Conceptos básicos

Cuenta de usuario

Es un objeto que posibilita el acceso a los recursos del dominio. No siempre representan a personas concretas, ya que pueden ser usadas como mecanismos de acceso a servicios, aplicaciones o un equipo remoto.

Las cuentas de usuario también pueden identificarse como entidades de seguridad

Las cuentas de usuario pueden posibilitar el acceso a los recursos de dos modos distintos:

- Permite **autenticar la identidad** de un usuario gracias al usuario y la contraseña
- Permite **autorizar o denegar el acceso** a los recursos de un dominio, ya que cada usuario tendrá acceso a los recursos de los que tiene permisos.

Cada cuenta de usuario tiene un identificador de seguridad único en el dominio (SID, Security IDentifier).

Por razones de seguridad, debemos evitar que varios usuarios usen la misma cuenta para iniciar sesión en el dominio.

Cuentas integradas

Cuando se crea el dominio se crean dos cuentas: “Administrador” e “Invitado”. Luego, cuando se necesita, se crea la cuenta “Asistente de ayuda”. Estas cuentas son las cuentas integradas y disponen de permisos predefinidos:

- **Administrador**: Control total sobre el dominio y no se puede eliminar ni retirar del grupo “Administradores”, pero podemos cambiarle el nombre o deshabilitarla.
- **Invitado**: De forma predeterminada viene deshabilitada y, aunque no se recomienda, se puede habilitar para permitir el acceso a usuarios que aún no tienen cuenta o que la tienen deshabilitada, por ejemplo. De forma predeterminada no tiene contraseña, pero el administrador puede agregar una.
- **Asistente de ayuda**: Se usa para iniciar sesiones de Asistencia remota y tiene acceso limitado al equipo. Se crea automáticamente cuando se solicita una sesión de asistencia remota, y se elimina cuando ya no hay solicitudes de este tipo.

Aunque la cuenta Administrador esté deshabilitada, podrá seguir usándose para acceder al controlador de dominio en modo seguro.

Desde el punto de vista de la seguridad, puede ser interesante cambiar el nombre de la cuenta Administrador

Cuenta de equipo

Igual que las cuentas de usuario, una cuenta de equipo sirve para autenticar a los equipos que se conectan al dominio permitiendo o denegando el acceso a los recursos.

Del mismo modo que las cuentas de usuario, las cuentas de equipo deben ser únicas en el dominio. Aunque una cuenta de equipo se puede crear manualmente, también se puede crear cuando el equipo se une al dominio.

Los sistemas Windows anteriores a XP no pueden disponer de cuentas de equipo, ya que estos sistemas carecen de características de seguridad avanzadas.

Cuenta de grupo

Un grupo es un conjunto de objetos que pueden administrarse como un todo. Puede estar formado por cuentas de usuario, cuentas de equipo, contactos y otros grupos.

Cuando una cuenta de usuario o de equipo está incluida en un grupo se dice que es “miembro del grupo”.

Los grupos pueden usarse para facilitar tareas como:

- **Simplificar la administración**: Podemos asignar permisos al grupo y afectarán a todos sus miembros.
- **Delegar la administración**: Se puede usar la directiva de grupo para asignar derechos de usuario una vez y, luego, agregar los usuarios a los que queramos delegar esos derechos.
- **Crear listas de distribución de correo electrónico**: Solo se usan con los grupos de distribución.

El Directorio Activo proporciona un conjunto de grupos predefinidos que pueden usarse para facilitar el control de acceso a recursos y para delegar roles administrativos. Por ejemplo, el grupo “Operadores de copias de seguridad” permite a sus miembros hacer copias de seguridad de todos los controladores de dominio en el dominio al que pertenecen.

Ámbito de los grupos

El ámbito de un grupo establece su alcance (en qué partes de la red puede usarse) y el tipo de cuentas que pueden formar parte de él. Pueden pertenecer a una de estas categorías:

- Ámbito local: Entre sus miembros pueden encontrarse uno o varios de estos objetos:
    - Cuentas de usuario o equipo
    - Otros grupos de ámbito local
    - Grupos de ámbito global
    - Grupos de ámbito universal

Las cuentas o grupos contenidos tendrán necesidades de acceso parecidas dentro del propio dominio.

- Ámbito global: Sólo incluyen otros grupos y cuentas que pertenezcan al dominio en el que esté definido el propio grupo. Los miembros de este tipo de grupos pueden tener permisos sobre los recursos de cualquier dominio dentro del bosque. Sin embargo, estos grupos no se replican fuera de su dominio, por lo que la asignación de derechos que alberguen no serán válidas en otros dominios del bosque.

  Los grupos de ámbito global son perfectos para contener objetos que se modifican mucho, ya que como no se replican fuera del dominio no generan tráfico en la red

- Ámbito universal: Entre sus miembros pueden encontrarse cuentas o grupos de cualquier dominio del bosque, a los que se le pueden asignar permisos sobre los recursos sobre cualquier dominio del bosque.

Tipos de grupos

Existen dos tipos de grupos en Active Directory:

- Grupos de distribución: Se usan junto con programas como Microsoft Exchange Server para crear listas de distribución de correo electrónico. Estos grupos no tienen características de seguridad, por lo que no pueden aparecer en las listas de control de acceso discrecional (DACL, Discretionary Access Control Lists)
- Grupos de seguridad: Permiten asignar permisos a las cuentas de usuario, equipo y grupos sobre recursos compartidos. Con los grupos de seguridad podemos:
  - Asignar derechos de usuario a los grupos de seguridad del Directorio Activo: De esta forma podemos establecer qué acciones pueden hacer sus miembros dentro de un dominio o del bosque.
  - Asignar permisos para recursos a los grupos de seguridad: Nos permite definir quién accede a cada recurso y bajo qué condiciones (control total, sólo lectura…). También establecen permisos de forma predeterminada sobre objetos del dominio para ofrecer distintos niveles de acceso.

Grupos integrados

Durante la instalación del Directorio Activo, se crean grupos de seguridad predeterminados que facilitan la delegación de ciertos aspectos de la administración en otros usuarios del sistema.

Los grupos se administran con el complemento “Usuarios y equipos de Active Directory”. Cuando ejecutemos esta herramienta, encontraremos los grupos predeterminados en dos contenedores.

Los grupos predeterminados incluidos en el grupo “Builtin” tienen un ámbito local.

En el contenedor “Users” podemos encontrar grupos predeterminados que tienen tanto ámbito local como global.

Los grupos de ambos contenedores pueden cambiarse de contenedor libremente, siempre que se mantengan dentro del mismo dominio. Los grupos ubicados en estos contenedores se pueden mover a otros grupos o unidades organizativas (OU) del dominio, pero no se pueden mover a otros dominios.

Debemos conocer los privilegios y derechos que ofrece cada grupo predeterminado a sus miembros antes de asignarle una cuenta de usuario o equipo

Crear cuentas de usuario

Las cuentas de usuario se crean desde la herramienta “Usuarios y equipos de Active Directory”, a la cual se puede acceder de varias formas:

- Desde el menú Herramientas del Administrador del Servidor
- Desde Ejecutar, escribiendo la orden dsa.msc
- Desde la consola “Herramientas comunes” si está creada.

Al crearlas, obtendremos la ventana “Nuevo Objeto: Usuario”, donde tendremos que rellenar los datos del usuario:

- Nombre de pila
- Apellidos
- Iniciales
- Nombre de inicio de sesión del usuario: Compuesto de dos partes, el propio nombre y el sufijo (elegido de una lista desplegable)
- Nombre de inicio de sesión de usuario (anterior a Windows 2000): Su objetivo es que se conecten al dominio clientes que usen Windows 95, 98 o NT.

Tras esto, debemos escribir la contraseña, que debe cumplir los siguientes requisitos:

- No puede contener el nombre de la cuenta ni el nombre completo del usuario.
- Debe contener tres de estos requisitos:
    - Mayúsculas de los idiomas europeos (incluye marcas diacríticas y caracteres griegos y cirílicos)
    - Minúsculas de los idiomas europeos(incluye marcas diacríticas y caracteres griegos y cirílicos)
    - Dígitos en base 10 (0 a 9)
    - Caracteres especiales (no se incluyen los símbolos de moneda como € o £)
    - Caracteres alfabéticos Unicode que no se clasifican como mayúsculas o minúsculas, como los caracteres asiáticos

  8 caracteres.

Además, en la parte inferior de la ventana hay cuatro opciones:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión (opción por defecto): Si marcamos esta opción, nos aseguramos de que sólo el usuario conoce su contraseña
- El usuario no puede cambiar la contraseña: Puede resultar interesante para que el administrador mantenga el control total sobre alguna cuenta temporal o de invitado
- La contraseña nunca expira: Hace que la contraseña no caduque en el plazo que establece el sistema operativo. Microsoft la recomienda para las cuentas de servicio, además de usar contraseñas seguras.
- La cuenta está deshabilitada: Mientras esté activada, no se podrá iniciar sesión en el sistema

Modificar valores de las cuentas de usuario

Para modificar cuentas de usuario, debemos hacer clic derecho sobre la cuenta en cuestión y escoger “Propiedades”.

De forma predeterminada, encontraremos la solapa General, que contiene los datos introducidos en la creación de la cuenta junto con otros datos complementarios, como una Descripción, Número de teléfono…

Hay un total de 13 solapas diferentes, pero una de las más interesantes es “Cuenta”. En ella podemos cambiar los nombres de inicio de sesión del usuario (el único valor imprescindible es el SID)

También podemos cambiar las opciones de la cuenta, aunque ahora disponemos de algunas opciones más:

- Almacenar contraseñas usando cifrado reversible: Solo se usa cuando la cuenta de usuario usará un cliente Apple para iniciar sesión en el dominio.
- La tarjeta inteligente es necesaria para un inicio de sesión interactivo: Sólo se usa en entornos donde los clientes tienen un lector de tarjetas y los usuarios un Número de Identificación Personal asociado (PIN). En estos casos, la contraseña se establece automáticamente con un valor complejo y aleatorio.
- La cuenta es importante y no se puede degradar: Esta opción permite el control sobre una cuenta de usuario, como una de invitado o temporal. Se puede usar cuando la cuenta no puede usarse por otra para delegar sobre ella.
- Usar tipos de cifrado DES de kerberos para esta cuenta: Habilita la compatibilidad con el estándar de cifrado de datos (DES)
- Esta cuenta admite cifrado AES de Kerberos de 128 y 256 bits: Estas opciones sólo estarán disponibles si el nivel de funcionalidad del dominio es WS 2008 (incluido R2) o WS 2003
- No pedir la autenticación Kerberos previa: Ofrece compatibilidad con implementaciones alternativas al protocolo Kerberos. Habilitar esta opción puede suponer una pérdida de seguridad en el sistema.

También podemos establecer una caducidad para la cuenta. Normalmente este valor estará en Nunca, pero puede ser útil para una cuenta que se usará por tiempo limitado, como para trabajadores temporales. Se establece una fecha para que la cuenta se deshabilite automáticamente.

Establecer horas de inicio de sesión

Dentro de la ventana Propiedades de la cuenta, dentro de la solapa Cuenta está el botón “Horas de inicio de sesión”

Se mostrará una tabla con las 24 horas del día y los 7 días de la semana. De forma predeterminada todas las casillas estarán marcadas en azul, por lo que se podrá iniciar sesión a cualquier hora.

- Para seleccionar una hora específica, debemos hacer clic a la casilla que la representa
- Para seleccionar una franja, podemos hacer clic en una esquina y llegar a la otra sin soltar el clic
- Para seleccionar un día entero, podemos hacer clic en el nombre del día.
- Para hacer un intervalo de varios días consecutivos, arrastramos el clic entre los días que queramos
- Para seleccionar toda la matriz a la vez, podemos pulsar el botón Todo (encima de Lunes).
- Para seleccionar una hora, pero todos los días, pulsamos su botón en la parte superior
- Para seleccionar un grupo de horas consecutivas todos los días, arrastramos desde la primera hora hasta la última (o al revés)

Cuando seleccionamos celdas de la matriz, debajo de ella aparecerá un mensaje que nos indica textualmente la selección que hemos hecho

Cuando queramos deshabilitar las horas que tengamos seleccionadas, pulsaremos la opción “Inicio de sesión denegado” de la parte derecha. Si queremos habilitarlas, pulsaremos la opción “Inicio de sesión permitido”.

Limitar los equipos desde los que un usuario puede iniciar sesión

También desde la solapa “Cuenta” dentro de Propiedades de la cuenta, escogeremos el botón “Iniciar sesión en…”

De forma predeterminada, el usuario podrá iniciar sesión en todos los equipos de la red. Si seleccionamos la opción “Los siguientes equipos” y, después, “Nombre de equipo”, podremos indicar el nombre de la cuenta del primer equipo desde el que el usuario podrá iniciar sesión en el dominio.

Después pulsaremos Agregar y el nombre del equipo aparecerá en un cuadro, que nos indicará los equipos en los que se puede iniciar sesión con la cuenta de usuario que estemos administrando.

Averiguar de qué grupos es miembro un usuario

Para ver esto, debemos ir a las Propiedades de la cuenta de usuario que queramos y acceder a la solapa “Miembro de”

Administrar cuentas de equipo

Crear una cuenta de equipo

Cuando localicemos el contenedor que nos interese, haremos clic derecho sobre él y seleccionaremos Nuevo > Equipo.

Aparecerá la ventana “Nuevo objeto: Equipo”, donde rellenaremos el Nombre de equipo. Esta es la única información que es obligatoria de ofrecer.

Automáticamente se completará el campo Nombre del equipo (anterior a Windows 2000) con los 15 primeros caracteres del Nombre de equipo. Este será el nombre NetBIOS de la cuenta y las minúsculas se convertirán en mayúsculas.

Si el cliente usará Windows 95, 98 o NT debemos marcar la opción “Asignar la cuenta de este equipo como un equipo anterior a Windows 2000”

Suele ser buena idea mantener las cuentas de equipo en una Unidad Organizativa diferente a la de las cuentas de dominio, ya que simplificaremos la aplicación de Políticas de grupo cuando se necesite

Modificar valores en las cuentas de los equipos

Debemos hacer clic derecho sobre la cuenta y escoger Propiedades. En las cuentas de equipo, las características se organizan en 7 solapas diferentes.

Restablecer cuentas de equipo

Uno de los motivos por los que no podemos iniciar sesión en el dominio aunque escribamos bien los datos puede ocurrir porque se haya desincronizado la contraseña que introducimos con la almacenada en la Autoridad de Seguridad Local (LSA, Local Security Authority).

Para arreglar este problema, haremos clic derecho en la cuenta que esté generando los problemas y seleccionaremos “Restablecer la cuenta”.

Nos aparecerá un cuadro de diálogo para confirmar la acción y, al pulsar “Sí”, la cuenta se habrá restablecido correctamente.

Administrar cuentas de grupo

Un grupo puede actuar como contenedor para cuentas de usuario y de equipos. Además, un grupo puede ser miembro de otro grupo.

Crear una cuenta de grupo

Debemos escoger un contenedor, hacer clic derecho sobre él y luego Nuevo > Grupo.

Dentro de la ventana “Nuevo objeto: Grupo”, rellenaremos el Nombre de grupo para nombrarlo.

Además, el nombre completará el campo “Nombre de grupo (anterior a Windows 2000)” pero, en este caso, no se aplican las restricciones de 15 caracteres y letras mayúsculas.

Modificar valores en las cuentas de los grupos

Debemos hacer clic derecho en la cuenta de grupo que queramos y escoger Propiedades.

Aparecerá la ventana “Propiedades: <nombre de la cuenta de grupo>”, donde dispondremos de multitud de características organizadas en 4 solapas.

En la solapa General se puede cambiar el “Nombre de grupo (anterior a Windows 2000), la Descripción y el correo electrónico donde se recibirán las incidencias relacionadas con el grupo. También se pueden modificar el Ámbito del grupo y el Tipo de grupo.

Desde la solapa Miembros, podemos escoger los usuarios, equipos o grupos que son miembros del grupo que estamos editando.

Desde la solapa “Miembros de” podremos hacer que este grupo sea miembro de otro grupo distinto.

La solapa “Administrado por” nos permite delegar la administración de este grupo en otro usuario diferente.

Añadir miembros a un grupo

Desde Propiedades, debemos ir a la solapa Miembros y pulsar el botón “Agregar”.

Dispondremos de un cuadro de texto, donde podemos indicar el nombre de la cuenta (si lo conocemos). De todas formas, si pulsamos el botón “Opciones Avanzadas” conseguiremos que se abra una ventana con un botón llamado “Buscar ahora”.

Esta ventana se desplazará hacia abajo con todas las cuentas. Podemos agregarlas seleccionándolas y pulsando Aceptar. Además, podemos usar Ctrl y Shift para realizar selecciones múltiples.

Ahora, podremos ver las cuentas que vayan a ser miembros de este grupo en el cuadro de texto anterior. Cuando pulsemos Aceptar, veremos dichas cuentas en la solapa Miembros de la ventana Propiedades.

Los pasos para añadir contactos, equipos y grupos son los mismos

Eliminar miembros de un grupo

Desde la solapa Miembros, elegiremos el usuario que queremos que deje de ser miembro del grupo y pulsaremos el botón Quitar.

Podemos usar Ctrl y Shift para elegir varias cuentas y eliminarlas al mismo tiempo.

Al eliminar una cuenta de la lista de miembros del grupo, no estamos borrando la cuenta, solo le estamos quitando los permisos heredados de dicho grupo.

Operaciones frecuentes con Unidades Organizativas

Las Unidades Organizativas (en inglés, Organizational Units o, simplemente, OUs) son contenedores del Directorio Activo que pueden incluir usuarios, equipos, grupos y otras OUs.

A una Unidad Organizativa podemos otorgarle valores de configuración de directiva de grupo o podemos delegar sobre ella una parte de la autoridad administrativa. Así, un usuario puede tener total libertad de administrar una unidad organizativa específica sin poder administrar el resto.

Crear una Unidad Organizativa

Desde “Usuarios y equipos de Active Directory”, debemos hacer clic derecho sobre el dominio y seleccionar Nuevo > Unidad organizativa.

Si queremos crear una Unidad organizativa dentro de otra Unidad organizativa, debemos hacer clic derecho sobre dicha UO.

A continuación, le daremos nombre a la unidad organizativa. También podremos dejar marcada la opción “Proteger contenedor contra eliminación accidental” para que el sistema no nos permita eliminarla por error.

Desplazar objetos de una ubicación a otra

En ocasiones, debemos cambiar la ubicación de algunos objetos para que el dominio refleje la estructura organizativa que hemos diseñado. Hay dos formas para hacerlo:

Primera Forma

Primero seleccionamos los objetos que queramos mover y haremos clic derecho sobre cualquiera.

Seleccionaremos la opción “Mover”, que contiene todos los posibles lugares a los que podemos mover los objetos seleccionados.

En Windows Server 2019 podemos tener unas Unidades Organizativas dentro de otras. Para encontrarlas puede ser necesario desplegar la rama correspondiente pulsando el botón “+” que hay al lado de algunos contenedores

Seleccionaremos el destino y pulsaremos Aceptar.

También podemos hacer clic sobre cualquier UO en el panel izquierdo y seguir el mismo proceso para trasladarla a otro lugar.

Podemos usar Shift y Ctrl para hacer selecciones múltiples.

Segunda Forma

Primero seleccionaremos los objetos que queramos mover. Luego, los arrastraremos con el ratón a la ubicación deseada.

Al hacerlo, aparecerá un aviso informando que el cambio de sitio de objetos puede alterar el funcionamiento del sistema, como por ejemplo las directivas de grupo que se aplican a los objetos desplazados.

Pulsaremos “Sí” y podremos observar que los objetos se han desplazado correctamente.

Eliminar una Unidad Organizativa

Haremos clic derecho sobre la UO que queramos y pulsaremos la opción “Eliminar”. Nos aparecerá un cuadro de diálogo para confirmar la acción.

Si la casilla “Proteger contenedor contra eliminación accidental” estaba desactivada, la UO se eliminará.

Si esta casilla está marcada, no podremos eliminarla. Para cambiar esto, debemos hacer clic en el menú “Ver” y seleccionar la opción “Características avanzadas”.

Después, volvemos a hacer clic derecho en la UO y escogemos “Propiedades”. Dentro de la solapa “Objeto”, podremos desmarcar la solapa “Proteger contenedor contra eliminación accidental”.

Un último caso que podemos encontrar es que la UO no esté vacía. Cuando esto ocurra, aparecerá una ventana de aviso.

Podremos hacer clic sobre “No” para anular la eliminación o pulsar “Sí” y eliminar todos los objetos que contenga.

Si la Unidad Organizativa contiene otras Unidades Organizativas, debemos elegir “Usar el control de servidor Eliminar subárbol” para eliminarlo todo.

El Centro de Administración de Active Directory

En Windows Server 2008 R2 se incorporó una herramienta llamada “Centro de administración de Active Directory”. Esta herramienta permite administrar los objetos del directorio usando cmdlets de PowerShell ofreciendo una interfaz gráfica para evitar conocer la sintaxis.

El Administrador del servidor facilita el acceso a los diferentes dominios que tengamos en la red, permitiendo centralizar de una forma sencilla la administración de estos objetos.

Para abrir el centro de administración de Active Directory, debemos desplegar el menú Herramientas del Administrador del servidor.

Se abrirá una nueva ventana llamada “Centro de administración de Active Directory” con varios paneles: el izquierdo muestra las diferentes categorías y el derecho un acceso sencillo a mucha información sobre el funcionamiento del Centro de administración de Active Directory. Además hay un panel central.

Para acceder a los objetos del dominio, debemos hacer clic sobre ellos en el panel izquierdo. Al hacerlo, aparecerán las categorías usadas recientemente.

En la parte inferior de la ventana se puede leer “HISTORIAL DE WINDOWS POWERSHELL” y, a la derecha, un botón que apunta hacia arriba. Si lo seleccionamos, tendremos acceso a los cmdlets que ha aplicado el “Centro de administración de Active Directory” para realizar las tareas que le indiquemos.

Para crear nuevas cuentas de usuario, grupo o equipo, debemos hacer clic derecho en cualquier espacio libre del panel central y escoger Nuevo > “cuenta que queramos”

Así, aparecerá un formulario vacío que debemos rellenar con los datos de las cuentas. A diferencia de lo que ocurría en “Usuarios y equipos de Active Directory”, aquí podemos indicar desde el principio todos los datos de la cuenta.