Configuración de sistemas operativos (Sistemas informáticos)

Configuración de usuarios y grupos locales

Los sistemas operativos actuales se pueden utilizar por uno o varios usuarios, en algunos sistemas pueden hacerlo simultáneamente y en otros no. Los usuarios se pueden crear localmente o en red, la gestión de usuarios locales sólo afecta al equipo desde el que se crean, modifican, eliminan, etc.

Los usuarios locales sólo sirven para iniciar sesión o acceder a recursos en el propio equipo, en cambio los usuarios en red pueden iniciar sesión en cualquier equipo de la red.

En la mayoría de los sistemas operativos, las personas que los utilizan necesitan autentificarse mediante una cuenta de usuario y, además, tener autorización para utilizar recursos como, por ejemplo, un archivo, una carpeta, un dispositivo, etc. Cuando hablamos de recursos, nos referimos a un elemento del sistema operativo que se puede controlar.

Algunas de las gestiones sobre usuarios y grupos que veremos hacen referencia a configuraciones propias de sistemas operativos en red (Windows Server) con instalaciones de un Directorio Activo (Active Directory).

Seguridad de cuentas de usuario

Usuarios

Las personas que quieren utilizar un sistema operativo necesitan disponer de un nombre de usuario y una contraseña.

Los usuarios deberían ser únicos e individuales aunque a veces no es así, esto conlleva un importante riesgo de seguridad porque no se identifica correctamente a los usuarios dentro del sistema.

Para crear un usuario es necesario tener permisos especiales, no todos los usuarios pueden crear otros usuarios.

A la hora de crear un usuario hay que seguir algunas normas que facilitarán recordar los nombres y llevar un correcto control.

Además de las cuentas que vienen instaladas por defecto en el sistema operativo, también se pueden crear otras cuentas. Los usuarios pueden ser administradores o usuarios limitados.

Las operaciones con usuarios son tareas de administración que sólo pueden ser realizadas por usuarios administradores.

Grupos

Un grupo es un conjunto de usuarios que simplifica la administración y la asignación de permisos, concediendo permisos sobre recursos a todo un grupo de usuarios a la vez, en lugar de concederlos a cuentas de usuarios individuales. Los usuarios pueden pertenecer o no pertenecer a uno o varios grupos distintos.

Las operaciones con usuarios son tareas de administración que sólo pueden ser realizadas por usuarios administradores.

Seguridad de contraseñas

Las contraseñas deben satisfacer unos requisitos de complejidad, con los siguientes ejemplos tenemos algunos requisitos que deberían cumplir:

Más información

- https://www.jesusninoc.com/08/27/contrasenas-seguras-con-powershell-generar-contrasenas-seguras/
- https://www.jesusninoc.com/07/03/contrasenas-seguras-con-powershell-longitud-de-la-contrasena/
- https://www.jesusninoc.com/10/20/contrasenas-seguras-con-powershell-la-contrasena-aparece-en-el-diccionario-de-la-rae/
- https://www.jesusninoc.com/07/07/contrasenas-seguras-con-powershell-convertir-en-hash-una-contrasena/
- https://www.jesusninoc.com/07/05/contrasenas-seguras-con-powershell-la-contrasena-aparece-en-google/
- https://www.jesusninoc.com/07/06/contrasenas-seguras-con-powershell-la-contrasena-aparece-en-un-diccionario/

Acceso a recursos. Permisos locales

Los permisos se utilizan para permitir o restringir el acceso a los archivos para determinados usuarios o grupos. Los permisos pueden ser para: leer, modificar, eliminar, renombrar…

En los sistemas de archivos suele ser normal compartir información con otros usuarios, esto hace necesario controlar el acceso a los archivos. Un permiso indica qué cosas puede hacer un usuario o un grupo de usuarios en cualquier archivo

(recordemos que un tipo de archivo era un directorio).

Veamos los permisos en:

Windows

Los permisos se pueden agregar o denegar a un usuario un grupo se usuarios.

En este apartado vamos a ver los seis permisos estándar para el sistema de ficheros NTFS:

- Control total: Cuando se aplica este tipo de permiso a un archivo, se pueden leer, escribir, cambiar y eliminar, también se pueden cambiar permisos de los archivos. En el caso concreto del tipo de archivo carpeta, significa que se permite leer, escribir, cambiar y eliminar.
- Modificar: En el caso de los archivos se pueden leer, escribir, cambiar y eliminar, con este permiso no se pueden modificar los permisos. En el caso concreto de las carpetas se puede leer, escribir, cambiar y eliminar ficheros y subcarpetas.
- Lectura y ejecución: Se puede acceder a los ficheros y ejecutarlos. En el caso de las carpetas se puede ver el contenido de una carpeta y ejecutar.
- Lectura: Se puede ver el contenido de los archivos pero no se pueden ejecutar. En el caso de las carpetas se puede acceder al contenido.
- Escritura: Cuando se aplica a los archivos esto quiere decir que se pueden modificar pero no eliminar. En el caso de las carpetas se pueden añadir fichero y subcarpetas.
- Mostrar el contenido: En el caso de los archivos de tipo carpeta se puede mostrar el contenido que hay en ellos.

Además de estos permisos generales también existen los permisos especiales.

Los permisos pueden ser: permisos explícitos y permisos heredados.

- Los permisos explícitos son aquellos que se establecen de forma predeterminada en archivos que no son secundarios cuando se crea el archivo, o los que crea el usuario.
- Los permisos heredados son los que se propagan a un archivo desde un archivo primario.

De forma predeterminada, los objetos de un contenedor heredan los permisos desde ese contenedor cuando se crean los objetos. Por ejemplo, cuando crea la carpeta ejemplo, todas las subcarpetas y archivos creados en la carpeta ejemplo carpeta heredan de forma automática los permisos de la carpeta. De esta manera, la carpeta ejemplo tiene permisos explícitos, mientras que las subcarpetas y los archivos heredan los permisos.

Los permisos heredados se pueden cambiar desde la configuración avanzada de permisos.

Linux

Los permisos se pueden agregar o eliminar a cada uno de los posibles usuarios del sistema, en Linux los tipos de usuarios son de:

- Propietario (owner): El creador del archivo.
- Grupo (group): Conjunto de usuarios.
- Resto de usuarios (others): Usuarios que no pertenecen a un grupo, ni son propietarios del archivo.

Los permisos en el sistema de fichero ext4 son:

- Permiso de lectura (r, read): Permite ver e imprimir archivos, en el caso de los archivos de tipo directorio se pueden ver todos los elementos.
- Permiso de escritura (w, write): Permite cambiar o

eliminar un archivo, en el caso de los archivos de tipo directorio también se pueden cambiar o eliminar.
- Permiso de ejecución (x, execute): El fichero puede ser usado ejecutado, en el caso de los directorios pueden ser buscados.

Servicios y procesos

Uno de los conceptos más importantes en los sistemas operativos es el proceso que se define como un programa en ejecución. Los programas son un conjunto de archivos que están almacenados en algún dispositivo de almacenamiento (disco duro, USB, etc.) y que por sí solos no tienen ningún funcionamiento, pero cuando ese conjunto de archivos se ejecutan entonces pasan a ser un proceso.

Los procesos en segundo plano que realizan distintas funciones, algunas relacionadas con el sistema operativo y otras no, se denominan servicios, y se están ejecutando permanentemente en el sistema.

Los servicios se pueden iniciar, detener, pausar, reanudar, etc. Estas acciones, normalmente, sólo las puede realizar el administrador de forma local o remota. Un ejemplo de servicio de sistema es el servicio de escritorio remoto, que permite conectarse remotamente al equipo.

Comandos de sistemas libres y propietarios

	Modo texto: Símbolo de sistema	**Modo texto: PowerShell**	**Modo texto: Bash**	**Modo gráfico**

Crear o modificar un archivo	edit	New-Item	vi nombre	Abir el programa mediante el icono
Crear un directorio	mkdir	New-Item	mkdir	Seleccionar la opción crear directorio pulsando al botón derecho
Ver el contenido de un archivo	type	Get-Content	cat	Abrir el programa mediante el icono
Acceder al contenido de un directorio	cd	Set-Location	cd	Abrir el programa mediante el icono
Listar el contenido de un directorio	dir	Get-ChildItem	ls	Abrir el programa mediante el icono
Ver la estructura de un directorio	tree	–	tree	Abir en el explorador
Eliminar un archivo	del	Remove-Item	rm	Botón de la derecha y eliminar
Eliminar un directorio	rmdir	Remove-Item	rm	Botón de la derecha y eliminar
Copiar un archivo o un directorio	copy	Copy-Item	copy	Botón de la derecha y copiar

Mover un archivo o un directorio	move	Move-Item	mv	Botón de la derecha y cortar
Renombrar un archivo o un directorio	rename	Rename-Item	mv	Botón de la derecha y cambiar nombre
Establecer permisos en un archivo o un directorio	icalcs	–	chmod	Botón de la derecha y después propiedades
Copiar un archivo o directorio manteniendo los permisos	xcopy	Get-Acl Set-Acl	–	–
Comprimir y descomprimir un archivo o un directorio	–	–	gzip	Botón de la derecha y comprimir
Imprimir un archivo	print	Out-Printer	lpr	En el menú archivo seleccionar imprimir

Herramientas de monitorización del sistema

Para no tener que recurrir a la restauración de copias de seguridad o reparación del sistema operativo, hay que detectar los problemas antes de que ocurran.