|  |
| --- |
|  |
| Administración de grupos |
|  |
| Ejercicios |

**[Escriba el nombre de la compañía]**

26 de febrero de 2018

Autor: Xabier

Administración de grupos

Ejercicios

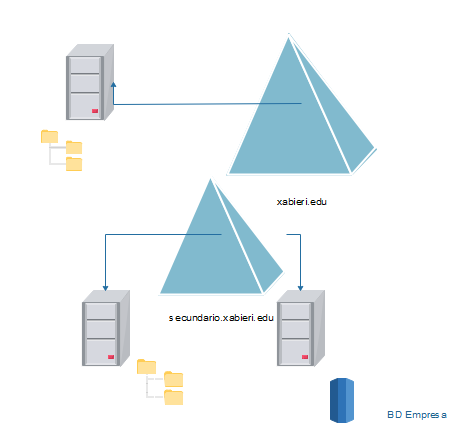
# Ejercicio 1

Tenemos el siguiente escenario:

En el dominio xabieri.edu tenemos un servidor de archivos

En el dominio secundario.xabieri.edu tenemos un servidor de archivos y un servidor de BD.

Tenemos personas una empresa en la que tenemos los departamentos de Ventas, Márquetin y Directivos.

Todos ellos tienen la necesidad de acceder a estos tres servidores con permiso de lectura.

Crear un grupo global GSecundarioVentas en el Dominio secundario.xabieri.edu

Crear un grupo global GPrimarioVentas en el Dominio xabieri.edu

Secundario.xabieri.edu:

Crear un grupo de dominio local ACL\_DL\_Ventas\_Lectura

Crear otro grupo local DB\_DL\_BDEmpresa\_select

En el dominio xabieri.edu:

Crear otro grupo local de dominio ACL\_Ventasgenerales\_Lectura

¿Desde cada uno de los grupos a qué otros grupos podría anidar cada uno de ellos?

**ACL\_Ventasgenerales\_Lectura**

Miembros:

*ACL\_DL\_Ventas\_Lectura?*

*GPrimario\_Ventas*

*GSecundario\_Ventas*

Miembros de:

*Nada*

**DB\_DL\_BDEmpresa\_select**

Miembros

*ACL\_DL\_Ventas\_Lectura*

*GPrimario\_Ventas*

*GSecundario\_Ventas*

Miembros de

*ACL\_DL\_Ventas\_Lectura*

**ACL\_DL\_Ventas\_Lectura**

Miembros

*DB\_DL\_BDEmpresa\_select*

*GPrimario\_Ventas*

*GSecundario\_Ventas*

Miembros de

*DB\_DL\_BDEmpresa\_select*

**GSecundarioVentas**

Miembros

*Ninguno*

Miembros de

*DB\_DL\_BDEmpresa\_select*

*ACL\_Ventasgenerales\_Lectura*

*ACL\_DL\_Ventas\_Lectura*

**GPrimarioVentas**

Miembros

*Nada*

Miembros de

*DB\_DL\_BDEmpresa\_select*

*ACL\_Ventasgenerales\_Lectura*

*ACL\_DL\_Ventas\_Lectura*

# Ejercicio 2 Crear un grupo bien documentado

En este ejercicio, crea un grupo para administrar el acceso a la carpeta Presupuesto y sigue las pautas recomendadas.

1. Inicie sesión en SERVER01 como administrador y abra el complemento Usuarios y equipos de Active Directory.

2. Seleccione la unidad organizativa de grupos en el árbol de la consola.

3. Haga clic con el botón derecho en la unidad organizativa Grupos, seleccione Nuevo y haga clic en Grupo.

4. Nombre **ACLPresupuestos\_Edit.**

5. Seleccione Dominio local en la sección Alcance del grupo y Seguridad en el Tipo de grupo, y luego haz clic en OK.

6. Haga clic en el menú Ver y asegúrese de que esté seleccionado Funciones avanzadas.

7. Haga clic con el botón derecho en el grupo ACL\_presupuestos\_Edit y elija Propiedades.

8. En la pestaña Objeto, active la casilla de verificación Proteger objeto de eliminación accidental y haga clic en Aceptar.

9. Abra las propiedades del grupo nuevamente.

10. En el cuadro Descripción, escriba PRESUPUESTO (EDIT).

11. En el cuadro Notas, escriba las siguientes rutas para representar las carpetas que tienen permisos asignado a este grupo:

\\ server23\data\finanzas\presupuestos

\\ server32\data $\finanzas\ proyecciones de ingresos

12. Haga clic en Aceptar.

# Ejercicio 3

Antes de realizar los ejercicios en esta práctica, debe crear los siguientes objetos en el dominio uno.edu:

* Un OU de primer nivel llamado Grupos
* Un OU de primer nivel llamado cuentas de usuario
* Objetos de usuario en la OU Cuentas de usuario para David Jones, Jeff Ford y Tony Krijnen

Ejercicio 1 Crear grupos

En este ejercicio, crea grupos de diferentes ámbitos y tipos.

1. Inicie sesión en SERVER01 como administrador. Abra el complemento Usuarios y equipos de Active Directory y haga clic en la OU Grupos en el panel de árbol.

Si el grupo Ventas ya existe, elimine el grupo.

2. Haga clic con el botón derecho en la unidad organizativa Grupos, seleccione Nuevo y luego haga clic en Grupo.

3. En el cuadro Nombre de grupo, escriba GVentas.

4. Seleccione el alcance del grupo global y el tipo de grupo de seguridad. Haga clic en Aceptar.

5. Haga clic con el botón derecho en el grupo Ventas y elija Propiedades.

6. En la pestaña Miembros, haga clic en Agregar. Escriba Jeff; Tony y haz clic en OK. Haga clic en Aceptar para cerrar el cuadro de diálogo Propiedades.

7. Repita los pasos 2 a 4 para crear dos grupos de seguridad globales llamados GMarketing y Consultores.

8. Repita los pasos 2 a 4 para crear un grupo de seguridad local de dominio denominado ACL\_Sales Folder\_Read.

9. Abra las propiedades del grupo ACL\_Sales Folder\_Read.

10. En la pestaña Miembros, haga clic en Agregar. Escriba GVentas;G Marketing; GConsultants y haga clic en Aceptar.

11. Haga clic en Agregar. Escriba David y haga clic en Aceptar. Haga clic en Aceptar para cerrar el cuadro de diálogo Propiedades.

12. Abra el cuadro de diálogo Propiedades del grupo GMarketing.

13. En la pestaña Miembros, haga clic en Agregar.

14. Escriba AC L\_Sales Folder\_Read y haga clic en Aceptar.

No puede agregar un grupo local de dominio a un grupo global.

15. Cierre todos los cuadros de diálogo abiertos.

16. Cree una carpeta llamada Ventas en la unidad C.

17. Haga clic con el botón derecho en la carpeta Ventas, haga clic en Propiedades y luego en la pestaña Seguridad.

18. Haga clic en Editar y luego en Agregar.

19 Haga clic en Avanzado y luego en Buscar ahora.

Tenga en cuenta que al usar un prefijo para nombres de grupo, como el prefijo ACL\_ para grupos de acceso a recursos, puede encontrarlos rápidamente, agrupados en la parte superior de la lista.

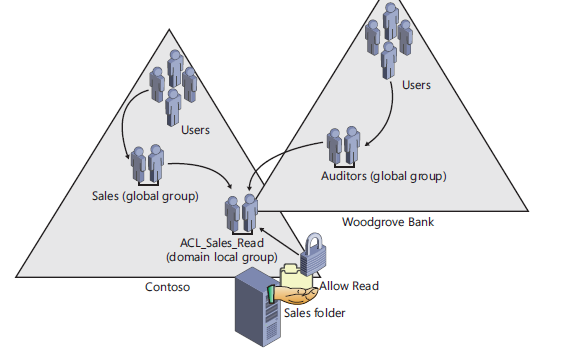
20. Cierre todos los cuadros de diálogo abiertos.

21. Cambie a usuarios y equipos de Active Directory, haga clic con el botón derecho en la unidad organizativa Grupos, haga clic en Nuevo y luego en Grupo.

22. En el cuadro Nombre de grupo, escriba Empleados.

23. Seleccione el ámbito del grupo Local del dominio y el tipo de grupo Distribución. Haga clic en Aceptar.

# Ejercicio 4



Considere la siguiente situación. El equipo de ventas en su dominio., acaba de completar su año fiscal. Los archivos de ventas del año anterior se encuentran en una carpeta llamada Ventas\_2017. El equipo de ventas necesita Acceso de lectura a la carpeta Ventas\_2017.

Además, un equipo de auditores de Woodgrove Bank, un inversor potencial, requiere acceso de Lectura a la carpeta entas\_2017para realizar una auditoría. Los pasos para implementar la seguridad requerida por este escenario, es el siguiente:

1. Asigne a los usuarios con responsabilidades laborales comunes como grupos de seguridad global.

Esto sucede por separado en cada dominio.

Los vendedores se agregan al grupo Ventas . Los auditores en Woodgrove Bank se agregan a un grupo de rol de Auditores.

2. Cree un grupo para representar la regla de negocio, **quién puede acceder a las** Ventas\_2017 **con permiso de lectura**.

Esto se implementa en el dominio que está administrando la regla de negocio.

En este caso, la regla de negocios es el acceso de nivel de lectura a la carpeta Ventas, el dominio (en el que reside la carpeta Ventas) administra el acceso.

El acceso al recurso se crea como un grupo local de dominio, ACL\_Sales Folders\_Read.

3. Agregue los grupos de roles al grupo de reglas de administración de acceso a recursos ACL\_Sales\_READ para representar la regla de gestión.

Los grupos de roles que agrega pueden provenir de cualquier dominio en el bosque.

4. Asigne al grupo de reglas el permiso que implementa el nivel de acceso requerido.

En este caso, otorgue el permiso Permitir lectura al grupo local de dominio ACL\_SalesFolders\_Read.

Esta estrategia da como resultado puntos únicos de administración, reduciendo la carga administrativa.

Un punto de administración define quién está en Ventas, y define quién es un Auditor.

Esos roles, por supuesto, es probable que tengan una variedad de permisos para recursos más allá de simplemente la carpeta Ventas del dominio.

Otro punto único de gestión determina quién tiene acceso de lectura a la carpeta Ventas. Y, por supuesto, la carpeta Sales podría no ser solo

carpeta en un solo servidor: podría ser una colección de carpetas en varios servidores, cada uno de

que asigna el permiso Permitir lectura al grupo local de un solo dominio.

Tenga en cuenta R ole-based management

La gestión basada en roles es un concepto utilizado en toda la tecnología de la información y protección de la información, y se puede lograr con las capacidades listas para usar de Active Directory.

IGDLA es la implementación de la administración basada en roles utilizando Active Directory.

Roles:

*Auditores (xabieri.edu)*

*Grupo Global*

*Ventas ( secundario.xabieri.edu)*

*Dl o Global*

Reglas:

*ACL\_Ventas2017\_Lectura (secundario.xabier.edu)*

Miembros:

*Ventas*

*Auditores*

Miembros de:

*Nada*

Ventajas de ROLES y REGLAS:

Conocemos los roles de cada usuario.

Único ACL por permiso

Fácil de resolver la pregunta de quién tiene acceso al directorio.

No se crean ACL huérfanas

# Ejercicio 5

En el dominio secundario, crear un usuario y asignar permiso de lectura sobre la carpeta Ventas\_2017

Eliminar el usuario ¿Qué sucede con el permiso?

***El permiso se mantiene***

En el dominio secundario crear un usuario y hacerlo miembro del grupo ACL\_DL\_Ventas2017.

Eliminar el usuario ¿qué sucede con el grupo, el usuario sigue siendo miembro del grupo?

***No el usuario desaparece***

# Ejercicio 6

Case Scenario: Implementing a Group Strategy

Usted es un administrador TI. Está en marcha una nueva iniciativa de desarrollo de productos llamada Sliced ​​Bread, y hay información confidencial sobre el proyecto en carpetas compartidas en tres servidores en tres sitios diferentes.

Los usuarios de Investigación, Marketing y Finanzas necesitan acceder a los datos del proyecto. Además, Gerente y su asistente necesitan acceso.

De estos, solo Marketing e Investigación requieren acceso de escritura. Actualmente hay varias personas trabajando en el departamento de Marketing, y desea evitar que obtengan acceso. Finalmente, un equipo de auditores de Woodgrove Bank, un inversor, también necesita acceso de lectura.

3. Describa la anidación de usuarios y grupos que implementa para lograr la seguridad requerida por este proyecto.

ROLES:

Investigación

Marketin

Finanzas

Dirección (Gerente y Asistente)

Auditores

Inversores

Miembros y Miembros de:

REGLAS:

ACL\_SB\_Lectura

Miembros

Marketin\_R

Finanzas

Dirección (Gerente y Asistente)

Auditores

Inversores

ACL\_SB\_Escritura

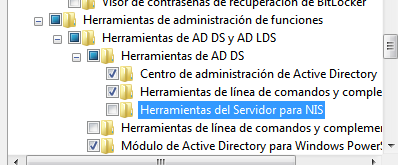
Miembros

Investigación

Marketin\_W

# Ejercicio 7

Instalar Herramientas de administración remota de Servidor 2008 en el equipo Windows 7

1. Descargar las Herramientas
2. Panel de Control -> Programas y Caracteriscticas -> Activar y Desactivar Características ->
3. 

# Ejercicio 8

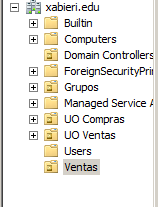
Delegar la administración del Grupo Ventas del dominio Local.

Se puede hacer de dos formas:

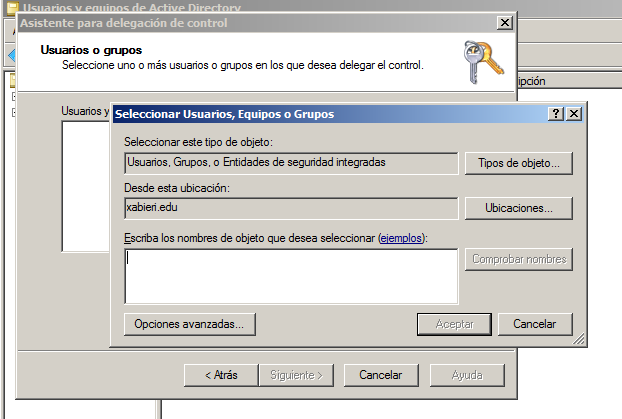
Delegar la administración de la UO.

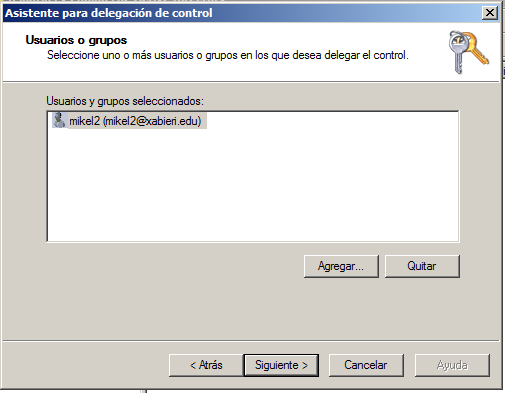
Por UO

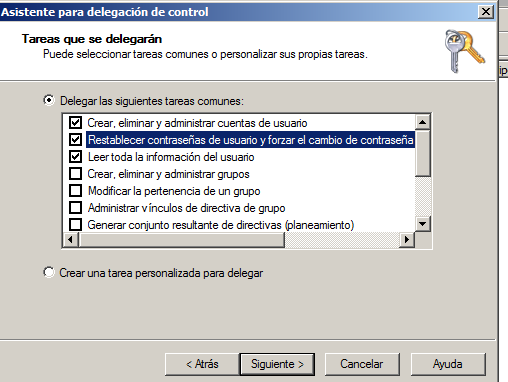
Crear UO Ventas



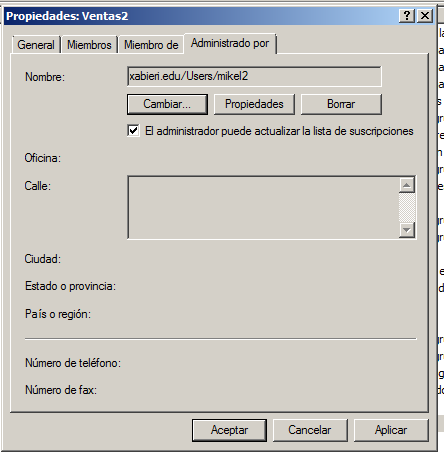
Botón derecho - > Delegar Control







Delegar la administración del grupo.



# Ejercicio 9

Crear un Usuario llamado Ion

Este usuario será administrador del Grupo Global Compras.

Se quiere delegar en este usuario la administración del departamento de Compras.

1. Añadir y quitar miembros del Departamento.

Crear una UO llamada Compras y mover el grupo de sitio.

1. Administrar los usuarios del Departamento.
2. Administrar las contraseñas

Realizar pruebas

Tras realizar las pruebas modificar la administración de la UO para que pueda modificar la pertenencia a un grupo.

¿Qué opción adicional nos ofrece esta opción?

Como podemos ver el administrador de la UO.

# Ejercicio 10

1. Crear una Unidad Organizativa llamada **CONTROL**, en vuestra empresa XXXX, utilizando la línea de comandos (**dsadd**).

|  |
| --- |
|  |

1. Dar de alta a 2 cuentas de usuario, ctr1 y ctr2.
2. Crear un grupo de seguridad **global**, utilizando la línea de comandos (**dsadd**).

|  |
| --- |
|  |

1. Incluir las 2 cuentas de usuario como miembros del grupo.
2. Dar de alta a un grupo de seguridad local de dominio, utilizando la línea de comandos(**dsadd**).

|  |
| --- |
|  |

1. Incluir como miembro del grupo local de dominio, el global creado anteriormente.
2. Delegar al usuario **ctr2** el poder para efectuar las tareas de administrador sobre la U.O **CONTROL** (Documentarlo).

|  |
| --- |
|  |

1. Probar la gestión, iniciando sesión con dicha cuenta, visualizando los permisos efectivos de dicha cuenta sobre la U.O **CONTROL** (Documentarlo).

|  |
| --- |
|  |

1. Crear un grupo de seguridad global **prueba**, en la Unidad Organizativa CONTROL (**dsadd**).

|  |
| --- |
|  |

11) Eliminarlo todo por medio de comandos

# Ejercicio 11 Con Powershell

1. Crear una Unidad Organizativa llamada **CONTROL**, en vuestra empresa XXXX, utilizando la línea de comandos (**dsadd**).

|  |
| --- |
|  |

1. Dar de alta a 2 cuentas de usuario, ctr1 y ctr2.
2. Crear un grupo de seguridad **global**, utilizando la línea de comandos (**dsadd**).

|  |
| --- |
|  |

1. Incluir las 2 cuentas de usuario como miembros del grupo.
2. Dar de alta a un grupo de seguridad local de dominio, utilizando la línea de comandos(**dsadd**).

|  |
| --- |
|  |

1. Incluir como miembro del grupo local de dominio, el global creado anteriormente.
2. Delegar al usuario **ctr2** el poder para efectuar las tareas de administrador sobre la U.O **CONTROL** (Documentarlo).

|  |
| --- |
|  |

1. Probar la gestión, iniciando sesión con dicha cuenta, visualizando los permisos efectivos de dicha cuenta sobre la U.O **CONTROL** (Documentarlo).

|  |
| --- |
|  |

1. Crear un grupo de seguridad global **prueba**, en la Unidad Organizativa CONTROL (**dsadd**).

|  |
| --- |
|  |

1. Eliminarlo todo por medio de comandos