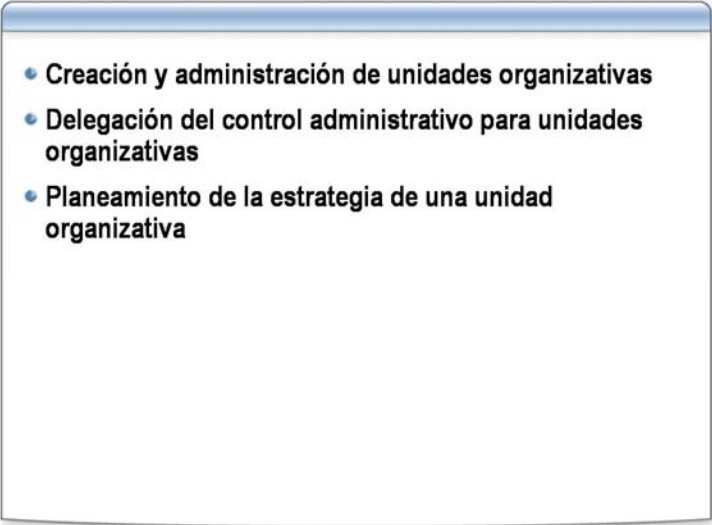


Implementación de la estructura de una unidad organizativa

Contenido

| | |
|--|----|
| Introducción | 2 |
| Lección: Creación y administración de unidades organizativas | 3 |
| Lección: Delegación del control administrativo para unidades organizativas | 15 |
| Lección: Planeamiento de la estrategia de una unidad organizativa | 26 |

Introducción

- 
- **Creación y administración de unidades organizativas**
 - **Delegación del control administrativo para unidades organizativas**
 - **Planeamiento de la estrategia de una unidad organizativa**

Introducción

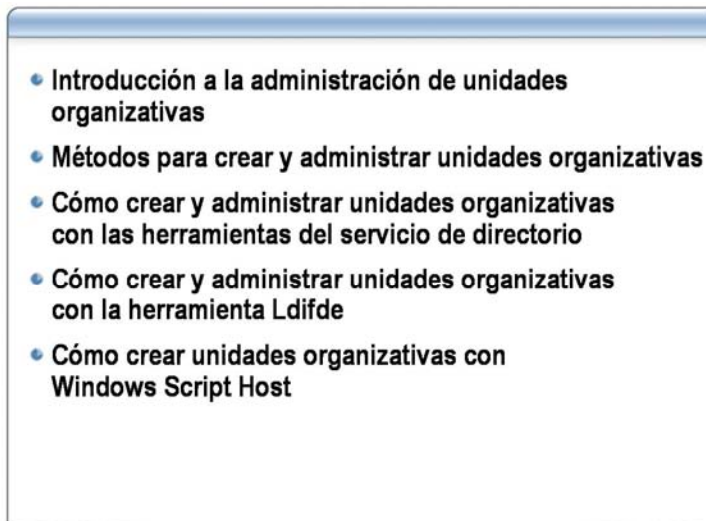
En este módulo se explica cómo crear y administrar unidades organizativas, cómo delegar tareas administrativas comunes y cómo planear la implementación de una estructura de unidad organizativa.

Objetivos

Después de finalizar este módulo, podrá:

- Crear y administrar unidades organizativas.
- Delegar el control de una unidad organizativa.
- Planear la estrategia de una unidad organizativa.

Lección: Creación y administración de unidades organizativas



Introducción

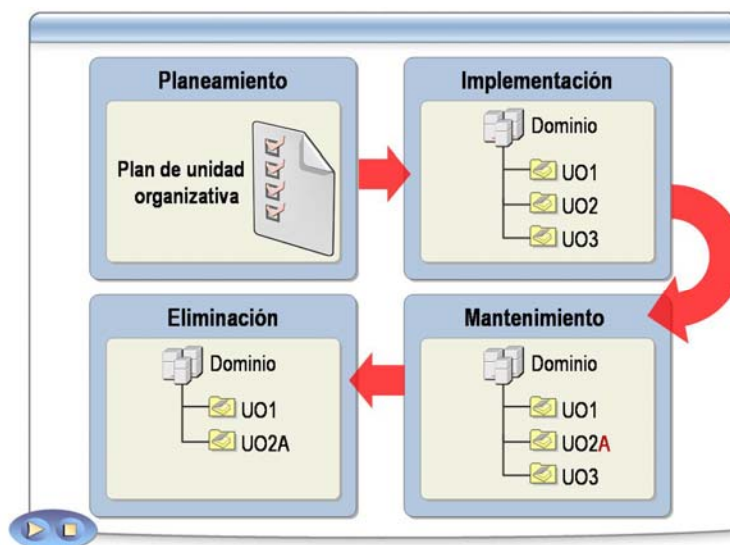
En esta lección se introduce el complemento Microsoft® Management Console (MMC) y las herramientas de línea de comandos para crear y administrar unidades organizativas, y se proporcionan los conocimientos necesarios para crear, modificar y eliminar unidades organizativas.

Objetivos de la lección

Después de finalizar esta lección, podrá:

- Describir el ciclo de vida de unidades organizativas.
- Describir los métodos para crear unidades organizativas.
- Administrar unidades organizativas utilizando las herramientas de línea de comandos de servicios de directorio.
- Administrar unidades organizativas utilizando la herramienta Ldifde de línea de comandos.
- Crear unidades organizativas utilizando Microsoft Windows Script Host.

Introducción a la administración de unidades organizativas



Introducción

Las unidades organizativas son contenedores del servicio de directorio de Active Directory® que se utilizan para colocar usuarios, grupos, equipos y otras unidades organizativas. Con las unidades organizativas podrá crear contenedores en un dominio que represente las estructuras jerárquicas y lógicas de su organización. Así, podrá administrar la configuración y el uso de cuentas y recursos en función de su modelo organizativo. Por ejemplo, puede utilizar las unidades organizativas para aplicar de forma automática directivas de grupo que definan opciones predeterminadas para cuentas de usuarios y equipos en Active Directory.

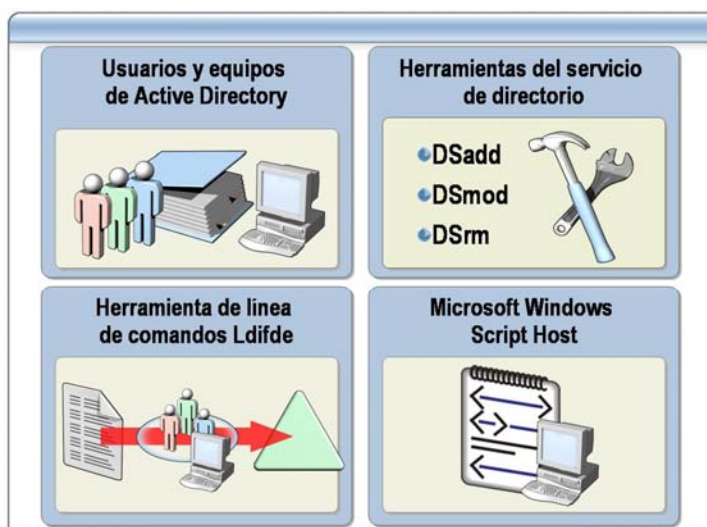
Ciclo de vida de las unidades organizativas

El ciclo de vida de las unidades organizativas tiene cuatro fases:

- **Planeamiento.** En esta fase se planea la estructura de la unidad organizativa. Se decide qué unidades organizativas se van a crear y cómo se va a delegar el control administrativo de éstas.
- **Implementación.** En esta fase se crea la estructura de la unidad organizativa tomando como base el plan de la unidad organizativa.
- **Mantenimiento.** Una vez que se haya creado la estructura de la unidad organizativa en Active Directory, podrá cambiar el nombre de las unidades organizativas, desplazarlas o modificarlas según sea necesario para satisfacer los requisitos continuos de la organización.
- **Eliminación.** Todos los objetos de Active Directory, incluidas las unidades organizativas, ocupan espacio en el controlador de dominio que aloja Active Directory. Cuando ya no necesite unidades organizativas, deberá eliminarlas.

Nota Para obtener más información acerca de las unidades organizativas, consulte el módulo 7, “Administrar el acceso a los objetos de las unidades organizativas”, en el curso 2146A, *Administración de un entorno Microsoft Windows Server 2003*.

Métodos para crear y administrar unidades organizativas



Introducción

Windows Server 2003 proporciona varios complementos y herramientas de línea de comandos que se pueden utilizar para crear unidades organizativas y para administrar la configuración y el uso de cuentas y recursos en el modelo organizativo. También puede utilizar Windows Script Host, un host de secuencias de comandos para plataformas de Microsoft Windows®, para administrar unidades organizativas.

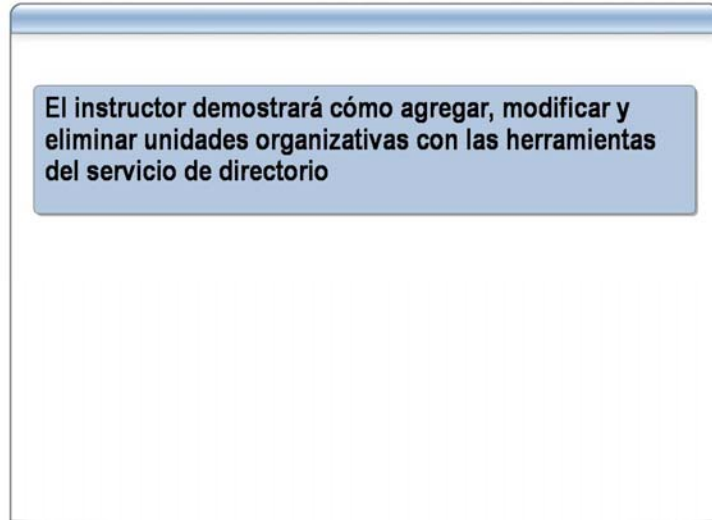
Métodos para crear y administrar unidades organizativas

En la siguiente lista se incluyen algunos de los complementos y herramientas de línea de comandos que se pueden utilizar para crear y administrar unidades organizativas:

- *Usuarios y equipos de Active Directory.* Complemento de MMC para crear, modificar y eliminar unidades organizativas. Utilice este complemento cuando tenga sólo unas pocas unidades organizativas que administrar o cuando desee administrar unidades organizativas de forma interactiva.
- *Herramientas del servicio de directorio.* Conjunto de herramientas de línea de comandos que puede utilizar para administrar objetos y para realizar consultas en Active Directory. Algunas de las herramientas de línea de comandos son Dsadd, Dsmod y Dsrm. Al utilizar estas herramientas con el parámetro ou puede agregar, modificar y eliminar unidades organizativas de Active Directory. También puede utilizar archivos de secuencias de comandos y archivos por lotes junto con estas herramientas para administrar los servicios de directorio.

- *Ldifde (Lightweight Directory Access Protocol Data Interchange Format Directory Exchange)*. Herramienta de línea de comandos para crear unidades organizativas y otros objetos de Active Directory en una operación por lotes. La herramienta Ldifde (Lightweight Directory Access Protocol Data Interchange Format Directory Exchange) utiliza un archivo de entrada que contiene información sobre los objetos que se desean agregar, modificar o eliminar. La información se almacena como una serie de registros separados por una línea en blanco en un archivo de entrada.
- *Microsoft Windows Script Host*. Pueden crear unidades organizativas utilizando las aplicaciones de Windows o mediante secuencias de comandos de Windows con los componentes que proporciona Active Directory Service Interface (ADSI). Mediante las secuencias de comandos puede crear unidades organizativas como parte de la instalación de la aplicación cuando sea necesario.

Cómo crear y administrar unidades organizativas con las herramientas del servicio de directorio



Introducción

Puede utilizar las herramientas de línea de comandos del servicio de directorio Dsadd, Dsmod y Dsrm para crear y administrar unidades organizativas desde el símbolo del sistema. También puede utilizar estos comandos en archivos de secuencias de comandos y en archivos por lotes.

Procedimiento para crear una unidad organizativa

Para crear una unidad organizativa, ejecute el siguiente comando **Dsadd** desde el símbolo del sistema:

```
dsadd ou NUnidadOrganizativa -desc Descripción -d Dominio -u NombreUsuario -p Contraseña
```

Donde:

- *NUnidadOrganizativa* indica el nombre completo de la unidad organizativa que desea agregar. Por ejemplo, para agregar una unidad organizativa denominada helpdesk al dominio nwtraders.msft, el nombre completo sería *ou=helpdesk,dc=nwtraders,dc=msft*.
- *Descripción* indica la descripción de la unidad organizativa que se desea agregar.
- *Dominio* indica el dominio al que conectar. Por defecto, el equipo se conecta al controlador de dominio en el dominio de inicio de sesión.

- *NombreUsuario* indica el nombre de usuario que se debe utilizar para iniciar la sesión en un servidor remoto. Por defecto, se utiliza el nombre de usuario de inicio de sesión. Se puede indicar un nombre de usuario utilizando uno de los siguientes formatos:
 - nombre de usuario (por ejemplo, Alicia)
 - dominio\nombre de usuario (por ejemplo, widgets\Alicia)
 - nombre principal de usuario (UPN, *User Principal Name*) (por ejemplo, Alicia@widgets.microsoft.com)
- *Contraseña* es la contraseña que se debe utilizar para iniciar la sesión en un servidor remoto. Si introduce un *, se le pedirá una contraseña.

Procedimiento para modificar una unidad organizativa

Para modificar la descripción de una unidad organizativa, ejecute el siguiente comando:

```
dsmod ou NUnidadOrganizativa -desc Descripción -d Dominio -u NombreUsuario -p Contraseña
```

Los parámetros introducidos en el comando **dsmod** son los mismos que los del comando **dsadd**. La nueva descripción se debe introducir como el parámetro *desc*.

Procedimiento para eliminar una unidad organizativa

Las unidades organizativas de Active Directory que ya no se utilicen se deben eliminar. Para eliminar una unidad organizativa, ejecute el siguiente comando:

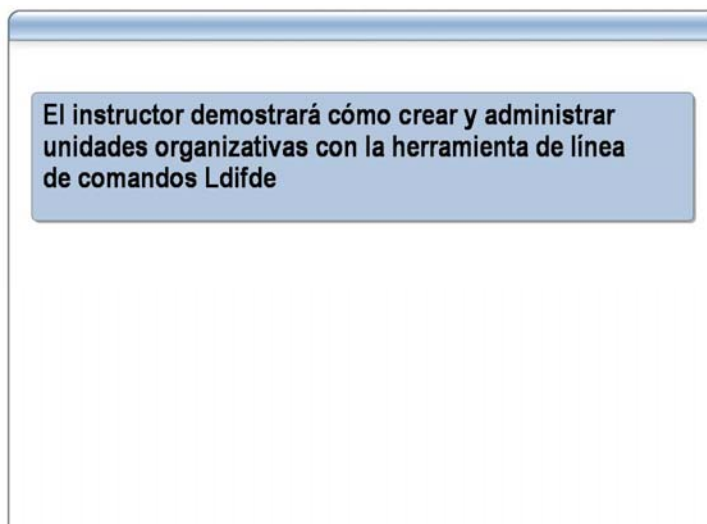
```
dsrm NUnidadOrganizativa -d Dominio -u NombreUsuario -p Contraseña
```

Los parámetros introducidos en el comando **dsrm** son los mismos que los del comando **dsadd**. Puede utilizar los parámetros adicionales siguientes con **dsrm**:

- *subtree*. Indica que se debe eliminar el objeto y todos los objetos contenidos en el subárbol bajo dicho objeto.
- *Exclude*. Indica que no se debe eliminar el objeto base proporcionado por el *NUnidadOrganizativa* al eliminar el subárbol que se encuentra bajo éste. Por defecto, sólo se elimina el objeto base indicado. El parámetro *Exclude* solo se puede indicar con el parámetro *subtree*.

Nota Para obtener más información acerca del uso de las herramientas de línea de comandos *Dsadd*, *Dsmod* y *Dsrm*, consulte Centro de ayuda y soporte técnico de Windows Server 2003.

Cómo crear y administrar unidades organizativas con la herramienta Ldifde



Introducción

Puede utilizar la herramienta de línea de comandos Ldifde para crear unidades organizativas en una operación por lotes y para configurar jerarquías de las unidades organizativas. También puede utilizar Ldifde para modificar y eliminar unidades organizativas.

Procedimiento

El primer paso para utilizar esta herramienta consiste en crear el archivo de entrada que se va a utilizar con Ldifde. Después de crear este archivo, se debe ejecutar el comando **Ldifde**.

Para crear unidades organizativas con la herramienta de línea de comandos Ldifde, realice los siguientes pasos:

1. Cree un archivo de entrada. En el siguiente ejemplo se muestra el formato del archivo:

```
dn: OU=UOEjemplo,DC=nwtraders,DC=msft
changetype: add
objectClass: organizationalUnit
```

Changetype indica el tipo de operación que se lleva a cabo en el objeto de Active Directory. **ObjectClass** indica la clase del objeto de Active Directory. En el ejemplo anterior, Ldifde agrega un objeto de unidad organizativa denominado *UOEjemplo* al dominio *nwtraders.msft*. Puede agregar múltiples unidades organizativas agregando más entradas como la anterior. Debe haber una línea en blanco antes de cada entrada dn, excepto en la primera.

2. Ejecutar Ldifde para crear, modificar o eliminar unidades organizativas introduciendo el siguiente comando:

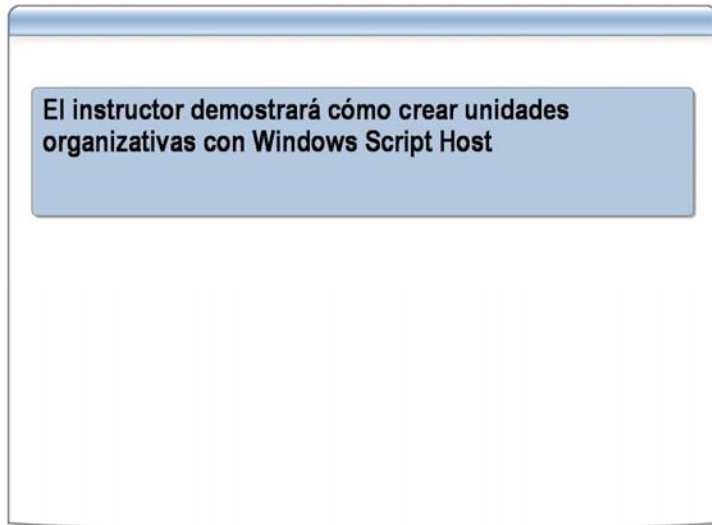
```
C:\>ldifde -i -k -f OUList.ldf -b NombreUsuario  
Dominio Password
```

Donde:

- *-i* indica el modo de importación. Si no se especifica, el modo por defecto es de exportación.
- *-k* ignora fallos durante una operación de importación y continua con el procesamiento.
- *-f* indica el nombre del archivo de importación o exportación.
- OUList.ldf es el archivo de entrada.
- *-b* indica el nombre de usuario, nombre de dominio y contraseña para la cuenta de usuario que se va a utilizar para realizar la operación de importación o exportación.

Nota Para obtener más información acerca de Ldifde, consulte los temas de Centro de ayuda y soporte técnico de Windows Server 2003.

Cómo crear unidades organizativas con Windows Script Host



Introducción

ADSI es una Interfaz de programación de aplicaciones (API, *Application Programming Interface*) que se puede utilizar desde una secuencia de comandos de Windows Script Host para automatizar la administración de Active Directory. ADSI utiliza el Protocolo ligero de acceso a directorios (LDAP, *Lightweight Directory Access Protocol*) para comunicarse con Active Directory. Todas las operaciones de ADSI que realice en Active Directory siguen el mismo procedimiento. Primero, hay que conectarse a Active Directory. A continuación, puede realizar tareas como recuperar información acerca de objetos y agregar, modificar o eliminar objetos. Si se realizan cambios en Active Directory, se deben guardar los cambios en la base de datos de Active Directory para hacerlos permanentes.

Procedimiento

Para crear una unidad organizativa con Windows Script Host, realice los siguientes pasos:

1. Utilice el Bloc de notas para crear un archivo de texto con extensión .vbs. Introduzca los siguientes comandos que se indican en los pasos a, b y c en el archivo y guárdelo.
 - a. Primero, conéctese al dominio en el que desee crear la unidad organizativa, como se indica en el siguiente ejemplo:

```
Set objDom = GetObject("LDAP://dc=nwtraders,dc=msft")
```

Importante En el ejemplo anterior, LDAP debe tener todas las letras en mayúscula o el comando no se ejecutará.

En este ejemplo, nwtraders.msft es el dominio en que se crea la unidad organizativa.

- b. A continuación, cree la unidad organizativa indicando `OrganizationalUnit` como el tipo de objeto de Active Directory que se va a crear y el nombre de la unidad organizativa como se indica en el siguiente ejemplo:

```
Set objOU = objDom.Create("OrganizationalUnit",  
"ou=UONueva")
```

En este ejemplo, UONueva es el nombre de la unidad organizativa que está creando.

- c. Por último, guarde la información en la base de datos de Active Directory, como se muestra en el siguiente ejemplo:

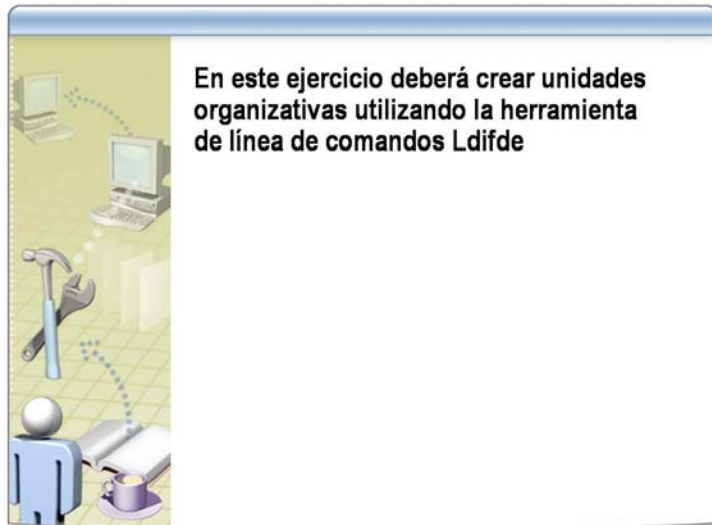
```
objOU.SetInfo
```

2. Para ejecutar los comandos del archivo `.vbs`, escriba lo siguiente en el símbolo del sistema:

```
wscript script_file_name.vbs
```

Nota Para obtener más información acerca de la creación de secuencias de comandos administrativas con Windows Script Host, consulte el centro Technet Script Center en: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/default.asp>
Consulte también el curso 2433, *Microsoft Visual Basic Scripting Edition and Microsoft Windows Script Host Essentials* (en inglés).

Ejercicio: Creación de unidades organizativas

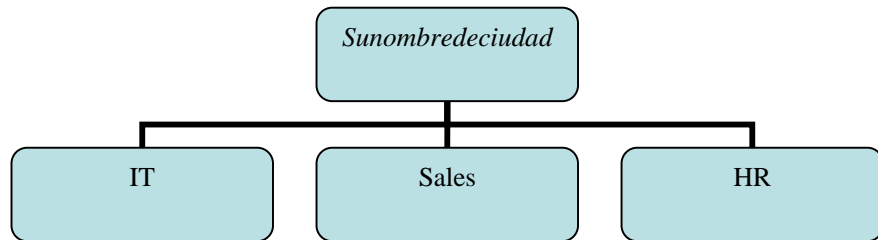


| | |
|----------------------|---|
| Objetivo | En este ejercicio deberá crear unidades organizativas en el dominio alojado en su equipo de alumno utilizando la herramienta de línea de comandos Ldifde. |
| Situación de ejemplo | Northwind Traders tiene varias sucursales. En su ubicación hay tres departamentos: Information Technology, Sales y Human Resources. Como administrador de la red de su oficina, deberá crear las unidades organizativas para estos departamentos. |

Ejercicio

Para crear unidades organizativas utilizando la herramienta Ldif de línea de comandos

1. Inicie sesión como **Nwtradersx\NombreDeEquipoUser** con la contraseña **P@ssw0rd**
2. Utilice el Bloc de notas para crear un archivo de entrada para las unidades organizativas que se indican en la siguiente ilustración.



3. Cree las nuevas unidades organizativas utilizando la herramienta Ldif de línea de comandos.

Lección: Delegación del control administrativo para unidades organizativas

- **Qué es la delegación de privilegios administrativos**
- **Tareas administrativas para unidades organizativas**
- **Cómo delegar el control administrativo**
- **Cómo personalizar el control administrativo delegado**
- **Cómo comprobar la delegación del control administrativo**

Introducción

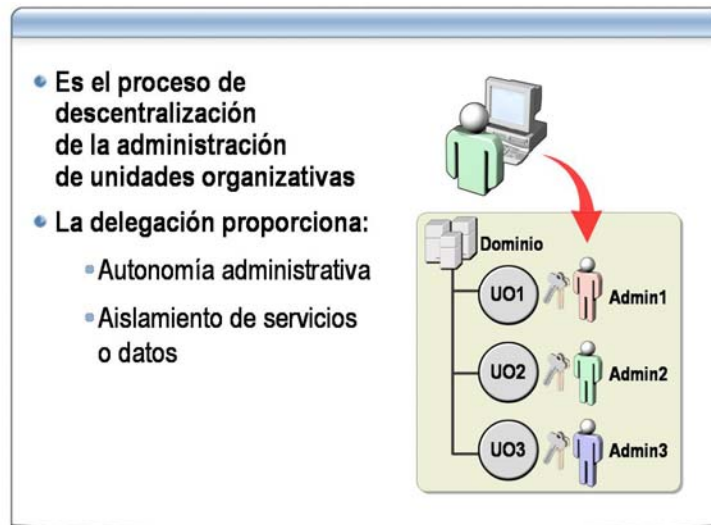
En esta lección se explica el propósito de delegar privilegios administrativos, las tareas administrativas que se pueden delegar, cómo delegarlas y como comprobar que se han delegado los privilegios necesarios para realizar dichas tareas.

Objetivo de la lección

Después de completar esta lección, los alumnos podrán:

- Describir las condiciones con las que se puede delegar el control administrativo a una unidad organizativa.
- Describir tareas administrativas comunes de unidades organizativas.
- Delegar control administrativo de una unidad organizativa mediante el Asistente para delegación de control.
- Personalizar el control administrativo delegado mediante la creación de una tarea personalizada que se vaya a delegar.
- Comprobar los privilegios administrativos que se han delegado.

Qué es la delegación de privilegios administrativos



Introducción

La razón principal para crear unidades organizativas es la distribución de tareas administrativas en la organización, delegando el control administrativo a otros administradores. Esta delegación resulta especialmente importante cuando se desarrolla un modelo administrativo descentralizado.

Qué es la delegación de administración

La delegación de administración es el proceso de descentralización de la responsabilidad de administrar unidades organizativas desde un administrador central a otros administradores. La capacidad de establecer el acceso a unidades organizativas individuales es una característica de seguridad importante en Active Directory; se puede controlar el acceso al nivel más bajo de una organización sin necesidad de crear muchos dominios de Active Directory.

La autoridad que se delega en el nivel de sitio permite expandir dominios o, por el contrario, no incluir destinos en el dominio. La autoridad delegada en el nivel de dominio afectará a todos los objetos del dominio. La autoridad delegada en el nivel de la unidad organizativa puede afectar al objeto y a todos sus objetos secundarios, o sólo al propio objeto.

Por qué delegar administración

Se delega control administrativo para proporcionar autonomía administrativa de servicios y datos a organizaciones o para aislar servicios o datos en una organización. Puede eliminar la necesidad de varias cuentas administrativas que tienen una autoridad amplia, como las de un dominio completo y seguir utilizando el grupo Admins. del dominio predeterminado para administrar el dominio completo.

La autonomía es la capacidad de los administradores de una organización para administrar de forma independiente:

- Toda la administración de servicio o parte de ésta (denominada *autonomía de servicio*).
- La totalidad o parte de los datos de la base de datos de Active Directory o de los equipos miembro que están unidos al directorio (denominada *autonomía de datos*).

Autonomía administrativa:

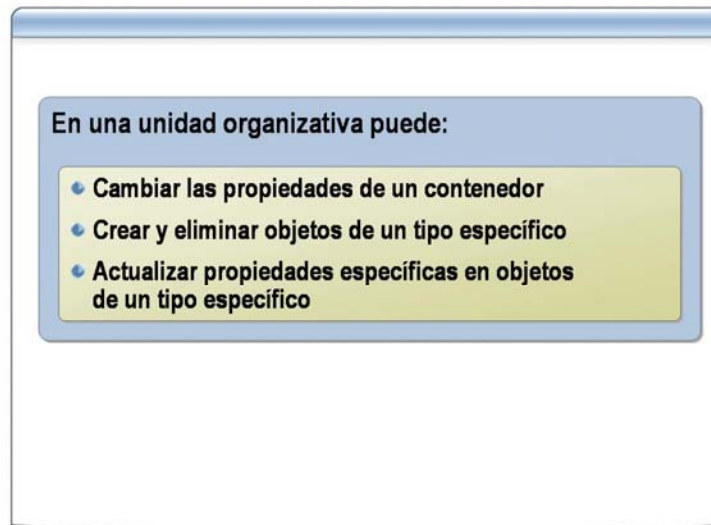
- Reduce el número de administradores que deben tener nivel de acceso alto.
- Limita el impacto de un error administrativo a un área de administración más reducida.

El aislamiento es la capacidad de los administradores de una organización para evitar que otros administradores puedan:

- Controlar o interferir con la administración de servicio (denominado *aislamiento de servicio*).
- Controlar o ver un subconjunto de datos en el directorio o en los equipos miembro que están unidos al directorio (denominado *aislamiento de datos*).

Windows Server 2003 contiene permisos y derechos de usuario específicos que se pueden utilizar para delegar control administrativo. Mediante una combinación de unidades organizativas, grupos y permisos puede designar derechos administrativos a un usuario particular, de modo que el usuario tenga un nivel adecuado de administración sobre un dominio completo, sobre todas las unidades organizativas de un dominio o sobre una única unidad organizativa.

Tareas administrativas para unidades organizativas



Introducción

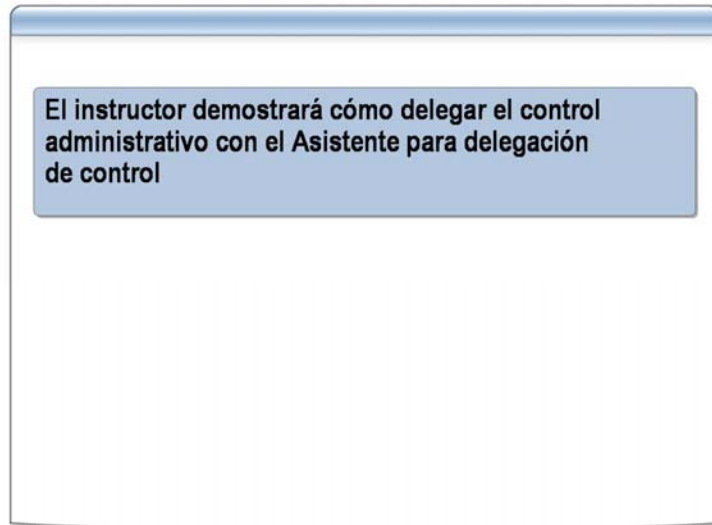
Utilice unidades organizativas para agrupar objetos de Active Directory por tipo, como usuarios, grupos y equipos, de modo que pueda administrarlos de forma eficaz.

Tareas administrativas comunes

Los administradores suelen realizar las siguientes tareas en Active Directory:

- *Cambiar las propiedades de un contenedor particular.* Por ejemplo, cuando está disponible un nuevo paquete de software, los administradores pueden crear una directiva de grupo que controle la distribución del software.
- *Crear y eliminar objetos de un tipo específico.* En una unidad organizativa, los tipos específicos pueden incluir usuarios, grupos e impresoras. Cuando se incorpora un trabajador nuevo en la organización, se puede crear una cuenta de usuario para el trabajador y, a continuación, agregar el trabajador a la unidad organizativa o el grupo adecuados.
- *Actualizar propiedades específicas en objetos de un tipo específico* en una unidad organizativa. La actualización de propiedades, que será quizá la tarea administrativa más común que realice, incluye tareas como restablecer contraseñas y cambiar la información personal de un trabajador, como su domicilio y teléfono, cuando cambia de domicilio.

Cómo delegar el control administrativo



Introducción

Se puede utilizar el Asistente para delegación de control con el fin de delegar el control administrativo de objetos de Active Directory, como unidades organizativas. Con el asistente se pueden delegar tareas administrativas comunes, como crear, eliminar y administrar cuentas de usuario.

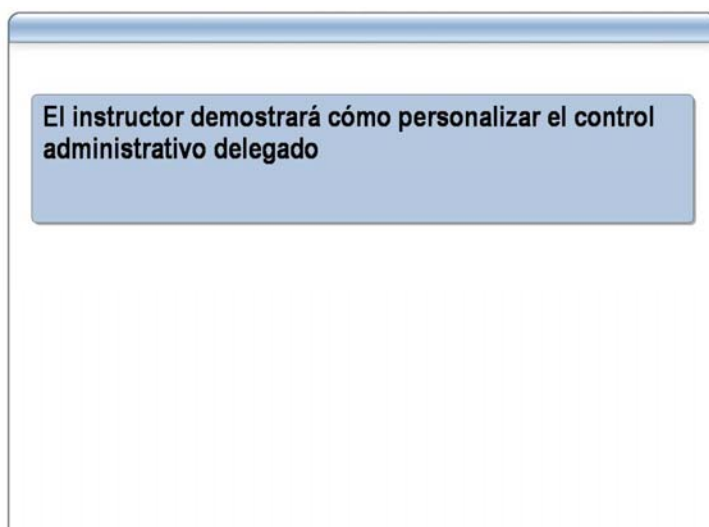
Procedimiento

Para delegar tareas administrativas comunes para una unidad organizativa, realice los siguientes pasos:

1. Inicie el Asistente para delegación de control como se indica a continuación:
 - a. Abra Usuarios y equipos de Active Directory.
 - b. En el árbol de la consola, haga doble clic en el nodo de dominio.
 - c. En el panel de detalles, haga clic con el botón secundario del *mouse* (ratón) en la unidad organizativa, elija **Delegar control** y haga clic en **Siguiente**.
2. Seleccione los usuarios o grupos a los que desee delegar tareas administrativas comunes. Para hacerlo, realice los siguientes pasos:
 - a. En la página **Usuarios o grupos**, haga clic en **Agregar**.
 - b. En el cuadro de diálogo **Seleccionar Usuarios, Equipos o Grupos**, escriba los nombres de los usuarios y grupos a los que desee delegar control de la unidad organizativa, haga clic en **Aceptar** y, a continuación, haga clic en **Siguiente**.
3. Asigne tareas comunes para delegar. Para hacerlo, realice los siguientes pasos:
 - a. En la página **Tareas que se delegarán**, haga clic en **Delegar las siguientes tareas comunes**.
 - b. En la página **Tareas que se delegarán**, seleccione las tareas que desee delegar y haga clic en **Siguiente**.
4. Haga clic en **Finalizar**.

Al delegar control a un usuario o grupo para crear objetos en Active Directory, éste podrá crear un número ilimitado de objetos. En Windows Server 2003 puede limitar el número de objetos que un principal de seguridad puede tener en una partición de directorio implementando una cuota para ese principal de seguridad.

Cómo personalizar el control administrativo delegado



Introducción

Además de utilizar el Asistente para delegación de control con el fin de delegar un conjunto personalizado de tareas administrativas, como la creación, eliminación y administración de cuentas de usuario, se puede utilizar el asistente para seleccionar un conjunto de tareas personalizadas y delegar control de únicamente esas tareas.

Por ejemplo, puede delegar control de todos los objetos existentes en una unidad organizativa y de todos los objetos nuevos que se agreguen, o puede seleccionar los objetos de la unidad organizativa de los que desee delegar control administrativo como, por ejemplo, sólo objetos de usuario de una unidad organizativa. También puede especificar que desea delegar sólo la creación del objeto seleccionado o la eliminación del objeto o ambas.

Procedimiento

Para delegar tareas administrativas personalizadas para una unidad organizativa, realice los siguientes pasos:

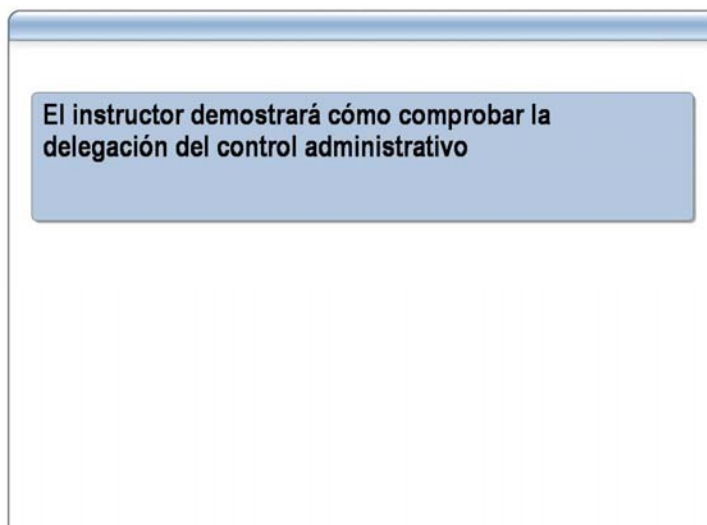
1. Inicie el Asistente para delegación de control.
2. Seleccione los usuarios o grupos a los que desee delegar tareas administrativas.

3. Asigne las tareas personalizadas que desee delegar. Para hacerlo, realice los siguientes pasos:
 - a. En la página **Tareas que se delegarán**, haga clic en **Crear una tarea personalizada** para delegar y, a continuación, en **Siguiente**.
 - b. En la página **Tipo de objeto de Active Directory**, realice una de las siguientes acciones:
 - i. Haga clic en **Esta carpeta, los objetos contenidos en la misma y la creación de nuevos objetos en esta carpeta** y, a continuación, haga clic en siguiente.
 - ii. Haga clic en **Sólo los siguientes objetos en la carpeta**, seleccione el tipo de objeto de Active Directory del que desea delegar control y, a continuación, haga clic en **Siguiente**.
 - c. Seleccione los permisos que desee delegar y haga clic en **Siguiente**.

Nota Para obtener una lista de los permisos que se pueden delegar para los objetos seleccionados o para delegar la creación y eliminación de objetos secundarios en los objetos seleccionados, active la casilla de verificación **Específico de la propiedad**.

4. Haga clic en **Finalizar**.

Cómo comprobar la delegación del control administrativo



Introducción

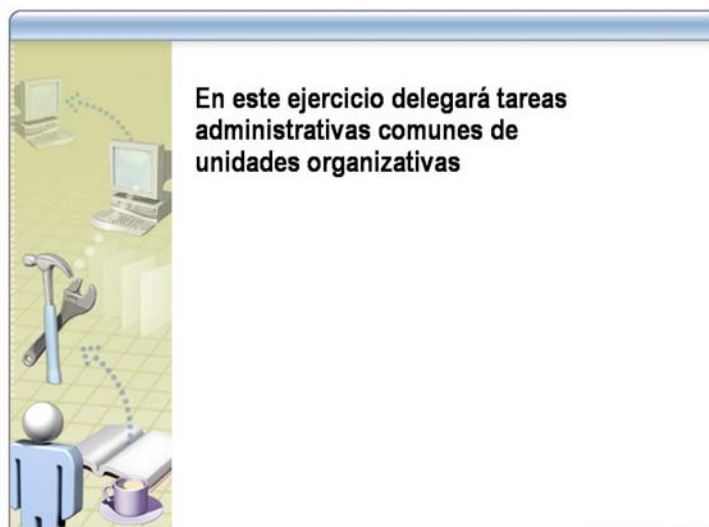
Utilice Usuarios y equipos de Active Directory para comprobar que el Asistente para delegación de control ha delegado correctamente la autoridad para realizar las tareas.

Procedimiento

Para comprobar la delegación de control, realice los siguientes pasos:

1. En Usuarios y equipos de Active Directory, en el menú **Ver**, haga clic en **Características avanzadas**.
2. En el árbol de la consola, haga doble clic en el nodo de dominio.
3. En el panel de detalles, haga clic con el botón secundario del *mouse* en la unidad organizativa y, a continuación, haga clic en **Propiedades**.
4. En la ficha **Seguridad**, haga clic en **Opciones avanzadas**.
5. En la ficha **Permisos**, en **Entradas de permisos**, vea los permisos asignados.

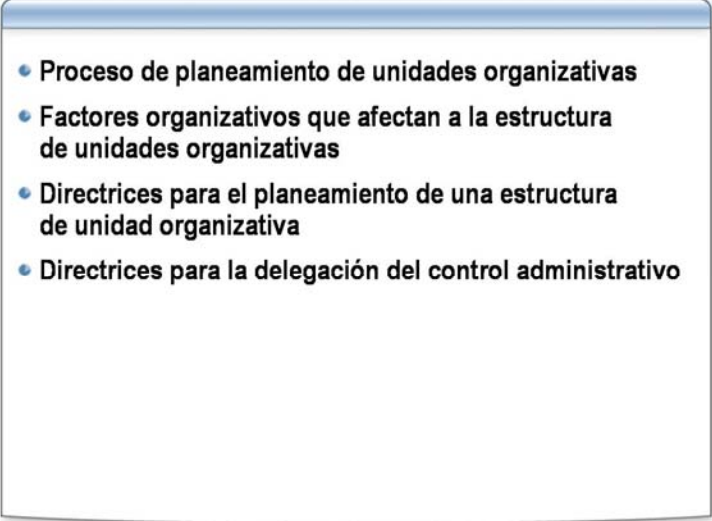
Ejercicio: Delegación de tareas administrativas para una unidad organizativa



| | |
|----------------------|--|
| Objetivo | En este ejercicio delegará tareas administrativas comunes de unidades organizativas en el dominio alojado en el equipo de alumno. |
| Situación de ejemplo | Usted es el administrador de red de Northwind Traders. Debido al tamaño de su compañía, no tiene tiempo para realizar las tareas administrativas rutinarias para cada unidad organizativa. Desea delegar control de las unidades organizativas al personal del departamento de soporte y a administradores de departamentos concretos. |
| Ejercicio | <p>Delegar tareas administrativas comunes de unidades organizativas en el dominio alojado en el equipo de alumno</p> <ol style="list-style-type: none">1. Inicie sesión como Nwtradersx\NombreDeEquipoUser con la contraseña P@ssw0rd2. Haga clic en Inicio, seleccione Herramientas administrativas, haga clic con el botón secundario del <i>mouse</i> en Usuarios y equipos de Active Directory y, a continuación, haga clic en Ejecutar como.3. En el cuadro de diálogo Ejecutar como, seleccione El siguiente usuario, escriba sudominio\Administrador como nombre de usuario con la contraseña P@ssw0rd y haga clic en Aceptar.4. Cree un grupo de seguridad local del dominio denominado DL NombreDeEquipoAdmins en la unidad organizativa NombreDeEquipo de su dominio (donde NombreDeEquipo es el nombre del equipo en el que está trabajando). |

5. Agregue el grupo global Nwtraders\G *NombreDeEquipo*Admins como un miembro del grupo local de dominio DL *NombreDeEquipo*Admins.
6. Delegue la capacidad de crear, eliminar y administrar cuentas de usuario en la unidad organizativa *NombreDeEquipo* al grupo DL *NombreDeEquipo*Admins.
7. Compruebe que se ha delegado el control para estas tareas visualizando los permisos asignados al grupo local de dominio para la unidad organizativa *NombreDeEquipo*.

Lección: Planeamiento de la estrategia de una unidad organizativa

- 
- **Proceso de planeamiento de unidades organizativas**
 - **Factores organizativos que afectan a la estructura de unidades organizativas**
 - **Directrices para el planeamiento de una estructura de unidad organizativa**
 - **Directrices para la delegación del control administrativo**

Introducción

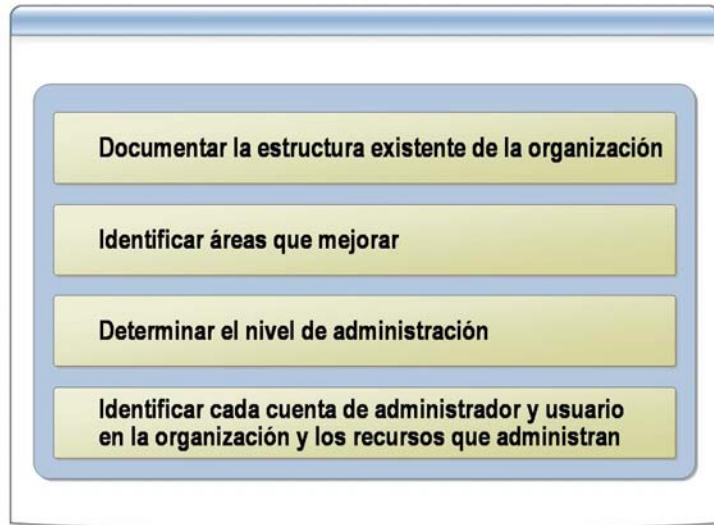
Las unidades organizativas son contenedores de cada dominio de Active Directory que representan las estructuras jerárquicas de una organización. Para crear una estructura de unidad organizativa que represente de la mejor forma la estructura de la organización, debe entender los factores de la organización que afectan a la creación de unidades organizativas. En esta lección se proporcionan los conocimientos y capacidades necesarios para planear una estrategia de unidad organizativa.

Objetivos de la lección

Después de finalizar esta lección, podrá:

- Describir el proceso de planeamiento de unidades organizativas.
- Describir los factores organizativos que afectan al planeamiento de unidades organizativas.
- Explicar las directrices para determinar la estructura de una unidad organizativa.
- Explicar las directrices para determinar cómo delegar control administrativo a una unidad organizativa.

Proceso de planeamiento de unidades organizativas



Introducción

La estructura de las unidades organizativas en Active Directory se basa en la estructura administrativa de la organización. El primer paso en el planeamiento de una estructura de unidad organizativa es documentar la estructura de la organización.

Proceso de planeamiento de unidades organizativas

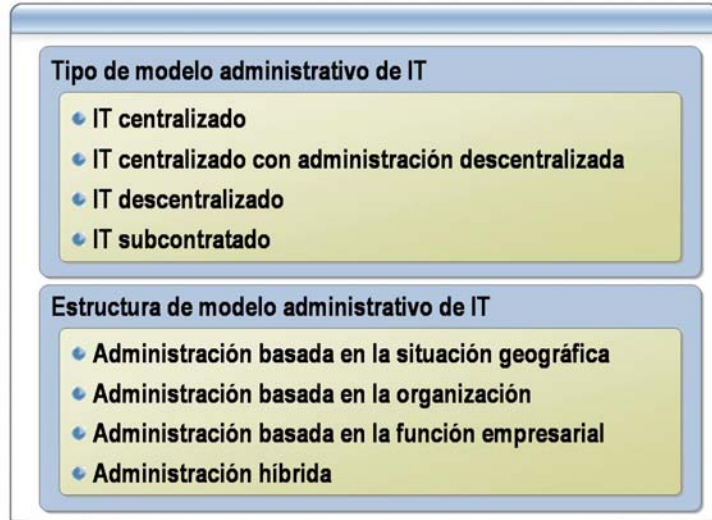
Para planear la estrategia de unidades organizativas para su organización, realice las siguientes tareas:

- *Documentar la estructura existente de la organización.* Al documentar la estructura existente de la organización, una estrategia es dividir las tareas administrativas en categorías y, a continuación, documentar los administradores que son responsables de cada categoría.
- *Identificar áreas que mejorar.* Trabaje con el equipo de planeamiento para identificar las áreas que hay que mejorar. Por ejemplo, puede ser más rentable combinar varios equipos de IT de distintas secciones. Puede seleccionar otros trabajadores que no sean de esta sección para ayudar en el proceso administrativo y reducir la carga de trabajo del personal de IT. De este modo, los administradores podrán centrarse en las áreas en que se requiera su experiencia.

A continuación, utilice los siguientes puntos como directrices para el plan de delegación:

- *Determinar el nivel de administración.* Decidir lo que va a controlar cada grupo y en qué nivel se va a delegar administración en la jerarquía administrativa. Al crear el plan, indique los grupos que:
 - Tendrán pleno control sobre objetos de una clase particular. Estos grupos podrán crear y eliminar objetos de una clase especificada y modificar cualquier atributo de los objetos de esa clase especificada.
 - Podrán crear objetos de una clase particular. Por defecto, los usuarios tienen control pleno sobre los objetos que crean.
 - Sólo podrán modificar atributos específicos de objetos existentes de una clase particular.
- *Identificar cada cuenta de administrador y usuario en la organización y los recursos que administran.* Esta información le ayudará a determinar la propiedad y los permisos asignados a las unidades organizativas que cree para facilitar el plan de delegación.

Factores organizativos que afectan a la estructura de unidades organizativas



Introducción

Los factores que afectan a la estructura de unidades organizativas son el tipo y la estructura del modelo administrativo de IT. El conocimiento de estos factores le ayudará a crear una estructura de unidades organizativas que se adapte de la mejor forma a los requisitos de su organización.

Tipos de modelos administrativos de IT

Las organizaciones de IT más comunes son:

- *IT centralizado.* En este modelo, la organización de IT informa a un individuo y, normalmente, el grupo es el responsable de todos los servicios de red y de información, aunque algunas tareas rutinarias se pueden delegar a ciertos grupos o departamentos.
- *IT centralizado con administración descentralizada.* En este modelo, un equipo central de IT ubicado en un lugar centralizado es el responsable de los servicios de infraestructura central, pero delega la mayor parte de las operaciones diarias a grupos de IT en sucursales, que proporcionan apoyo administrativo local a los usuarios.
- *IT descentralizado.* Este tipo de organización permite distintas unidades empresariales para seleccionar un modelo de IT adecuado que cumpla cumplir los requisitos. Este tipo de organización puede tener varios grupos de IT con requisitos y objetivos distintos. Siempre que haya iniciativas tecnológicas que afecten a la organización, como una actualización de una aplicación de mensajería, los grupos de IT deben trabajar juntos para implementar los cambios.
- *IT subcontratado.* Algunas organizaciones contratan a una empresa externa para administrar la totalidad o parte de su organización de IT. Cuando sólo se subcontratan partes de la organización de IT, es imprescindible implementar un modelo de delegación adecuado. De este modo, el grupo de IT interno mantiene el control de la organización sin comprometer los acuerdos de nivel de servicio que la otra empresa se ha comprometido a proporcionar.


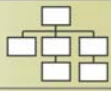


Estructura del modelo administrativo de IT

La estructura del modelo administrativo refleja el modo en que una organización administra sus recursos de IT, como usuarios, equipos, grupos, impresoras y archivos compartidos.

Algunas de las distintas formas en que se estructuran los modelos administrativos son:

- *Administración basada en la situación geográfica.* La organización de IT está centralizada, como en las sedes centrales, pero la administración de la red está distribuida de forma geográfica; por ejemplo, cada sucursal tiene su propio grupo administrativo que administra los recursos de su ubicación.
- *Administración basada en la organización.* En esta estructura, la organización de IT se divide en departamentos o unidades comerciales y cada una tiene su propio grupo de IT.
- *Administración basada en la función empresarial.* Una organización de IT descentralizada a menudo basa su modelo administrativo en funciones empresariales de la organización.
- *Administración híbrida.* Esta estructura combina la eficacia de varios modelos para satisfacer las necesidades administrativas de la organización.

Directrices para el planeamiento de una estructura de unidad organizativa

| Modelo administrativo | Diseñar estructura de UO basada en: |
|--|--|
| Basado en la situación geográfica  | Ubicación |
| Basado en la organización  | Estructura de la organización |
| Basado en la función empresarial  | Funciones de la organización |
| Híbrido  | <ul style="list-style-type: none"> ▪ Ubicación para las unidades organizativas o dominios superiores ▪ Estructura de la organización para unidades organizativas o dominios inferiores |

Introducción

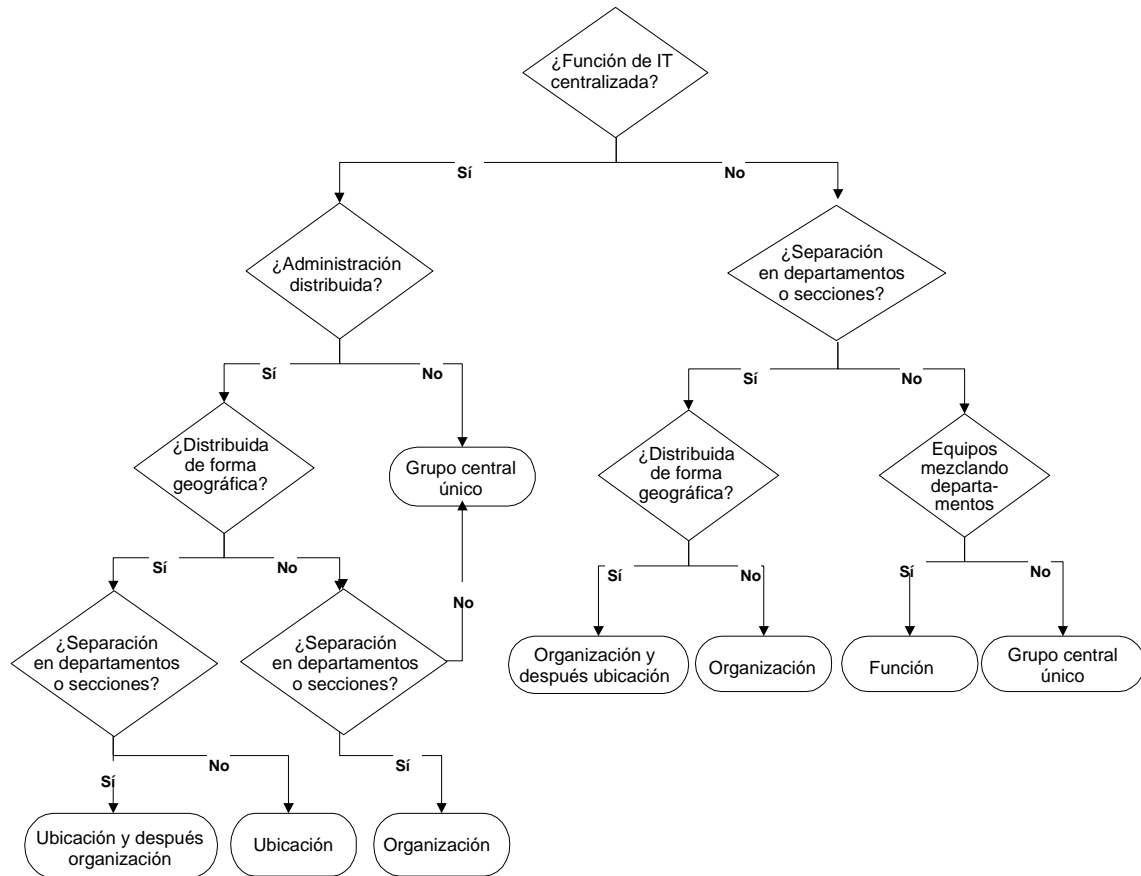
El diseño de las unidades organizativas se basa en el modelo administrativo de IT de una organización.

Directrices

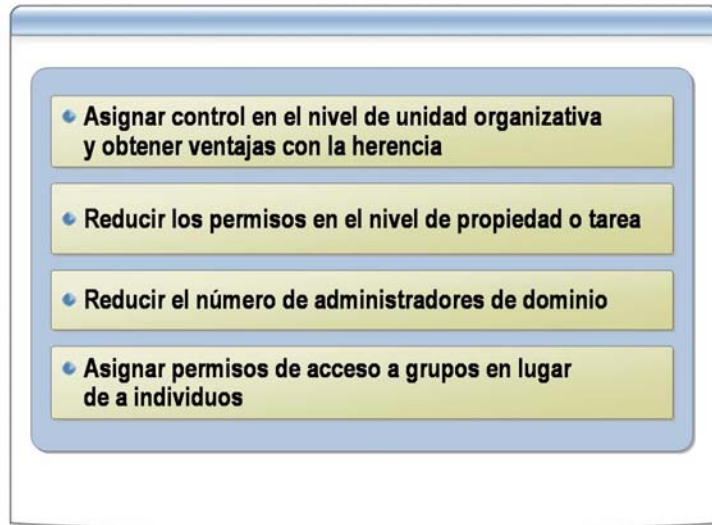
Utilice las siguientes directrices como ayuda al planear la estructura de la unidad organizativa de una organización. La estructura puede basarse en:

- *La situación geográfica.* Si el modelo administrativo está distribuido de forma geográfica y si los administradores están presentes en cada ubicación, organice la estructura de Active Directory por ubicación.
- *La organización.* Si la administración de IT se basa en un departamento o sección, diseñe Active Directory basándose en la estructura de la organización. Asegúrese de seguir la estructura administrativa en lugar del diagrama organizativo al diseñar Active Directory en función de la organización. Puede que el diagrama organizativo no determine las necesidades administrativas de una organización.
- *Las funciones empresariales.* Si la administración de IT es descentralizada, diseñe la estructura de Active Directory basándose en las funciones de la organización. Elija esta alternativa sólo cuando la función de IT no se base en la ubicación o la organización. Esta estructura es idónea y, en realidad, la única apropiada, para organizaciones pequeñas que tienen funciones de trabajo que abarcan varios departamentos.
- *El modelo híbrido.* Si se trata de una organización con alto grado de distribución con una función de IT centralizada y una separación estricta en departamentos o secciones, diseñe las unidades organizativas o dominios superiores por ubicación y los niveles inferiores de unidades organizativas o dominios por organización. Puesto que los niveles superiores se basan en la ubicación, este modelo tiene menos probabilidades de cambio y, por lo tanto, es menos probable que requiera un gran esfuerzo durante una reorganización.

Utilice el siguiente diagrama de flujo como un árbol de decisiones para determinar la estructura de unidad organizativa apropiada para una organización.



Directrices para la delegación del control administrativo



Introducción

Siempre que sea posible, delegue la capacidad de conceder permisos para conservar el esfuerzo y los gastos administrativos, con lo que se reducen los gastos totales de propiedad. Antes de asignar permisos a los usuarios de una organización, debe decidir quién puede y quién no puede tener acceso a un objeto y a su contenido y el tipo de acceso que una persona puede o no puede tener.

Directrices

Tenga en cuenta las siguientes directrices al planear la delegación de control administrativo en la organización:

- *Asignar control en el nivel de unidad organizativa más alto posible y utilizar la herencia.* De este modo, podrá administrar los permisos de forma más eficaz. Se crea una pista de auditoría más simple y hay menos posibilidades de desastre si un administrador comete un error al iniciar la sesión con una cuenta administrativa.

Nota Los miembros del grupo Admins. del dominio siempre podrán asumir la propiedad de un objeto en el dominio y cambiar los permisos, lo que supone una razón para limitar el número de usuarios en dicho grupo. Cuando un miembro del grupo Administradores crea o asume la propiedad de un objeto, el grupo Administradores se convierte en el propietario del objeto. Para poder realizar un seguimiento, Windows Server 2003 muestra el nombre de dicho miembro.

- *Evitar la asignación de permisos en el nivel de propiedad o de tarea para simplificar la administración.* Tenga en cuenta la colocación de objetos en unidades organizativas separadas en función de cómo se van a administrar en lugar de administrar las propiedades utilizando Listas de control de acceso discrecional (DACL, *Discretionary Access Control List*) separadas para los objetos de una unidad organizativa individual.

Al asignar permisos:

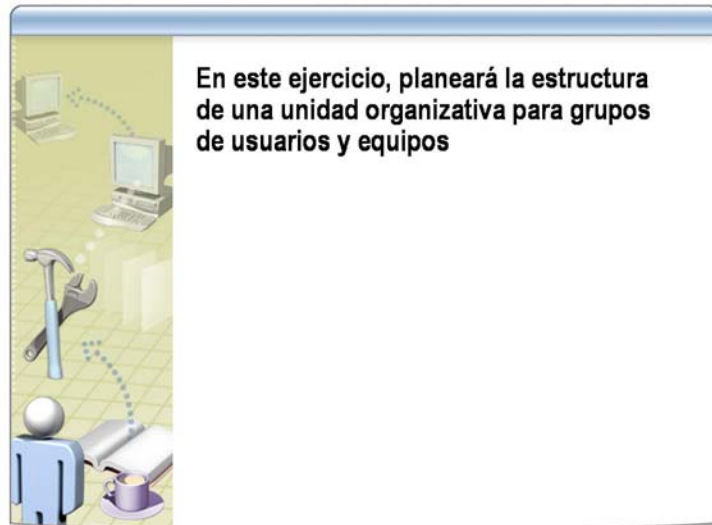
- Delege la capacidad de asignar permisos de control de acceso para objetos a usuarios o grupos de usuarios. En otras palabras, delege la capacidad de delegar.
- Asigne permisos comunes o especiales sobre objetos.
- Utilice la herencia para permitir que los permisos de control de acceso alcancen los objetos secundarios. Sin embargo, en algunas ocasiones deberá bloquear la herencia para evitar que un objeto secundario adquiera permisos establecidos para los objetos primarios. Al bloquear la herencia, se dificulta la documentación y la solución de problemas de permisos para un objeto, por lo que debe evitarlo.
- *Asignar permisos de acceso a grupos en lugar de a individuos.* Los permisos a grupos facilitan el mantenimiento de DACL en redes que tienen muchos usuarios y objetos. Además, la asignación de permisos a grupos resulta muy eficaz, ya que le permite anidar grupos, con lo que se reduce el número total de objetos que administrar.

Importante Delege control administrativo a grupos locales de dominio al asignar permisos a los objetos de un dominio. Delege control administrativo a grupos globales o universales al asignar permisos a objetos en la partición de configuración o para atributos que estén publicados en el catálogo global.

- *Reducir el número de administradores de dominio.* El grupo Admins. del dominio tiene capacidades especiales en un dominio, como la capacidad de asumir la propiedad de cualquier objeto y definir directivas de seguridad para todo el dominio. Cuando desee controlar de cerca los privilegios de los administradores de dominio, conceda derechos administrativos a los usuarios de las distintas unidades organizativas y limite los miembros del grupo Admins. del dominio.

Nota Para obtener más información acerca de la delegación de control, consulte la guía *The Windows Server 2003 Deployment Planning Guide* en <http://www.microsoft.com/reskit>. Consulte también *Active Directory Service Interfaces Overview* (en inglés) en <http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adsilinks.asp>.

Ejercicio: Planeamiento de la estructura de una unidad organizativa



Objetivo

En este ejercicio se trabajará en parejas para planear una estructura de unidad organizativa para Northwind Traders.

Situación de ejemplo

Northwind Traders se está preparando la instalación de Windows Server 2003 en sus ubicaciones de Sacramento, California y Portland (Oregón). El equipo de diseño de Active Directory utilizará un dominio raíz vacío, `nwtradersx.msft`, y un subdominio, `corp.x.nwtradersx.msft`, donde x es un número que le asignará el instructor.

Todas las cuentas de equipo y de usuario se encuentran en el dominio `corp.x`. Northwind Traders tiene 1.500 usuarios en seis departamentos en estas dos ubicaciones.

Portland tiene 600 usuarios en los siguientes departamentos:

- Accounting
- IT
- Purchasing
- Shipping

Sacramento tiene 900 usuarios en los siguientes departamentos:

- Accounting
- Human Resources (HR)
- IT
- Purchasing
- Sales

En cada departamento hay un administrador local que administra las cuentas de usuario y la configuración de directivas de grupo. El departamento de IT quiere delegar la capacidad de administrar a todos los usuarios de un departamento específico o de administrar a todos los usuarios de un departamento de una ubicación específica.

Procedimiento

Trabaje con su compañero para planear una estructura de unidad organizativa. Utilice el siguiente cuadro para documentar el plan para la estructura de la unidad organizativa.

