Administración de Usuarios

Transcribed on August 4, 2025 at 10:07 AM by Minutes AI

Speaker 1 (00:07)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a hablar de la administración de usuarios y permisos, vamos a hablar de los usuarios de Windows, hablaremos de los grupos, ya hablaremos de los permisos del sistema de archivos NTFS y las ACL que son las que gestionan estos permisos.

El sistema de permisos de Windows sobre NTFS es un excelente recurso para administrar los privilegios de los usuarios sobre los recursos de archivos.

Nos permite ajustar perfectamente las opciones para que un usuario pueda acceder o no a dichos recursos.

Actualmente el protocolo NTFS está bien diseñado y no se conocen graves problemas de seguridad.

Las configuraciones por defecto no son excesivamente relajadas.

Y para afinar el control de permisos NTFS primero es necesario entender los grupos de usuarios de Windows.

Dentro de los grupos de usuarios tenemos el usuario administrador, que tiene el control absoluto del sistema, no puede ser borrado y a partir de Windows Vista está deshabilitado por defecto, aunque si arrancamos a modo prueba de fallos con F bastará habilitado.

Luego tenemos el usuario invitado, permite acceder al equipo por red si hay recursos compartidos sin necesidad de usuario y contraseña, aunque con privilegios restringidos.

Está deshabilitado por defecto y además se recomienda que se mantenga deshabilitado.

Y luego el usuario inicial, es el usuario que se crea durante el proceso de instalación del sistema operativo.

Se asigna al grupo de administradores.

Existen otras cuentas especiales del sistema operativo que Microsoft utiliza para ejecutar varios servicios.

Estas cuentas especiales de Windows La cuenta de sistema, que pertenece al grupo de administradores y dispone de todos los privilegios sobre el sistema.

Un administrador podría ejecutar con privilegios de SYSTEM.

A través del comando ADD se creará una tarea que se ejecuta como SYSTEM.

A partir de Windows Vista nada que se ejecute bajo SYSTEM se muestra en pantalla.

Habría que utilizar por ejemplo la herramienta de SysInternal PSsec y de esta manera podríamos ejecutar algo que tendría salida forzosa por pantalla, aunque se ejecutará bajo SYSC.

Luego tenemos LOCAL service, que presenta credenciales anónimas en la red y tiene pocos privilegios, tiene permiso de presentación en el sistema.

Y luego tenemos NETWORK SERVICE, que actúa como el sistema a la red.

Es posible listar las cuentas de usuario en Windows con el comando que tenéis en la diapositiva.

Los grupos de Windows son los Tenemos el grupo Administradores, que es el grupo que tiene permisos completos sobre el sistema y a este grupo sólo debería pertenecer el administrador y el usuario creado para administrar el equipo.

Tenemos los operadores de copia que proporcionan servicios para realizar copias de seguridad y no está destinado al uso de usuarios, sino más bien para programas o tareas que se ejecutan en el sistema.

Tendríamos al grupo Invitados.

Este grupo tiene un acceso limitado al sistema y se recomienda dejar deshabilitado.

Tenemos operadores de red que poseen privilegios para la configuración de TCP IP del equipo.

Y después tenemos el grupo Usuarios.

Los usuarios con acceso limitado al sistema son los usuarios creados por defecto cuando los creamos con el administrado y pueden ejecutar aplicaciones pero no realizar modificaciones críticas en el sistema.

Hay otros grupos especiales del sistema que son los que vamos a enumerar a continuación.

Sería el grupo Propietarios, que es el grupo al que pertenece la cuenta que ha creado o tomado posesión de un objeto, de un fichero, de una carpeta y tiene todas las licencias sobre ese objeto.

Luego tenemos el grupo Todos que incluye a cualquiera que tenga acceso al equipo con o sin contraseña.

Tendríamos el grupo Interactivo que son los usuarios locales que se presentan al sistema introduciendo usuario y contraseña.

El grupo Network, que son los usuarios que acceden mediante la red, usuarios autenticados que acceden al sistema mediante una identidad y contraseña válida, Anonymous, Logo, que son usuarios anónimos, por ejemplo cuando se utiliza un servicio como Internet Information Service, servicio web, pues nosotros hacemos una solicitud de la página web con un usuario anónimo.

Y luego tenemos los usuarios de servidor de terminal que son los que se conectan utilizando Terminal Server.

Estos grupos no son administrados por el usuario, el propio sistema asigna la pertenencia a estos grupos para diferentes propósitos.

Bueno, vamos a la máquina virtual.

Bueno, estamos en la máquina virtual, nos vamos a la administración de equipo.

Dentro de la parte de administración de equipo nos vamos a la parte de usuarios y grupos y aquí tendríamos los diferentes usuarios que nosotros tuviéramos en el dispositivo, en el equipo vemos los usuarios que tenemos el usuario administrador, tendríamos aquí el usuario de inicio, otro usuario sin privilegios, tendríamos la cuenta por defecto y la cuenta de invitados.

Si nosotros seleccionamos cualquiera de estos usuarios podemos ir a la parte de propiedades y dentro de la parte de propiedades podemos ver las opciones de configuración podemos ver si pertenecen a un determinado grupo, incluso podemos añadirlo a diferentes grupos y tendríamos aquí la parte del perfil, luego tendríamos aquí la parte de grupos.

Dentro de la parte de grupos tenemos los diferentes grupos que tenemos disponibles en el sistema operativo y luego tendríamos aquí una descripción con información sobre para qué sirve este determinado grupo.

Otra manera que tenemos de poder ver información sobre los grupos o sobre los usuarios es si abrimos una consola y nosotros desde aquí podemos utilizar diferentes comandos para lo que sería la parte de administrar los grupos o para verificar la información de los usuarios o los grupos.

Una de las opciones sería utilizar el comando vmicuseracountlistful que nos daría información sobre las diferentes cuentas que vamos a tener en el dispositivo.

Tenemos información detallada sobre las cuentas que tenemos en el dispositivo y las características y atributos de estas cuentas.

De esta manera veríamos información detallada sobre el usuario que estamos utilizando, información sobre los permisos relacionados con el usuario y los tokens que tenemos o los privilegios que tenemos asignados relacionados con ese usuario.

También podríamos utilizar el comando juanmigroups para ver información relacionada con el uso de los grupos en el sistema de ficheros NTFS.

La protección mediante ACLs van a definir los permisos de los usuarios, grupos o programas.

Sobre los objetos tenemos tres tipos de listas de control de acceso Tenemos las DACL que son discrecionales, definidas por el administrador o por el dueño del objeto, tenemos las MACL que son mandatory predefinidas por el sistema y que no están bajo el control del usuario o dueño de un objeto y no hay una forma gráfica de establecerlas o administrarlas.

Y tenemos las SACL que son reglas del sistema que permiten auditar el acceso a objeto.

El sistema de permisos puede administrarse gráficamente con las propiedades de los objetos en la pestaña de seguridad o por línea de comandos con IKCLS.

La forma correcta para trabajar con los permisos de seguridad es configurar permisos de permitir.

Si algo no se permite tiene una denegación implícita.

Solo se asignan permisos de denegar en situaciones muy específicas porque prevalecen sobre los permisos de permitido.

La recomendación es asignar permisos a grupos antes que a usuarios y a carpetas en lugar de archivos.

Permite una administración que es más eficiente al mover o copiar archivos entre volúmenes.

Con sistemas NTFS permite conservar los permisos propios del objeto, aunque no los permisos heredados.

También se puede modificar o configurar la herencia de permisos de un determinado objeto.

Además, la pestaña de permisos efectivos o acceso efectivo ofrece la posibilidad de auditar el acceso de un determinado usuario en función de los grupos a los que pertenezca y diferentes permisos asignados.

Si nosotros queremos ver las opciones de ICACLS, simplemente lo ponemos en una consola de comandos y nos aparecerían todas las opciones que tendríamos disponibles con los diferentes parámetros que tenemos para la asignación y administración de permisos.

Vemos que es un comando que tiene muchísimos parámetros y en la parte de abajo del todo vamos a tener también diferentes ejemplos que nos muestran cómo sería el uso de este comando.

Vemos en la parte del final de la información de la ayuda, donde nosotros vamos a tener también diferentes elementos o diferentes ejemplos que nos muestran cómo se utilizaría.

Y de ACLS.

Bueno, si nosotros creamos un objeto, por ejemplo una carpeta, creamos la carpeta confidencial y si nos vamos a la parte de propiedades, dentro de la pestaña de seguridad, en permisos avanzados, nosotros vamos a tener aquí los diferentes permisos que tenemos asociados a este objeto.

Estos permisos recordad que son permisos de NTFS del sistema de archivos.

Si nosotros aquí damos añadir, podemos seleccionar cualquier usuario o cualquier grupo y podemos darle permisos a ese determinado grupo.

Si le damos permisos de lectura al usuario anónimo, pues tendríamos aquí esos permisos asignados.

Tenemos la posibilidad también aquí de editar la herencia, podemos convertir los permisos heredados en permisos del objeto o podemos eliminar la herencia de estos objetos.

Tendríamos aquí la pestaña de auditoría y tendríamos aquí la pestaña de acceso efectivo.

Si nosotros seleccionamos aquí un usuario, por ejemplo voy a seleccionar el usuario ángel, damos a OK, vemos los permisos efectivos y podemos ver la información relacionada con los permisos que tiene el usuario ángel sobre este determinado objeto.

Para concluir, la gestión de identidades y un buen conocimiento de los grupos y de los usuarios, junto con la administración de permisos sobre los objetos, nos van a ofrecer un mecanismo eficiente para gestionar correctamente el acceso a los datos, a los servicios y al dispositivo.

Es fundamental entender las características y los pormenores de todos estos elementos para mantener unos niveles adecuados de seguridad en el sistema de archivos NTFS y los objetos del sistema operativo Windows.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.