

UD 07_03 – Administración centralizada de redes con Windows Server 2016

Administración de usuario y grupos. Unidades Organizativas.

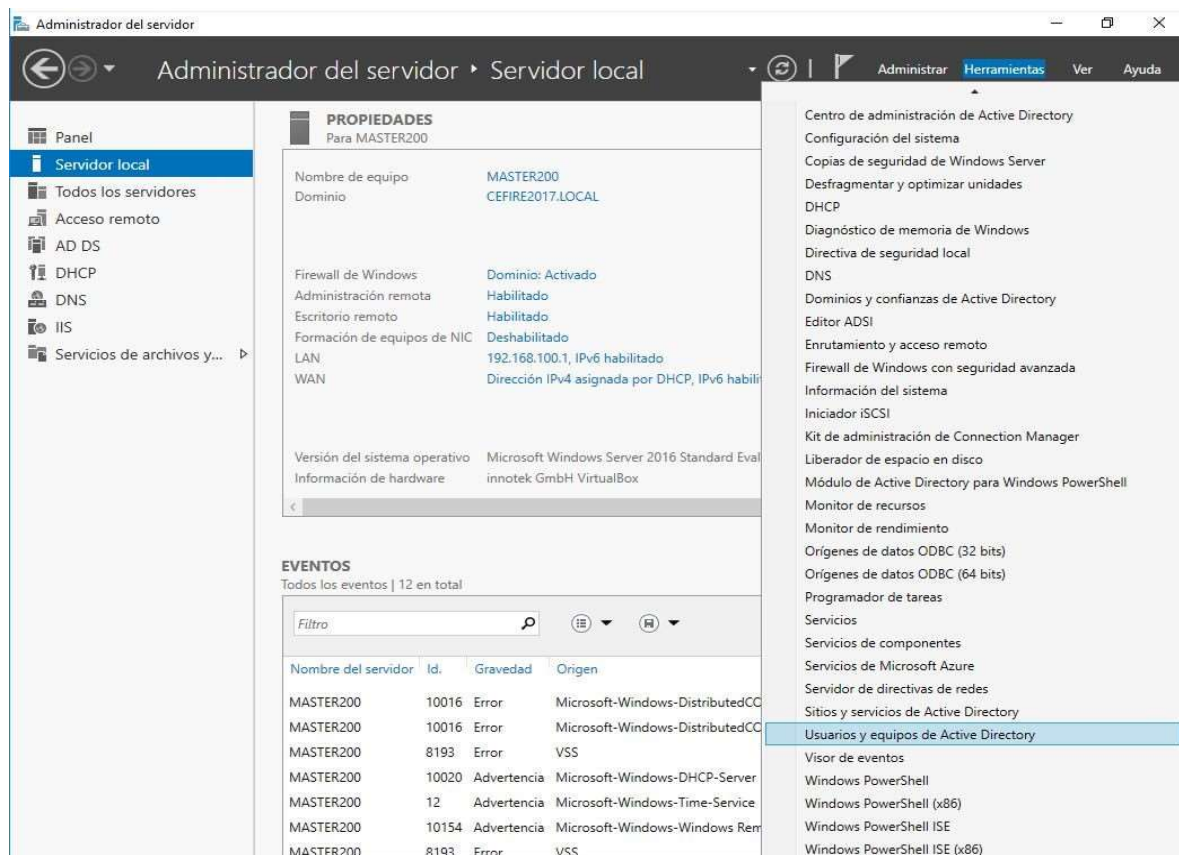
(Del curso “Administración centralizada de redes con Windows Server 2016” del profesor Alberto Aparicio Vila)

Contenido

| | |
|---|-----------|
| Creación de usuarios | 2 |
| Eliminación y deshabilitación de usuarios..... | 5 |
| Deshabilitar cuentas | 6 |
| Configuración de la cuenta de usuario..... | 7 |
| Configuración de inicio de sesión..... | 7 |
| Creación de grupos | 9 |
| Grupos predefinidos | 10 |
| Creación de grupos | 12 |
| Añadir usuarios a grupos | 13 |
| Unidades Organizativas | 16 |
| Creación de Unidades Organizativas | 16 |
| Borrar una OU | 19 |
| Actividades tema 3 | 20 |
| Actividad 3.1..... | 20 |
| Actividad 3.2..... | 21 |

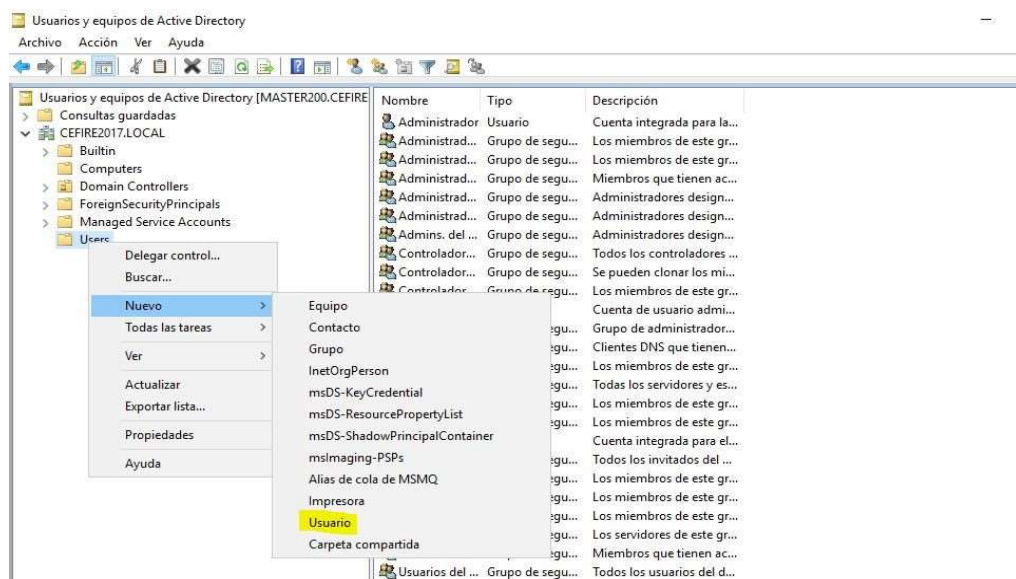
Creación de usuarios

Los usuarios del dominio deben tener una cuenta para poder acceder a los recursos del mismo tras su autenticación frente al controlador de dominio. Para **crear una cuenta de usuario** mediante la interfaz gráfica accederemos a **la herramienta 'Usuarios y equipos de Active Directory' desde el Panel del Administrador --> Herramientas:**



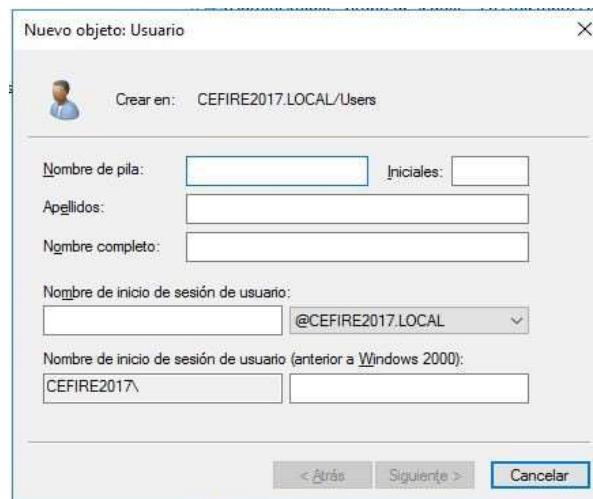
Usuarios y equipos de AD

Una vez abierto el administrador de 'Usuarios y equipos de Active Directory', se hace clic con el **botón derecho sobre 'Users'** y en el menú que aparece, se selecciona 'Nuevo' y a continuación 'Usuario':



Nuevo usuario

Nos aparece el asistente para la creación del nuevo usuario:

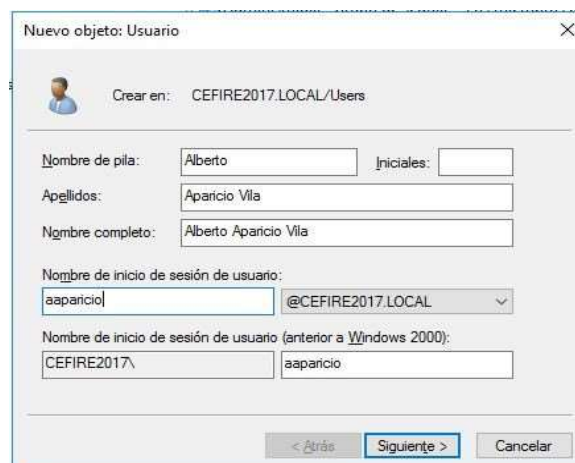


Creación de nuevo usuario

Normas de creación de usuarios

Como normas generales al crear un nombre de usuario hay que observar que:

- Las cuentas de usuario deben ser únicas.
- Los nombres de inicio de sesión se pueden formar con una combinación de letras, mayúsculas o minúsculas, y caracteres alfanuméricos.
- No se aceptan los caracteres: /, |, :, ;, =, <, > ni *. La cuenta de usuario puede tener hasta 20 caracteres.



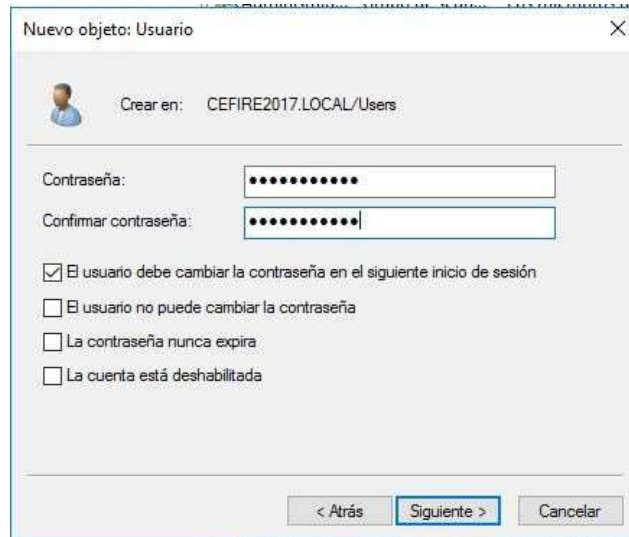
Asistente para crear usuario

En el cuadro de diálogo anterior se puede introducir el nombre, la(s) inicial(es) del segundo nombre y los apellidos del usuario. Hasta aquí toda esta información es meramente informativa, podría haber, por ejemplo, dos usuarios cuyo nombre completo fuera "Alberto Aparicio Vila". En el **cuadro de texto 'Nombre de inicio de sesión de usuario'** se introduce el nombre de usuario siguiendo la estructura que haya predefinido el administrador del sistema (como se ha indicado anteriormente, este nombre debe ser único en todo el dominio).

Algunos ejemplos de criterios para la creación del nombre de usuario podrían ser los siguientes:

- Dos primeras letras del nombre y apellidos. El nombre de inicio de sesión del usuario Alberto Aparicio Vila sería: alapvi
- Inicial del primer nombre y primer apellido completo. El nombre de inicio de sesión del ejemplo anterior sería: aaparicio
- Diferentes caracteres para separar la inicial del primer nombre y el apellido completo: a.aparicio , etc.
- Primer nombre completo y primer apellido completo separados por un punto: alberto.aparicio.

A continuación, se solicitará que se introduzca la contraseña del usuario. Esta debe cumplir con los criterios de complejidad establecidos. Además, aparecen una serie de opciones para configurar las propiedades de la contraseña:



Creación de usuarios

En la figura anterior aparecen cuatro opciones para la contraseña

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca expira.
- La cuenta está deshabilitada.

La primera de las opciones es útil para que el administrador cree el nuevo usuario con una contraseña convencional. El usuario cuando se autentifique por primera vez en el sistema entrará con la contraseña que le ha proporcionado el administrador, pero automáticamente, el sistema le indicará que debe ser cambiada. De esta manera, el administrador ya no conocerá la contraseña del usuario, garantizándose la privacidad de esta.



Mensaje para cambio de contraseña

El segundo de los casos ('El usuario no puede cambiar la contraseña') está pensado para crear usuarios genéricos, supongamos que creamos una cuenta de usuario para utilizar un ordenador conectado a un escáner, y queremos que los usuarios que deseen utilizar ese escáner, siempre entren con la misma cuenta al equipo asociado al escáner.

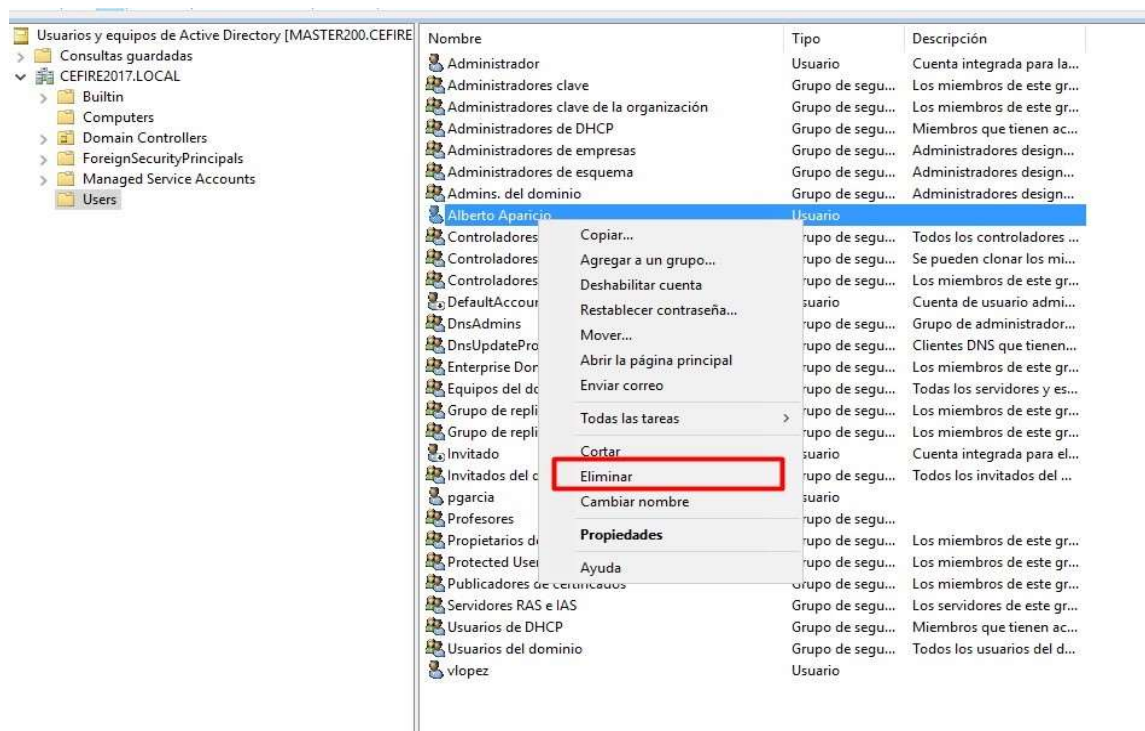
La inhabilitación del tercer caso ('La contraseña nunca expira'), tiene por objetivo evitar que el sistema pida al usuario que cambie la contraseña periódicamente. Resulta interesante mantener esta opción, aunque pueda resultar incómodo cambiar la contraseña cada, por ejemplo, seis meses. De esta manera estamos protegiéndonos de posibles accesos indebidos por parte de alguien que haya averiguado la contraseña de alguna manera.

Finalmente, la cuarta opción ('La cuenta está deshabilitada') sirve para bloquear usuarios que no queremos que tengan acceso al sistema, pero tampoco queremos eliminarlos, ya que se invalidarían los permisos referidos a este usuario. También puede servir para crear usuarios que no queremos que estén operativos hasta un momento determinado.

Eliminación y deshabilitación de usuarios

Cada cuenta de usuario creada en un dominio tiene un identificador de seguridad (SID) único. Si eliminamos una cuenta de usuario y después volvemos a crearla exactamente igual, el identificador SID será diferente. Esto se traduce en que no se podrán recuperar los permisos y privilegios de la cuenta eliminada.

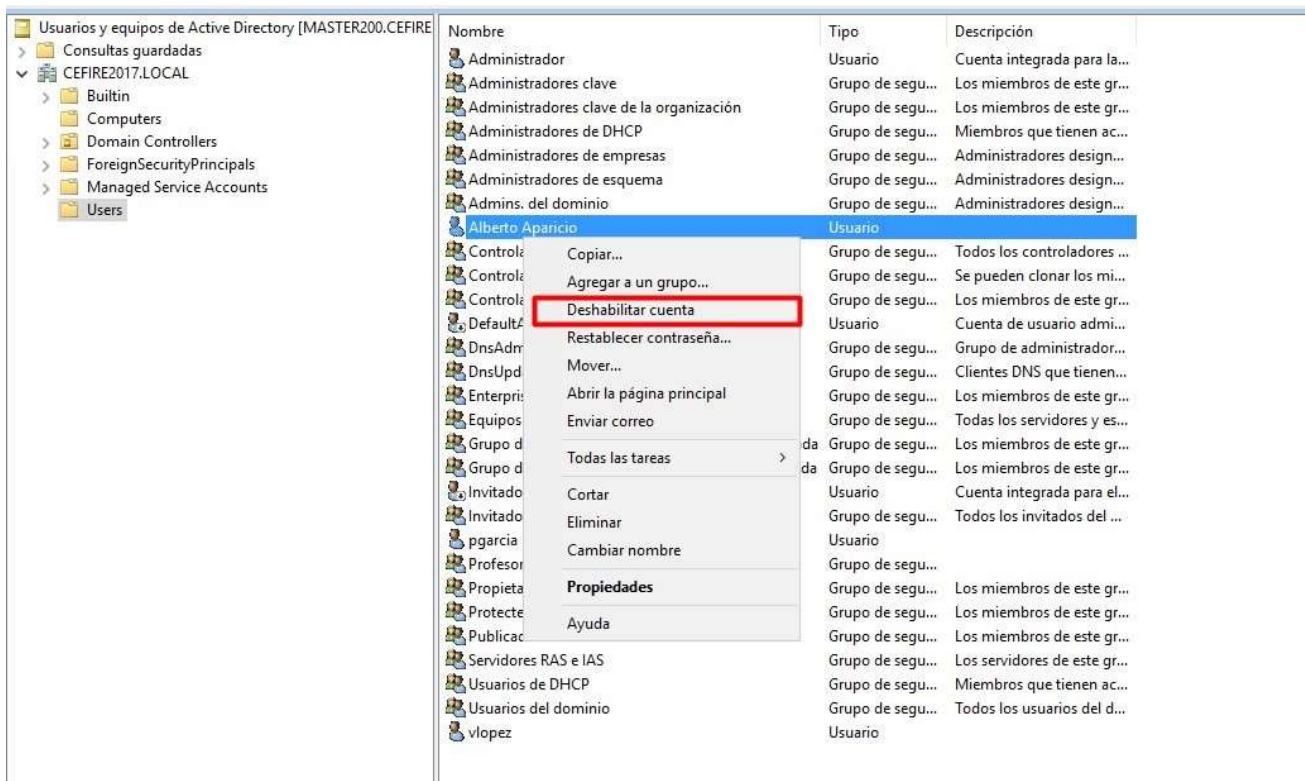
Si finalmente decidimos eliminar la cuenta, accederemos a 'Usuarios y equipos de Active Directory', seleccionaremos el usuario a eliminar, haremos clic con el botón derecho y luego 'Eliminar':



Eliminar usuario de AD

Deshabilitar cuentas

Para evitar posibles problemas con la eliminación de cuentas, el cual es un proceso definitivo, se suele optar por la deshabilitación de cuentas.



Deshabilitar cuenta

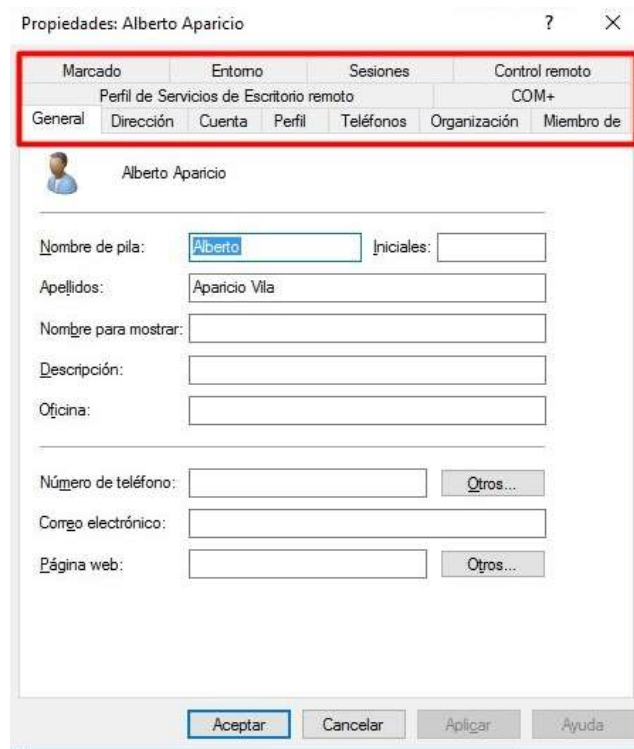
Supongamos una empresa en la que un trabajador va a cesar su actividad. El administrador de sistemas deshabilitará su cuenta en la fecha en la que el trabajador vaya a dejar de prestar sus servicios. De esta manera el trabajador cesado ya no podrá iniciar sesión en el dominio, pero si pasado un tiempo hiciera falta volver a iniciar sesión, bastaría con habilitar de nuevo la cuenta.

Otro ejemplo real podría ser una universidad, en la que cada alumno tiene una cuenta de usuario. Cuando finaliza sus estudios, la cuenta es deshabilitada, pero si posteriormente cursa otros estudios, la cuenta volvería a habilitarse.

Como antes, accederemos a 'Usuarios y equipos de Active Directory' y haciendo clic con el botón secundario sobre el usuario a bloquear, seleccionaremos la opción 'Deshabilitar la cuenta'.

Configuración de la cuenta de usuario

Las cuentas de usuarios creadas en el dominio se pueden configurar de una manera detallada en la ventana 'Propiedades de la cuenta', para ello se hace clic con el botón derecho del ratón sobre la cuenta de usuario que se desea editar:



Propiedades usuario

Las propiedades de la cuenta de usuario que más utilizaremos durante este curso serán:

- **General:** Se puede modificar el Nombre, Apellido, etc. y además modificar información administrativa como la descripción, oficina, teléfono, email y página web.
- **Cuenta:** Se puede configurar algunas características de la contraseña de usuario, las horas de inicio de sesión, la caducidad de la cuenta, desbloquear la cuenta, etc.
- **Perfil:** En esta ficha se pueden editar aspectos importantes como son la ubicación física del perfil del usuario y el fichero de comandos de inicio de sesión.
- **Miembro de:** Se muestra el listado de grupos a los que el usuario pertenece.

Configuración de inicio de sesión

A partir de Windows Server 2008 se permite configurar los horarios en los que se puede iniciar sesión. Esta funcionalidad puede ser útil para controlar accesos al sistema a horas 'anómalas', o para evitar que usuarios de, por ejemplo, el turno de tarde, puedan acceder al sistema con la cuenta de un usuario del turno de mañana.

Para establecer los horarios en los que se puede iniciar sesión se seguirán los siguientes pasos.

En 'Usuarios y Equipos de Active Directory' se selecciona el usuario buscado, y haciendo clic con el botón derecho se accede a 'Propiedades'.

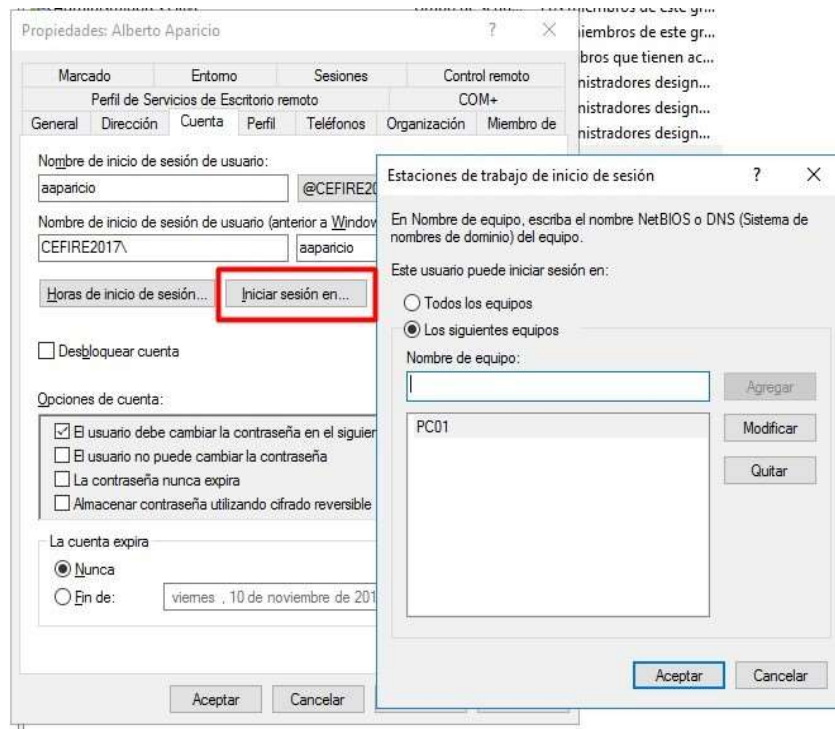
- Se abre el cuadro de diálogo 'Propiedades' de la cuenta seleccionada.
- Se hace clic en la ficha 'Cuenta' y después se hace clic en el botón 'Horas de inicio de sesión'

Horas de inicio de sesión

En color azul se muestran las horas de inicio permitidas. Para denegar el acceso basta con seleccionar las horas a las que se desea limitar el acceso y se marca la opción 'Inicio de sesión denegado':

Horas de inicio de sesión

También es posible configurar el inicio de sesión en determinados equipos. Para ello basta con hacer clic en el botón 'Iniciar sesión en...'. Se puede seleccionar si el usuario puede iniciar sesión en 'Todos los equipos' o solo en algunos equipos determinados:



Iniciar sesión en...

Creación de grupos

Los grupos son un tipo de contenedor que permiten definir conjuntos de usuarios y definir permisos basándonos en esa pertenencia al grupo, en lugar de hacerlo de modo individual, usuario por usuario. Eso no sólo facilita la administración del dominio, sino que también permite trabajar de un modo menos propenso a errores. Como pauta general, la agrupación de objetos suele facilitar las tareas de administración reduciendo las posibilidades de error.

Existen dos grandes tipos de grupos en el Directorio Activo de Windows:

- **Grupos de seguridad:** este tipo de grupos permite definir permisos para recursos del dominio. Son los utilizados en las listas de control de accesos (ACLs) que se estudiarán más adelante. Este tipo de grupos son los que se utilizarán en la administración de la red.
- **Grupos de distribución:** no poseen características de seguridad, únicamente son un listado de usuarios para mensajería.

Dentro de los grupos de seguridad existen a su vez tres ámbitos:

- **Grupo Universal:** es un grupo cuyos permisos se extienden a diversos dominios. Además este tipo de grupos puede estar formado por usuarios o grupos de usuarios de diferentes dominios.
- **Grupo Global:** es muy similar a los grupos universales, es decir pueden permitir el acceso a recursos de cualquiera de los dominios del árbol del Directorio Activo, pero con la salvedad de que todos los miembros del grupo deben pertenecer al mismo dominio.
- **Grupo Local del Dominio:** es un grupo creado en un dominio con miembros que pueden provenir de otros dominios y que únicamente puede tener acceso a recursos dentro de su dominio.

¿En qué casos utilizar un ámbito de grupo u otro?

Los **grupos universales** suelen tener su utilidad en grandes empresas en las que se ha definido un **bosque de dominios asignando dominios a cada uno de sus departamentos o divisiones**. En este tipo de estructuras, cuando se realiza una modificación en el grupo, esta debe replicarse en todos los controladores de domino que estén configurados como catálogo global.

En **redes de dominio único** se pueden aplicar **grupos globales** que tendrán mayor sentido cuando se defina un segundo dominio, lo que puede ocurrir en el momento en el que haya una ampliación de la organización.

Como pautas generales para la administración de redes tendremos en cuenta las siguientes consideraciones

1. No se debe asignar un ámbito más amplio del necesario.
2. Los grupos locales de dominio no se pueden procesar en otros dominios.
3. Un grupo global no se replica fuera del dominio ya que no forma parte del plan de replicación del catálogo global.
4. Los grupos universales se replican por toda la red generando tráfico que puede tener una cierta incidencia en el rendimiento de esta (aunque este aspecto se ha optimizado a partir de Windows Server 2008).
5. Si un grupo universal está compuesto por grupos globales y se producen cambios dentro de los grupos globales, no se produce un cambio en el catálogo global, y por tanto esa modificación no conlleva una replicación en todos los controladores de domino del bosque.

Grupos predefinidos

Al instalar el Directorio Activo podemos comprobar que se han generado automáticamente una serie de grupos predefinidos con unos permisos acorde a sus funciones asignadas:

| Nombre | Tipo | Descripción |
|---|------------------------------------|---|
| Administradores de DHCP | Grupo de seguridad - Dominio local | Miembros que tienen acceso administrativo al servicio DHCP |
| DnsAdmins | Grupo de seguridad - Dominio local | Grupo de administradores de DNS |
| Grupo de replicación de contraseña RODC denegada | Grupo de seguridad - Dominio local | Los miembros de este grupo no pueden replicar las contraseñas a ningún controlador de dominio de solo lectura en el |
| Grupo de replicación de contraseña RODC permitida | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden replicar las contraseñas a todos los controladores de dominio de solo lectura en e |
| Publicadores de certificados | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden publicar certificados en el directorio |
| Servidores RAS e IAS | Grupo de seguridad - Dominio local | Los servidores de este grupo pueden obtener propiedades de acceso remoto de los usuarios |
| Usuarios de DHCP | Grupo de seguridad - Dominio local | Miembros que tienen acceso de solo vista al servicio DHCP |
| Administradores clave | Grupo de seguridad - Global | Los miembros de este grupo pueden realizar operaciones administrativas en los objetos clave del dominio. |
| Admins. del dominio | Grupo de seguridad - Global | Administradores designados del dominio |
| Controladores de dominio | Grupo de seguridad - Global | Todos los controladores de dominio del dominio |
| Controladores de dominio clonables | Grupo de seguridad - Global | Se pueden clonar los miembros del grupo que sean controladores de dominio. |
| Controladores de dominio de sólo lectura | Grupo de seguridad - Global | Los miembros de este grupo son controladores de dominio de solo lectura en el dominio. |
| DnsUpdateProxy | Grupo de seguridad - Global | Clientes DNS que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes (tales como serv |
| Equipos del dominio | Grupo de seguridad - Global | Todas los servidores y estaciones de trabajo unidos al dominio |
| Invitados del dominio | Grupo de seguridad - Global | Todos los invitados del dominio |
| Profesores | Grupo de seguridad - Global | |
| Propietarios del creador de directivas de grupo | Grupo de seguridad - Global | Los miembros de este grupo pueden modificar la directiva de grupo del dominio |
| Protected Users | Grupo de seguridad - Global | Los miembros de este grupo tienen protecciones adicionales frente a las amenazas contra la seguridad de autenticación |
| Usuarios del dominio | Grupo de seguridad - Global | Todos los usuarios del dominio |
| Administradores clave de la organización | Grupo de seguridad - Universal | Los miembros de este grupo pueden realizar operaciones administrativas en los objetos clave del bosque. |
| Administradores de empresas | Grupo de seguridad - Universal | Administradores designados de la empresa |
| Administradores de esquema | Grupo de seguridad - Universal | Administradores designados del esquema |
| Enterprise Domain Controllers de sólo lectura | Grupo de seguridad - Universal | Los miembros de este grupo son controladores de dominio de solo lectura en la empresa. |

Grupos predefinidos

| Nombre | Tipo | Descripción |
|--|------------------------------------|---|
|  Acceso compatible con versiones anteriores de Windows 2000 | Grupo de seguridad - Dominio local | Un grupo de compatibilidad anterior que permite acceso de lectura a todos los usuarios y grupos en el dominio |
|  Acceso DCOM a Serv. de certif. | Grupo de seguridad - Dominio local | Los miembros de este grupo se pueden conectar a entidades de certificación en la empresa. |
|  Administradores | Grupo de seguridad - Dominio local | Los administradores tienen acceso completo y sin restricciones al equipo o dominio |
|  Administradores de Hyper-V | Grupo de seguridad - Dominio local | Los miembros de este grupo tienen acceso completo y sin restricciones a todas las características de Hyper-V. |
|  Creadores de confianza de bosque de entrada | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden crear confianza de entrada unidireccional a este bosque |
|  Duplicadores | Grupo de seguridad - Dominio local | Pueden replicar archivos en un dominio |
|  Grupo de acceso de autorización de Windows | Grupo de seguridad - Dominio local | Los miembros de este grupo tiene acceso al atributo tokenGroupsGlobalAndUniversal calculado en objetos de |
|  IIS_IUSRS | Grupo de seguridad - Dominio local | Grupo integrado usado por Internet Information Services. |
|  Invitados | Grupo de seguridad - Dominio local | De forma predeterminada, los invitados tienen el mismo acceso que los miembros del grupo Usuarios, except |
|  Lectores del registro de eventos | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden leer registros de eventos del equipo local. |
|  Operadores criptográficos | Grupo de seguridad - Dominio local | Los miembros tienen autorización para realizar operaciones criptográficas. |
|  Operadores de asistencia de control de acceso | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden consultar de forma remota los atributos de autorización y los permisos p |
|  Operadores de configuración de red | Grupo de seguridad - Dominio local | Los miembros en este equipo pueden tener algunos privilegios administrativos para administrar la configuraci |
|  Operadores de copia de seguridad | Grupo de seguridad - Dominio local | Los operadores de copia de seguridad pueden invalidar restricciones de seguridad con el único propósito de h |
|  Opers. de cuentas | Grupo de seguridad - Dominio local | Los miembros pueden administrar cuentas de usuario y de grupo del dominio. |
|  Opers. de impresión | Grupo de seguridad - Dominio local | Los miembros pueden administrar impresoras instaladas en controladores de dominio |
|  Opers. de servidores | Grupo de seguridad - Dominio local | Los miembros pueden administrar servidores del dominio |
|  Servidores de acceso remoto RDS | Grupo de seguridad - Dominio local | Los servidores de este grupo permiten a los usuarios de programas RemoteApp y escritorios virtuales personal |
|  Servidores de administración RDS | Grupo de seguridad - Dominio local | Los servidores de este grupo pueden realizar acciones administrativas rutinarias en servidores que ejecuten Ser |
|  Servidores de extremo RDS | Grupo de seguridad - Dominio local | Los servidores de este grupo ejecutan máquinas virtuales y hospedan sesiones donde se ejecutan los program |
|  Servidores de licencias de Terminal Server | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden actualizar las cuentas de usuario en Active Directory con información sol |
|  Storage Replica Administrators | Grupo de seguridad - Dominio local | Los miembros de este grupo tienen acceso completo y sin restricciones a todas las características de la réplica |
|  System Managed Accounts Group | Grupo de seguridad - Dominio local | Los miembros de este grupo los administra el sistema. |
|  Usuarios | Grupo de seguridad - Dominio local | Los usuarios no pueden hacer cambios accidentales o intencionados en el sistema y pueden ejecutar la mayor |
|  Usuarios COM distribuidos | Grupo de seguridad - Dominio local | Los miembros pueden iniciar, activar y usar objetos de COM distribuido en este equipo. |
|  Usuarios de administración remota | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden acceder a los recursos de WMI mediante protocolos de administración (c |
|  Usuarios de escritorio remoto | Grupo de seguridad - Dominio local | A los miembros de este grupo se les concede el derecho de iniciar sesión remotamente |
|  Usuarios del monitor de sistema | Grupo de seguridad - Dominio local | Los miembros de este grupo tienen acceso a los datos del contador de rendimiento de forma local y remota |
|  Usuarios del registro de rendimiento | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden programar contadores de registro y rendimiento, habilitar proveedores d |

Grupos Built-in

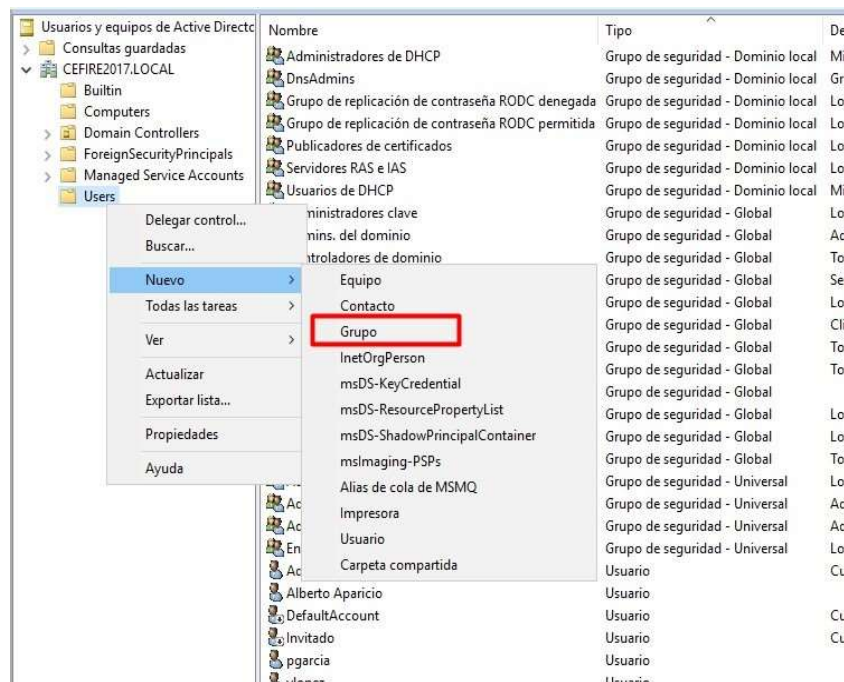
Examinemos las funciones de algunos de los grupos más utilizados:

- Usuarios del dominio: grupo global que contiene todas las cuentas de usuarios el dominio.
- Administradores del dominio: grupo global que permite a sus miembros realizar tareas de administración del dominio.
- Administradores de empresa: grupo universal que permite a sus miembros realizar tareas de administración en todos los dominios de la red.
- Administradores de esquema: grupo universal que permite a sus miembros modificar la estructura de los objetos del Directorio Activo.
- Administradores: grupo local que permite a sus miembros realizar tareas de administración en el controlador de dominio.
- Operadores de copias de seguridad: grupo local que permite a sus miembros realizar copias de seguridad o restaurar archivos dentro del dominio.
- Operadores de cuenta: grupo local que permite a sus miembros crear, editar y eliminar cuentas de usuario y grupos.
- Operadores de impresión: grupo local que permite a sus miembros configurar y administrar el uso de impresoras de red.
- Operadores de servidor: grupo local que permite a sus miembros crear carpetas compartidas en el servidor y realizar copias de seguridad o restaurar archivos en el controlador de dominio.
- Usuarios: grupo local que limita las posibilidades de que un usuario haga un cambio accidental en el sistema, pero sí permite ejecutar la mayoría de las aplicaciones.

Es importante darse cuenta del considerable ahorro de tiempo para el administrador que permite la existencia de grupos predefinidos para tareas muy concretas.

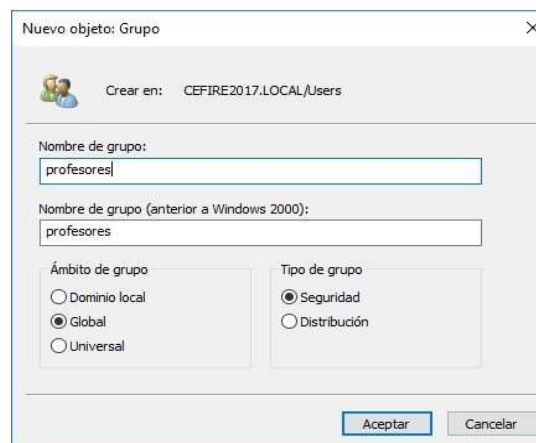
Creación de grupos

La forma de crear los grupos es muy parecida a la que hacíamos para crear a los usuarios. Para ello desde la opción de Usuarios y equipos de Active Directory, con el botón de la derecha del ratón, nuevo --> Grupo:



Creación de grupos

Se abrirá el siguiente cuadro de diálogo:



Creación de grupos

Por defecto se nos indica que el ámbito del grupo será 'Global' y el tipo de grupo será de 'Seguridad'. En principio, si no tenemos unas necesidades que justifiquen lo contrario, crearemos los grupos con esas propiedades. Tras pulsar 'Aceptar' nos aparecerá el nuevo grupo en el listado de 'Usuarios y equipos de Active Directory':

| Usuarios y equipos de Active Directory | Nombre | Tipo | Descripción |
|--|---|------------------------------------|---|
| Consultas guardadas | Administradores de DHCP | Grupo de seguridad - Dominio local | Miembros que tienen acceso administrativo al servicio DHCP |
| CEFIRE2017.LOCAL | DnsAdmins | Grupo de seguridad - Dominio local | Grupo de administradores de DNS |
| Builtin | Grupo de replicación de contraseña RODC denegada | Grupo de seguridad - Dominio local | Los miembros de este grupo no pueden replicar las contraseñas a ningún |
| Computers | Grupo de replicación de contraseña RODC permitida | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden replicar las contraseñas a todos los c |
| Domain Controllers | Publicadores de certificados | Grupo de seguridad - Dominio local | Los miembros de este grupo pueden publicar certificados en el directorio |
| ForeignSecurityPrincipals | Servidores RAS e IAS | Grupo de seguridad - Dominio local | Los servidores de este grupo pueden obtener propiedades de acceso reme |
| Managed Service Accounts | Usuarios de DHCP | Grupo de seguridad - Dominio local | Miembros que tienen acceso de solo vista al servicio DHCP |
| Users | Administradores clave | Grupo de seguridad - Global | Los miembros de este grupo pueden realizar operaciones administrativas |
| | Admins. del dominio | Grupo de seguridad - Global | Administradores designados del dominio |
| | Controladores de dominio | Grupo de seguridad - Global | Todos los controladores de dominio del dominio |
| | Controladores de dominio clonables | Grupo de seguridad - Global | Se pueden clonar los miembros del grupo que sean controladores de dom |
| | Controladores de dominio de sólo lectura | Grupo de seguridad - Global | Los miembros de este grupo son controladores de dominio de solo lectur |
| | DnsUpdateProxy | Grupo de seguridad - Global | Clientes DNS que tienen permiso para efectuar actualizaciones dinámicas |
| | Equipos del dominio | Grupo de seguridad - Global | Todas los servidores y estaciones de trabajo unidos al dominio |
| | Invitados del dominio | Grupo de seguridad - Global | Todos los invitados del dominio |
| | Profesores | Grupo de seguridad - Global | |
| | Propietarios del creador de directivas de grupo | Grupo de seguridad - Global | Los miembros de este grupo pueden modificar la directiva de grupo del d |
| | Protected Users | Grupo de seguridad - Global | Los miembros de este grupo tienen protecciones adicionales frente a las a |
| | Usuarios del dominio | Grupo de seguridad - Global | Todos los usuarios del dominio |
| | Alumnos | Grupo de seguridad - Global | |
| | Administradores clave de la organización | Grupo de seguridad - Universal | Los miembros de este grupo pueden realizar operaciones administrativas |
| | Administradores de empresas | Grupo de seguridad - Universal | Administradores designados de la empresa |
| | Administradores de esquema | Grupo de seguridad - Universal | Administradores designados del esquema |
| | Enterprise Domain Controllers de sólo lectura | Grupo de seguridad - Universal | Los miembros de este grupo son controladores de dominio de solo lectur |
| | Administrador | Usuario | Cuenta integrada para la administración del equipo o dominio |
| | Alberto Aparicio | Usuario | |
| | DefaultAccount | Usuario | Cuenta de usuario administrada por el sistema. |
| | Invitado | Usuario | Cuenta integrada para el acceso como invitado al equipo o dominio |
| | nnarcia | Usuario | |

Creación de grupos

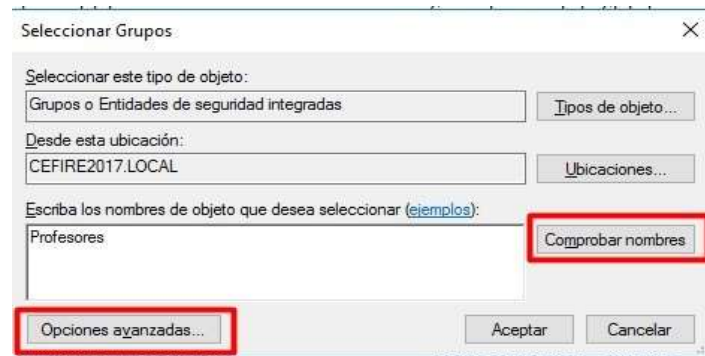
Añadir usuarios a grupos

Para poder añadir un usuario a un grupo, lo podemos hacer de varias maneras. La primera de ellas mediante basta con seleccionar el usuario y en el menú que se abrirá al hacer clic con el botón derecho, acceder a la opción 'Agregar a un grupo':

| Usuarios y equipos de Active Directory | Nombre | Tipo | Descripción |
|--|---|------------------------------------|--------------|
| Consultas guardadas | Administradores de DHCP | Grupo de seguridad - Dominio local | Miembros de |
| CEFIRE2017.LOCAL | DnsAdmins | Grupo de seguridad - Dominio local | Grupo de ad |
| Builtin | Grupo de replicación de contraseña RODC denegada | Grupo de seguridad - Dominio local | Los miemb |
| Computers | Grupo de replicación de contraseña RODC permitida | Grupo de seguridad - Dominio local | Los miemb |
| Domain Controllers | Publicadores de certificados | Grupo de seguridad - Dominio local | Los miemb |
| ForeignSecurityPrincipals | Servidores RAS e IAS | Grupo de seguridad - Dominio local | Los servido |
| Managed Service Accounts | Usuarios de DHCP | Grupo de seguridad - Dominio local | Miembros de |
| Users | Administradores clave | Grupo de seguridad - Global | Los miemb |
| | Admin | Grupo de seguridad - Global | Administra |
| | Contro | Grupo de seguridad - Global | Todos los c |
| | Contro | Grupo de seguridad - Global | Se pueden |
| | Contro | Grupo de seguridad - Global | Los miemb |
| | DnsUp | Grupo de seguridad - Global | Clientes DN |
| | Equipos | Grupo de seguridad - Global | Todas los s |
| | Invitac | Grupo de seguridad - Global | Todos los ir |
| | Profes | Grupo de seguridad - Global | |
| | Propie | Grupo de seguridad - Global | Los miemb |
| | Protec | Grupo de seguridad - Global | Los miemb |
| | Usuari | Grupo de seguridad - Global | Todos los u |
| | Alumnr | Grupo de seguridad - Global | |
| | Admin | Grupo de seguridad - Universal | Los miemb |
| | Admin | Grupo de seguridad - Universal | Administra |
| | Admin | Grupo de seguridad - Universal | Administra |
| | Enterp | Grupo de seguridad - Universal | Los miemb |
| | Admin | Usuario | Cuenta inte |
| | Alberto Aparicio | Usuario | |
| | DefaultAccount | Usuario | Cuenta de |
| | Invitado | Usuario | Cuenta inte |
| | pgarcia | Usuario | |
| | vlopez | Usuario | |

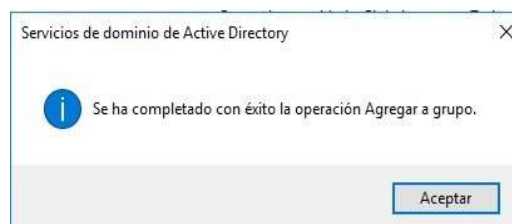
Añadir usuario a grupo

Se abrirá un cuadro en el que podremos indicar/buscar el grupo al que queremos añadir el usuario. Mediante comprobar nombres nos mostrará las coincidencias del grupo que hemos añadido. Con las opciones avanzadas podemos hacer una búsqueda del grupo:

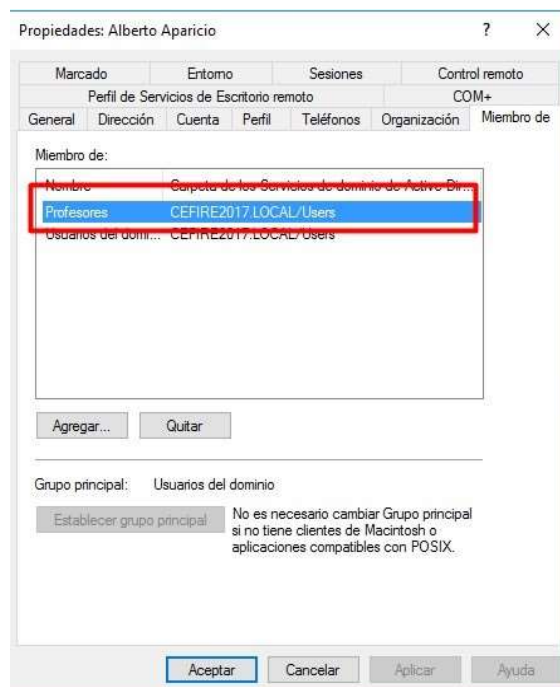


Añadir usuario a grupo

Tras aceptar, aparecerá un mensaje indicando que la operación se ha realizado con éxito y podremos comprobar en las propiedades del usuario que efectivamente es miembro del grupo 'Profesores':

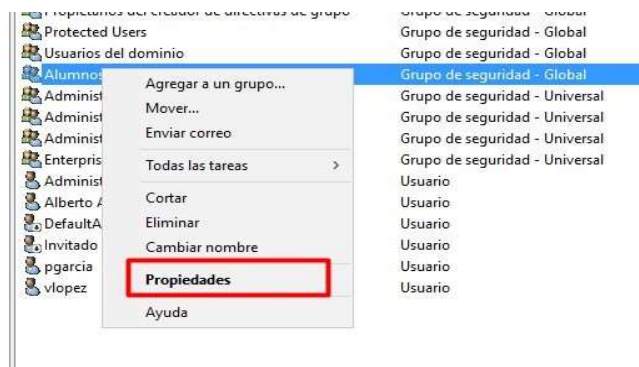


Añadir usuario a grupo



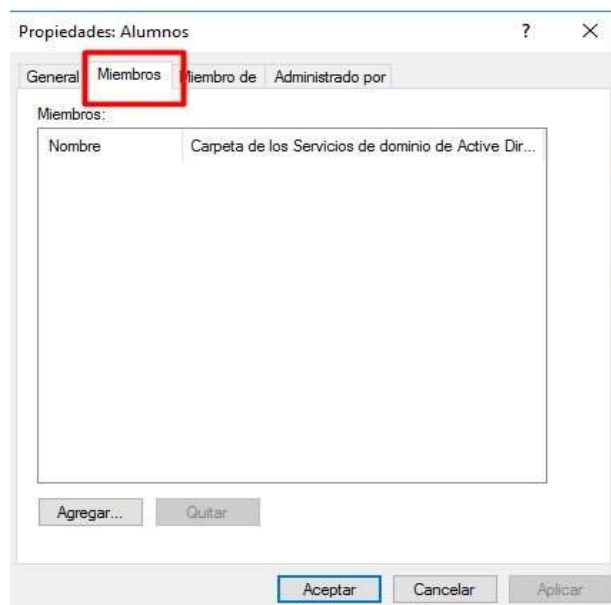
Miembro de

También podemos añadir usuarios a un grupo a partir del grupo. Para ello podemos seleccionar el grupo y con el botón de la derecha propiedades, accedemos a la pestaña miembros:



Añadir usuarios a grupos

Y accedemos a la pestaña miembros:



Añadir usuarios a grupos

Y desde la opción Agregar podemos añadir los usuarios miembros del grupo.

Unidades Organizativas

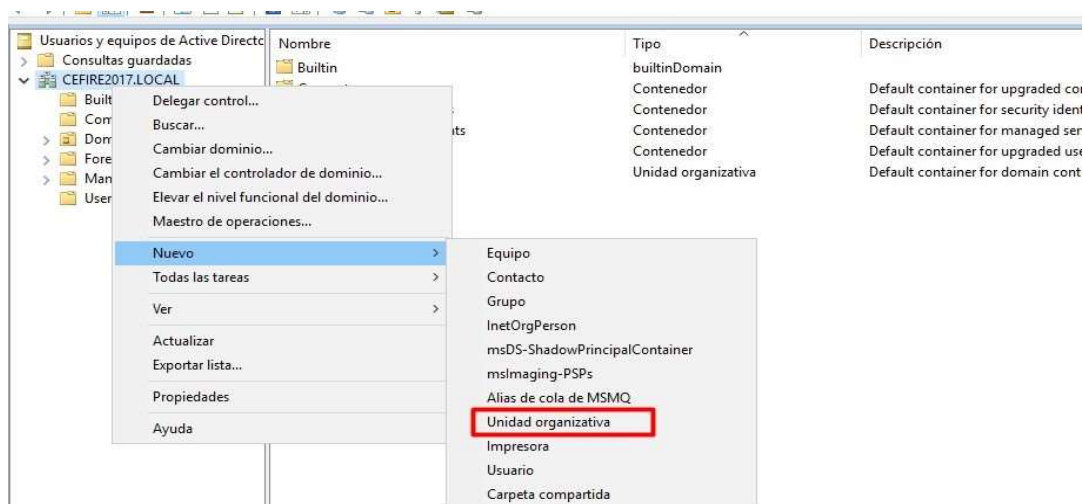
Una unidad organizativa es un contenedor de objetos (usuarios, grupos, equipos, otras unidades organizativas, etc.) pertenecientes a un mismo dominio. Son especialmente útiles para reproducir la estructura de la empresa donde se halle el dominio. Es decir, si, por ejemplo, una empresa está dividida en tres departamentos (dirección, ventas y producción), podemos crear tres unidades organizativas correspondientes a estos tres departamentos, donde incluyamos todos los objetos del dominio correspondientes a cada una de las áreas de la empresa.

Su utilidad radica en dos aspectos fundamentales:

1. De esta manera es muy sencillo establecer directivas de seguridad (las veremos en el siguiente tema) que se apliquen a todos los objetos de cada departamento.
2. Como dentro de la unidad organizativa, se pueden introducir otras unidades organizativas, se puede replicar la estructura jerárquica de la empresa sin necesidad de crear más dominios o subdominios.

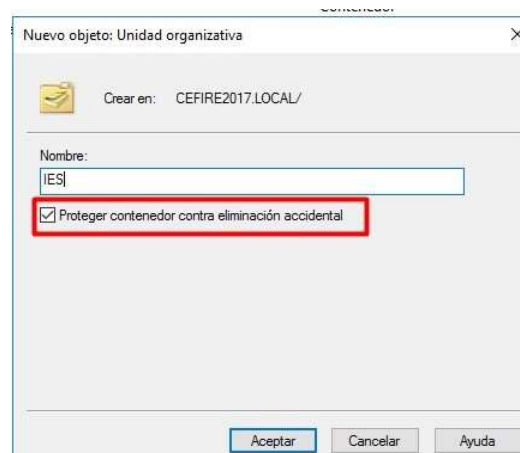
Creación de Unidades Organizativas

Para crear una unidad organizativa abriremos la ventana 'Usuarios y Equipos de Active Directory' (desde el Panel del Administrador, 'Herramientas Administrativas'). A continuación, nos situamos sobre el dominio y haciendo clic con el botón secundario seleccionamos 'Nuevo' y 'Unidad Organizativa'



Unidades Organizativas

A continuación, se abrirá el diálogo que nos permite indicar el nombre del nuevo objeto:



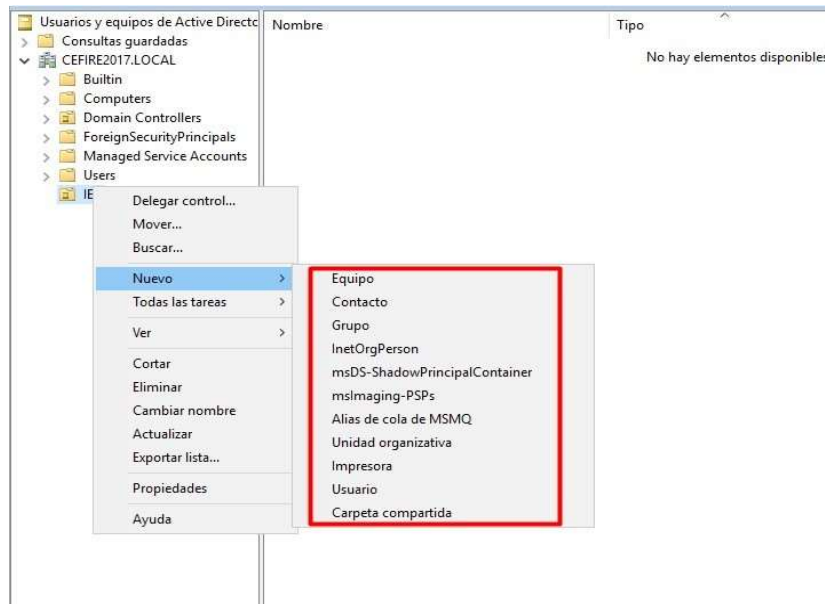
Creación OU (Organizational Unit)

Al pulsar en Aceptar, se creará la Unidad Organizativa (OU) dentro de nuestro dominio. Notad también que por defecto se crea una protección contra posibles errores de eliminación. Por defecto la unidad no se podrá eliminar de manera accidental.



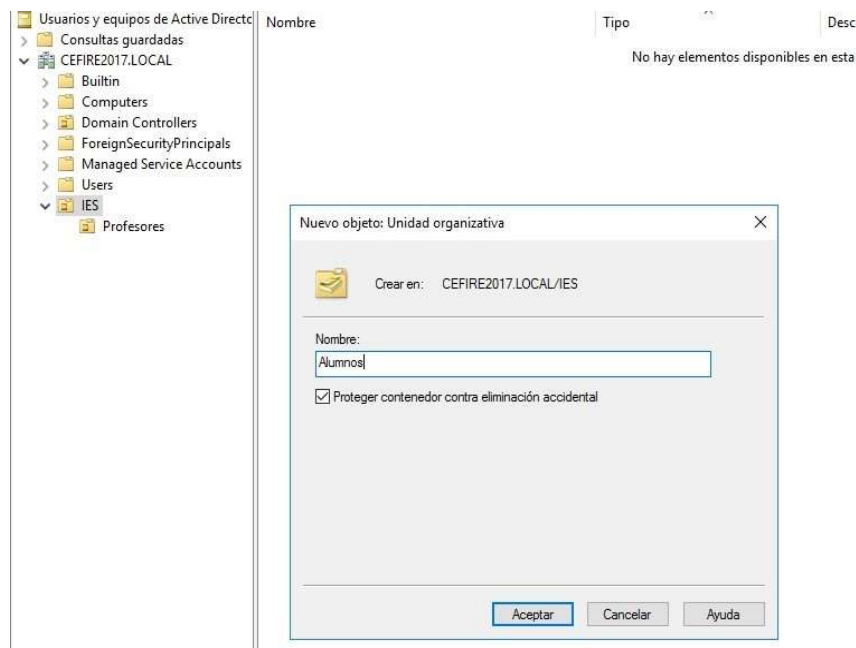
Creación de una OU

Dentro de una Unidad Organizativa podemos añadir objetos, usuarios, grupos, más unidades organizativas, etc. para ello seleccionamos la OU y con el botón derecho del ratón accedemos a la opción Nuevo:



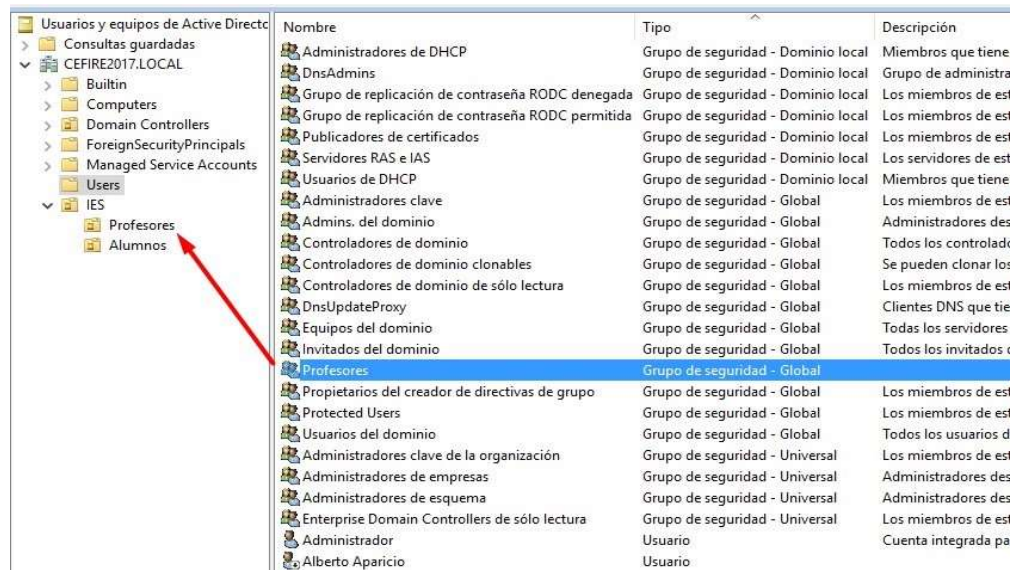
Añadir objetos a una OU

Podemos añadir dos unidades organizativas dentro, una para Alumnos y otra para Profesores:

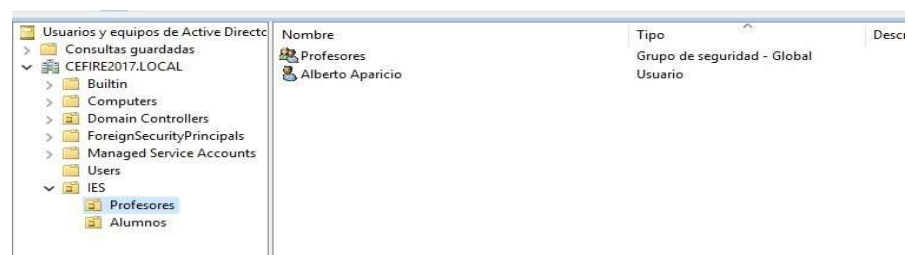


Crear elementos dentro de una OU

También podemos arrastrar elementos de una unidad a otra, por ejemplo, vamos a arrastrar los grupos de Alumnos y Profesores y los usuarios que hemos creado. Seleccionamos el grupo Profesores y lo arrastramos a la unidad organizativa Profesores:



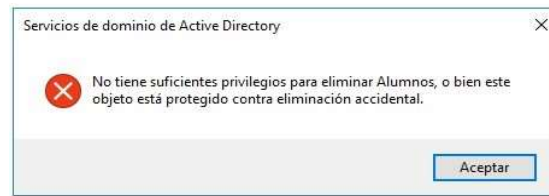
Mover objetos a OU



Mover objetos entre OU

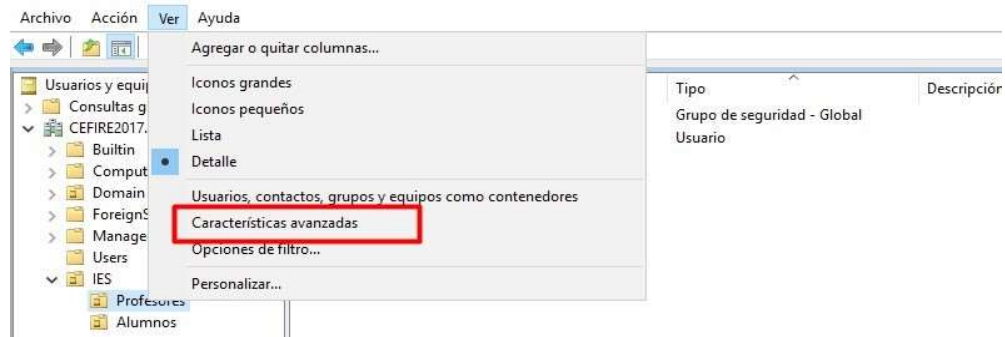
Borrar una OU

Si tratamos de borrar una OU, veremos que nos aparece un mensaje de que no tenemos los suficientes privilegios para poder realizar la acción de borrado. Esto es debido a la protección contra eliminaciones accidentales de las que hemos comentado anteriormente:



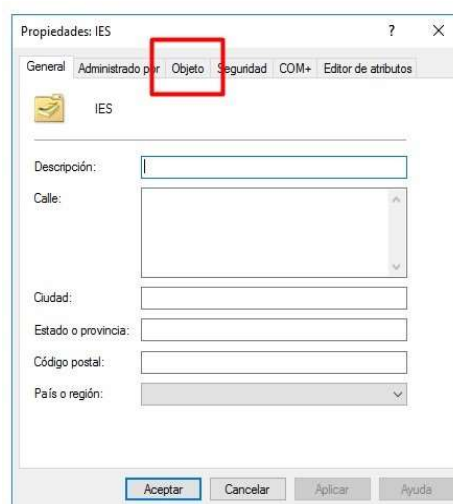
Borrar OU

Para eliminar las unidades organizativas, en primer lugar deberemos activar las 'características avanzadas' seleccionando en el menú 'Ver' la opción 'Características Avanzadas'.



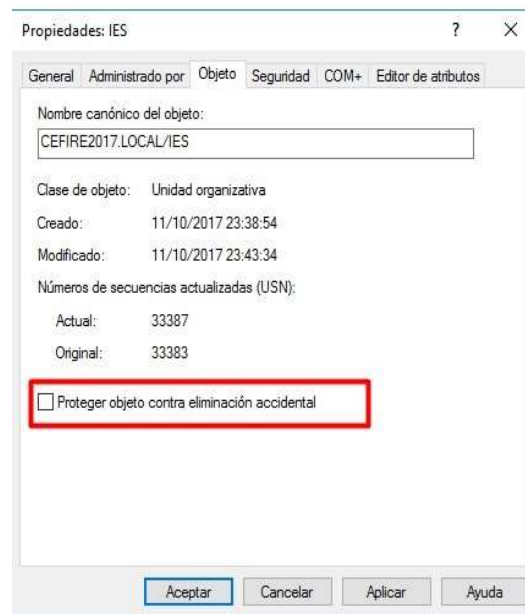
Borrado de una OU

Nos aparecerá la ventana de la OU:



Desproteger una OU

Desmarcamos el check de protección contra eliminaciones accidentales:



Desactivar protección

Ahora ya sí podemos eliminar la OU. Dejamos de nuevo desactivadas las opciones avanzadas desde la opción menú. En el próximo tema, utilizaremos las unidades organizativas para gestionar de manera eficaz el dominio, aplicando directivas de seguridad específicas a cada unidad organizativa.

Actividades tema 3

Actividad 3.1

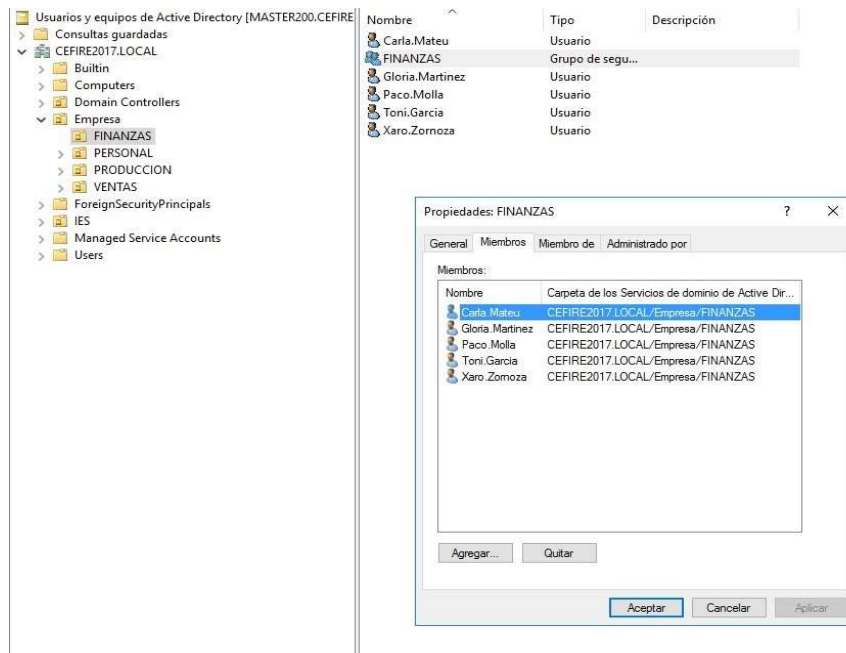
Para poder realizar todo lo que se pide en esta actividad, deberás disponer de un segundo cliente con Windows 10 instalado y unido al dominio. A este segundo equipo le podríamos llamar PC02. No es necesario que tengas los dos clientes funcionando a la vez si la memoria de tu ordenador no lo permite.

Crea dos usuarios con el nombre usuario1 y usuario2. Ponles a ambos la contraseña "Abc123!" y configura las cuentas de usuario para que no tengan que cambiar la contraseña al iniciar sesión por primera vez. Agrega estos usuarios al grupo global Alumnos y deshabilita la cuenta de usuario2.

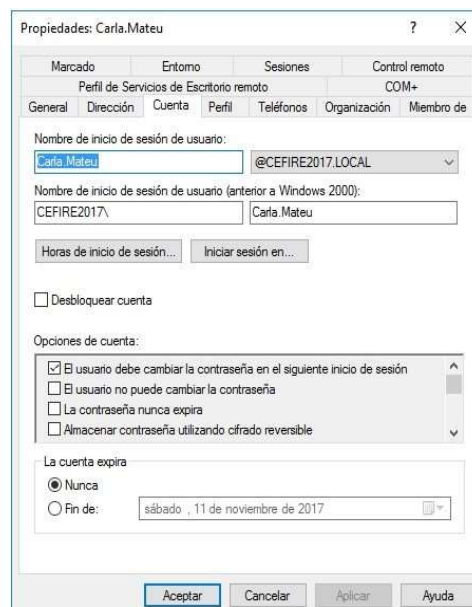
1. Adjunta una captura de pantalla del error que sale al intentar acceder desde un equipo cliente con el usuario2. Habilita de nuevo la cuenta de usuario2.
2. Configura la cuenta usuario1 para que solamente pueda iniciar sesión desde PC01. Adjunta una captura de pantalla de la configuración realizada y una captura de pantalla del error que sale cuando usuario1 intenta acceder desde un segundo cliente W10, PC02.
3. Configura la cuenta de usuario2 para que pueda iniciar sesión en cualquier equipo del dominio solamente de lunes a viernes de 8.00 a 18.00. Adjunta una captura de la pantalla de la configuración de los horarios de acceso al sistema del usuario2.
4. Intenta iniciar sesión en el equipo controlador de dominio con usuario2 (es decir, localmente en el servidor). ¿Por qué no puedes? ¿Qué podrías hacer para que usuario2 pudiera iniciar sesión en el controlador de dominio?

Actividad 3.2

Crea la siguiente estructura de UO que puedes ver en Empresa (es suficiente con que crees un par de usuarios en dos unidades organizativas y los grupos correspondientes):



De manera que el usuario tendrá el login compuesto por el nombre y el apellido, de manera que Carla Mateu, tendrá un login carla.mateu:



Propiedades usuario

La contraseña por defecto será "practica0703." y será necesaria cambiarla en el siguiente inicio de sesión.

Adjunta capturas de pantalla donde se pueda ver la configuración realizada.