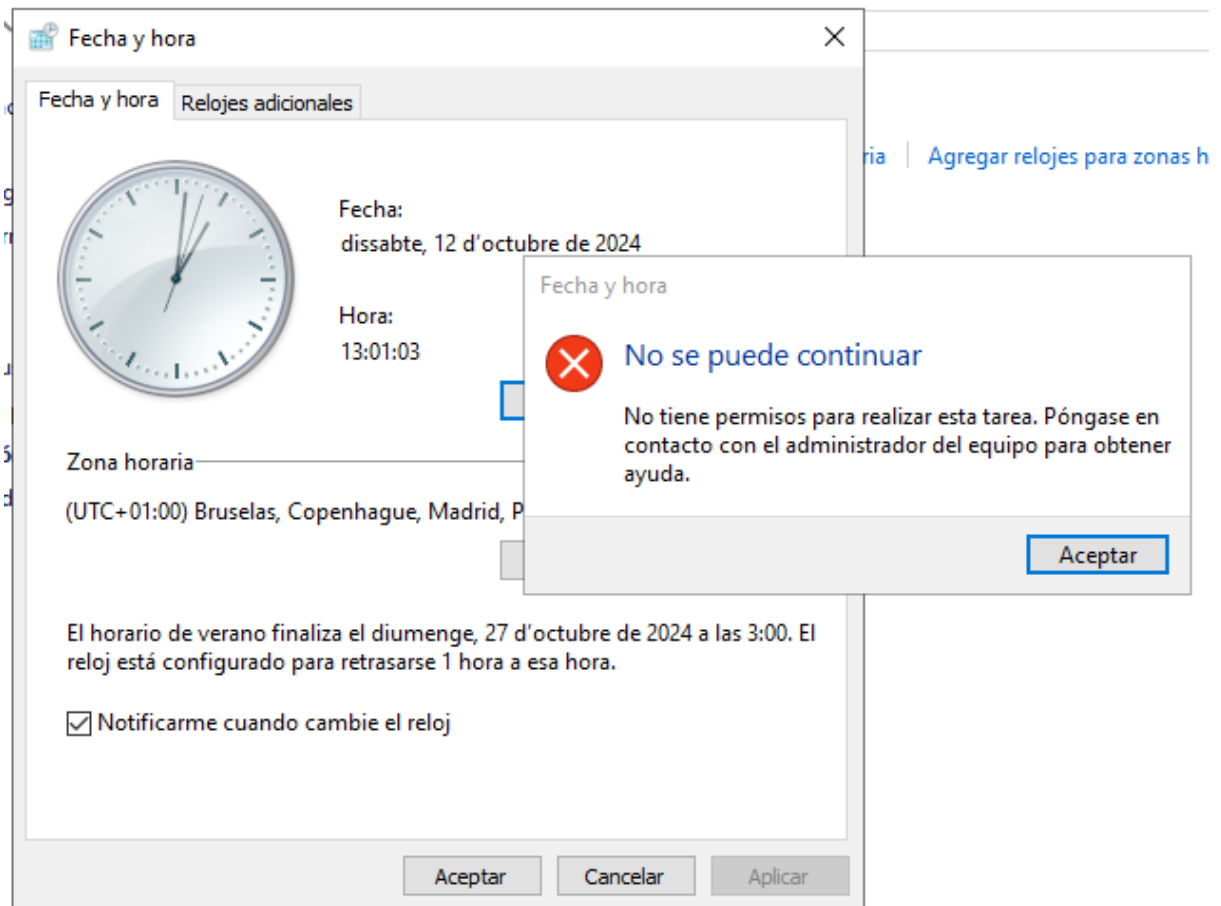


Dominio: SMX2B

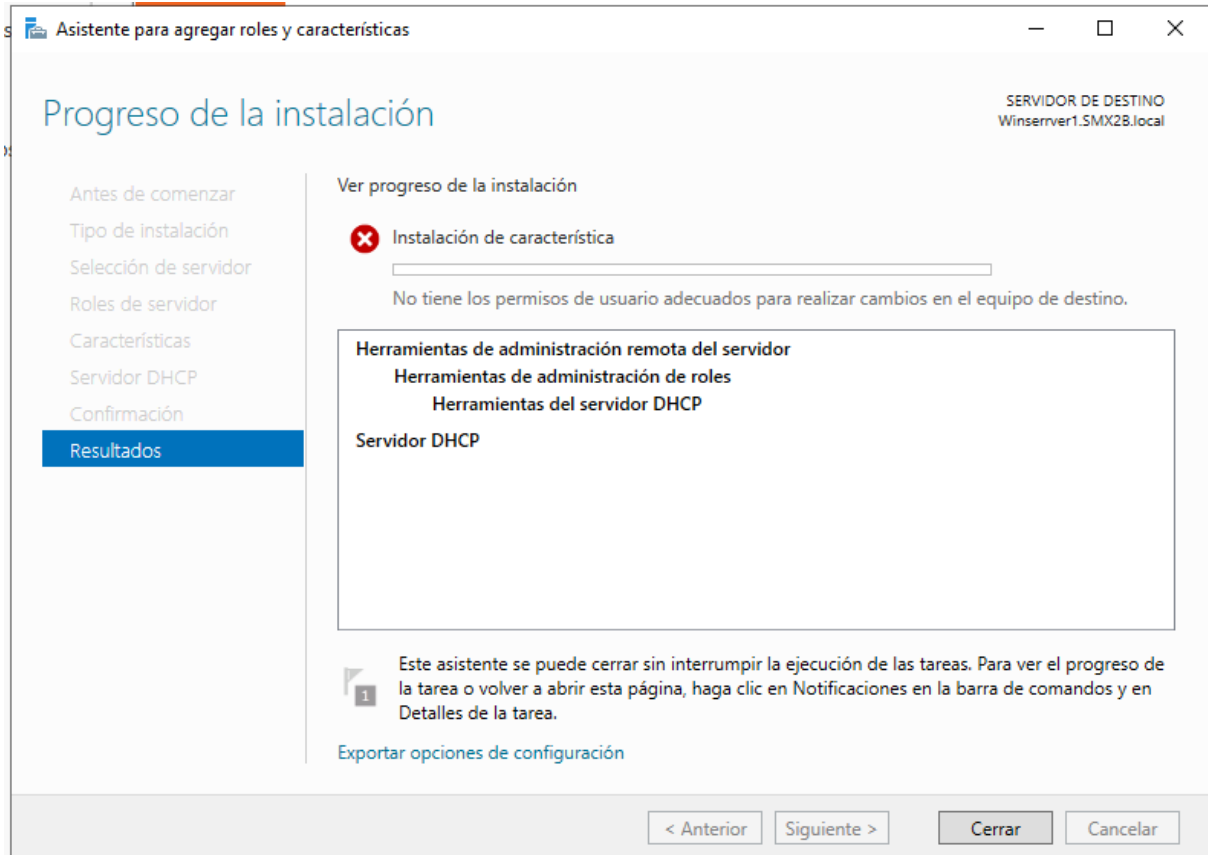
[Más opciones](#)

Sí

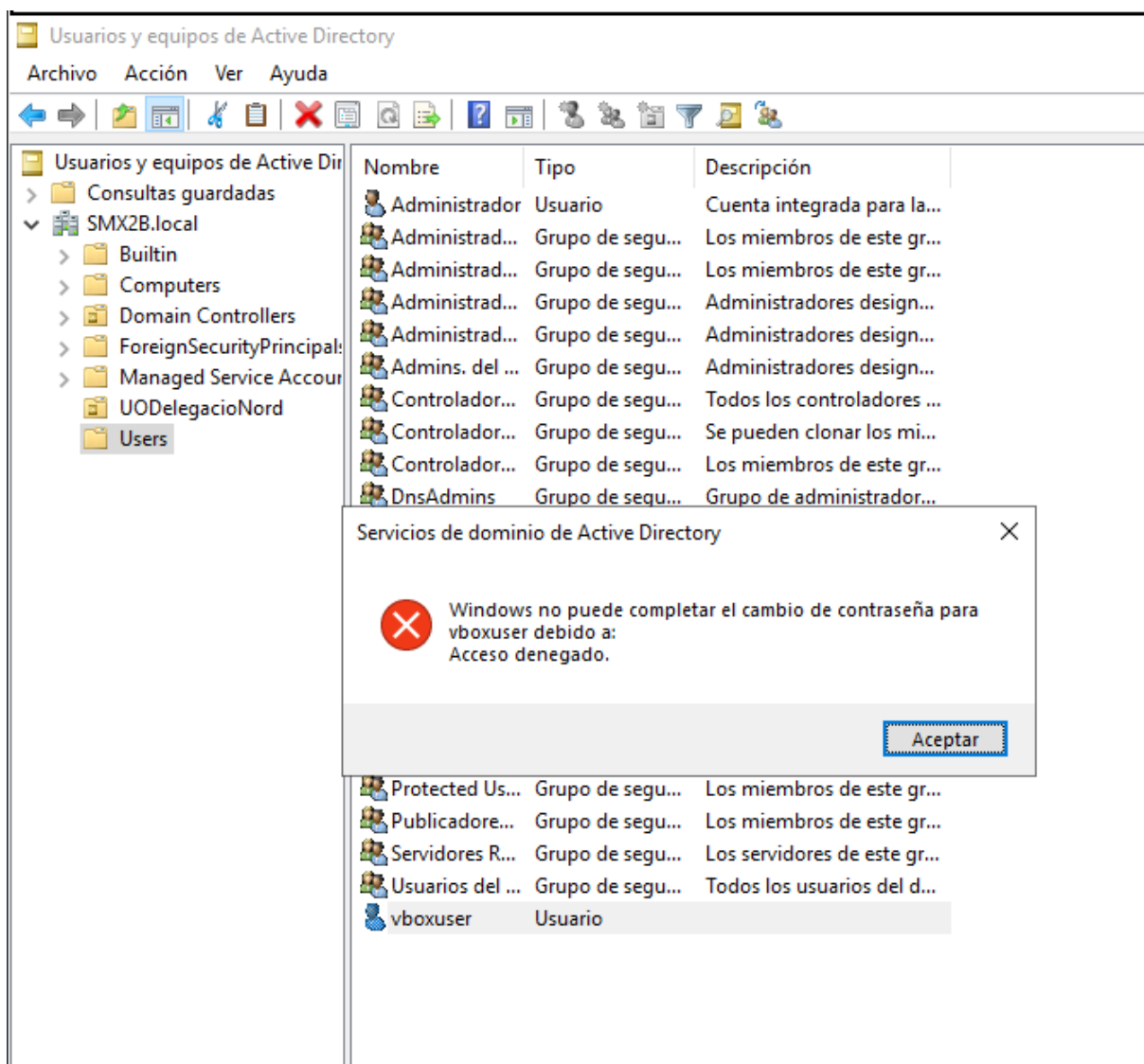
No



18



18



2.5 Conclusions . . . . . 19

tomas@portatil: ~ | 19

Fitxer Edita Vista Cerca Terminal Ajuda

rosa@portatil:/\$ sudo apt update  
[sudo] contrasenya per a rosa:  
rosa no està al fitxer sudoers. S'informarà d'aquest incident.

tomas@portatil: ~ | 20

Fitxer Edita Vista Cerca Terminal Ajuda

rosa@portatil:/\$ sudo date --set="2026-01-01 00:00:00"  
[sudo] contrasenya per a rosa:  
rosa no està al fitxer sudoers. S'informarà d'aquest incident.

3 Gestió dels usuaris amb delegació. Característiques avançades del dsamc.msc 20

- SMX2B.local
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal
  - Keys
  - LostAndFound
  - Managed Service Account
  - Program Data
  - System
  - UODelegacioNord
  - Users
  - NTDS Quotas
  - TPM Devices

jefeNord	Usuario
user1	Usuario
user2	Usuario

Propiedades: UODelegacioNord

General Administrado por Objeto Seguridad COM+ Editor de atributos

Nombre canónico del objeto:  
SMX2B.local/UODelegacioNord

Clase de objeto: Unidad organizativa

Creado: 12/10/2024 0:18:16

Modificado: 12/10/2024 18:37:00

Números de secuencias actualizadas (USN):

Actual: 32879

Original: 20490

☐ Proteger objeto contra eliminación accidental

Aceptar Cancelar Aplicar Ayuda

- > Computers
- > Domain Controllers
- > ForeignSecurityPrincipal:
- > Keys
- > LostAndFound
- > Managed Service Account
- > Program Data
- > System
- > UODelegacioNord
- > Users
- > NTDS Quotas
- > TPM Devices

user2

Usuario

Propiedades: UODelegacioNord

General Administrado por Objeto Seguridad COM+ Editor de atributos

Nombres de grupos o usuarios:

- CREATOR OWNER
- SELF
- Usuarios autenticados
- SYSTEM
- jefeNord (jefeNord@SMX2B.local)
- Admins. del dominio (SMX2B\Admins. del dominio)

Agregar... Quitar

Permisos de jefeNord

	Permitir	Denegar
Control total	<input type="checkbox"/>	<input type="checkbox"/>
Leer	<input type="checkbox"/>	<input type="checkbox"/>
Escribir	<input type="checkbox"/>	<input type="checkbox"/>
Crear todos los objetos secundarios	<input type="checkbox"/>	<input type="checkbox"/>
Eliminar todos los objetos secundarios	<input type="checkbox"/>	<input type="checkbox"/>

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Aceptar Cancelar Aplicar Ayuda

# 1 Les UO

Com ja hem explicat les UO són un objecte contenidor, d'ahi que es representa al GUI amb una icona similar a la de els carpetes. El contingut de les UO són altres objectes: usuaris, grups, carpetes compartides i també altres UO.

## Per a què es creen les UO?

Les UO són transparents a l'usuari. Un comptable pot detectar que forma part d'alguna “agrupació” de companys del mateix despatx o continus i intuir que són un “grup” d'usuaris. Però li costaria més intuir o deduir la existència de UOs. De mode simplificat podríem dir que les UO es creen per administrar la xarxa per parts. Per a que els adminstradors, o usuaris avançats habilitats, puguem repartir-se la faena d'administrar la xarxa sencera.

Els criteris o raons per crear UO poden ser tres:

1- Dividir l'administració del domini atenent a un **criteri geogràfic**. Delegacions de països, zones... o centres d producció distints. 2- Dividir l'administració del domini atenent a un **criteri organitzatiu**. Agrupant departaments de l'empresa, per exemple. 3- Crear agrupacions d'objectes de forma **dinàmica** per a projectes temporals. Una UO amb tots els recursos (objetes) per crear una aplicació software nova, per desenvolupar un prjecte urbanístics...

## La divisió del treball duu l'especialització

El que està clar és que abandonem el paradigam de l'*administrador o administradors de tot el domini* i obrim les portes a que un usuari (no necessàriament administrador) pugui fer tasques (encara que bàsiques) en el Servidor pròpies d'un administrador.

## 2 La delegació de control de la UO

Ja hem vist en aquesta unitat (U3.2) com es creen les UO i com es modifiquen. Ara vorem com es delega el control en un usuari. Delegar el control en un usuari Administrador del domini pot semblar un poc absurd; interessa delegar en un altre tipus d'usuari que no siga Administrador del tot per a convertir-lo en un “quasi-administrador” d'una part del domini (la UO).

### 2.1 Seleccióem l'usuari, usuaris o grups

En el nostre exemple triarem un usuari *jefeNord* per a la *UO-DelegacióNord*.

Hem de buscar i seleccionar correctament l'usuari.



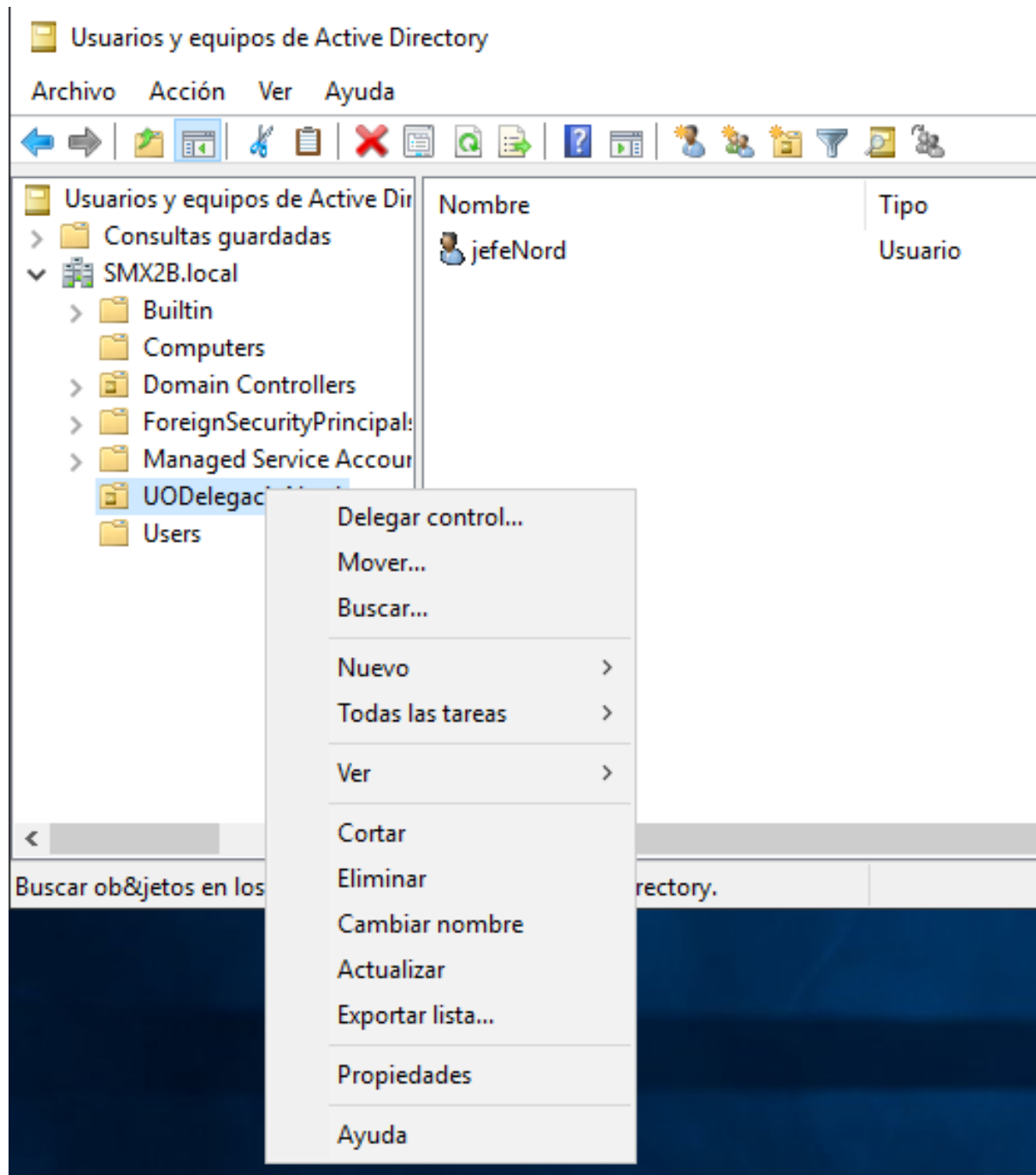


Figura 1: *Figura 1:Delegar control*

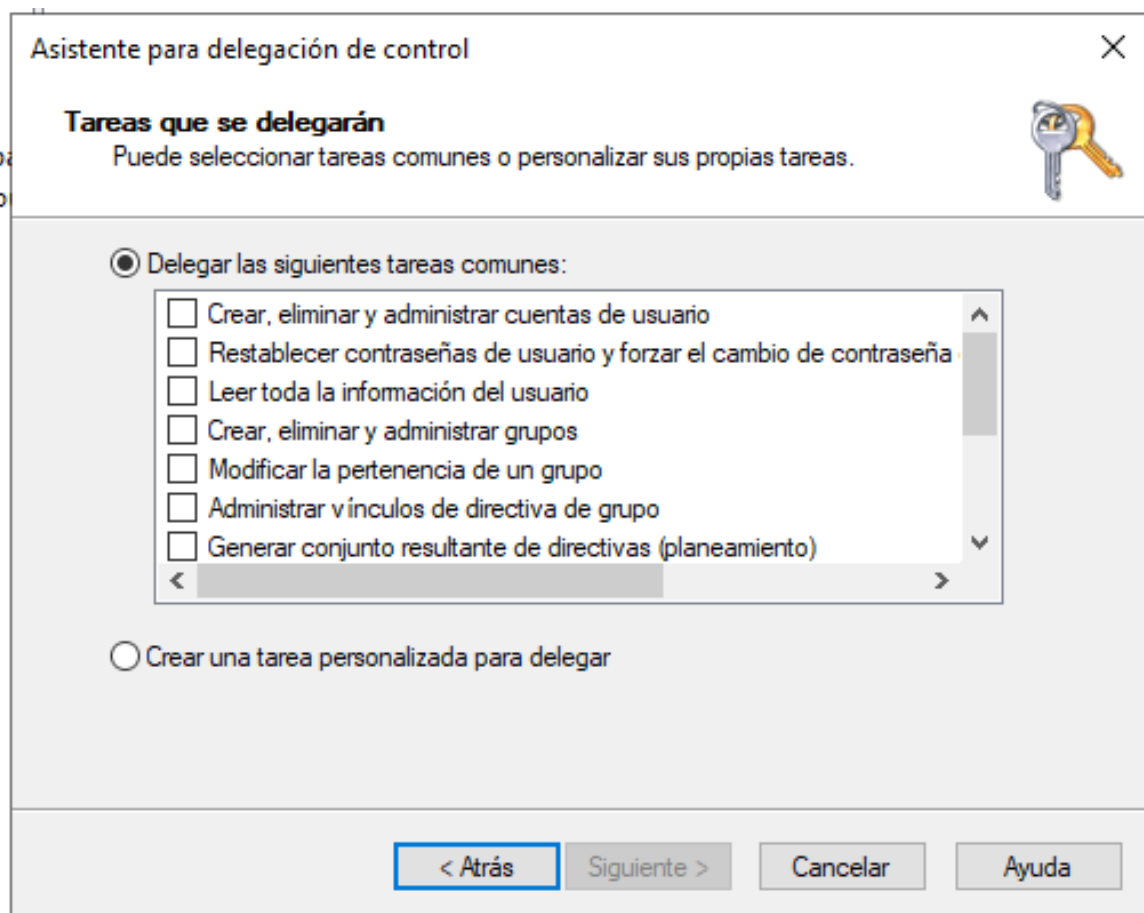


Figura 2: *Figura 2: Assignar drets en la delegació*

## 2.2 Assignem drets

---

Un exemple d'ús senzill és d'autoritzar a un usuari de la Delegació, Centre de Producció o Projecte que represente la UO per a que reinicie les contrassenyes dels usuaris. Així cada vegada que un operador d'ordinador se li oblida la contrasenya no cal que cride a l'administrador

Nota:

Fixem-nos en el detall que parlem de “drets” i no de “permisos” que és un terme que circumscriurem a l'àmbit del sistema de fitxers.

## 2.3 Habilem l'usuari per a iniciar sessió.

Com bé sabem, tal com ve configurat per defecte el Windows Server, hi ha uns grups d'usuaris que poden iniciar sessió al servidor són *administradors del domini* o *administradors del servidor (Domain Controller)* (Admins. del dominio, Administradores, Operadores de copias...).

Això té la seua raó en la seguretat evidentment. El nostre usuari no pertany (ni ha de pertànyer) a cap d'aquests grups: és un *usuario del dominio*, no és “l'informàtic de l'empresa”.

Del que es tracta és de fer una excepció i permetre l'accés al servidor a aquest usuari del domini per a que faci només **estrictament** les accions que hem especificat adés com a drets (Restablecer contraseñas...)

A la *Unitat 5. Windows Server. Monitorització i ús* tractarem l'inici de sessió remota, ara farem l'inici local.

### Spoiler: directiva de seguretat

Tot i que les Directives de Seguretat es tracten a la *Unitat 4. Administració i configuració avançada* s'imposa la necessitat de fer un spoiler.

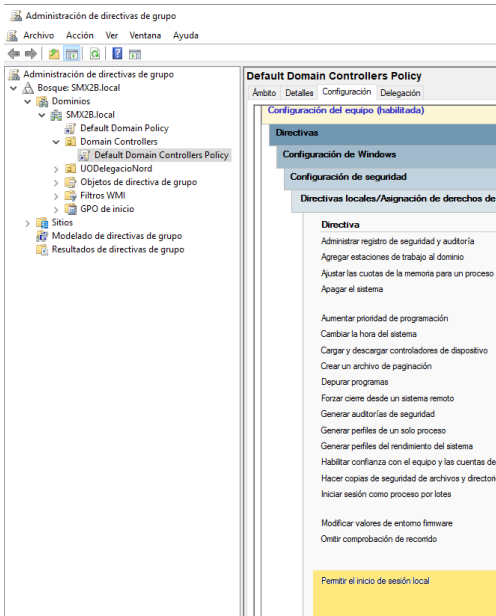
### Canvi de la directiva: “Permitir inicio en sesión local”

1- Executar **gpmc.msc**

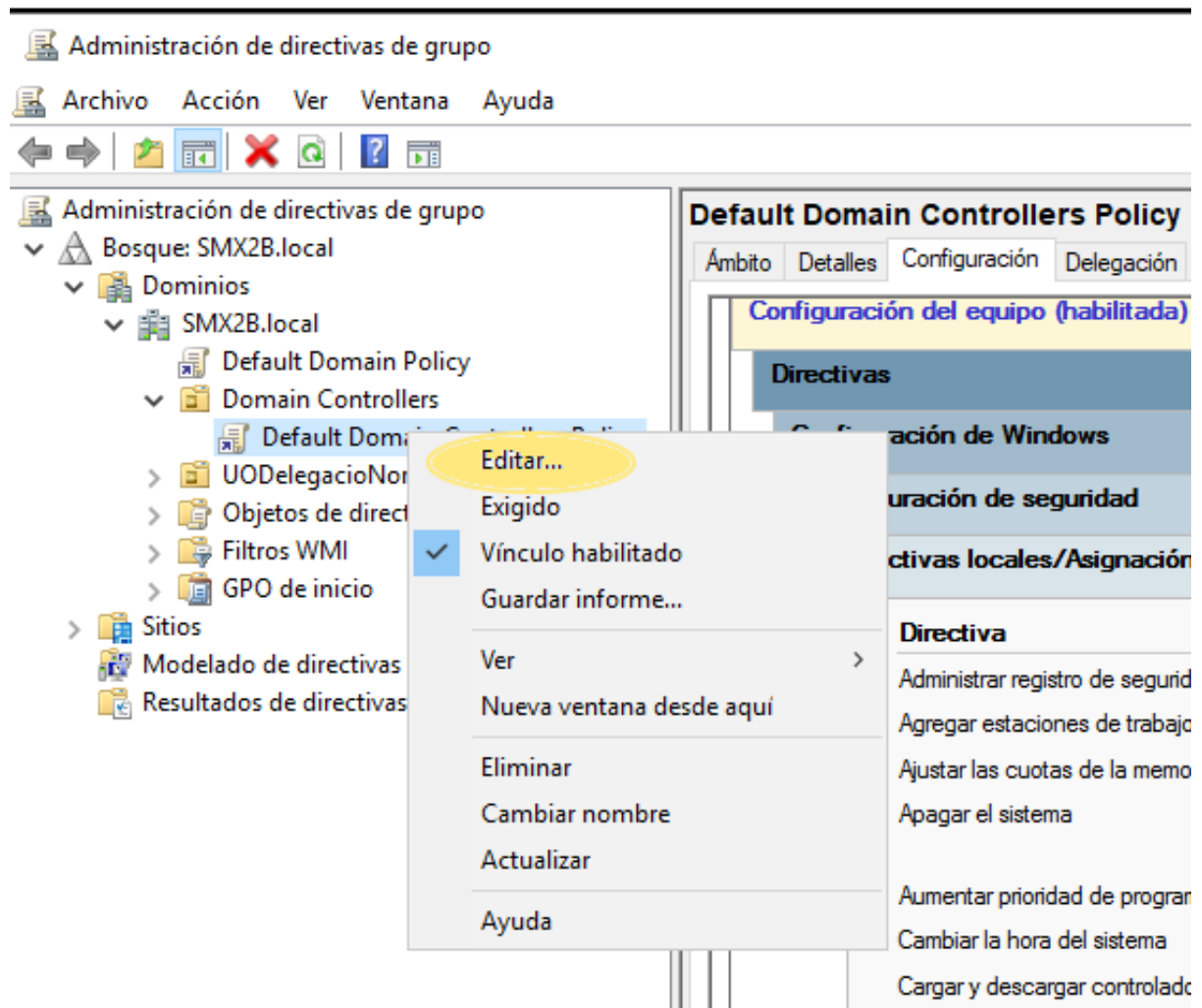
A la *Unitat 4* tractem un poc més a fons les directives en general

Busquem una directiva que afecta a la màquina (**Domain Controller**) ja que es tracta de permetre iniciar sessió local, per tant modificarem la plantilla de directives que ve per defecte de **Default Domain Controller Policy** la directiva: **Permitir el inicio de sesión local**

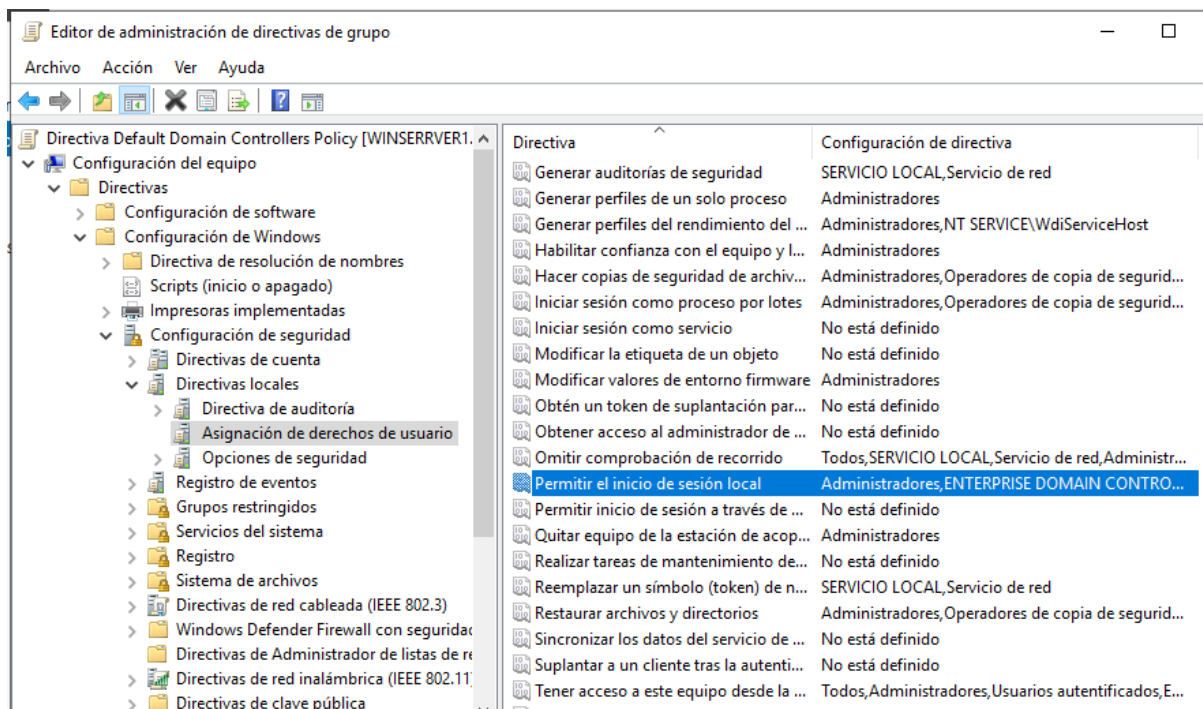
- Observem quins grups poden iniciar sessió localment en aquesta màquina.



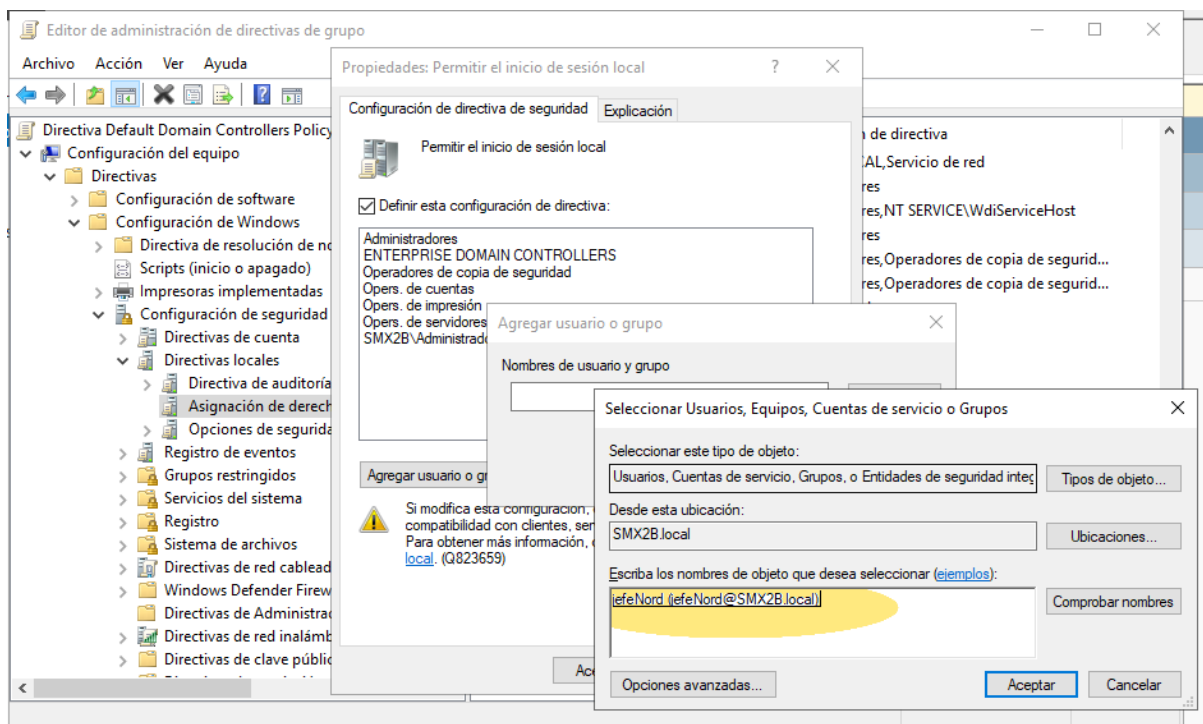
- Botó contrari:**EDITAR**



- Seleccionem la directiva que volem canviar



- Afegim l'usuari



- Sempre que teniu **APLICAR** recordeu polsar abans que **Aceptar**

**Comprovem...** Provem tancar la sessió de l'administrador en ús i comprovar que l'usuari ja pot iniciar sessió localment al servidor. Efectivament, pot.

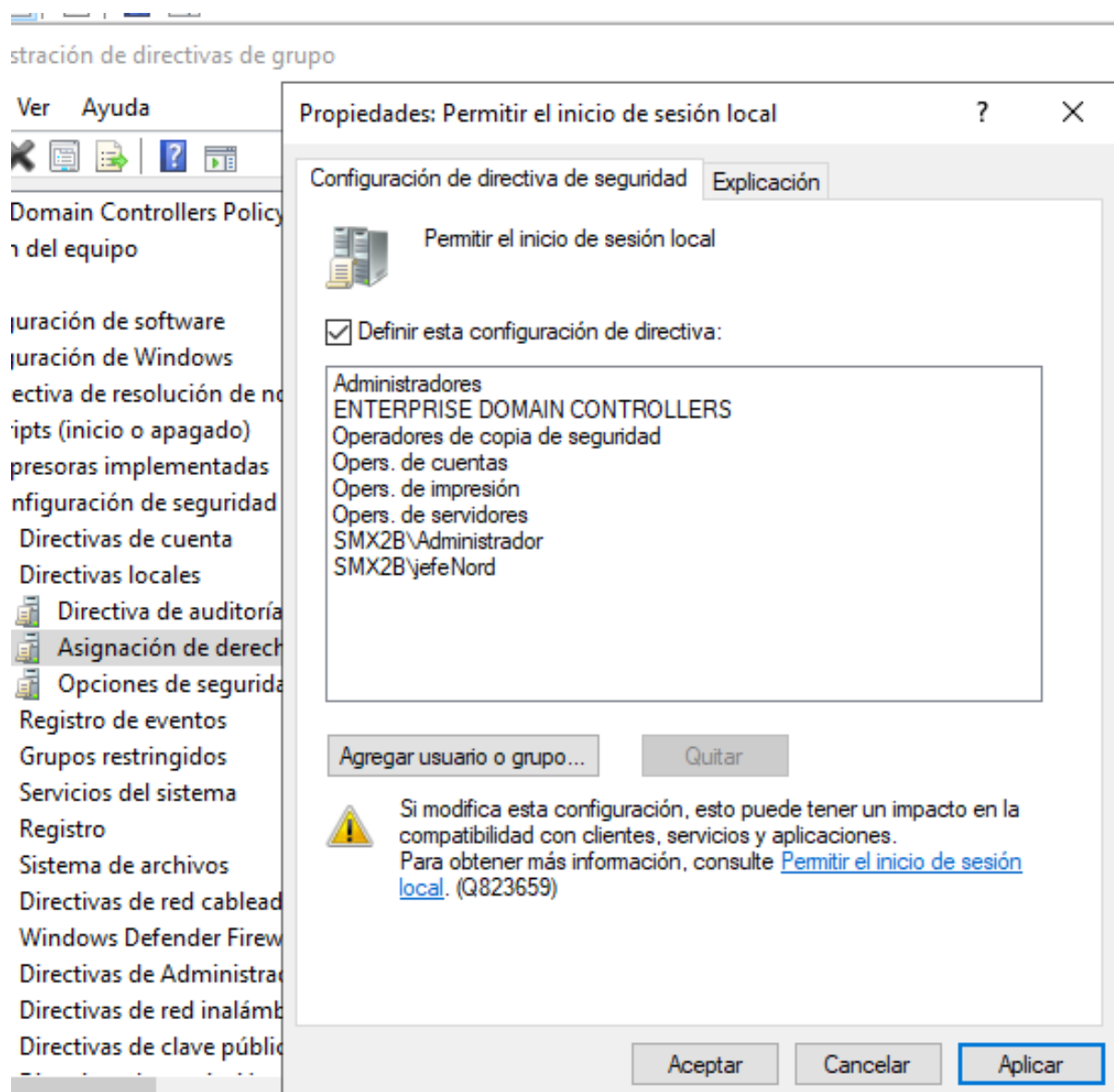


Figura 3: Figura 7: Edición de la directiva local de seguridad

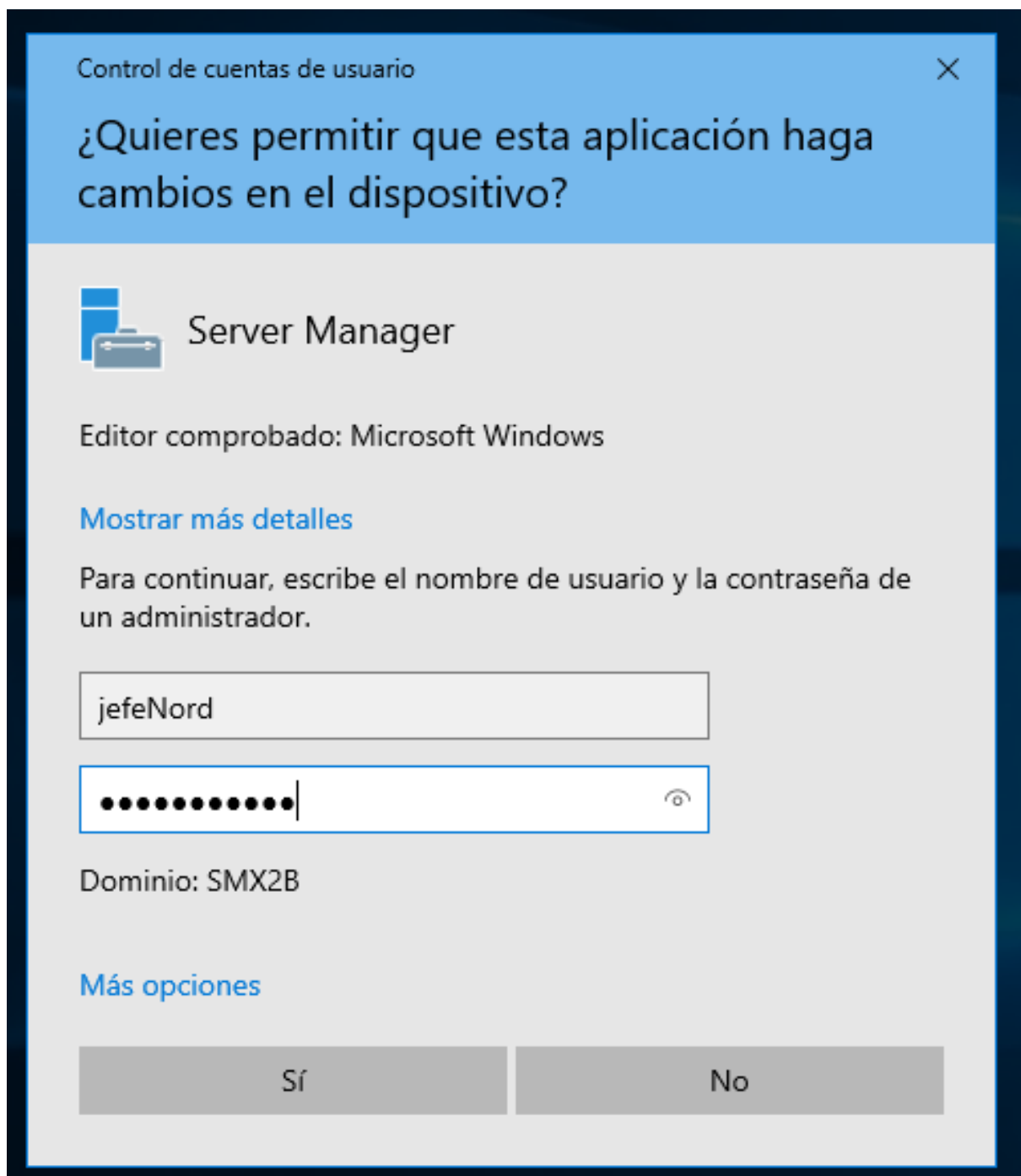
## 2.4 Comprovació de les accions que podem fer

Per defecte, no se'ns obri el panel d'Administració de Servidor. Cosa lògica si entenem que no som Administradors ni del servidor (local) ni del domini.

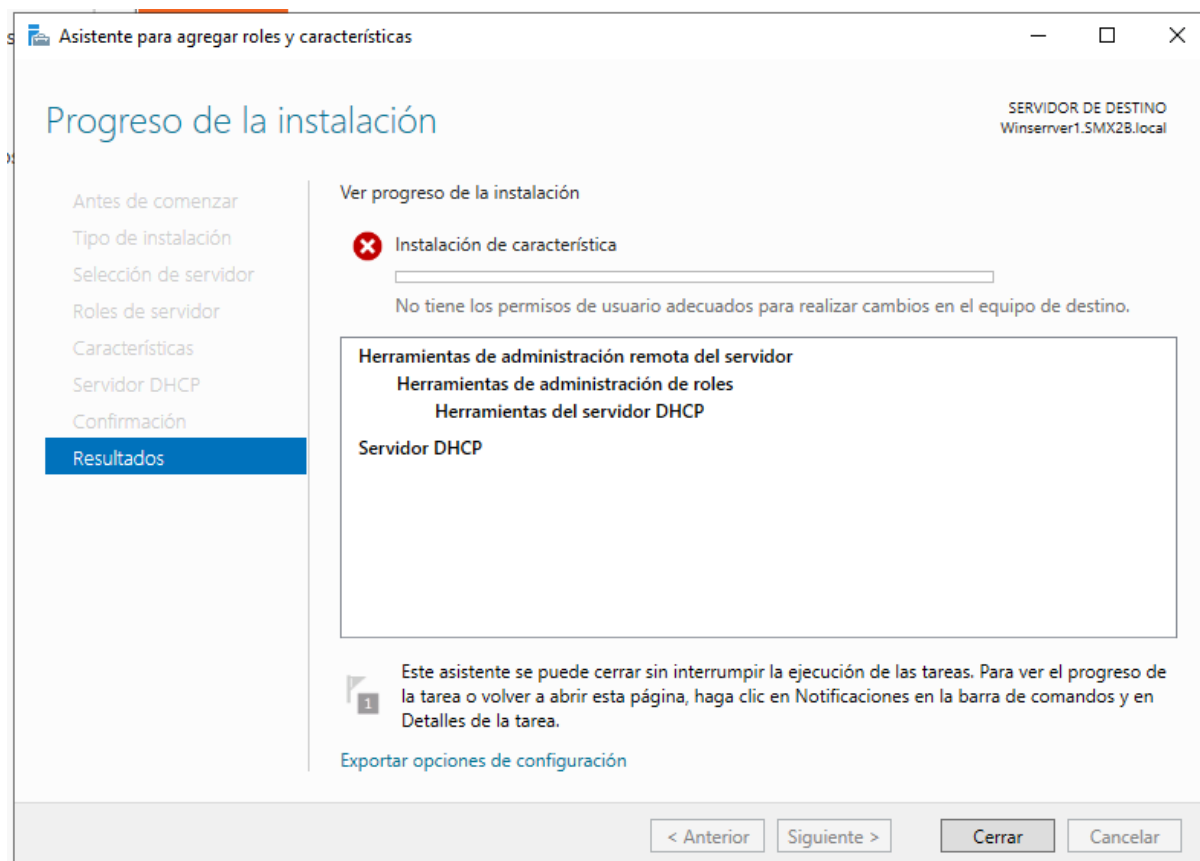
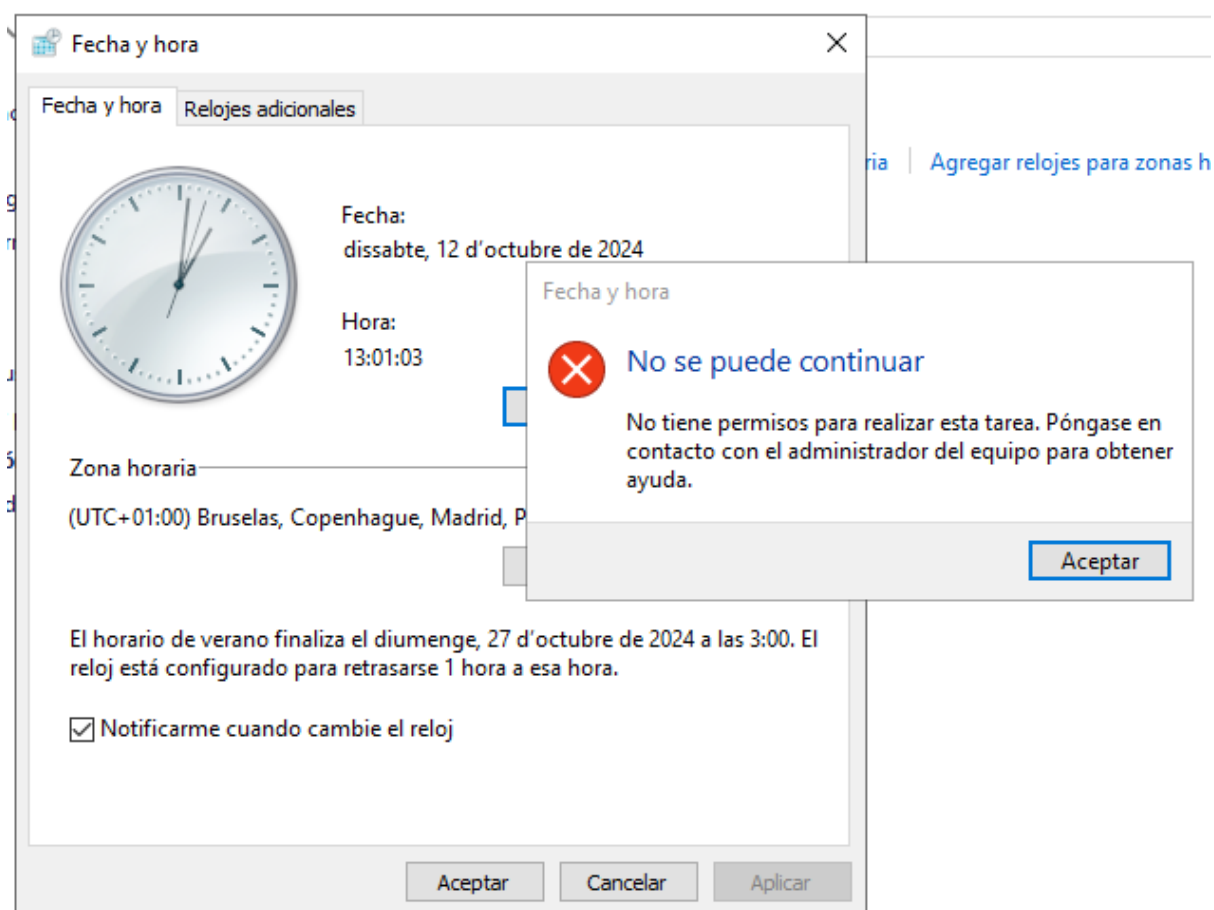
### Accés a eines d'administració

Si intentem accedir a alguna eina d'administració com les consoles de Microsoft (dsa.mmc, per exemple), l'administrador del servidor (servermanager.exe), panel de control per fer un canvi... Ens demanarà que ens autèntiquem...

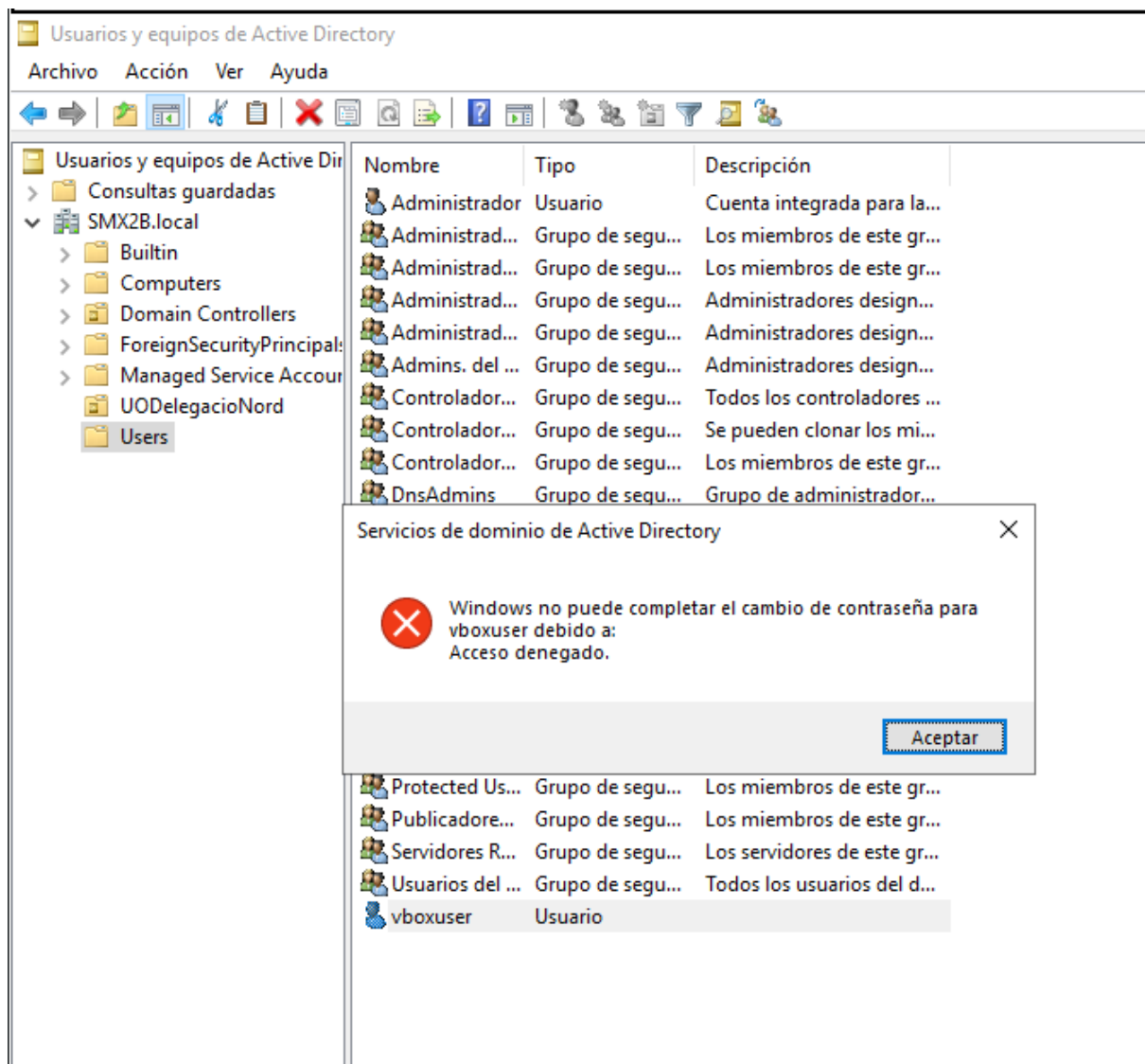




Una vegada ens autèntiquem com a l'usuari delegat veiem que podem entrar sense problemes (en principi). És més, encara que l'acció no estava entre les autoritzades (apartat 2.2 i Figura 2), potser ens deixi "iniciar-la", fer com uns "primers passos" dins de cada eina GUI però arriba un moment en que se'ns denega.



Una prova que heu de fer és la provar les accions permeses dins de la UO on tenim delegat el control i fora.



## 2.5 Conclusions

### Analogia i recordatori de SOM

A partir dels coneixements teòrics i pràctics del curs passat a SOM, podem entendre què ha passat i on. El que passa és exactament el que ens passava a l'aula de SOM, l'any anterior si, amb l'usuari d'alumne intentàvem executar un "sudo..."

**Exemple 1** No podem instal·lar un ROL com quan en Linux no podíem instal·lar un paquet...

```
tomas@portatil: ~  
Fitxer  Edita  Vista  Cerca  Terminal  Ajuda  
rosa@portatil:/$ sudo apt update  
[sudo] contrasenya per a rosa:  
rosa no està al fitxer sudoers.  S'informarà d'aquest incident.
```

**Exemple 2** No podem canviar l'hora des del Panel de Control del Windows Server, ve a dir-nos que no “som sudoer”

```
tomas@portatil: ~  
Fitxer  Edita  Vista  Cerca  Terminal  Ajuda  
rosa@portatil:/$ sudo date --set="2026-01-01 00:00:00"  
[sudo] contrasenya per a rosa:  
rosa no està al fitxer sudoers.  S'informarà d'aquest incident.
```

## Les capes del SO

### 1- Interfície usuari

GUI: L'eina de configuració (consola msa.msc, per exemple) és un aplicació de sistema. Hi està a la capa externa que es comunica amb nosaltres (usuaris) i ¡, així, li donem les indicacions sobre què volem que faci la màquina.

CLI: El terminal de Linux (o Powershell com vorem) també fan la mateixa funció.

Realment quan ens deixa executar inicialment, és com qual al terminal ens deixa escriure “sudo apt...”. És quan li donem a Enter ( o Aplicar/Aceptar) quan **enviem l'ordre al kernel** quan...

**2- Seguretat i protecció** El Kernel (nucli del SO) de Windows i de Linux comprovem que l'usuari no està autoritzat.

### Comproveu l'abast de la delegació

És important que comproveu que l'usuari té el control dins de la UO estrictament. En un altra UO o a l'arrel del Domini (exemple de la imatge següent), no.

---

## 3 Gestió dels usuaris amb delegació. Característiques avançades del dsamc.msc

Per poder eliminar o fer canvis d'ubicacions de les UO, cal inhabilitar una protecció que tenen contra errors accidentals.

- Aquesta no està visible i hem danar a **Ver>Características Avanzadas** de la consola.

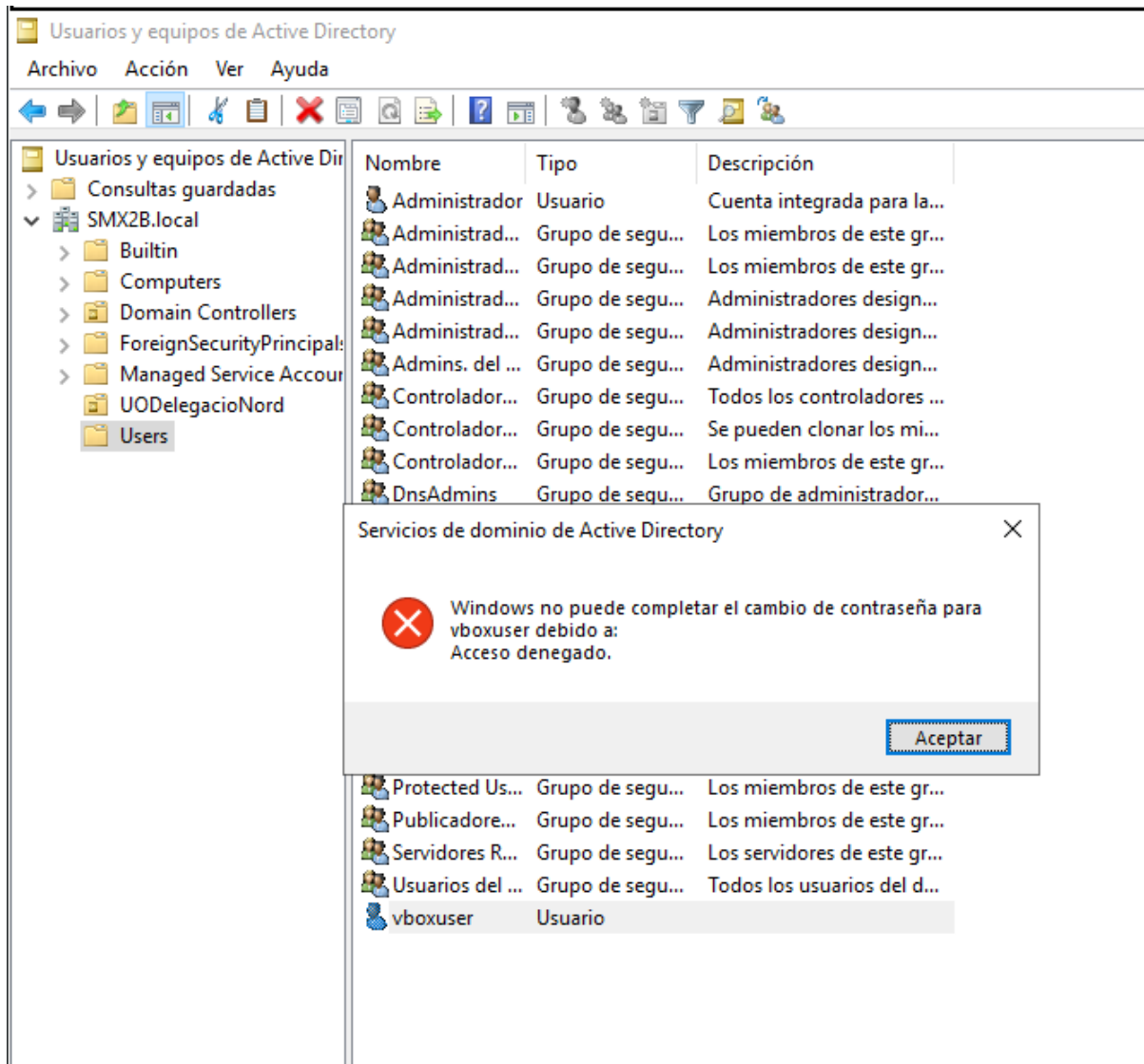


Figura 4: Figura 14: Fora del UO no pot fer cap acció

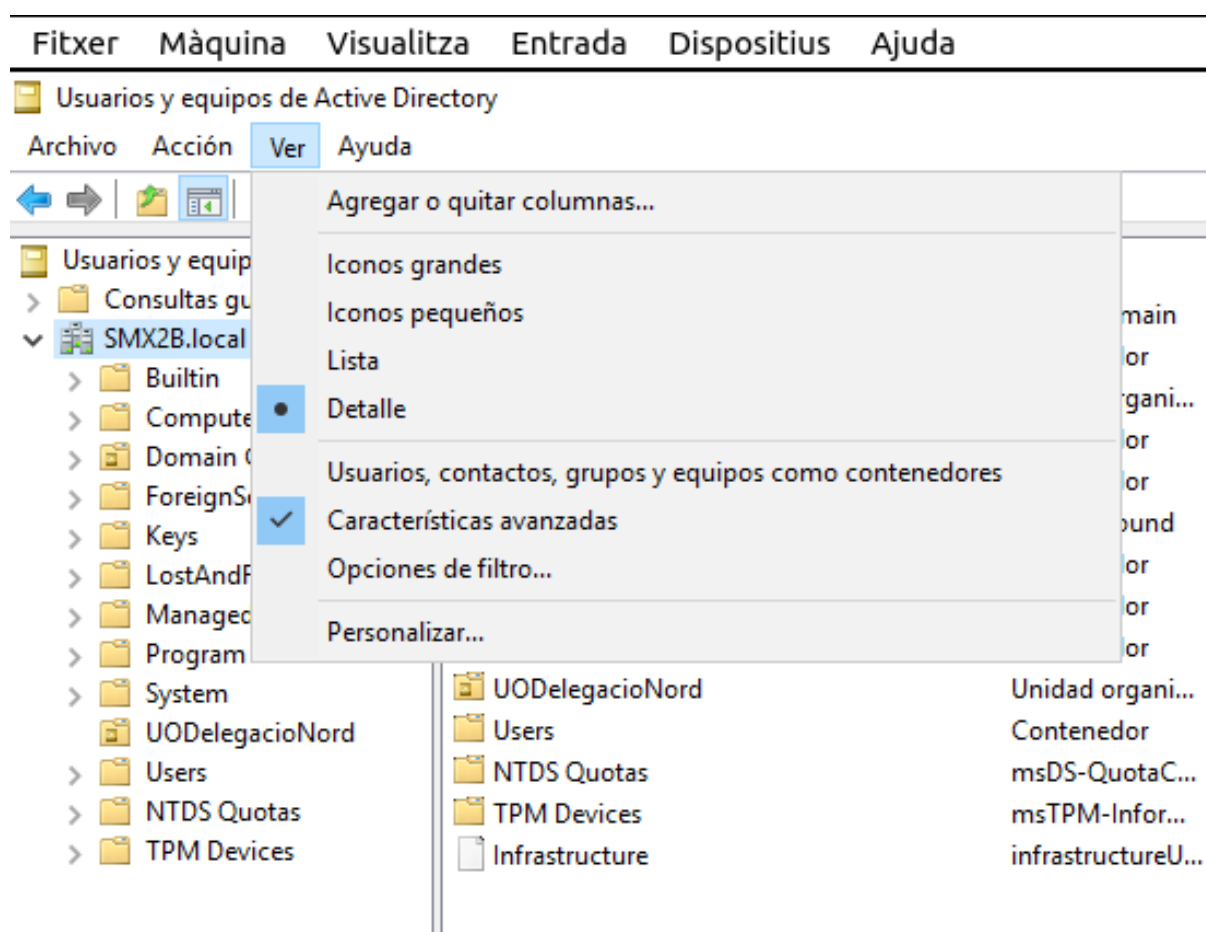
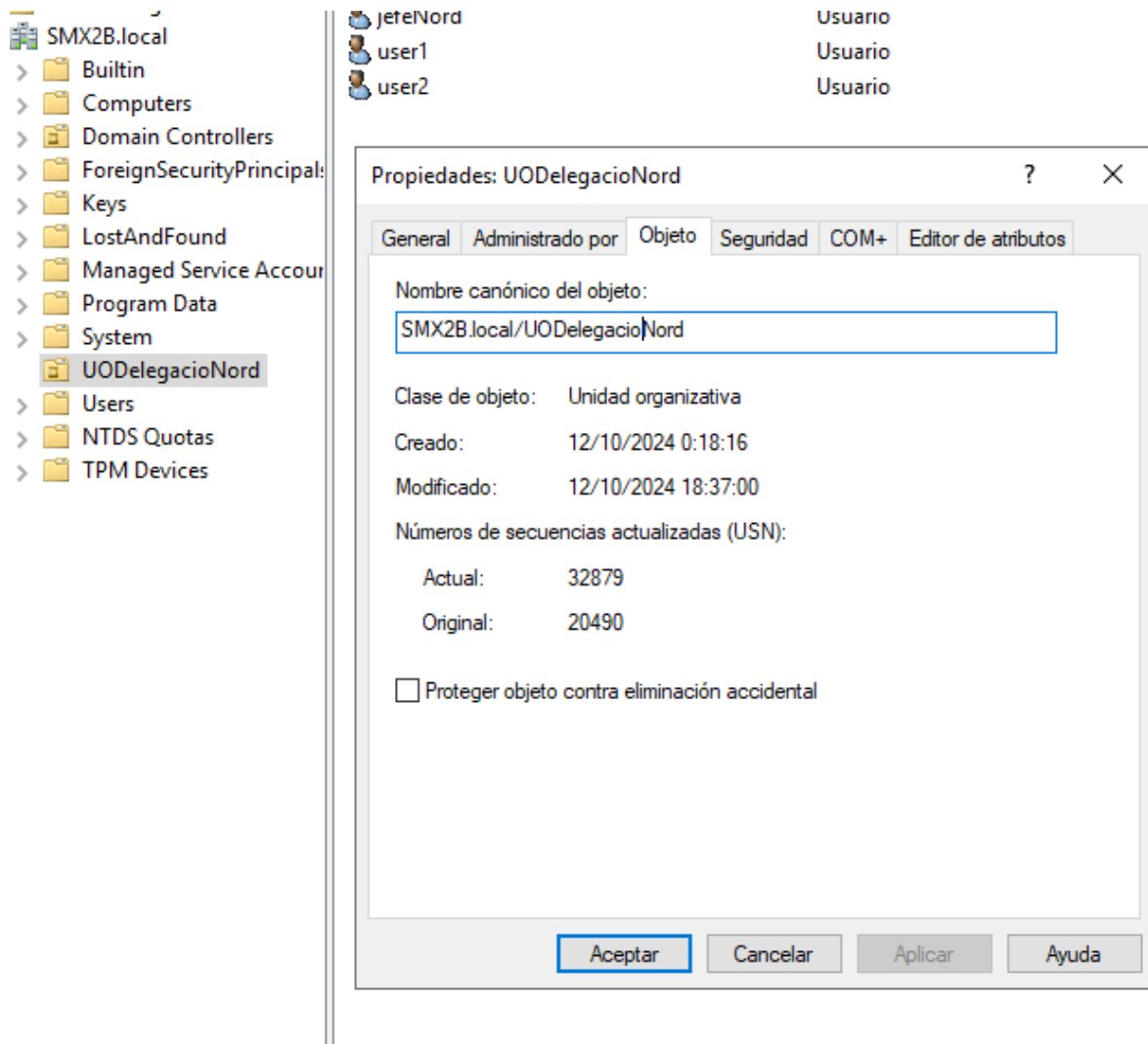
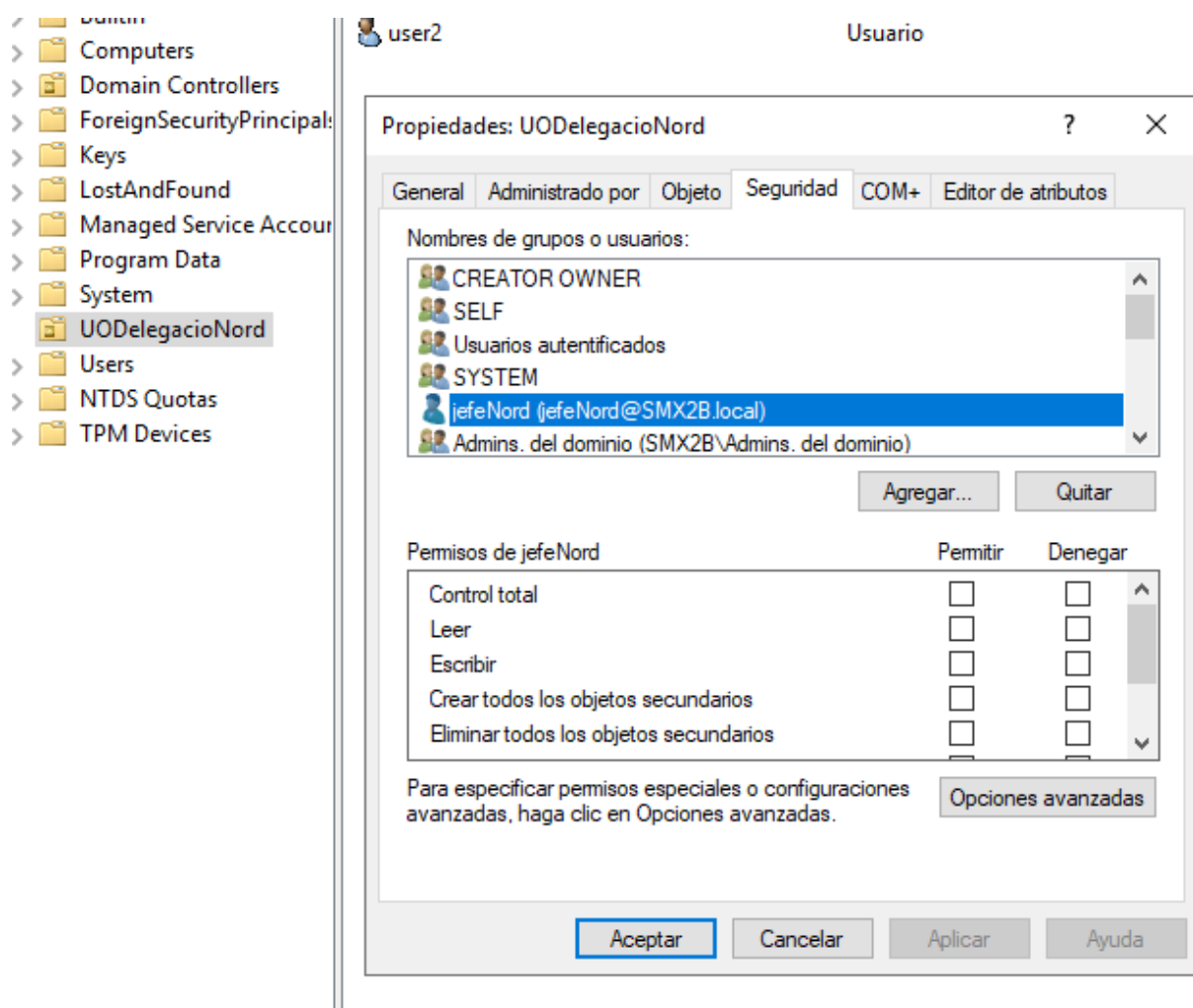


Figura 5: Figura 15: Veure-ho tot en dsa.msc

- Ara ja apareix la pestanya *Propiedades>Objeto* en per desprotegir (convindria que la tornàreu a deixar com estava en acabar).



- També ens apareix la pestanya *Propiedades>Seguridad* on podem veure quin usuari té el control.



- Entrem en *Características Avanzadas* i veiem tot la informació detallada sobre quins usuaris i quins drets tenen sobre la UO. Des d'ací podem afegir i llevar usuaris i drets.



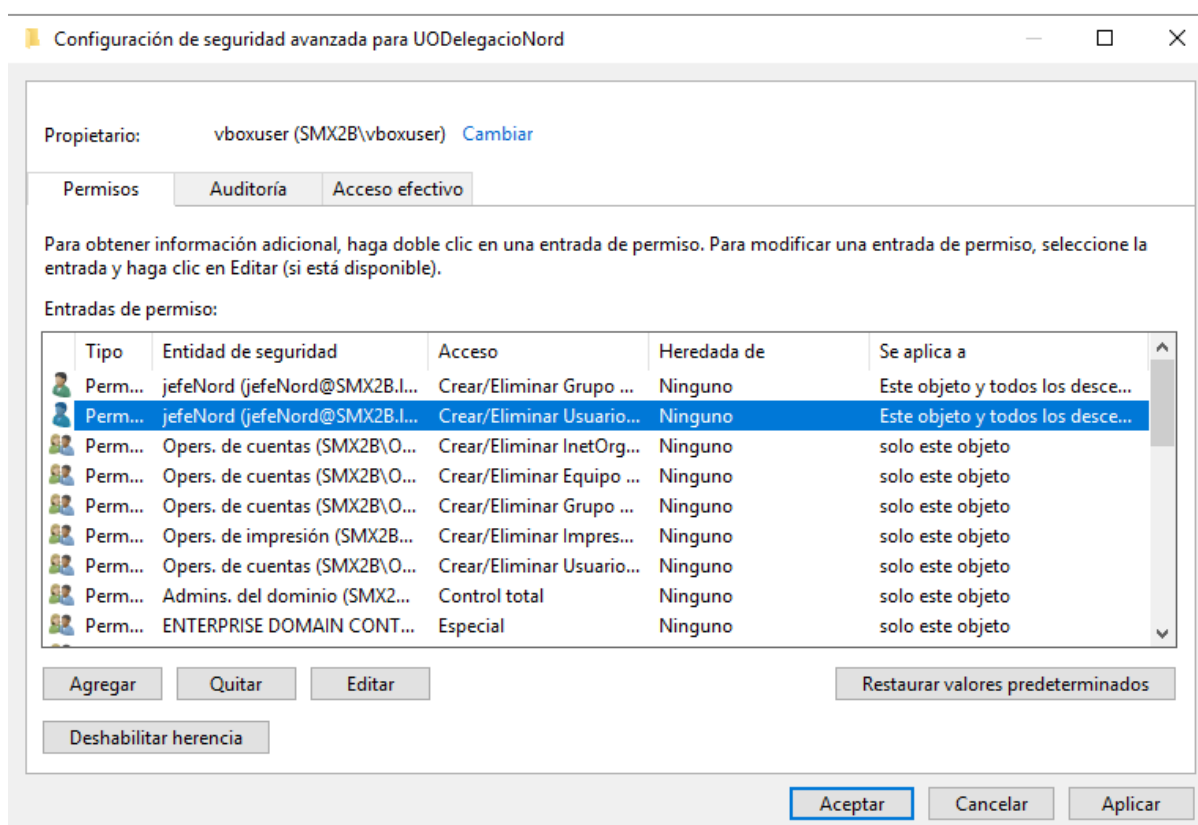


Figura 6: \*Figura 18: Gestió de drets i usuaris sobre la UO