

U3. WINDOWS SERVER. ADMINISTRACIÓ I CONFIGURACIÓ (V)

GESTIÓ DE UO I AVANÇ DIRECTIVES LOCALS DE SEGURETAT

@tofermos 2024

Índex

1 Les UO	2
Per a què es creen les UO?	2
La divisió del treball duu l'especialització	2
2 La delegació de control de la UO	2
2.1 Selecció de l'usuari, usuaris o grups	2
2.2 Assignem drets	5
2.3 Habilitem l'usuari per a iniciar sessió.	5
2.4 Comprovació de les accions que podem fer	6
2.5 Conclusions	11
3 Gestió dels usuaris amb delegació. Característiques avançades del dsamc.msc	15

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 contigut 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.

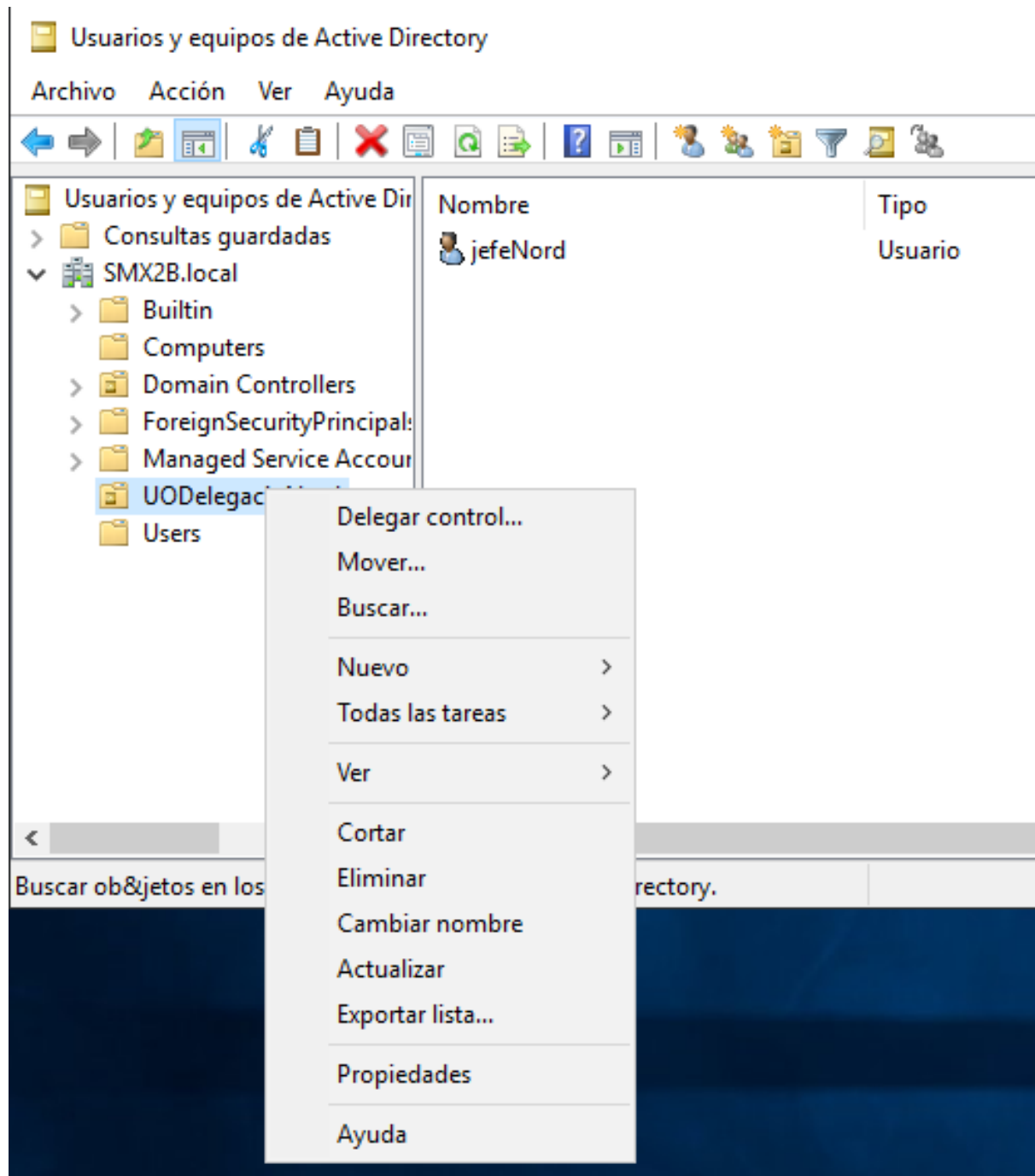


Figura 1: *Figura 1:Delegar control*

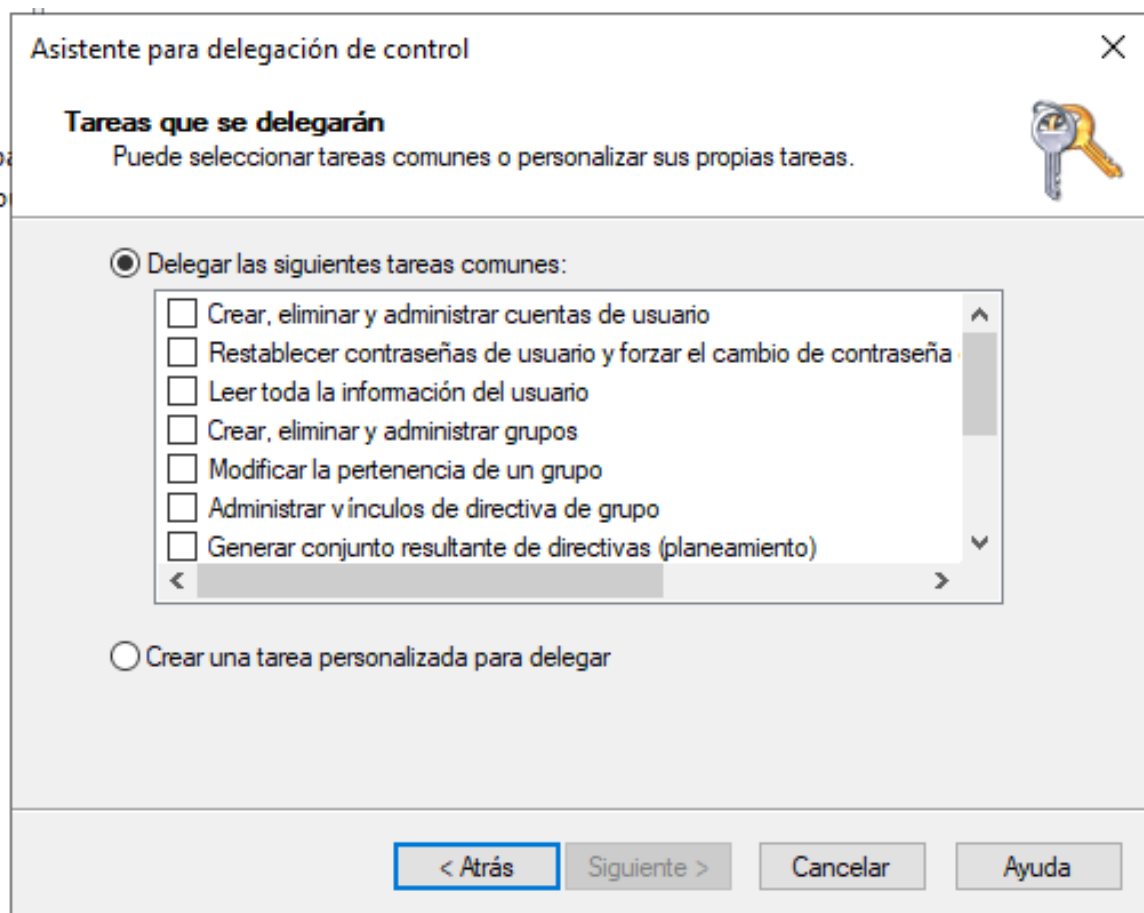


Figura 2: *Figura 2: Assignar drets en la delegació*

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 oblidia 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, els grups d'usuaris que poden iniciar sessió al servidor per defecte, en acabar la instal·lació de Windows Server, són alguns grups predeterminats que direm genèricament i mal dit “administradors” (Administradors del servidor, del domini, operadors de comptes...). Té la seua raó en la seguretat evidentment.
























Nombre	Tipo	Descripción
 Administrador	Usuario	Cuenta integrada para la administración del equipo o dominio
 Administradores clave	Grupo de segu...	Los miembros de este grupo pueden realizar operaciones administrativas en los objetos clave del dominio.
 Administradores clave de la organización	Grupo de segu...	Los miembros de este grupo pueden realizar operaciones administrativas en los objetos clave del bosque.
 Administradores de empresas	Grupo de segu...	Administradores designados de la empresa
 Administradores de esquema	Grupo de segu...	Administradores designados del esquema
 Admins. del dominio	Grupo de segu...	Administradores designados del dominio
 Controladores de dominio	Grupo de segu...	Todos los controladores de dominio del dominio
 Controladores de dominio clonables	Grupo de segu...	Se pueden clonar los miembros del grupo que sean controladores de dominio.
 Controladores de dominio de sólo lectura	Grupo de segu...	Los miembros de este grupo son controladores de dominio de solo lectura en el dominio.
 DnsAdmins	Grupo de segu...	Grupo de administradores de DNS
 DnsUpdateProxy	Grupo de segu...	Cientes DNS que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes (tales como servidores DHCP).
 Enterprise Domain Controllers de sólo lect...	Grupo de segu...	Los miembros de este grupo son controladores de dominio de solo lectura en la empresa.
 Equipos del dominio	Grupo de segu...	Todas los servidores y estaciones de trabajo unidos al dominio
 Grupo de replicación de contraseña RODC ...	Grupo de segu...	Los miembros de este grupo no pueden replicar las contraseñas a ningún controlador de dominio de solo lectura en el dominio.
 Grupo de replicación de contraseña RODC ...	Grupo de segu...	Los miembros de este grupo pueden replicar las contraseñas a todos los controladores de dominio de solo lectura en el dominio.
 Invitado	Usuario	Cuenta integrada para el acceso como invitado al equipo o dominio
 Invitados del dominio	Grupo de segu...	Todos los invitados del dominio
 Propietarios del creador de directivas de gr...	Grupo de segu...	Los miembros de este grupo pueden modificar la directiva de grupo del dominio
 Protected Users	Grupo de segu...	Los miembros de este grupo tienen protecciones adicionales frente a las amenazas contra la seguridad de autenticación. Consulte http://
 Publicadores de certificados	Grupo de segu...	Los miembros de este grupo pueden publicar certificados en el directorio
 Servidores RAS e IAS	Grupo de segu...	Los servidores de este grupo pueden obtener propiedades de acceso remoto de los usuarios
 Usuarios del dominio	Grupo de segu...	Todos los usuarios del dominio
 vboxuser	Usuario	

Figura 3: *Figura 3: Usuaris per defecte*

Com ja hem exposat, ara, anem a fer una excepció permentent l'accés al servidor a un usuari del domini (no és un informàtic dedicat a l'administració de la LAN) per a que faça només **estrictament** les accions que hem especificat adés com a drets.

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

Spoiler: directiva de seguretat

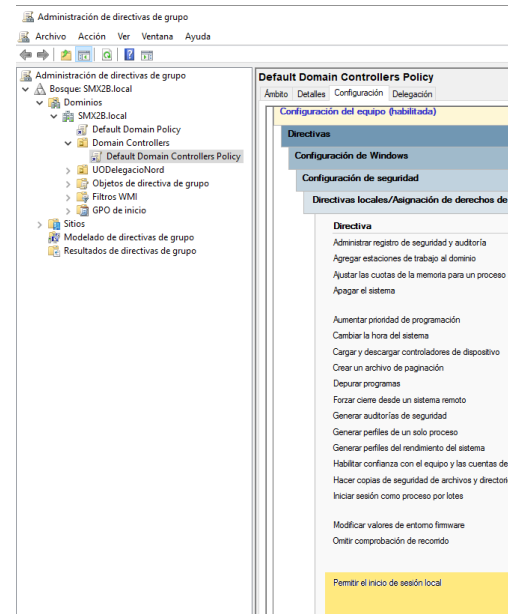
Tot i que les Directives de Seguretat es tracten a la *Unitat 4. Administració i configuració avançada* s'imposa la necessitat de fer un spoiler.

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 pulsar 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.

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).

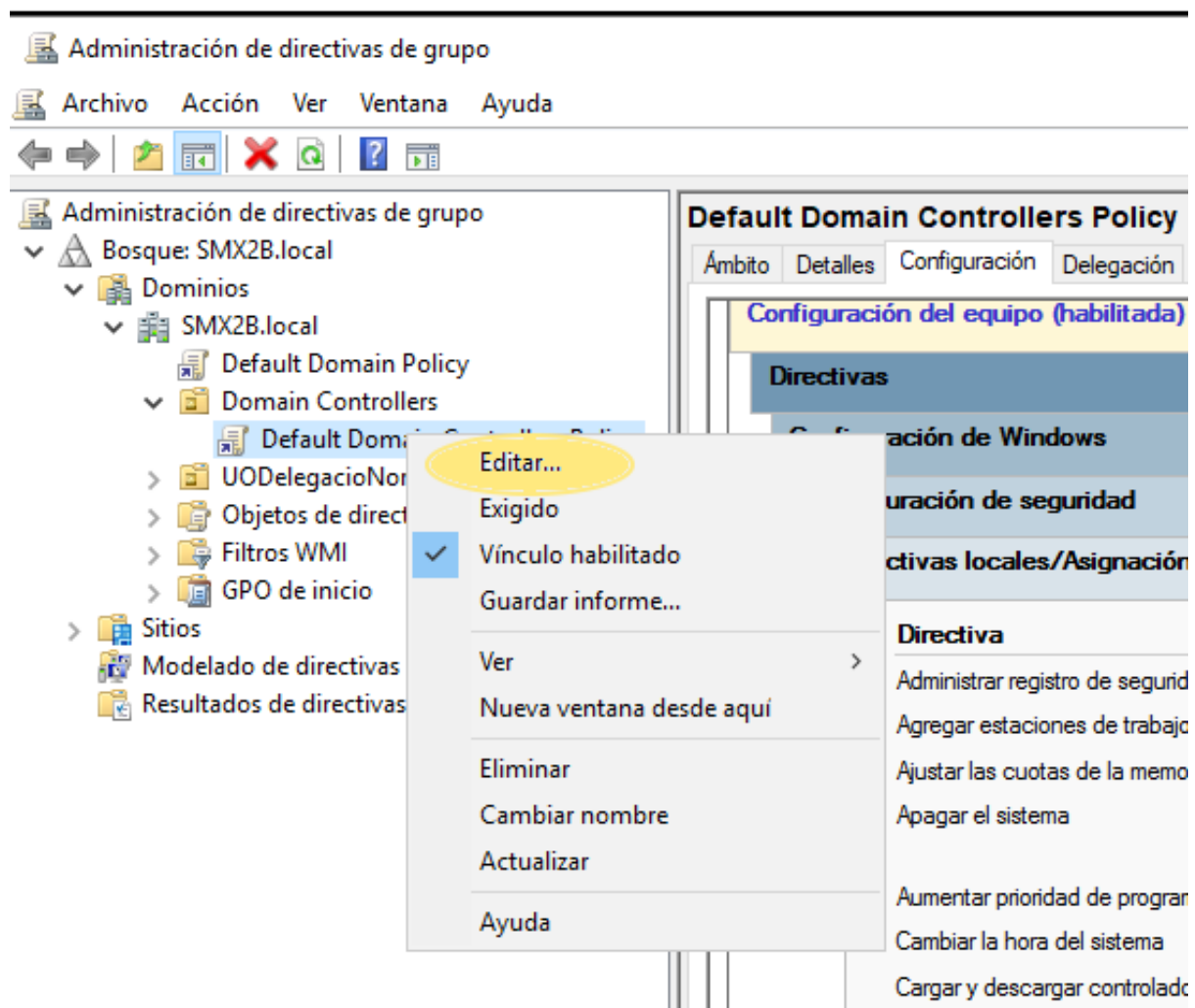


Figura 4: *Figura 5: Edició de la directiva local de seguretat*

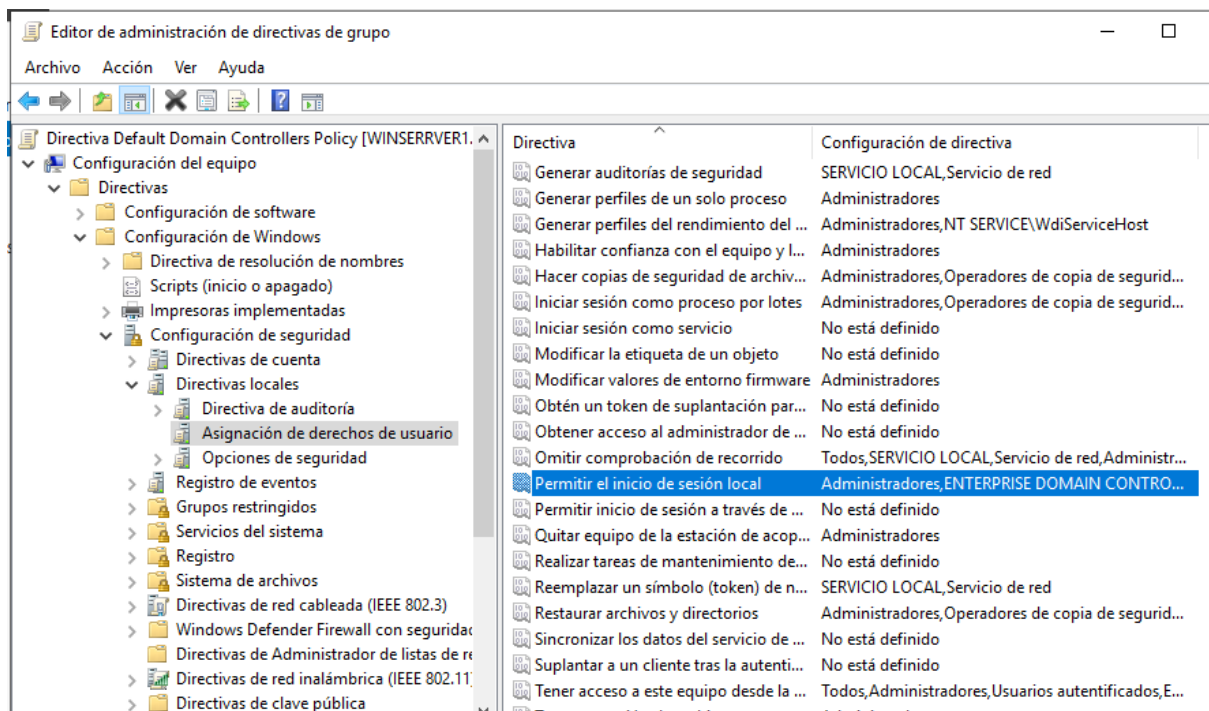


Figura 5: Figura 6: Edició de la directiva local de seguretat

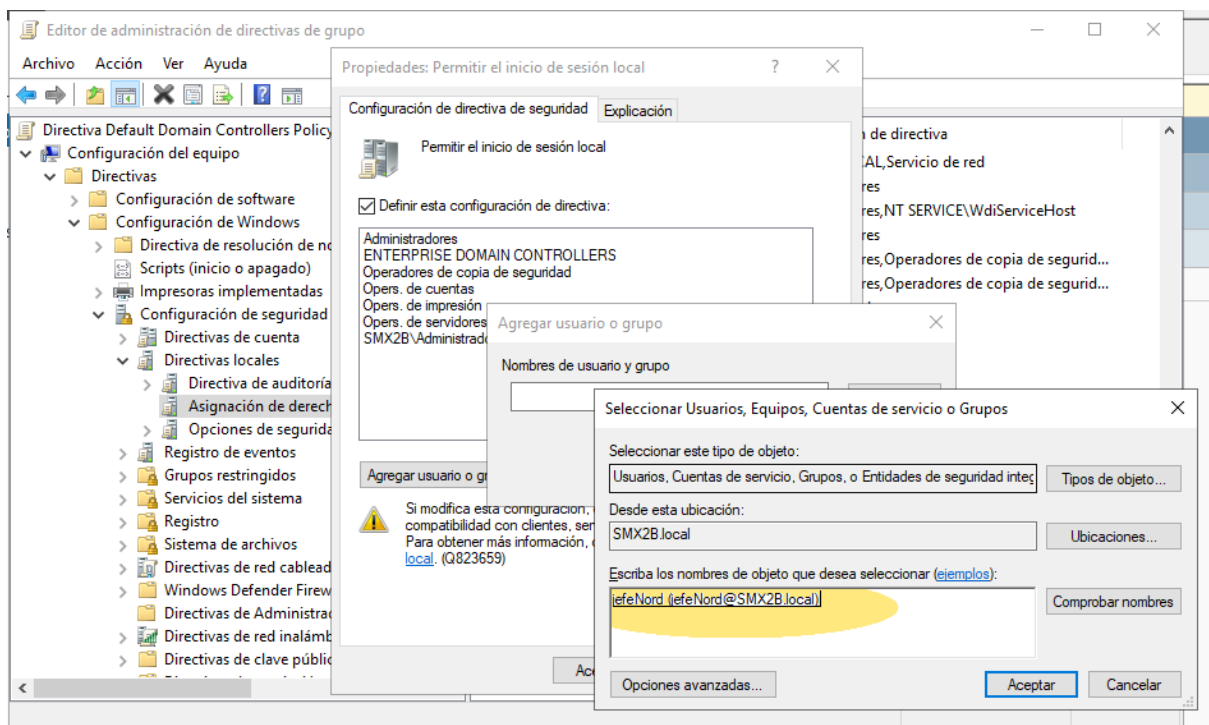


Figura 6: Figura 7: Edició de la directiva local de seguretat

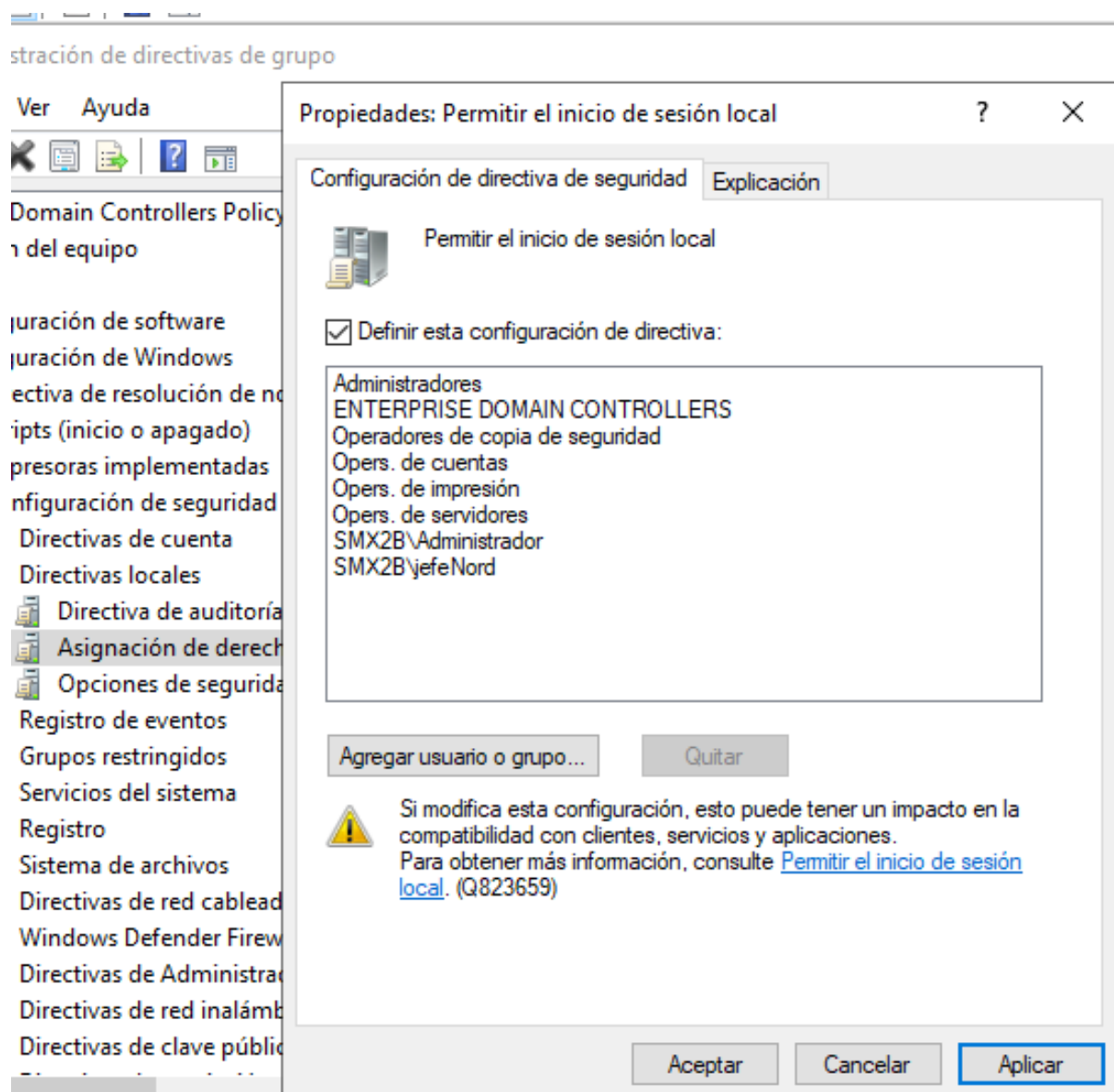


Figura 7: Figura 8: Edició de la directiva local de seguretat

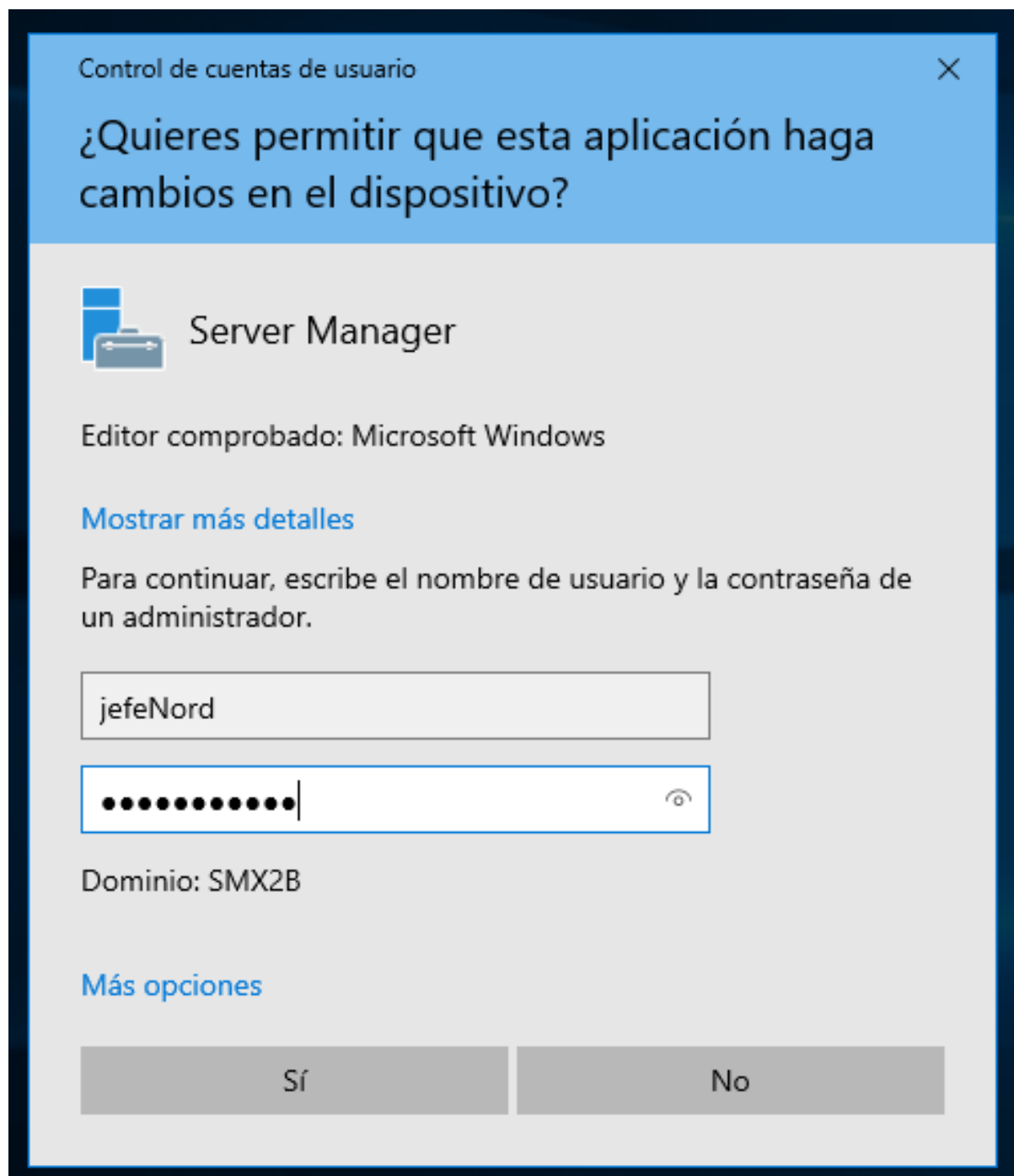


Figura 8: Figura 9: Autenticació d'usuari

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 pasos” dins de cada eina GUI però arriba un moment en que se'ns denega.

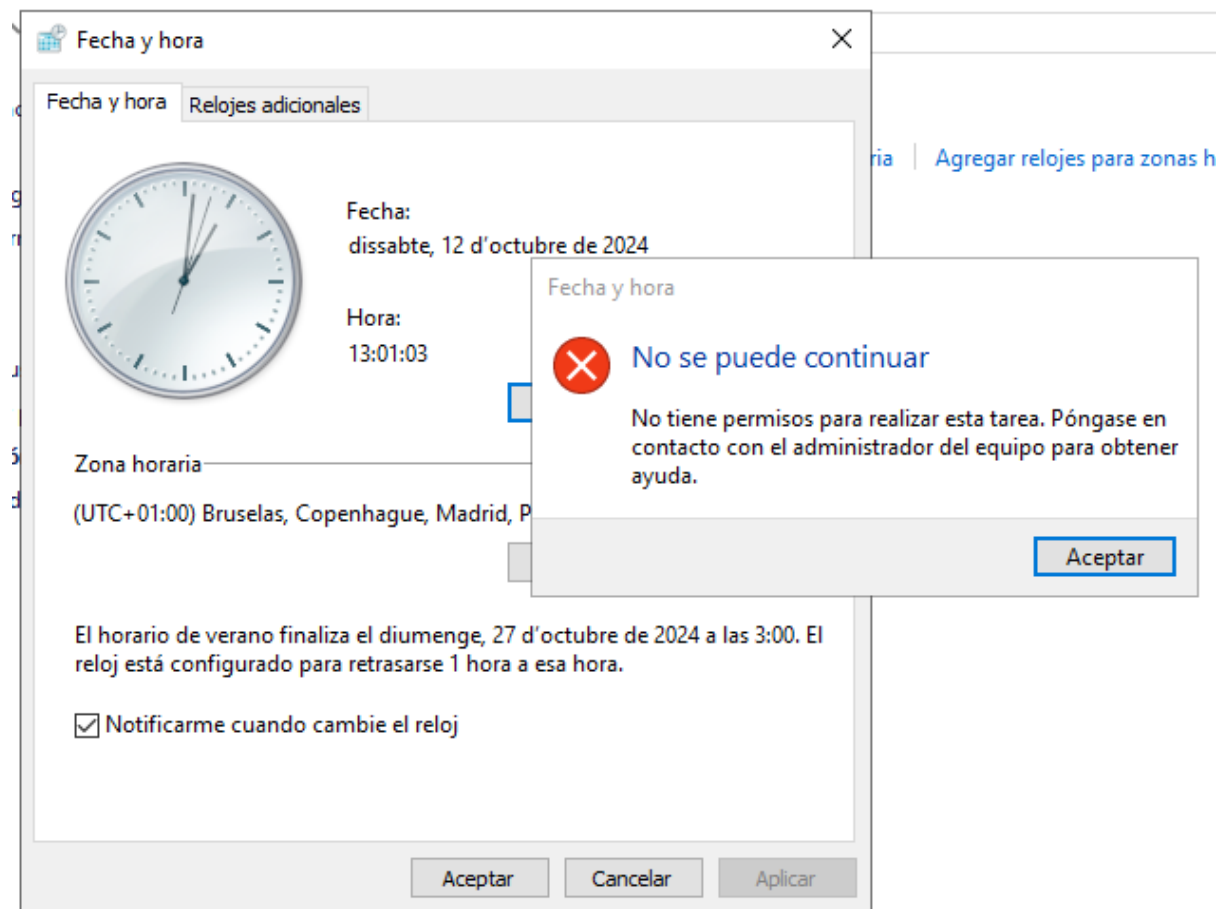


Figura 9: Figura 10: Panel de control, canviar hora

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...

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

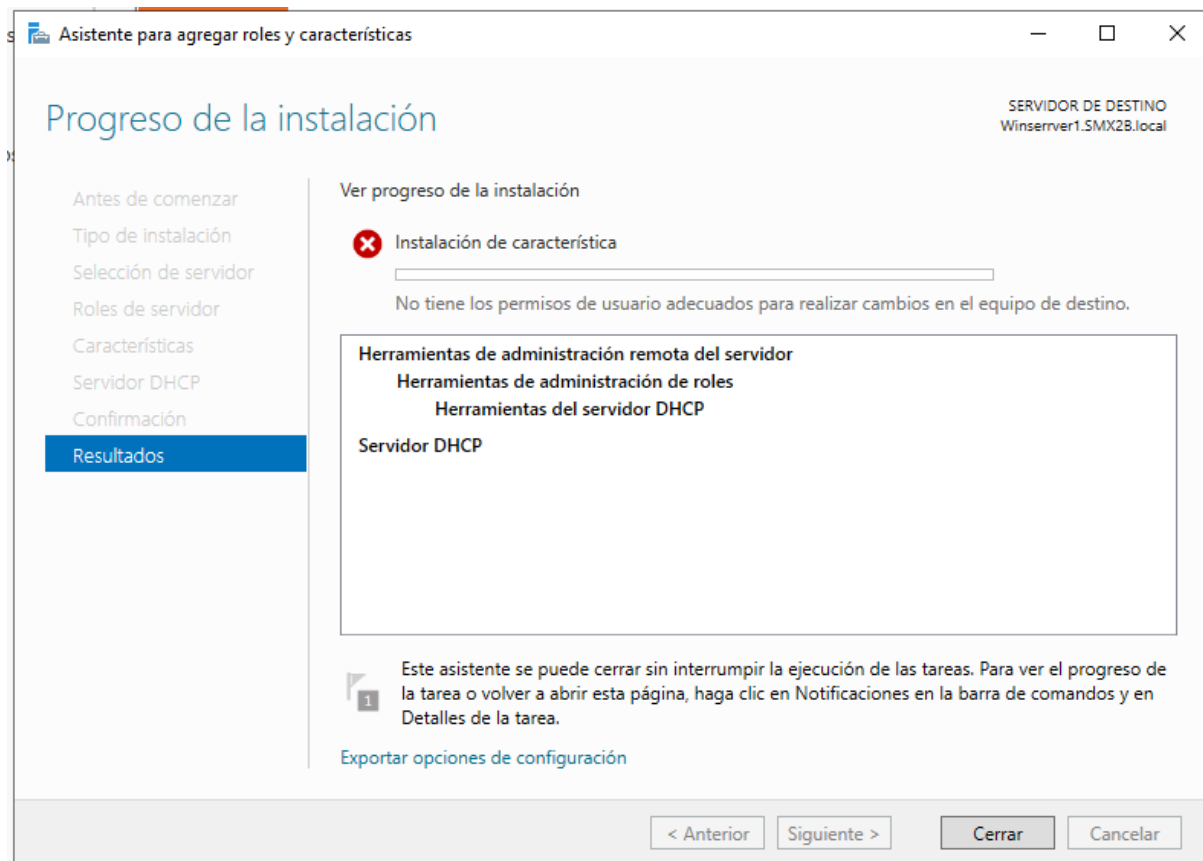


Figura 10: *Figura 11: Instal·lar ROL*

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.

Relament quan ens deixa executar inicialment, és com qual al terminal ens deixa escriure "sudo apt...". És quan li donem a Enter (o Aplicar/Aceptar) quen **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.

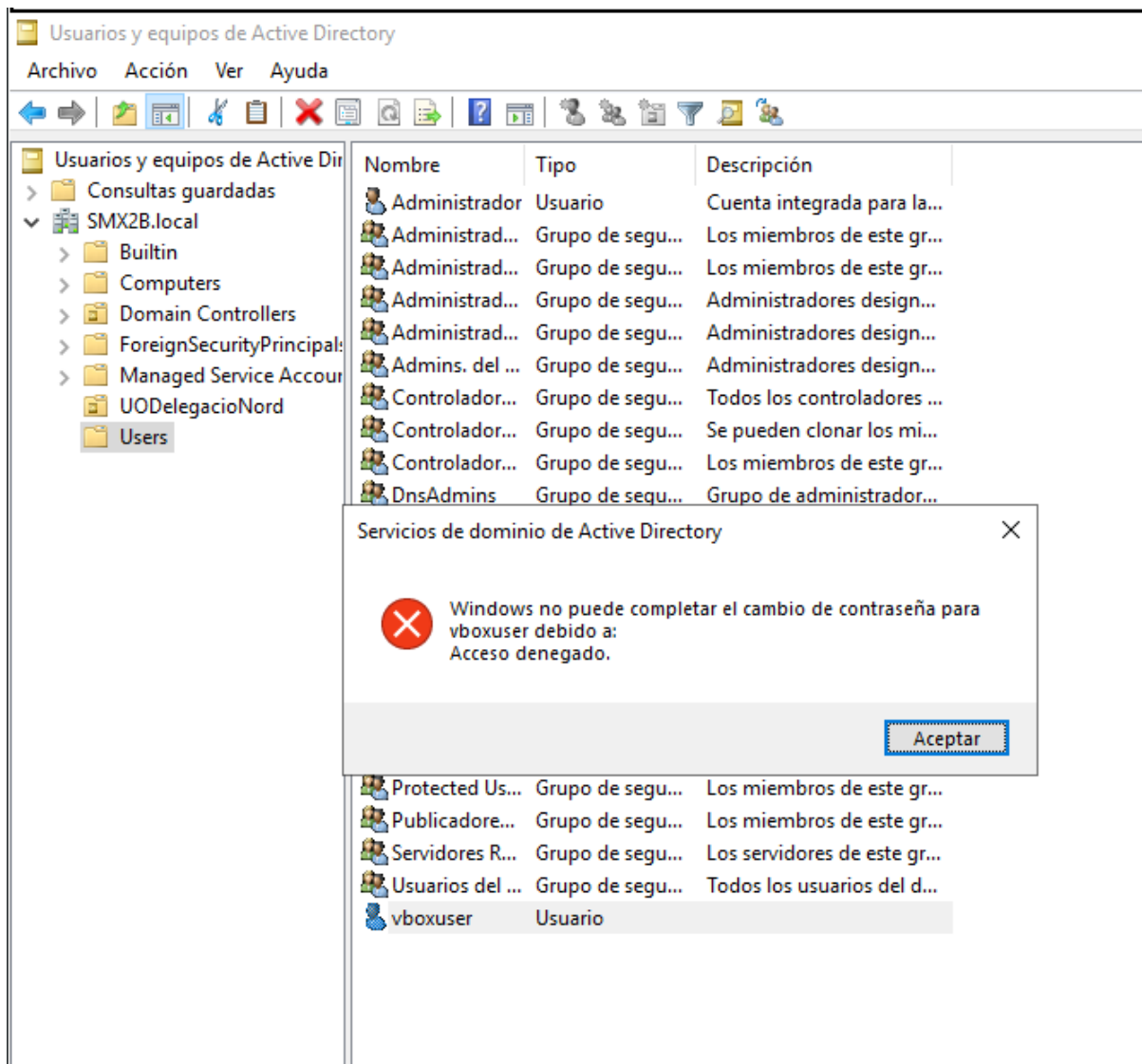


Figura 11: Figura 12: Accions permeses però fora de la UO

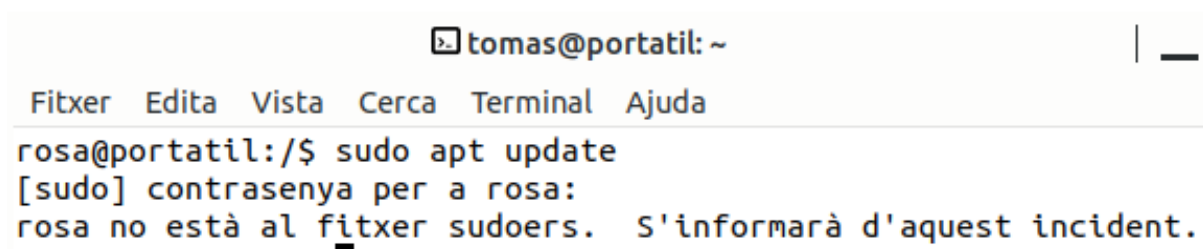


Figura 12: Figura 13: Eines per instal·lar apt

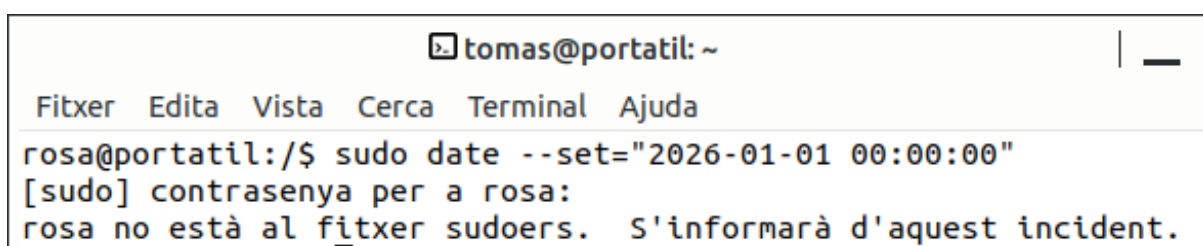


Figura 13: Figura 14: Canvi de data

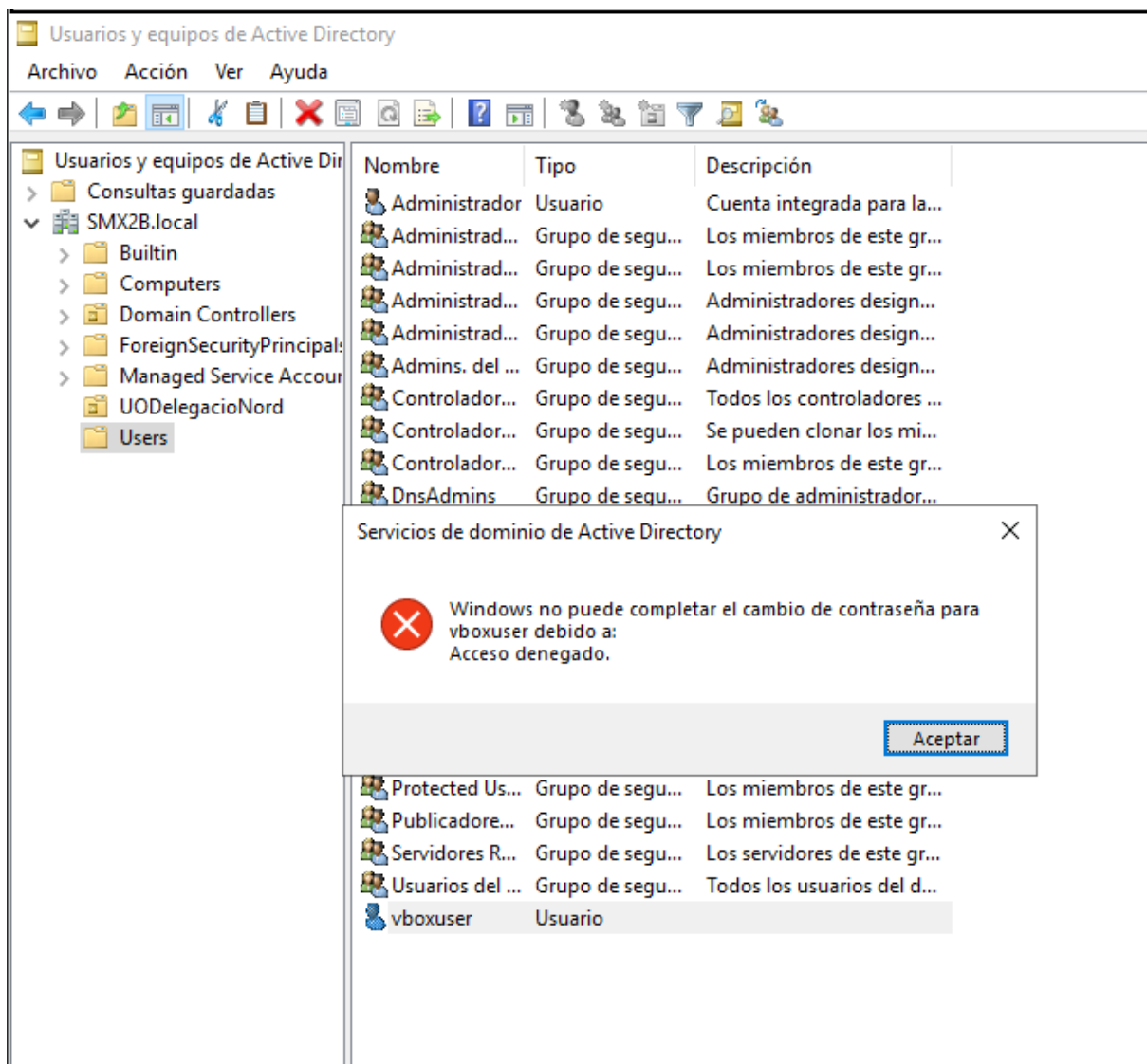


Figura 14: Figura 15: Fora del UO no pot fer cap acció

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 d'anar a **Ver>Características Avanzadas** de la consola.

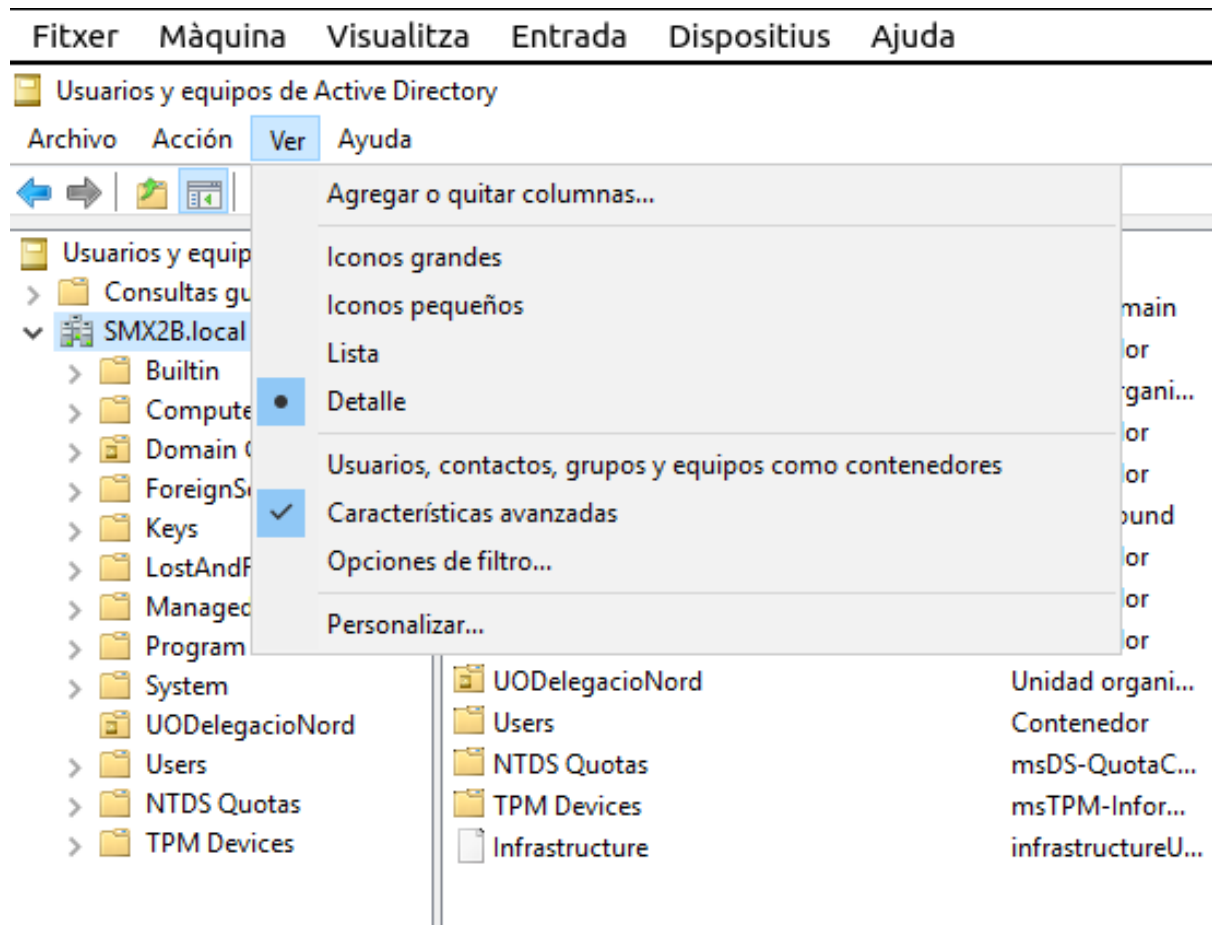


Figura 15: Figura 16: Veure-ho tot en dsa.msc

- 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.

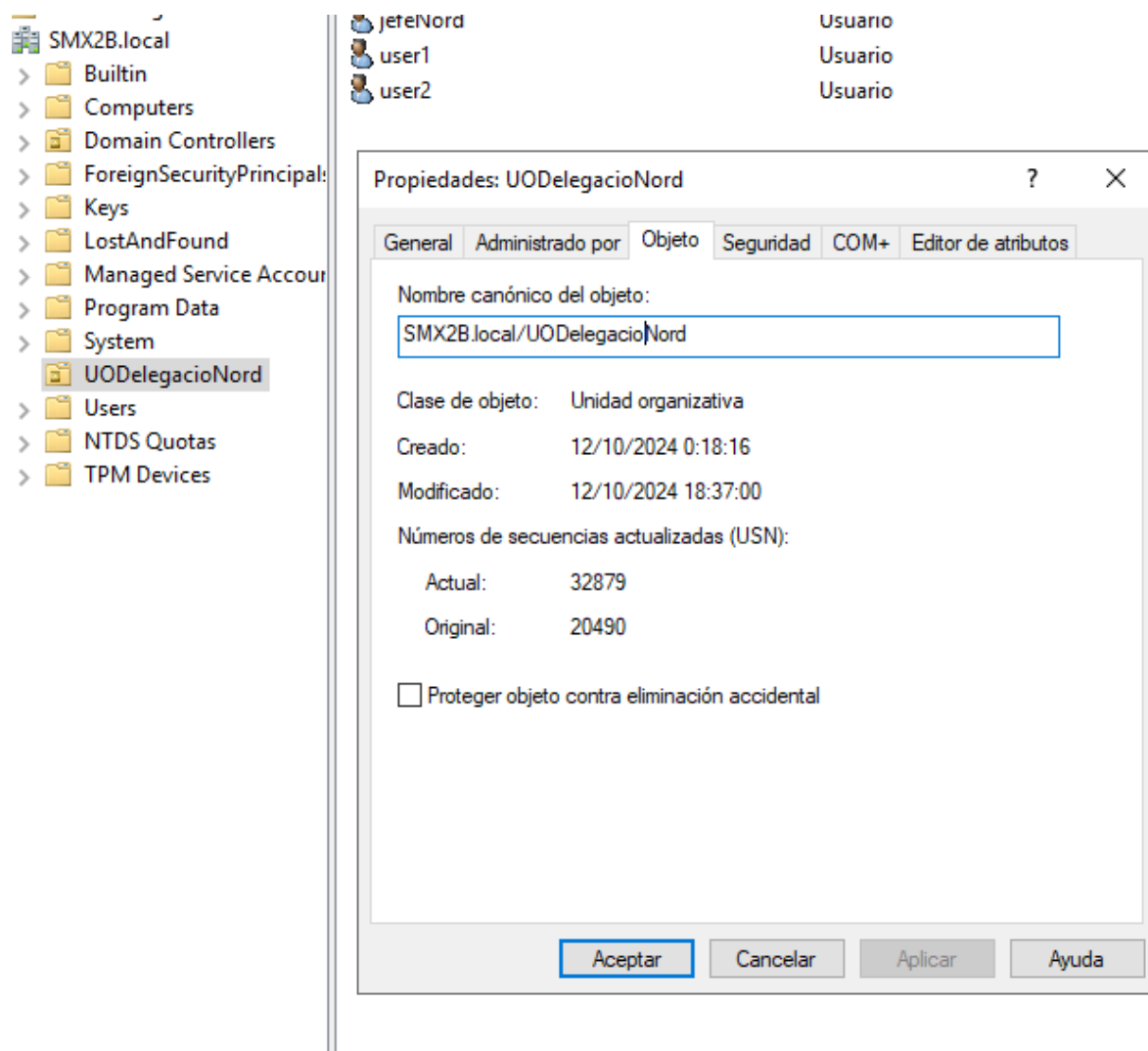


Figura 16: Figura 17: Desproteger temporalment les UO

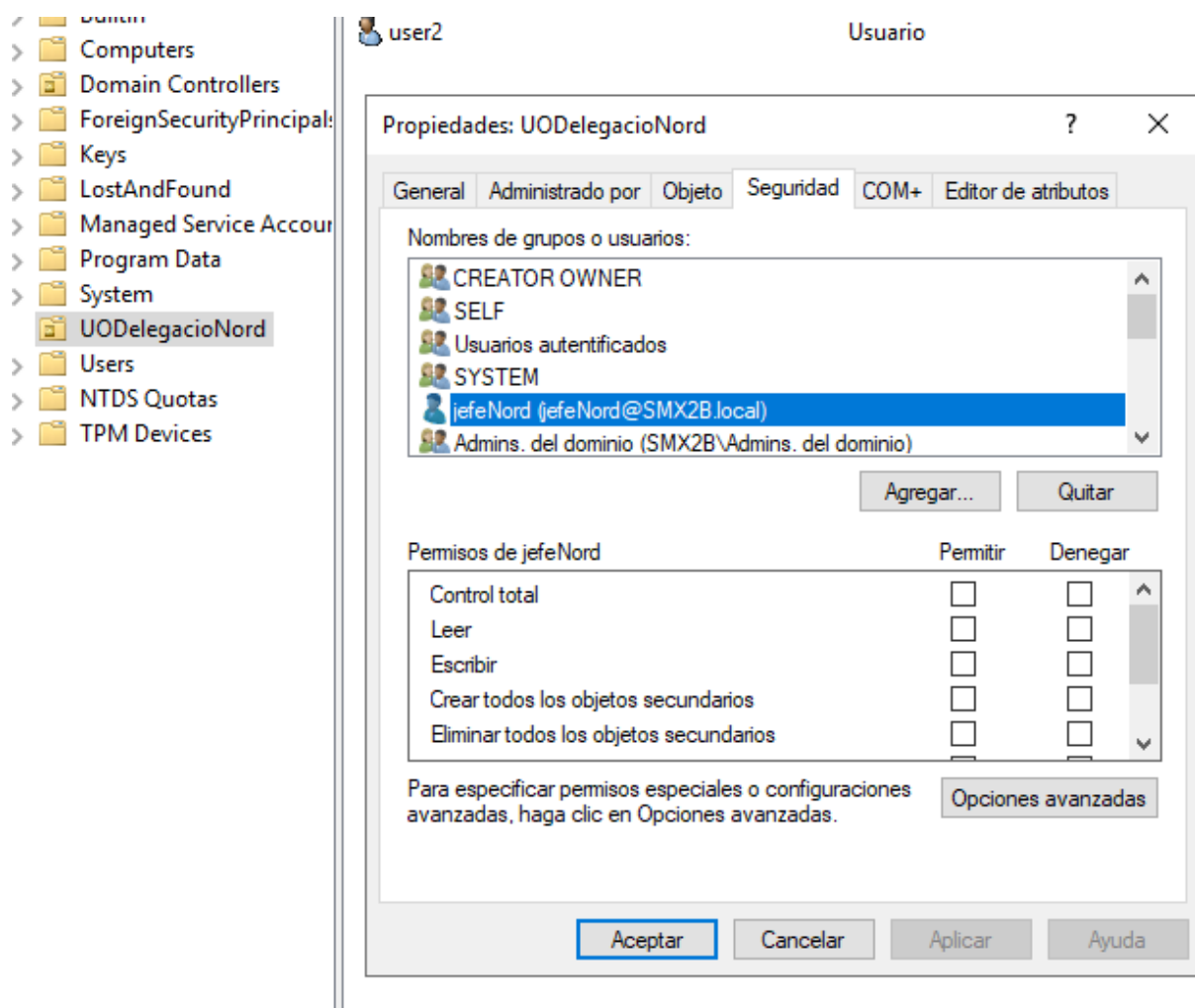


Figura 17: Figura 18: Qui té el control de la UO

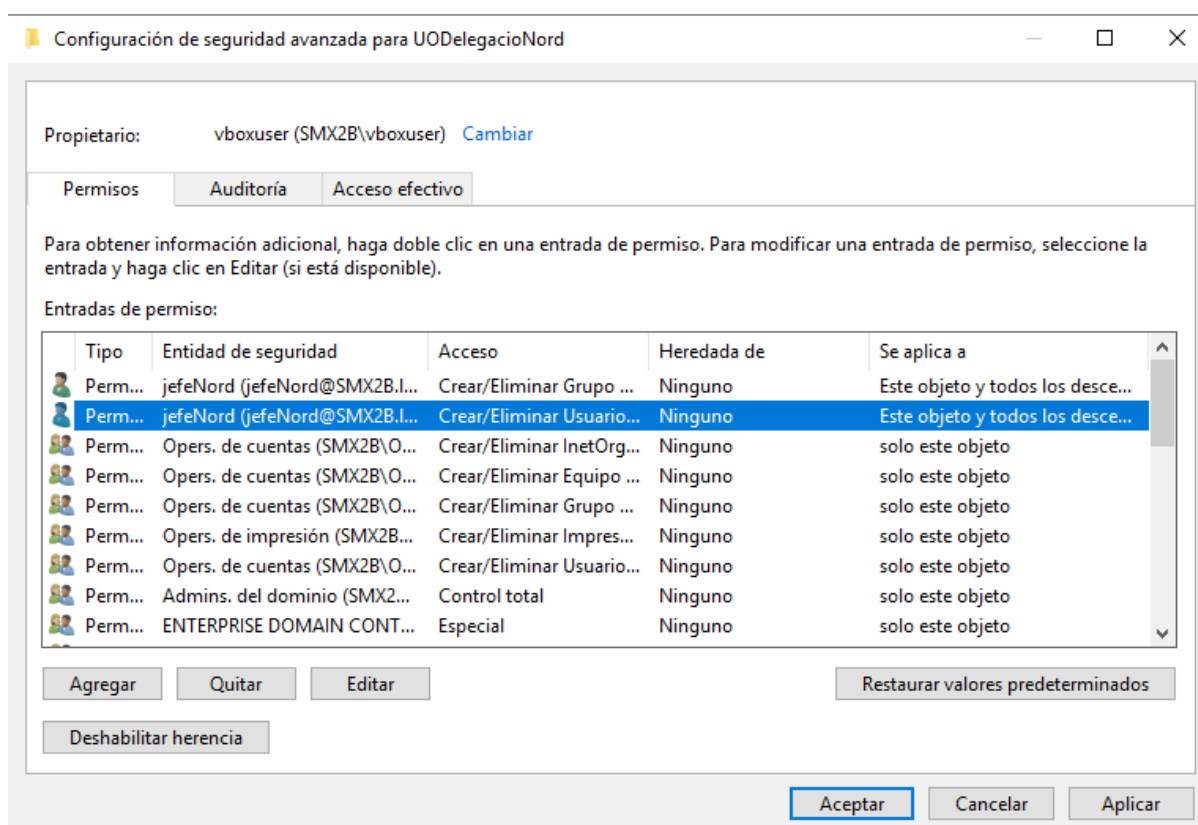


Figura 18: *Figura 19: Gestió de drets i usuaris sobre la UO