Gestión de Usuarios

Transcribed on August 6, 2025 at 1:09 PM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de los usuarios y equipos de Active Director.

Vamos a hablar de las cuentas de usuario, de las propiedades de los usuarios, hablaremos también de los grupos del directorio activo y hablaremos de las unidades organizativas y las cuentas de equipo.

El primer objeto con el que trabajamos habitualmente dentro de Active Directory dentro de una estructura de dominio son las cuentas de usuario.

Las cuentas de usuario van a representar una identidad que después un trabajador o usuario del dominio va a utilizar para poder acceder a los recursos, van a permitir o denegar el acceso a los equipos, van a permitir el acceso a los diferentes procesos, recursos o servicios y también nos van a servir para poder administrar los permisos a los recursos de red.

Podemos crear las cuentas de usuario usando la consola de usuarios y equipos de Active Directory, el centro administrativo del directorio activo, también tenemos comandos de Windows PowerShell para poder crear usuarios y también podemos hacerlo mediante línea de comandos con comandos como dsad.

Algunas consideraciones que debemos tener en cuenta en lo que se refiere a la parte de gestión de usuarios es el nombre, que tiene que tener un formato único por cada uno de los usuarios y especialmente el User principal, Name, el UPM, que va a ser el nombre con el que el usuario va a iniciar sesión.

Dentro de las propiedades del usuario vamos a tenerlas divididas por categorías.

Vamos a tener aquellas propiedades que tienen que ver con los elementos de inicio de sesión, como puede ser el nombre de inicio de sesión UPN, las horas a las que puede iniciar sesión, cuando expira la cuenta, cuando tiene que cambiar el password el usuario, si necesita necesita utilizar una tarjeta inteligente para iniciar sesión, si el password nunca aspira, si se almacena con un fibrado reversible o si la cuenta puede ser sometida a denegaciones.

Luego tendremos la parte de organización, donde tendremos diferentes datos relacionados con la parte descriptiva de la organización, la pertenencia a grupos, luego tendremos configuraciones de contraseñas y luego tendremos la parte del perfil.

Dentro de la parte del perfil nosotros vamos a poder configurar perfiles de usuario para que almacenen sus datos bien dentro del dispositivo local o bien a través de una ubicación de red y utilizar un servidor como contenedor centralizado para todos los perfiles de los usuarios, que sería un poco lo recomendable.

Y luego tendríamos la parte de Policy y Policy silos para los procesos de autenticación y las extensiones, donde tendríamos la posibilidad de ver, por ejemplo, los atributos de un determinado objeto, en este caso de un objeto usuario.

Desde Server Manager, si nos vamos a la parte de Tools, vamos al Centro Administrativo de Active Directory, dentro del Centro Administrativo del Directorio Activo vamos a tener la posibilidad de crear, administrar o eliminar diferentes objetos.

Si nos vamos a la parte del Dominio, dentro de la parte del Dominio vamos a tener aquí los diferentes componentes, entre ellos, una de las cosas que se recomienda cuando vamos a iniciar la configuración del dominio es habilitar la papelera de reciclaje.

Daríamos ahí, seleccionaríamos para habilitar la papelera de reciclaje, damos a OK, nos indica que refresquemos el Centro Administrativo de Active Directory para que en este momento nos aparezca un contenedor adicional que es el de objetos eliminados.

Si yo me voy a la parte de Usuarios, dentro de la parte de Usuarios, en el contenedor de Usuarios, yo voy a tener los diferentes grupos o los diferentes usuarios que yo creé.

Si quiero crear un nuevo usuario, simplemente doy a Nuevo, selecciono Usuario y aquí me va a aparecer un asistente con todos los datos que yo puedo gestionar o puedo utilizar para crear el usuario.

Voy a crear el usuario Angel, importante poner el UPN, que tiene que ser único para que inicie sesión y la contraseña.

Con estos datos nosotros podríamos ya iniciar sesión.

En este caso yo voy a seleccionar que el password nunca aspire y ya tendríamos creado un usuario.

Si yo me voy nuevamente a las propiedades del usuario, me vuelve a aparecer el mismo asistente o la misma consola donde creé el usuario y aquí voy a tener un poco las diferentes opciones relacionadas con el objeto usuario, es decir, cada uno de estos elementos me va a permitir crear un dato en un atributo que pertenece al objeto de usuario.

Muchas veces nosotros creamos un usuario, asignamos la contraseña, asignamos en la parte de organización aquí todos los datos de la empresa, el departamento, la compañía, etc.

Y una de las cosas que muchas veces no se hace en las organizaciones y tiene importancia en la parte de seguridad es asignar, por ejemplo, las horas a las que el usuario puede iniciar sesión.

Entonces yo lo que puedo hacer, por ejemplo, es que puedo seleccionar que si este usuario el fin de semana no va a iniciar sesión o no tiene que realizar trabajo, pues que no pueda iniciar sesión o que no pueda iniciar sesión a unas determinadas horas de la noche.

De esta manera nosotros estamos impidiendo que ese usuario pueda iniciar sesión en el dominio dentro de ese horario que no está permitido.

Y esto tiene una serie de ventajas.

Por ejemplo, nosotros aunque no pensemos que ese usuario vaya a realizar un ataque, sí que alguien puede hacerse con las credenciales de ese usuario o sí que un malware puede interactuar con las credenciales con el uso de ese usuario.

Entonces no vamos a tener la misma capacidad de reacción un día de semana en horario laboral que a lo mejor un sábado a las dos de la mañana.

Entonces es una medida que puede marcar la diferencia en los tiempos de reacción cuando una identidad es vulnerada.

Otro elemento que podemos configurar es en qué equipos inicia sesión el usuario.

Entonces por defecto vemos que un usuario puede iniciar sesión en cualquier equipo.

Esto no es del todo cierto porque un usuario, por ejemplo, que no tenga privilegios no puede iniciar sesión en un controlador de dominio, no lo tiene permitido.

Pero eso es por una configuración del controlador de dominio, no por una configuración del usuario.

Entonces una de las cosas que podemos configurar cuando creamos un usuario es que sólo pueda iniciar sesión en determinados equipos.

La mayor parte de los usuarios sólo deberían poder iniciar sesión en los dispositivos que van a utilizar, en los dispositivos que le pertenecen.

Entonces son pequeñas acciones, pequeños detalles en la parte de configuración que nosotros tenemos que tener claros porque pueden marcar una diferencia en lo que se refiere a la parte de seguridad.

Luego tendríamos aquí la opción de miembro de es decir, a qué grupos pertenece.

También la configuración relacionada con los objetos de password, lo veremos más adelante.

El perfil del usuario, que bien podemos definir un perfil local o podemos definir un perfil en un servidor central.

Es una de las opciones más interesantes, aunque también es verdad que muchas de estas opciones ahora mismo están cambiando con la integración de las infraestructuras con la nube.

En muchos casos ahora los usuarios utilizan un dispositivo con una cuenta de Microsoft 365 que a su vez está sincronizada con OneDrive y nosotros almacenamos los datos de ese usuario en la nube, bien en la parte de OneDrive, en la parte de SharePoint o en la parte de infraestructura que nosotros tengamos desplegada a la nube.

Luego tendríamos las políticas de autenticación, las policy sidos y luego tendríamos la parte de extensiones.

Dentro de la parte de extensiones recordamos el editor de atributos e importante, el distinguishname.

El distinguishname siempre va a tener este aspecto, CN, en este caso, Argel CN Users, desde Hackers, desde acá.

Otro elemento importante, aparte del Distinguish Name, es el Identificador de seguridad, que es este, el SID.

Y este identificador de seguridad es el que se va a asignar a los permisos.

Mucho ojo con esto, porque cuando yo doy permisos a un usuario, cuando yo doy permisos a un grupo, realmente lo que asocio a ese recurso, a ese servicio, a esa aplicación, es el identificador de seguridad, es el nombre del objeto, no es el distinguido, no es el nombre del usuario, no es el UP, es el identificador de seguridad, el SIT relacionado con ese objeto, que bien puede ser un usuario, bien puede ser una cuenta de equipo, o bien puede ser un grupo de seguridad.

Si yo, por ejemplo, elimino un usuario y tengo habilitada la papelera de reciclaje, voy a dar aquí a borrar el usuario, elimino este usuario y si me voy a la parte de objetos eliminados, voy a encontrar aquí el usuario.

Si yo doy aquí a restaurar, puedo seleccionar que se restaure donde estaba, es decir, en la carpeta de usuarios, o puedo seleccionar que se restaure a la ubicación que yo quiero.

Entonces yo podría seleccionar aquí una unidad organizativa u otro contenedor.

En este caso voy a seleccionar la carpeta de usuarios y volvemos a tener totalmente funcional el usuario aquí.

Otra cosa que nosotros podemos hacer con los usuarios es que podemos desactivarlos.

Una de las cosas que podemos hacer es simplemente damos a desactivar, entonces se nos pondría en otro color diferente, con una pequeña marca y esa cuenta de usuario está desactivada.

Esto es obligatorio cuando nosotros tenemos un trabajador que, por ejemplo, se da interacciones, cuando tenemos un trabajador que, por ejemplo, está en una baja media, entonces en este momento ese usuario no va a realizar la actividad y lo mejor es que tengamos esa cuenta desactivada.

Podemos hacerlo también con otro tipo de cuentas de seguridad que se utilizan para procesos de recuperación de claves, para procesos de recuperación de certificados, donde normalmente ese tipo de cuentas las vamos a tener desactivadas y solo las vamos a habilitar para realizar una determinada tarea y luego volvemos a deshabilitarlas, volvemos a dejarlas inactivas.

Si yo quiero volver a activarlo, simplemente voy aquí, doy Enable y automáticamente esa cuenta vuelve a funcionar correcta.

Si nosotros nos vamos a la parte de herramientas, tenemos otra consola que es la de usuarios y equipos del directorio activo.

Y la consola de usuarios y equipos del directorio activo también nos permite realizar un poco las mismas tareas.

Entonces si yo me voy aquí a la parte de usuarios, vemos que en la parte de usuarios tengo el usuario.

Si yo quiero crear un usuario, exactamente lo mismo, nuevo, voy a usuario, creo el usuario, le pongo el nombre de inicio de sesión, le voy a poner una contraseña y selecciono las opciones de contraseña.

Damos a siguiente y ya tendría creado este otro usuario.

Aparte de este otro usuario, si yo voy a la parte de propiedades, me voy aquí a la parte de propiedades y voy a tener una serie de elementos, como puede ser lo mismo, información sobre el usuario, a qué grupo os pertenece, etc.

Pero si nos fijamos aquí no me aparece, aparece el perfil, pero no me aparecen todas las opciones disponibles.

Esto es porque yo lo que tengo es venir aquí a la parte de vistas y hay una parte donde pone características avanzadas que tengo que tener habilitado para ver toda la estructura del directorio activo.

Veis que me aparecen muchos más contenedores.

Entonces ahora selecciono el usuario, este mismo usuario, me voy a la parte de propiedades y ahora en la parte de propiedades veis que me aparecen aquí muchísimas más pestañas de información, entre ellas me aparece el editor de atributo, donde yo puedo ver los diferentes objetos relacionados con este objeto usuario, entre ellos el Distinguish Name y en la parte de abajo tendríamos el identificador de seguridad, este si, el identificador de seguridad, que es el objeto que se utiliza para asignar los permisos relacionados con las cosas que puede realizar o que tiene permitido hacer este determinado usuario.

Otro elemento que debemos tener en cuenta son los grupos.

Una administración a base de dar permisos a cada uno de los usuarios de forma individual sería muy difícil de mantener, sobre todo organizaciones grandes.

Entonces generalmente lo que vamos a hacer es que vamos a organizar los usuarios dentro de grupos.

Van a pertenecer a uno o varios grupos y lo que vamos a hacer es luego hacer las configuraciones sobre esos grupos, otorgar los permisos a esos grupos.

Vamos a tener dos tipos de grupos de distribución y grupos de seguridad.

Los grupos de distribución no tienen un identificador de seguridad, por lo que no podemos asignar permisos a estos grupos.

Su función es para tareas de envío de correo.

Los grupos de seguridad sí que tienen un identificador de seguridad, vamos a poder asignar permisos a estos grupos y además los grupos de seguridad también se les pueden asignar funcionalidades relacionadas con Luego vamos a tener diferentes áreas de ámbito de un grupo, Entonces vamos a tener grupos locales de los equipos que sólo van a funcionar o solo van a permitir acceso dentro del propio equipo.

Luego tendremos los grupos locales de dominio que van a permitir acceso a los recursos del dominio, Los grupos globales que van a permitir el acceso a objetos a través de todo el bosque.

Y esto es muy importante porque los grupos por defecto que se crean son grupos globales de dominio.

Esto quiere decir que normalmente la pertenencia a un grupo otorga privilegios a lo largo de todos los dominios del bosque.

Es decir, habíamos explicado que cuando nosotros teníamos un bosque con varios dominios, aunque esos dominios tengan nombres diferentes, como están en el mismo bosque hay una relación de confianza de seguridad implícita.

Un usuario de un dominio puede iniciar sesión o acceder a recursos de otro dominio que está en el mismo bosque y esto es porque normalmente pertenecen a grupos globales de seguridad.

Luego tendríamos los grupos universales que compilan características de los grupos globales y locales de dominio para utilizar en redes que sean multidomin.

Tenemos además una serie de grupos con privilegios que son los que tenéis en la diapositiva, que son los administradores de empresa, administradores de esquema, administradores de baby, Operadores de ser.

Todos estos grupos son grupos con privilegios y debemos tenerlos siempre controlados.

Hay que tener siempre muy presente cuando unimos un usuario a uno de estos grupos o cuando un determinado usuario está utilizando los privilegios de pertenecer a alguno de estos elementos, a una de estas Estamos en usuarios equipos de Active Directory y lo mismo que nosotros tenemos usuarios, pues aquí vamos a poder crear grupos.

Si damos botón derecho, seleccionamos Nuevo, seleccionamos grupo que nos va a aparecer aquí para poner el nombre del grupo y vamos a ver que tenemos aquí las opciones de que el grupo sea Grupo de seguridad, Grupo de distribución, Grupo de dominio local, Grupo Global o Grupo universal.

La configuración por defecto es Grupo de seguridad global.

Una vez que nosotros creamos el grupo, nosotros automáticamente desde el grupo podemos añadir ese grupo a otro grupo.

Podemos ir a la parte de propiedades y dentro de la parte de propiedades podemos ir a la parte de miembros y aquí podemos añadir a un determinado usuario.

Seleccionamos el usuario automáticamente va a pertenecer a ese grupo.

Si nos vamos al editor de atributos, vamos a tener exactamente un Distinguish Name, exactamente igual que tienen los usuarios, porque el grupo es un objeto dentro de Active Directory, y vamos a tener también un identificador de seguridad, un SI que vamos a tener aquí, que es el que se va a utilizar para asignar los permisos.

Si yo selecciono un usuario, voy a este usuario, puedo lo que es aquí directamente añadirlo a un grupo, selecciono el nombre del grupo y automáticamente ese usuario pertenecería a ese grupo.

Si yo ahora entro en el grupo, voy a la parte de miembros y vemos que tenemos ya dos usuarios incluidos en ese grupo.

Además nosotros tenemos las cuentas de equipo.

Las cuentas de equipo van a ser aquellas que representan los diferentes dispositivos que hemos unido a un vídeo.

Las cuentas de equipo se almacenan por defecto en un contenedor llamado Computers, pero lo recomendable es que se genere una estructura donde la desorganización y que esas unidades organizativas sean las que tengamos las diferentes cuentas de equipo.

Podemos reconfigurar el contenedor por defecto para que cuando un equipo se una al dominio, en vez de ir a la carpeta de Computers, se vaya a una unidad organizativa, por ejemplo que le llamemos Equipos nuevos, donde se le apliquen automáticamente una serie de configuraciones previas y después ya movemos esa cuenta de equipo la ubicación de la unidad organizativa que nosotros queramos.

Además las unidades organizativas nos van a permitir también hacer delegaciones o nos van a permitir también personalizar las configuraciones mediante objetos de directiva de grupo.

Hablaremos en vídeos posteriores con más detalle de las unidades organizativas.

Otro elemento que debemos tener en cuenta es que cuando nosotros unimos un equipo al dominio, se crea un canal de seguridad entre ese equipo y el controlador de dominio.

Debemos tener en cuenta organizativas.

Hablaremos en vídeos posteriores, los controladores de dominio y hay un intercambio de claves entre ese equipo y el controlador de dominio ya hay un intercambio de claves, se almacena la clave tanto en el equipo como en el controlador de dominio y tienen que coincidir esas claves para poder generar una comunicación correcta.

Hay una serie de casos en los que se puede romper ese canal de seguridad, como por ejemplo cuando se reinstala un equipo o se genera un proceso de backup o un checkpoint desde una máquina virtual.

Pues en ese momento el controlador de dominio puede manejar un password para esa cuenta de equipo y el equipo puede tener un password diferente, porque el password se va actualizando de forma automática cada 30 días.

Entonces, generalmente el procedimiento que hace la mayor parte de la gente es sacar ese equipo del dominio, eliminar esa cuenta y volver a meter el equipo del dominio y funciona realmente.

El equipo puede volver a unirse al dominio, se genera un nuevo par de claves que es la misma en este caso para el controlador de dominio y el equipo, y el equipo puede conectar.

Pero esto va a generar entornos que son inconsistentes, nos puede generar problemas porque cuando nosotros sacamos un equipo del dominio y volvemos a introducirlo, el Distinguish Name, el UPN es el mismo.

Yo saco equipo 13 y vuelva a inventor equipo 13 va a tener el mismo Distinguish Name, pero el identificador de seguridad, el SIP va a ser diferente, se va a crear un nuevo SIP y se le va a asignar al equipo.

Esto quiere decir que si yo he dado permisos o he hecho configuraciones en las que está incluido el identificador de seguridad de esa cuenta de equipo, pues me van a fallar.

Entonces hay que tenerlo en cuenta.

Cuando nosotros estamos trabajando con algún tipo de permiso sobre una cuenta de equipo, tenemos opciones para restaurar este canal de seguridad, tener que sacar el equipo del dominio y la forma correcta de hacerlo sería a través de comandos como Netto NLT, mediante Windows PowerShell Contest, Computer Security Channel Repair o incluso mediante usuarios equipos Active Directory manda el botón de reset a la cuenta.

Tenemos opciones para restaurar este canal de seguridad sin tener que sacar el equipo del dominio y la forma correcta de hacerlo sería a través de comandos como NetDO MLT, mediante Windows PowerShell Contest, Computer Security Channel Repair o incluso mediante usuarios equipos de Active Directory da el botón de reset a la cuenta.

Aunque esta última opción yo reconozco que no me funciona, pero sí que funciona, por ejemplo Windows PowerShell o Netum funcionan bastante bien.

Como conclusión, entender que Active Directory es un entorno donde nosotros vamos a generar una serie de objetos y donde es fundamental planificar correctamente toda la estructura del directorio activo, generar una estructura de unidades organizativas y planificar los grupos que vamos a utilizar y quién va a pertenecer a esos grupos.

Esto nos va a permitir desarrollar organizaciones que son seguras y escalables.

Hay una serie de grupos controlados por el sistema operativo, que son identidades especiales como Anonymous, Logo Everyone, Interactive Network o los propietarios de un determinado recurso.

Entonces hay que entender también cómo funcionan estos grupos para mantener unos niveles de seguridad aceptables.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.