Gestión de Objetos de Servicios de Dominio de Active Directory

Administración de Sistemas Operativos

¿Cuál es la diferencia entre una cuenta de usuario local y una de dominio?

¿Qué es una cuenta de usuario?

¿Cuáles serian las recomendaciones para contraseñas seguras?

TECSUP
Pasión por la Tecnología

Introducción

- Se presentará la importancia de la administración de usuarios, grupos y equipos de Active Directory Domain Services (AD DS), para lograr que su estructura jerárquica permita mantenerlos con componentes de una red, como también permisos, asignación de recursos y políticas de acceso.

Capacidades de la sesión

- Administrar cuentas de usuario con herramientas gráficas.
- Administrar grupos con herramientas gráficas.
- Administrar cuentas de equipo.
- Delegar permisos para realizar tareas de administración de los servicios de dominio de Active Directory® (AD DS).

1. Administrando cuentas de usuario

- Herramientas administrativas en AD DS
- Creación de cuentas de usuario
- Configuración de Atributos de cuentas de usuarios
- Creación de perfiles de usuario
- Creación de cuentas de usuario usando plantillas de cuentas de usuario
- Demostración: Administrando cuentas de usuario mediante la herramienta Usuarios y equipos de Active Directory

1.1. Herramientas administrativas de AD DS

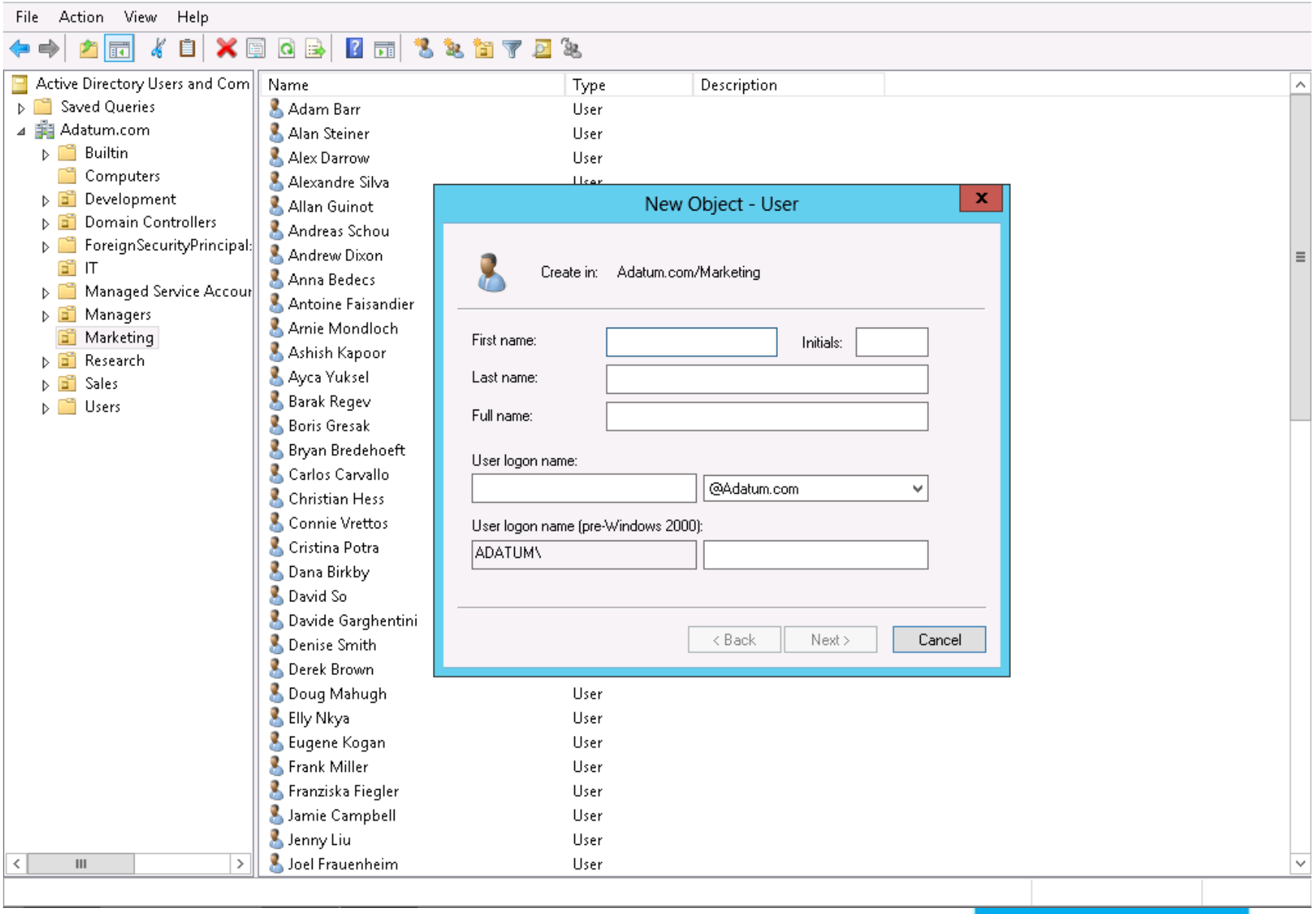
Para administrar los objetos de AD DS, puede utilizar las siguientes herramientas gráficas :

- Active Directory Administration snap-ins
- Active Directory Administrative Center

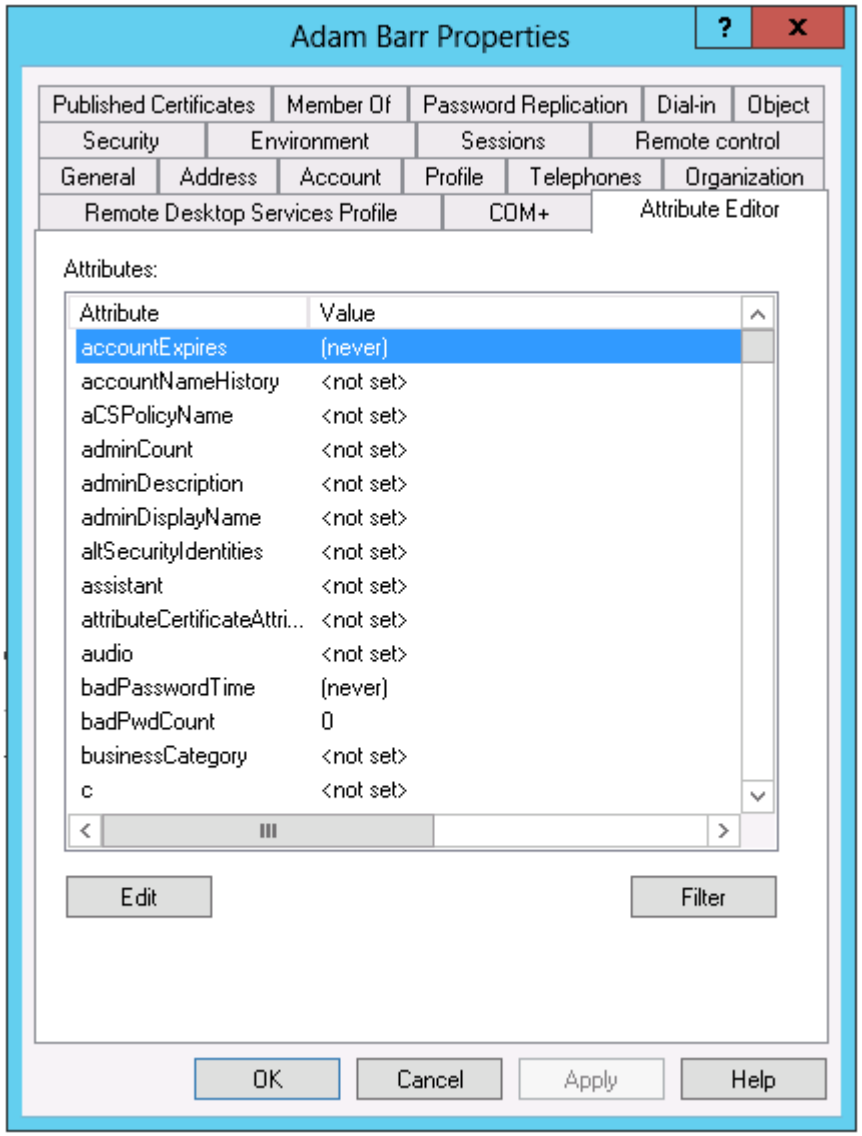
También puede utilizar las siguientes herramientas de línea de comandos:

- Modulo Active Directory en Windows PowerShell
- Comandos del Directory Service

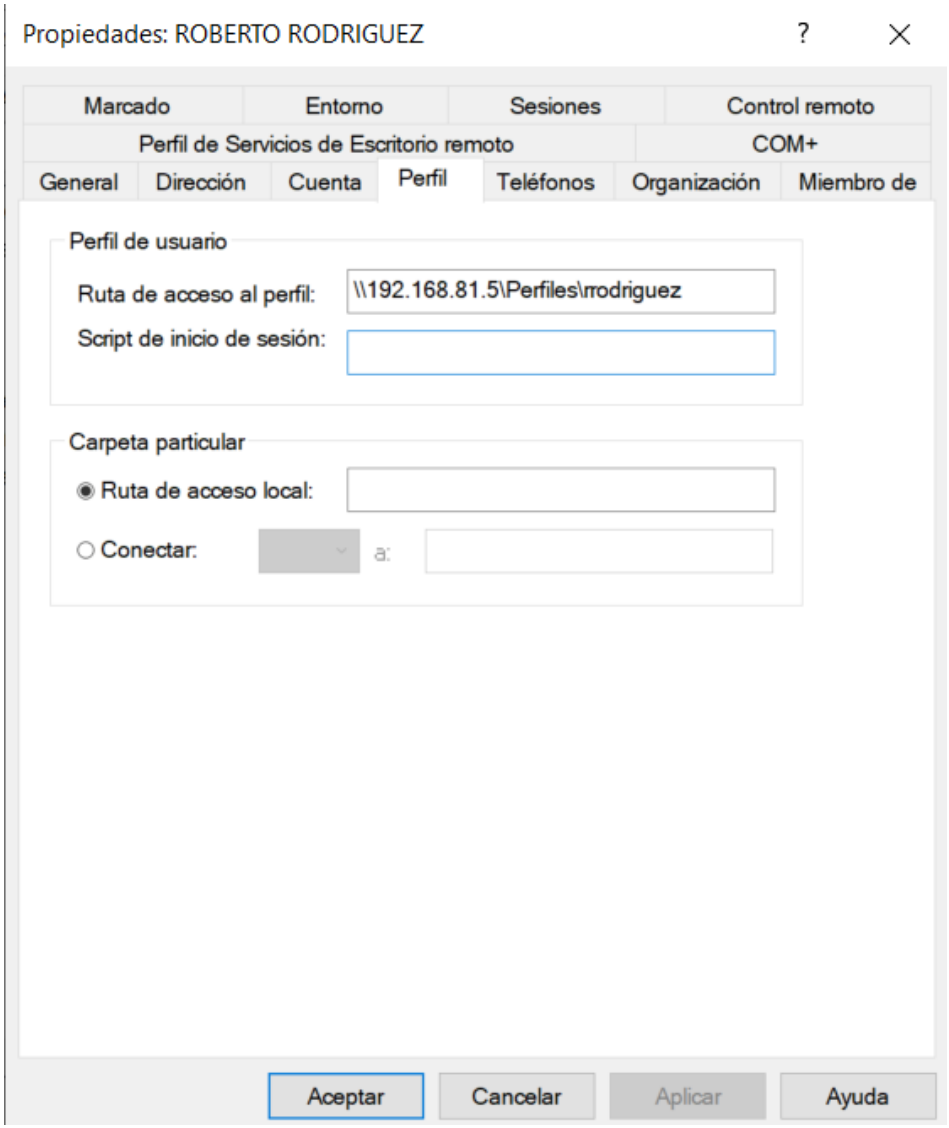
1.2. Creación de cuentas de usuario



1.3. Propiedades de Cuentas de Usuario

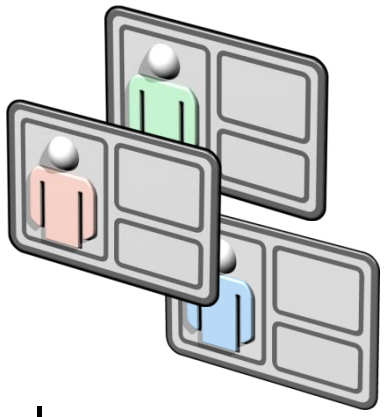


1.4. Creación de perfiles de usuario



1.5. Creación de cuentas de usuario usando plantillas de cuentas de usuario

Una plantilla de cuenta de usuario es una cuenta con propiedades comunes que se han configurado previamente



Las plantillas de cuentas de usuario se aprovechan de las similitudes entre cuentas de usuario

Se pueden crear nuevas cuentas de usuario mediante la creación de plantillas de cuentas de usuario:

- Crear varios usuarios típicos que reflejan diversos grupos dentro de su organización
- Copiar la cuenta de usuario que es la más parecida a la nueva cuenta que desea crear
- Modificar los atributos de cuenta tales como nombre, dirección de correo electrónico, y el nombre de inicio de sesión

TECSUP
Pasión por la Tecnología

1.6. Demostración: Gestión de cuentas de usuario mediante Usuarios y equipos de Active Directory

En esta demostración, verá cómo:

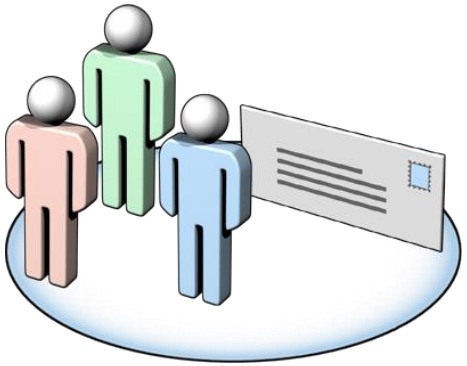
- Abra la herramienta Usuarios y equipos de Active Directory
- Eliminar una cuenta de usuario
- Crear una plantilla de cuenta de usuario
- Crear una nueva cuenta de usuario desde una plantilla
- Modificar las propiedades de una cuenta de usuario
- Cambiar el nombre de una cuenta de usuario
- Mover una cuenta de usuario

2. Gestión de cuentas de grupo

- Tipos de grupo
- Ámbitos de grupo
- Implementando administración de grupo
- Grupos predeterminados e Identidades especiales
- Demostración: Administrar grupos

2.1. Tipos de Grupos

- Grupos de Distribución
  - Sólo se utiliza con aplicaciones de correo electrónico
  - Sin seguridad habilitada (no SID); no se puede otorgar permisos
- Grupos de Seguridad
  - Seguridad principal con un SID; se puede dar permisos
  - También puede ser habilitada para correo electrónico



2.2. Ámbito de Grupos

- **Grupo de ámbito de dominio local.**

2.2. Ámbito de Grupos (cont.)

- **Grupo de ámbito global.**

2.2. Ámbito de Grupos (cont.)

- **Grupo de ámbito universal.**

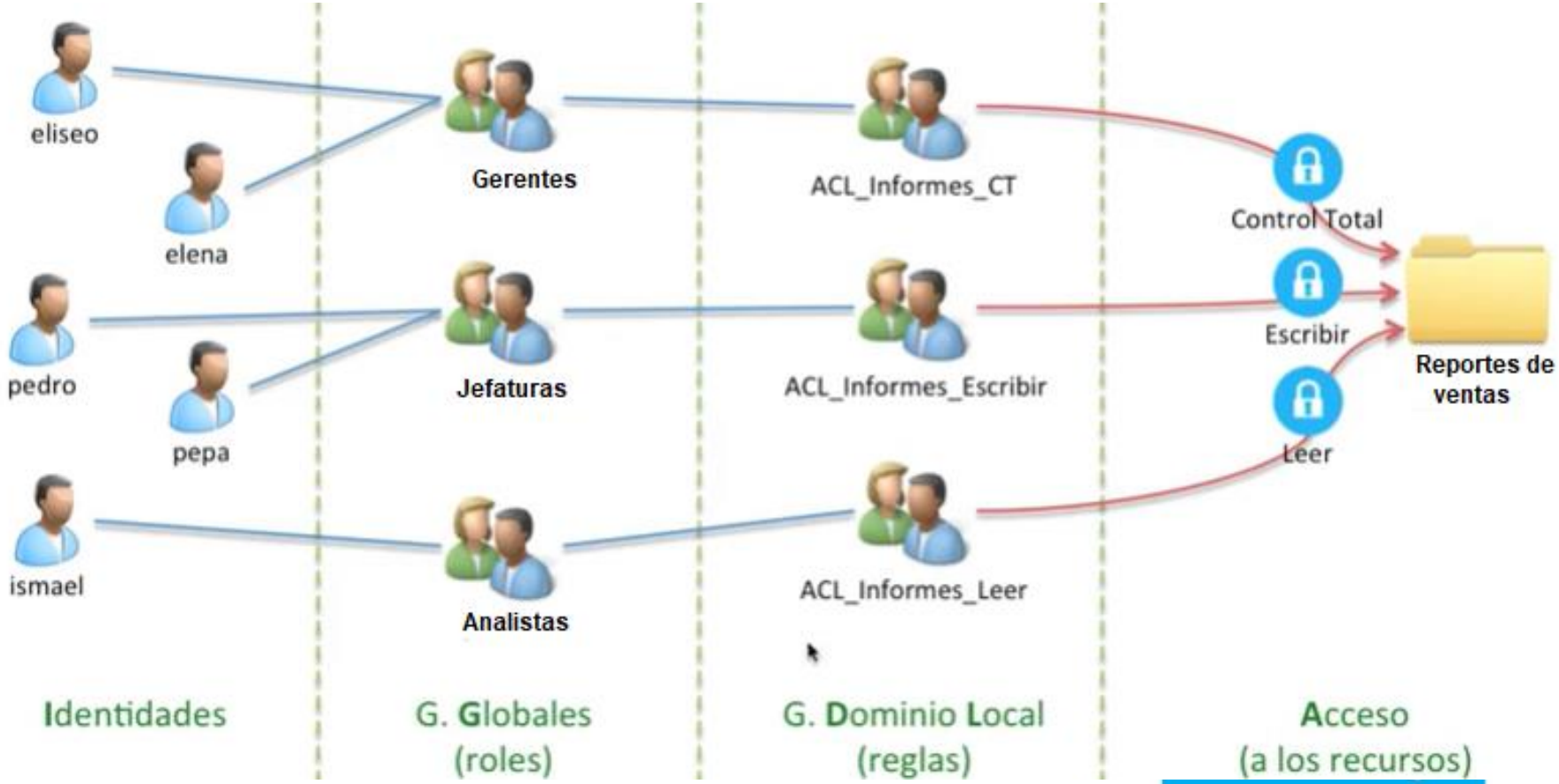
2.3. Implementando la Administración de Grupos – metodología IGDLA

- Es una buena práctica para el anidamiento de grupos.
- Tiene como objetivo diseñar un esquema de objetos de dominio que resuelva de manera consistente y flexible el acceso de los usuarios a los recursos de dominio.
- IGDLA significa: Las **I**dentidades (pueden ser cuentas de usuarios o equipos) son miembros de Grupos **G**lobales que representan roles en las empresas. Estos roles (grupos globales) son miembros de grupos de **D**ominio **L**ocal que representan niveles de acceso de los recursos. A estos grupos de dominio local finalmente se les concede **A**cceso a los recursos.

2.3. Implementando la Administración de Grupos – metodología IGDLA (cont.)

- La seguridad debe plantearse a nivel de roles (grupos globales) y no a nivel de usuario individuales.
- La seguridad debe plantearse por niveles de acceso al recursos y no en función de qué usuarios o grupos van a tener los permisos.

2.3. Implementando la Administración de Grupos – metodología IGDLA (cont.)



2.4. Grupos predeterminados e Identidades especiales

Windows Server proporciona dos grupos adicionales :

- **Grupos predeterminados**
  - Los grupos predeterminados que proporcionan privilegios administrativos deben ser administrados con cuidado :
    - Por lo general tienen privilegios más amplios que los necesarios para ambientes más delegados
    - A menudo aplican protección a sus miembros

- **Identidades especiales**
  - Grupos para los que la pertenencia es controlado por el sistema operativo
  - La importancia de estas identidades especiales es que se puede utilizar para proporcionar acceso a los recursos en función del tipo de autenticación o conexión, en lugar de la cuenta de usuario.

2.5. Demostración: Administrando Grupos

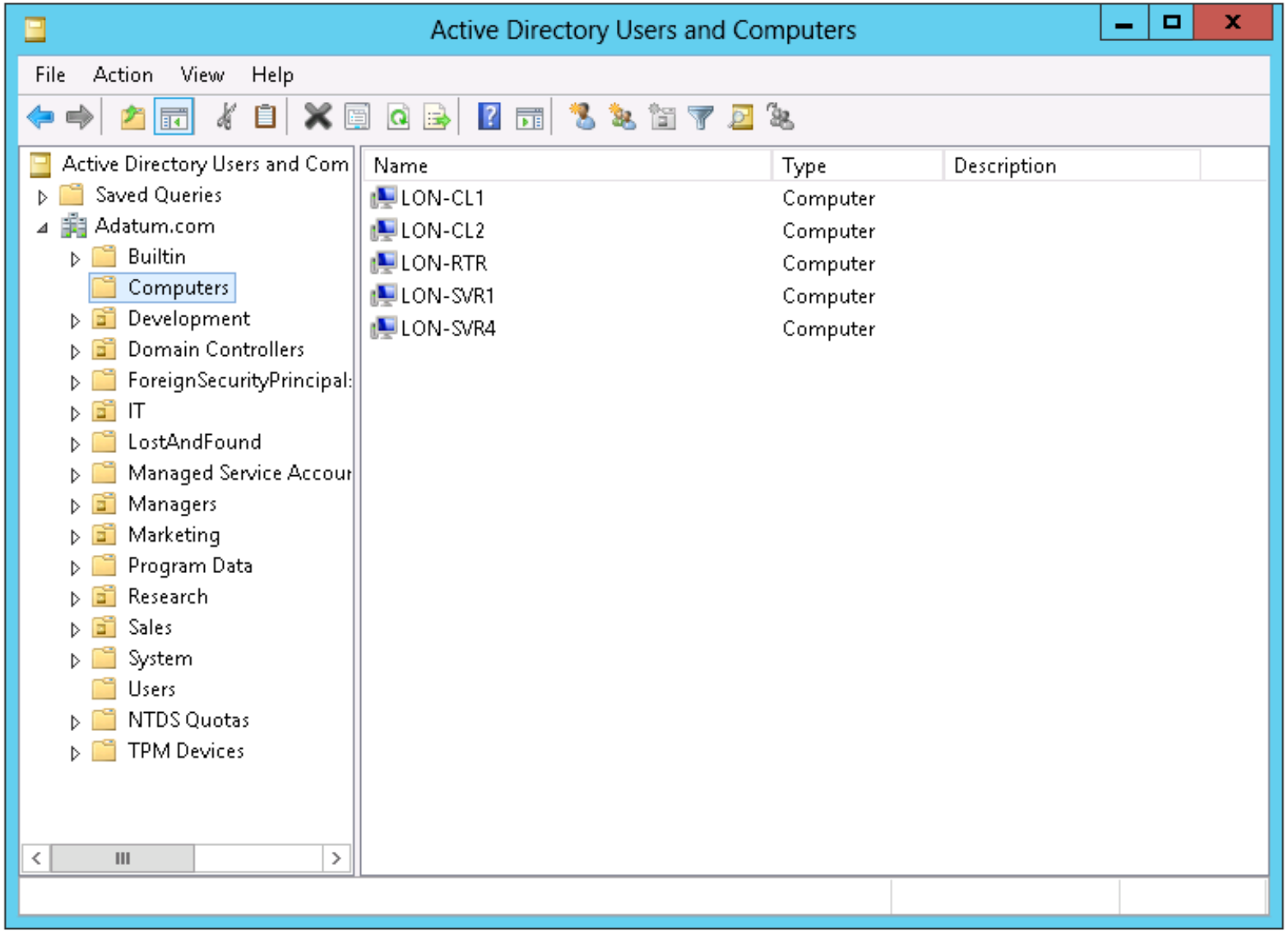
En esta demostración, verá cómo:

- Crear un nuevo grupo
- Agregar miembros al grupo
- Añadir un usuario al grupo
- Cambiar el alcance y el tipo de grupo

3. Gestión de cuentas de equipo

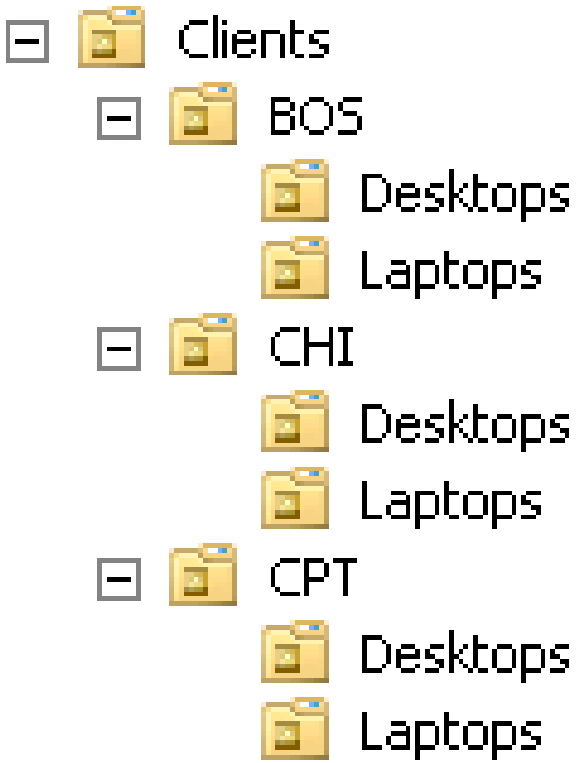
- ¿Qué es el contenedor de Equipos?
- Especificación de la ubicación de cuentas de equipo
- Control de permisos para crear cuentas de equipo
- Cuentas de equipo y canales seguros
- Restablecer el canal seguro

3.1. ¿Qué es el contenedor de Equipos?

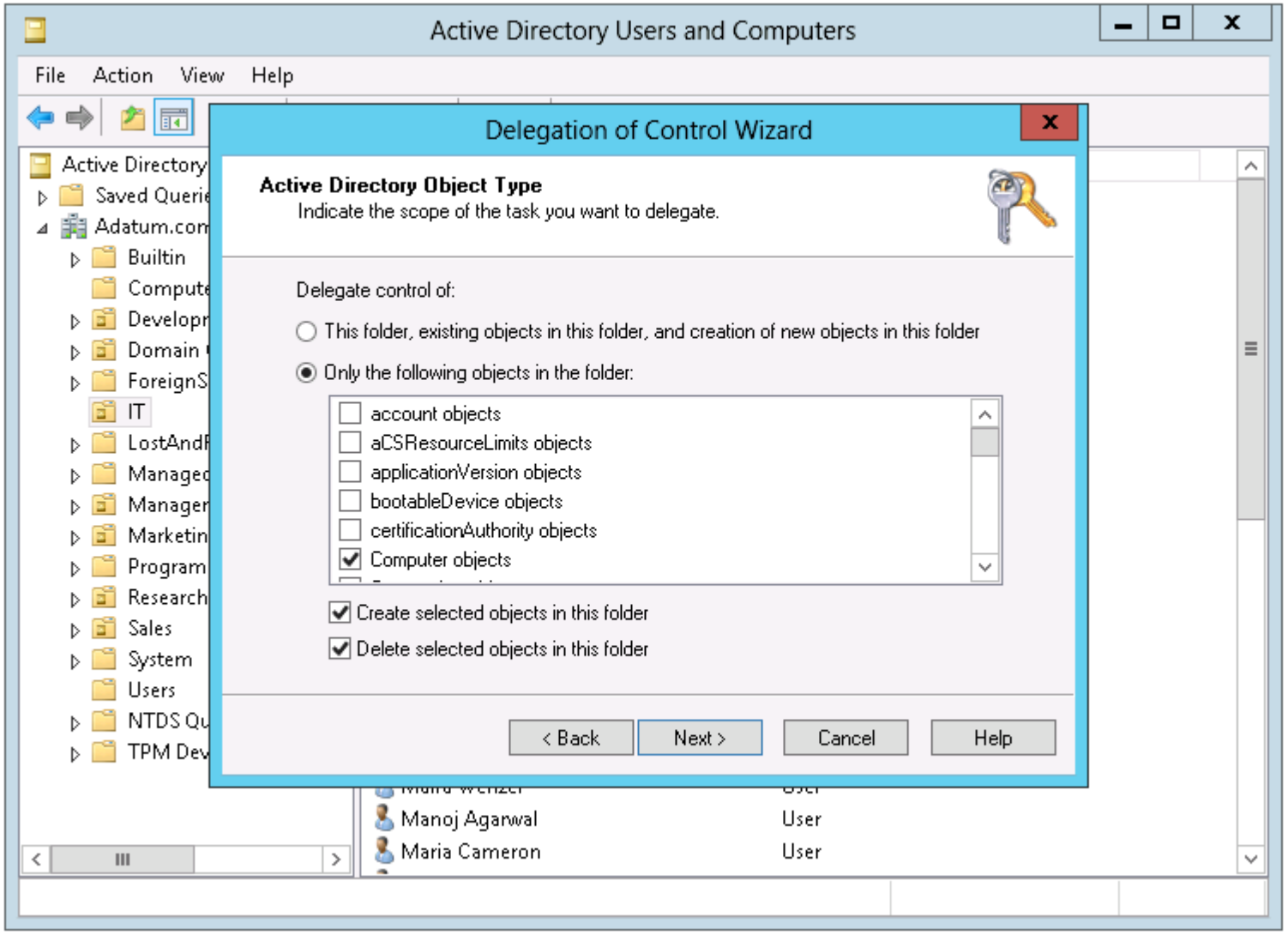


3.2. Especificación de la ubicación de cuentas de equipo

- La mejor práctica es crear unidades organizativas para objetos de equipo
  - Servidores
    - Normalmente subdividido por rol de servidor
  - Equipos Clientes
    - Normalmente subdivididos por región
- Divida las unidades organizativas :
  - Por administración
  - Para facilitar la configuración de directiva de grupo



3.3. Control de permisos para crear cuentas de equipo



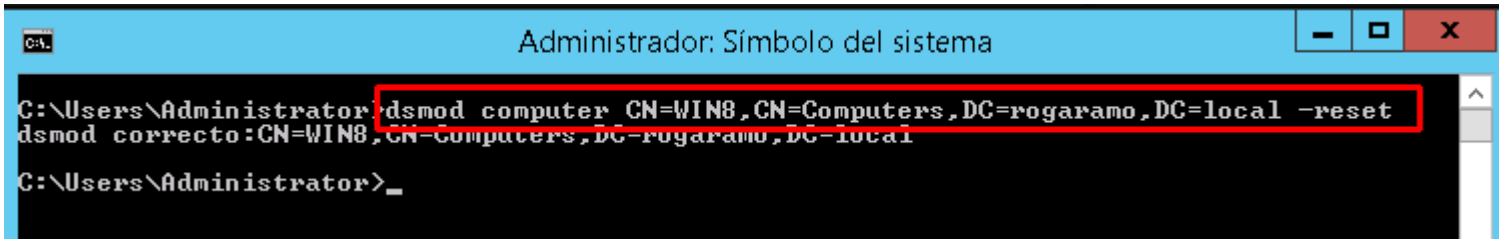
3.4. Cuentas de equipo y canales seguros

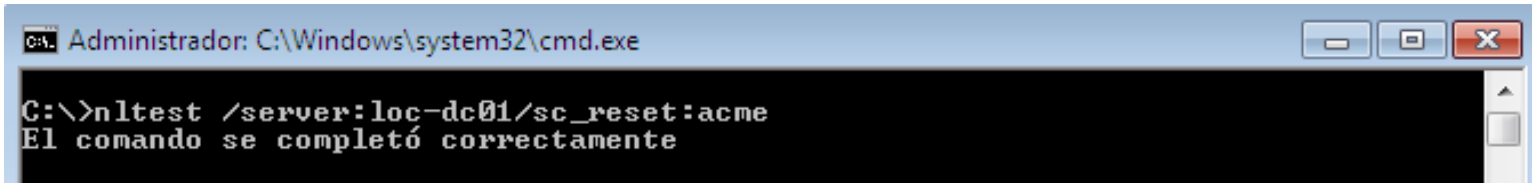
- Los equipos tienen cuentas
  - sAMAccountName y contraseña
  - Se utiliza para crear un canal seguro entre el ordenador y un controlador de dominio
- Escenarios donde un canal seguro puede ser quebrantado
  - Restauración de un equipo desde una copia de seguridad antigua, o reversión de un equipo a una imagen anterior
  - Restauración del controlador de dominio (si fuese el único).
  - Equipo y Dominio no están de acuerdo sobre cual es la contraseña

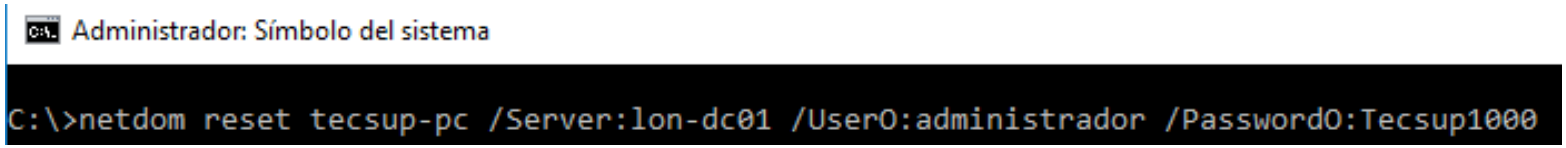
3.5. Restablecer el canal seguro

- No elimine un equipo del dominio y simplemente trate de volver a unirlo.
  - Crea una nueva cuenta: nuevo SID, la pertenencia a grupos se pierde
- Opciones para restablecer el canal seguro
  - Usuarios y equipos de Active Directory
  - DSMod
  - NetDom (Desde el DC)
  - NLTest (Desde el cliente)
  - Windows PowerShell

3.5. Restablecer el canal seguro (cont.)







Bibliografía

- VanJones, M & Deman , T & Elmale, F. & Desfarges, G (2018) Windows Server 2016 Administración avanzada. Barcelona: Ediciones ENI
- Carretero Pérez, Jesús (2001). Sistemas operativos. Una visión aplicada. Madrid: Mc Graw-Hill (005.43/C28)
- Charte Ojeda, Francisco (2008). Windows Server 2008. Madrid: Anaya Multimedia (005.43WI/C525)
- Raya Gonzalez, Laura. (2005).Sistemasoperativos en entorno monousuarios y multiusuarios . México D.F.: Alfaomega (005.43/R28R)

FIN DE LA UNIDAD

TECSUP
Pasión por la Tecnología

Próxima Sesión:

Automatización de Administración de Servicios de Dominio de Active Directory

Administración de Sistemas Operativos