
UD04

Usuarios, equipos y grupos



Índice

- [Introducción.](#)
- [Cuenta de usuario.](#)
 - [Cuentas integradas.](#)
- [Cuenta de equipo.](#)
- [Cuenta de grupo.](#)
 - [Grupos integrados.](#)
 - [Ámbito de los grupos.](#)
 - [Grupos locales.](#)
 - [Grupos globales.](#)
 - [Grupos universales.](#)
 - [Tipos de grupos.](#)
 - [Grupos de seguridad.](#)
 - [Grupos de distribución.](#)



Introducción



Introducción



- El **objetivo** final de una infraestructura de red es **administrar recursos** presentes en la misma, es decir, el **control y administración** de los **usuarios, equipos y grupos**.
- Por ello, **aprenderemos a**
 - **Crearlos.**
 - **Modificarlos.**
 - **Organizarlos.**
 - **Eliminarlos.**
- Además, deberemos **asignar privilegios** para cada uno de ellos, de modo que podamos establecer en qué medida y bajo qué condiciones podrán **beneficiarse de los recursos de la red**.
- Por eso, lo primero será dominar algunos **conceptos básicos**, como son:
 - **Cuenta de usuario.**
 - **Cuenta de equipo.**
 - **Cuenta de grupo.**



Cuenta de usuario



Cuenta de usuario



- Una cuenta de **usuario de un dominio** no tiene porque representar a **personas concretas**.
- Una cuenta de usuario, en el sentido más amplio, es un **mecanismo de acceso a determinados servicios o aplicaciones** de la máquina **local** o en un equipo **remoto**.
- Dentro de **Active Directory**, una cuenta de usuario es un **objeto que posibilita el acceso a los recursos del dominio**, ya que:
 - **Permite autenticar la identidad de un usuario**: sólo podrán **iniciar sesión** aquellos usuarios que dispongan de una cuenta en el sistema.
 - **Permite autorizar, o denegar, el acceso a los recursos del dominio**: una vez iniciada la sesión sólo se tendrá **acceso a los recursos** para los que haya recibido los permisos correspondientes.
- Cada **cuenta de usuario** dispone de un **identificador de seguridad (SID, Security IDentifier)** que es **único en el dominio**. Por ello, las cuentas de usuario **también** suelen denominarse **entidades de seguridad**.



Cuenta de usuario

Cuentas integradas

- Llamamos **cuentas integradas** a las cuentas de usuario:
 - **Administrador.**
 - **Invitado.**
 - **Asistente de ayuda.**
- Las cuentas **Administrador e Invitado** se crean automáticamente **durante** el proceso de **instalación del dominio**.
- La cuenta **Asistente de Ayuda** se crea automáticamente **cuando se solicita una sesión de asistencia remota** y se **elimina cuando ya no existen solicitudes** de asistencia **pendientes** de satisfacer.
- Como es lógico, estas **cuentas integradas** disponen de una serie de **derechos y permisos**, que exponemos a continuación:



Cuenta de usuario

Cuentas integradas

- **Administrador:**
 - Tiene **control total** sobre el dominio.
 - Podremos **cambiarle el nombre**.
 - Podremos **deshabilitarla** pero, aunque esté deshabilitada, podrá seguir usándose para acceder a **controlador dominio en modo seguro**
 - **No** se podrá **eliminar ni retirar** del **grupo** Administradores.
- **Invitado:**
 - Está **deshabilitada** de forma **predeterminada**.
 - Se crea para permitir el **acceso a los usuarios que aún no tienen cuenta** en el sistema **o** que la **tienen deshabilitada**.
 - De forma **predeterminada no requiere contraseña**, aunque esto se puede modificar por el administrador.
 - Permitir el **acceso a usuarios de forma no controlada** es una **falla de seguridad**, por lo que no se recomienda que se habilite.
- **Asistente de ayuda:**
 - **Acceso limitado** al equipo mientras tiene lugar la **asistencia remota**.



Cuenta de equipo





Cuenta de equipo

- Como ocurre con las cuentas de usuario, una **cuenta de equipo de un dominio** sirve para **autenticar** a los diferentes **equipos que se conectan al dominio**, permitiendo o denegando su acceso a los diferentes recursos del dominio.
- Del mismo modo que con las cuentas de usuario, las cuentas de equipo deben **ser únicas en el dominio**.
- Las cuentas de equipo **se pueden crear**:
 - De forma **automática** cuando un **equipo se une a un dominio**, tal como vimos en la unidad anterior.
 - De forma **manual**, como veremos en esta unidad.

Curiosidad: los sistemas de escritorio **Windows** que sean **anteriores a XP** no pueden disponer de **cuentas de equipo en un dominio** Windows Server 2019. El motivo es que estos sistemas **carecen** de características de **seguridad avanzadas** exigidas.



Cuenta de grupo





Cuenta de grupo

- Un **grupo en un dominio** es un **conjunto de objetos** del dominio. Puede estar **formado** por:
 - Cuentas de **usuario**.
 - Cuentas de **equipo**.
 - **Contactos**.
 - Otros **grupos**.
- La ventaja de utilizar grupos es que pueden **gestionarse como un todo** y **facilitar** algunas tareas como:
 - **Simplificar la administración**: Podemos **asignar permisos** al **grupo** y estos afectarán a todos sus **miembros**.
 - **Delegar la administración**: Podemos utilizar la **directiva de grupo para asignar derechos** a un grupo para administrar un conjunto de objetos y, **más tarde, agregar** al grupo aquel usuario o usuarios a los que queramos **delegar la administración de esos objetos**.
 - **Crear listas de distribución de correo electrónico**: Sólo se utilizan con los **grupos de distribución**.



Cuenta de grupo

Grupos integrados

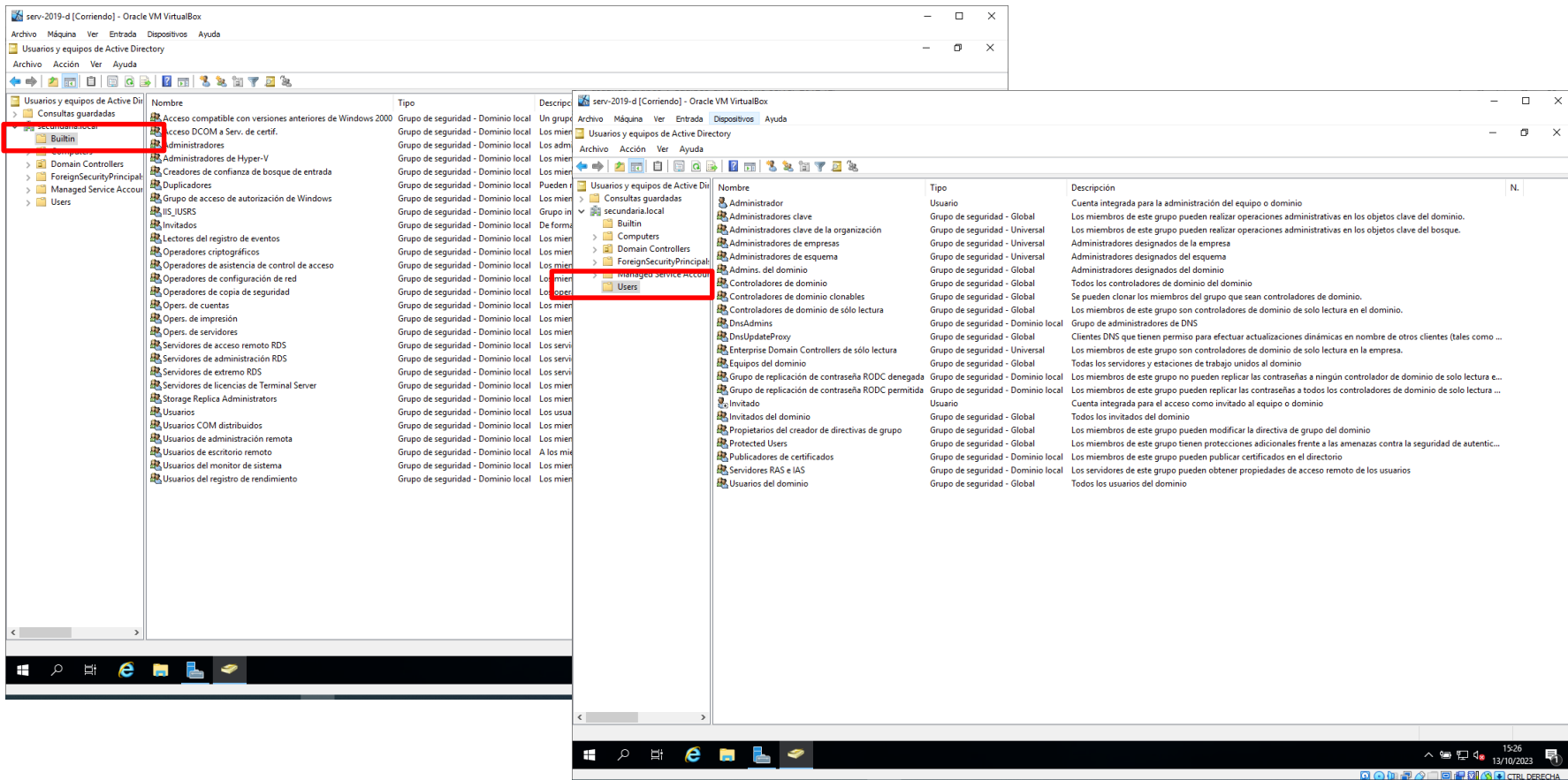
- De modo similar a las cuentas integradas, **durante el proceso de instalación del dominio**, se crean en Active Directorio un conjunto de **grupos predefinidos** que pueden utilizarse tanto para **facilitar el control de acceso a los recursos** como para **delegar determinados roles administrativos**. Por **ejemplo**:
 - **Grupo Operadores de copia de seguridad**: permite a sus **miembros** realizar **copias de seguridad de todos los controladores** de dominio, en el dominio al que **pertenecen**.
 - **Grupo Operadores de configuración de red**: permite a sus **miembros** **cambiar la configuración TCP/IP** en los **controladores** de dominio, en el dominio al que **pertenecen**.
- Los grupos integrados **se pueden mover a otros grupos o unidades organizativas (OU) del dominio**, pero **no se pueden mover a otros dominios**.

Cuenta de grupo

Grupos integrados



- Los grupos integrados se gestionan en la herramienta “Usuarios y equipos de Active Directory”, dentro de los contenedores “Builtin” e “Users”, tal como se muestra en las siguientes imágenes:





Cuenta de grupo

Ámbito de los grupos

- El **ámbito** de un grupo establece su **alcance**, es decir:
 - En **qué partes** de la red puede **utilizarse**.
 - El **tipo de cuentas** que pueden **formar** parte de él.
- Se distinguen **tres clases diferentes** en relación al ámbito de actuación:
 - Grupos **locales**.
 - Grupos **globales**.
 - Grupos **universales**.



Cuenta de grupo

Ámbito de los grupos. Grupos locales

- **Grupos locales:**
 - Estos grupos se **definen en un dominio y no se replican fuera de su propio dominio**. Esto quiere decir que **solo podemos ver** este grupo dentro del **dominio** en el que ha sido **definido**.
 - La asignación de **derechos y permisos** que alberguen, **sólo** serán válidas en el **dominio donde han sido definidos**, por tanto, su alcance son los **recursos del propio dominio**.
 - **No será posible darle permisos** sobre recursos de **otros dominios** del bosque.
 - Grupo **idóneo** para integrar miembros con **necesidades** de acceso **similares dentro** del propio **dominio**. Por ejemplo, acceso a impresora
 - Un grupo de ámbito local puede contener **uno o varios** de los siguientes tipos de **objetos**:
 - **Cuentas de usuario o equipo.**
 - **Otros grupos locales.**
 - **Grupos globales.**
 - **Grupos universales.**



Cuenta de grupo

Ámbito de los grupos. Grupos globales

- **Grupos globales:**
 - Igual que los grupos locales, se **definen en un dominio, y no se replican fuera de su propio dominio** y, por tanto, **solo podemos verlos dentro del dominio en el que ha sido definido**.
 - La asignación de **derechos y permisos** que alberguen, **sólo serán válidas en el dominio donde han sido definidos**.
 - Pero, a **diferencia** de los grupos **locales**, los **miembros** de este tipo de grupos **sí pueden tener permisos** sobre los **recursos de cualquier dominio** dentro del bosque.
 - Es el tipo de **grupo ideal** para contener **objetos** que se **modifican con frecuencia**, ya que **no generarán tráfico de red por la replicación de los cambios** con los controladores de otros dominios.
 - Un grupo de ámbito global **sólo** puede incluir **otros grupos y cuentas** que **pertenezcan al dominio en el que esté definido** el propio grupo.



Cuenta de grupo

Ámbito de los grupos. Grupos universales

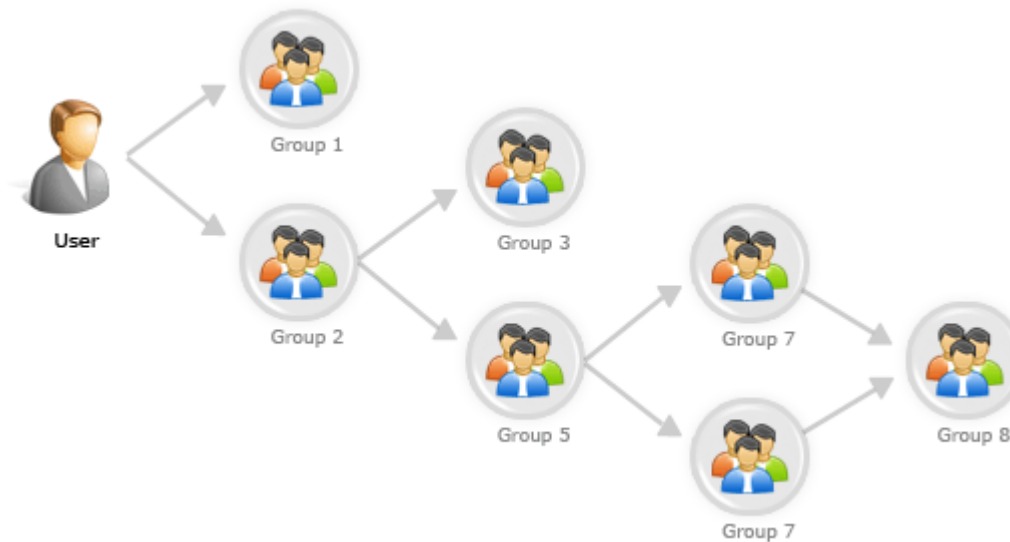
- **Grupos universales:**
 - Estos grupos se **definen en un dominio** pero se replican a todos los dominios del bosque.
 - Por tanto, los grupos universales **son vistos en todos los dominios** del bosque.
 - A los **miembros** se les pueden asignar **permisos** sobre los **recursos de cualquier dominio del bosque**.
 - Entre sus **miembros** pueden encontrarse **cuentas o grupos** de cualquier dominio del bosque.



Cuenta de grupo

Tipos de grupos

- Existen **dos tipos** de grupos en Active Directory:
 - Grupos de **seguridad**.
 - Grupos de **distribución**.





Cuenta de grupo

Tipos de grupos. Grupos de seguridad

- **Grupos de seguridad:** Permiten **asignar permisos** a cuentas de **usuario**, de **equipo** y **grupos** sobre los **recursos compartidos**. Podemos:
 - **Asignar derechos de usuario a grupos de seguridad de AD:**
 - Establecer **qué acciones** pueden llevar a cabo sus **miembros dentro del dominio** (o del bosque).
 - Durante la **instalación** del dominio, se crean **grupos de seguridad predeterminados** (**grupos integrados**) que **facilitan** al administrador la **delegación** de ciertos **aspectos** de la **administración en otros usuarios** del sistema.
 - **Asignar permisos para recursos a los grupos de seguridad:**
 - Permite definir **quién accede** a cada recurso y bajo **qué condiciones** (control total, sólo lectura, etc.)
 - También se establecen **permisos de forma predeterminada sobre diferentes objetos del dominio** para ofrecer distintos niveles de acceso (Grupos integrados).



Cuenta de grupo

Tipos de grupos. Grupos de distribución

- **Grupos de distribución:**
 - Se utilizan en combinación **con programas como Microsoft Exchange Server**, para crear **listas** de distribución de **correo electrónico**.
 - Estos grupos no **disponen de características de seguridad**, por lo que **no** pueden aparecer en las **listas de control de acceso discrecional** (DACL, Discretionary Access Control Lists).