1. GESTIÓN DE MEMORIA

Consiste en la asignación física de memoria (RAM) de capacidad limitada a los distintos procesos que lo soliciten, con el objetivo de activarse y poderse ejecutar, pues solo si los procesos tienen asignada una parte de la memoria pueden pasar ha estado preparados y entrar a ejecución.

La memoria es un recurso compartido, que, a diferencia del procesador, puede ser utilizado simultáneamente por varios procesos.

Sin memoria los procesos no pueden existir por dos motivos fundamentales:

Hace falta una zona donde almacenar el programa o instrucciones.

Para realizar una operación de E/S hace falta una zona de memoria llamada buffer.

1. MEMORIA REAL

**Tenemos distintos tipos de asignación de Memoria.**

1. **Asignación de memoria contigua simple. Monoprogramación.**

**(No hay gestión de la memoria)**

1. **Asignación de memoria particionada**

* **Particiones de memoria contigua.**
* **Fijas (del mismo tamaño): Proceso muy grande y no caber o muy pequeño y desaprovecharse**
* **Variables (de distinto tamaño): si el proceso ocupaba 500mb tenía que estar ese espacio de forma contigua (o seguida).**
* **Particiones de memoria discontinua. (SWAP) se podría**
* **Paginación dividíamos la memoria en marcos (partes) la página se divide el proceso y la RAM en trozo del mismo tamaño llamadas paginas las partes el resto en la swap. Solo necesita tener la página que en ese momento quiera ejecutar.**

**Surgió cuando se empezó a hacer la paginación y la segmentación. Sin esto no podría existir la swap.**

* **Segmentación.**

Es posible comenzar a ejecutar un programa, cargando solo una parte del mismo en memoria, y el resto se cargará cuando se solicite.

Al no necesitarse cargar un programa completo en memoria para su ejecución, se puede aumentar el número de programas cargados en memoria.

MEMORIA VIRTUAL

La memoria virtual nace para solucionar el problema que se plantea cuando tenemos un programa, sus datos y la pila del mismo y ocupan más memoria que la que se posee físicamente. La solución consiste en que el Sistema Operativo deja en la memoria principal las partes del programa que se están usando y el resto se almacena en el disco. Según se van necesitando partes del programa del disco se pasan a la memoria y algunos de la memoria al disco.

LA MEMORIA VIRTUAL en WINDOWS, es ni más ni menos que un fichero que crea el Sistema Operativo, para que en caso de que se llene la memoria RAM, el sistema pueda seguir trabajando.

El tamaño recomendado del área swap en Windows es 1,5 veces la memoria RAM.

SE PUEDE VER A TRAVES DEL FICHERO PAGEFILE.SYS (ESTA OCULTO)

Diagrama

Descripción generada automáticamenteEN WINDOWS SE PUEDE DECIDIR SI LO NECESITAS Y EN LINUX ES UNA PARTICION.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteTexto

Descripción generada automáticamenteLa técnica de la memoria virtual también se conoce como técnica de swapping, por eso cuando se instala un sistema Unix o linux se reserva una parte del disco duro para el SWAP: partición SWAP (FIJA).

Windows 10 – Panel de Control, Sistema y Seguridad, Sistema, Configuración avanzada, configuración avanzada del Sistema o Cambiar configuración, Rendimiento, Opciones avanzadas, CAMBIAR memoria virtual.

Hiberfil.sys 🡪 fichero de hibernación. Guarda el contenido de la RAM durante el proceso de hibernación. Ayuda a la función de inicio rapido.

Swapfile.sys 🡪 Este archivo es usado para cambiar el nuevo estilo de aplicación de Microsoft llamadas aplicaciones “universales” de Windows — conocidas anteriormente como aplicaciones Metro.

Tamaño recomendado 1,5 \* 4096 megas = 6144 Megas valor óptimo de la memoria virtual.

Valor mínimo = 6134

Valor real = 6144

Valor máximo= 6154

Gestión W:

IPconfig /ALL: configuración actual, para la MAC /ALL

Netview: sirve para ver el nombre de las maquinas de nuestro sistema en la red.

Pasos a seguir antes de probar comunicacion:

Misma red interna

La IP (misma subred)

Diferente SID

Diferente MAC

Desactivado el firewall

Gestión W2:

**Windows 10 Home** es la edición de escritorio centrada en el consumidor. Version más básica y si queremos un dominio no será posible.

LA PARTICIÓN DE 500 MB la crea el sistema y no tiene letra.

gestor de discos (DISKMGMT.MSC).

**Autentificación:** Para usar el sistema es necesario abrir una sesión de trabajo (login) para lo cual tendremos que autentificarnos, proporcionando al sistema un nombre de usuario y una contraseña. En caso de no tener una cuenta de usuario abierta en el sistema, será imposible entrar en el mismo.

**Autorización**: Una vez que el usuario se ha autentificado y abierto sesión, cada vez que quiera usar un recurso (un fichero, una carpeta, una impresora, etc) el sistema comprobará si está autorizado o no para realizar esa acción. Los administradores del sistema pueden modificar estas autorizaciones mediante unas listas de acceso.

Usuarios locales.

Un usuario local es una cuenta a la que se puede conceder permisos y derechos para el equipo donde se está creando la cuenta. Está disponible en equipos que no son controladores de dominio, no pueden usarse para conectarse a ningún dominio...

Administrador:

La cuenta del Administrador del sistema (Administrador). Todos los sistemas Windows tienen una cuenta especial conocida como Administrador. Esta cuenta tiene todos los derechos sobre todo el equipo. Puede crear otras cuentas de usuario y es el responsable de gestionar el sistema. Muchas funciones del sistema están limitadas para que solo puedan ser ejecutadas por el Administrador. Es posible crear cuentas de usuario y darles los mismos derechos que la cuenta Administrador (integrándolas como miembros del grupo Administradores), aunque Administrador solo puede haber uno. **Esta cuenta siempre debe contar con contraseña y se crea en el momento de la instalación del sistema.**

Invitado:

La cuenta de Invitado. (Guest). Es la contraria a la cuenta de Administrador, está totalmente limitada, no cuenta apenas con ningún permiso o derecho, pero permite que cualquier usuario pueda entrar en nuestro sistema sin contraseña (lo que se denomina acceso anónimo) y darse un “paseo” por el mismo. Por defecto, en Windows esta cuenta esta desactivada. Es altamente recomendable nunca activar dicha cuenta, ya que representa un riesgo altísimo de seguridad.

Admin pude haber más de uno y cada uno de ellos puede limitar a los administradores.

Admin solo hay uno.

E invitado puede acceder sin autenticación y tiene limitaciones en el sistema.

Nota: No se puede borrar una cuenta de un usuario si tiene sesión abierta en el sistema.

1. Gestion de cuentas usuarios locales y grupos

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInicio – Ejecutar y escribir ó tecla de Windows+R LUSRMGR.MSC para abrir el entorno gráfico del administrador de usuarios y grupos locales desde cmd

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente¿Sabes explicarlo?

**Indica el nombre** que desea dar al usuario para conectarse, con un máximo de 20 caracteres

**El usuario debe cambiar la contraseña en el siguiente inicio de sesión** (está obligado, a la que tu quieres iniciar sesión no puedes porque estarás obligado a cambiar la contraseña).

**El usuario no puede cambiar la contraseña**

**La contraseña nunca expira**

**Cuenta deshabilitada (vacaciones)** No borra la cuenta, pero impide que sea usada. Es el estado por defecto de la cuenta Invitado.

La cuenta está bloqueada: Normalmente esta casilla está desactivada y, en caso de estar activada, se utiliza para desbloquear una cuenta que se ha bloqueado por haber intentado iniciar una sesión un número excesivo de veces sin introducir la contraseña correcta. No se puede utilizar para bloquearla

NETPLWIZ: Crear usuarios.

**Comandos:**

**COMANDOS NET USER:**

* **Net help 🡪 ayuda nosotros veremos la parte de crear usuarios y crear grupos.**
* **Net share🡪 Es para ver las carpetas que tenemos compartidas**
* **Net /? Y Net user /? 🡪 nos dan una breve descripción del comando**
* **Net user /help 🡪 podemos visualizar una ayuda para el comando mucho más detallada.**

**CONSULTAR BASE DE DATOS DE CUENTAS O DATOS DE UNA CUENTA EN CONCRETO**

* **Net user 🡪 Nos muestra los usuarios que tenemos creados ya.**
* **Net user ana 🡪 visualiza la información del usuario indicado**
* **Net user domain—> Nos visualiza los usuarios que tenemos creados en el dominio cuando tenemos un dominio.**

**AÑADIR O CREAR USUARIOS LOCALES.**

* **Net user Luis /ADD 🡪 Nos crea el usuario Luis con todo por defecto**
* **Net user Luis \* /ADD 🡪 Nos pide por teclado la contraseña que va a tener este usuario y asi no se ve en el fichero o en la orden tecleada.**
* **Net user Luis Password1. /ADD🡪 Se crea el usuario Luis con contraseña Password1.**

**REQUERIMIENTO DE PASSWORD AL INICIO DE SESIÓN**

**Net user fulanito passwordreq: yes 🡪 para establecer que la cuenta nos solicite el password al inicio de sesión o no.**

**CONCEDER O REVOCAR EL PERMISO DE CAMBIAR LA CONTRASEÑA AL USUARIO.**

**Net user fulanito passwordchg:yes 🡪 con yes damos permiso al usuario para que el mismo pueda cambar su contraseña, si colocamos el no, el usuario no tendrá permiso para cambiarla**

**CAMBIAR LA CONTRASEÑA A UN USUARIO YA CREADO**

**Net user fulanito \* (TE PEDIRÁ LA NUEVA CONTRASEÑA)**

**Net user fulanito Password2 (ESTABLECE Password2 COMO NUEVA CONTRASEÑA)**

**EXPIRACIÓN DE LA CUENTA**

**Net user fulanito /expires:Never 🡪 la cuenta nunca expira**

**Net user fulanito /expires:mm/dd/aa 🡪 la cuenta expira en la fecha indicada**

**FORZAR CAMBIO DE CONTRASEÑA DE LA CUENTA**

**Net user fulanito /logonpasswordchg:yes 🡪 El usuario debe cambiar la contraseña en el próximo inicio de sesión.**

**RESTRINGIR LAS HORAS DE ACTIVIDAD A UN USUARIO**

**Net user fulanito /times:lunes-viernes,6am-6pm 🡪 Tiene pemiso de inicio de sesión en esa franja horaria (formato 1)**

**Net user fulanito /times:lunes-viernes,8:00-18:00 🡪 Tiene pemiso de inicio de sesión en esa franja horaria (formato 2)**

**DESHABILITAR/HABILITAR UNA CUENTA DE USUARIO**

**Net user Luis /active:no** 🡪 Deshabilitamos la cuenta

**Net user Luis /active:yes** 🡪 Esta es la opción por defecto y quiere decir que la cuenta está activa

**BORRAR USUARIOS**

Net user Luis /delete 🡪 Borramos el usuario Luis

**PODEMOS HACER USO DE ESTOS COMANDOS EN EL MOMENTO DE LA CREACIÓN DEL USUARIO COMO SE VE EN LOS DOS SIGUIENTES EJEMPLOS.**

* **Net user mama P@ssw0rd /passwordchg:yes /ADD**: 🡪 crea el usuario mama con la opción de poder cambar la contraseña, si ponemos /paswordchg:no restringimos ese privilegio y el usuario no podrá cambiar la contraseña.
* **Net user mama P@ssw0rd /logonpasswordchg:yes /fullname:”cuenta de mama” /comment:”Descripción de la cuenta”/ADD** 🡪 crea el usuario mama con password
* **/logonpasswordchg:yes /no** Con esto establecemos que en el próximo inicio de sesión el usuario deberá cambiar la contraseña.
* **/fullname**:”cuenta de mama” con esto establecemos que el nombre completo del usuario será lo que pongamos entre comillas.
* **/comment**:” Descripción de la cuenta” con esto establecemos una breve descripción del uso que tendrá esta cuenta

Con el comando **net user /help**

Tabla

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteVemos en la sintaxis, como además de los elementos anteriores podemos escribir algunas opciones. Las opciones más utilizadas son las siguientes:

Obviamente la mayor potencia de la interfaz de línea de comandos, (shell de texto o CLI) aparece cuando usamos scripts. Estos scripts son pequeños programas que podemos realizar con un editor de texto y que se ejecutan directamente en nuestro sistema operativo.

**GRUPOS**

**CONSULTA BASE DE DATOS DE GRUPOS Y DATOS DE UN GRUPO EN CONCRETO.**

* Net localgroup 🡪 visualiza los grupos creados
* Net localgroup familia 🡪 Nos visualiza los usuarios que pertenecen al grupo familia

**CREACIÓN Y BORRADO DE UN GRUPO.**

* Net localgroup familia /add 🡪 nos crea un grupo local con nombre familia
* Net localgroup familia /delete 🡪 Eliminamos el grupo familia

**AÑADIR O ELIMINAR USUARIOS DE UN GRUPOS.**

Una vez hemos creado el grupo familia, el siguiente paso es añadir miembros al grupo. Un grupo puede contener 🡪 usuarios, contactos, equipos u OTROS GRUPOS.

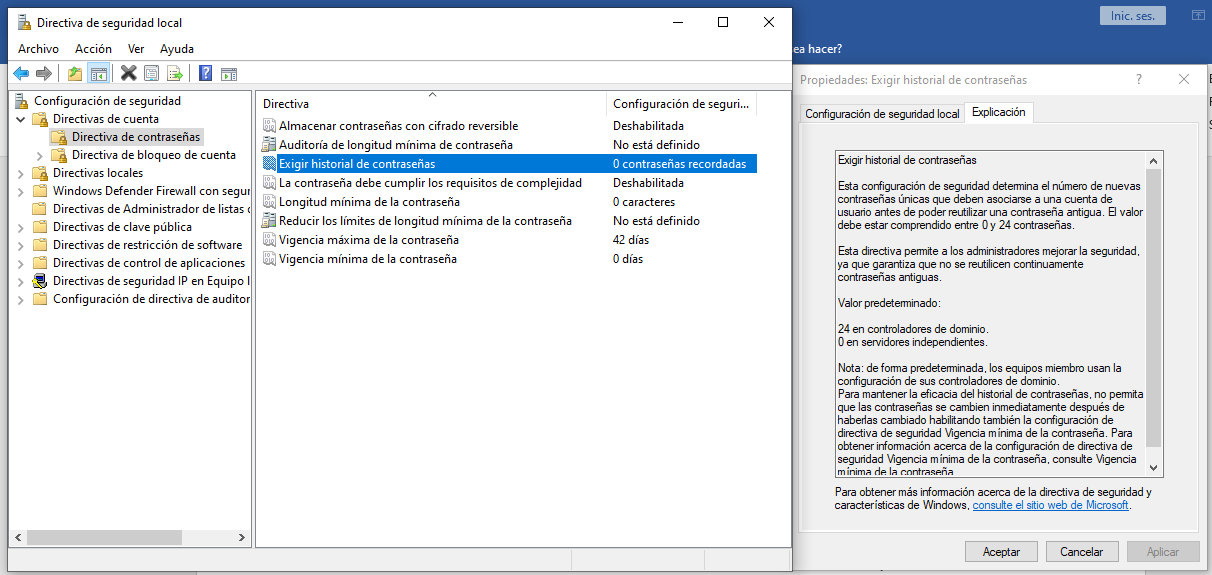
* Net localgroup familia jefe1 jefe2 /add 🡪 Agrega los usuarios jefe1 y jefe2 al grupo familia. (ojo, hemos añadido 2 usuarios de golpe, hay que teclearlos con espacios pero sin comas entre ellos)
* Net localgroup familia jefe1 /delete 🡪 Eliminará el usuario jefe1 del grupo familia

**DIRECTIVAS DE SEGURIDAD LOCAL**

Windows es un sistema operativo muy configurable por parte del usuario. Aunque estas configuraciones suelen estar algo ocultas para que no sean accesibles por los usuarios normales, y solo pueden ser modificadas desde las consolas del sistema.

En concreto, desde la consola de Configuración de Directivas de Seguridad Local, podemos gestionar varios aspectos sobre las contraseñas. Esta consola se denomina **SECPOL.MSC**, y para gestionar las contraseñas, debemos entrar en Configuración de Seguridad, Directivas de Contraseña. **: InicioHerramientas Administrativas Directiva de Seguridad local.**

Las configuraciones más útiles que podemos gestionar desde aquí son:

**DIRECTIVAS DE CONTRASEÑAS**

* Interfaz de usuario gráfica, Aplicación

  Descripción generada automáticamenteForzar el historial de contraseñas. Impide que un usuario cambie su contraseña por una contraseña que haya usado anteriormente, el valor numérico indica cuantas contraseñas recordará.
* Las contraseñas deben cumplir los requerimientos de complejidad. Obliga a que las contraseñas deban cumplir ciertos requerimientos, como son mezclar letras mayúsculas, minúsculas y números, no parecerse al nombre de la cuenta, etc.

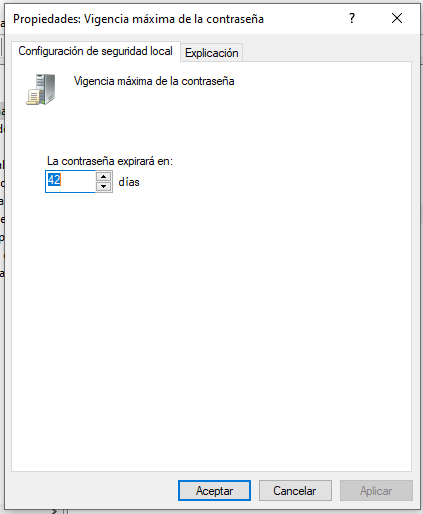
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación

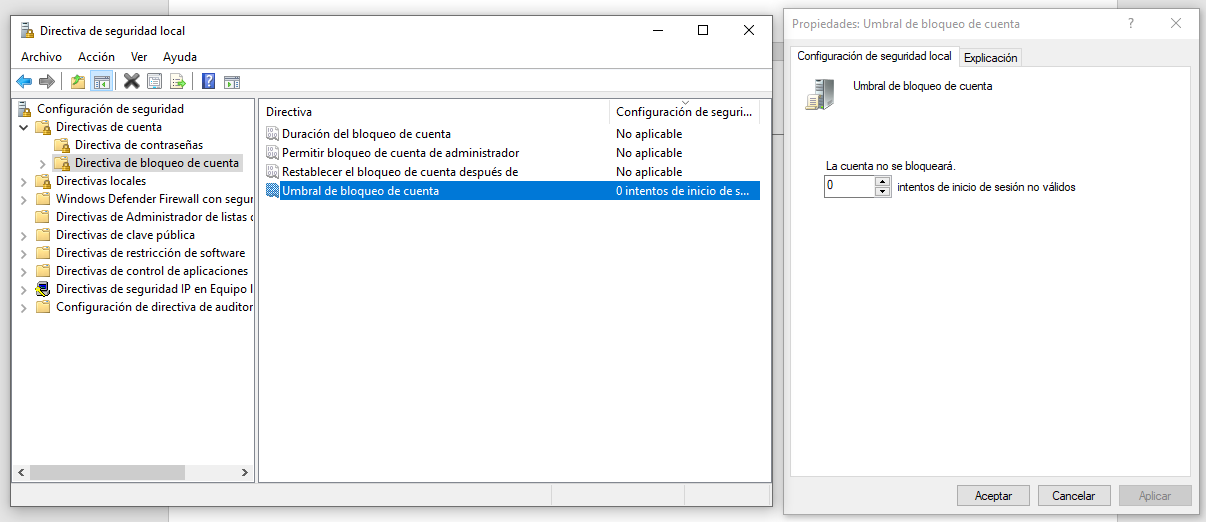
Descripción generada automáticamente

* Interfaz de usuario gráfica, Texto, Aplicación

  Descripción generada automáticamenteLongitud minina de la contraseña. Indica cuantos caracteres debe tener la contraseña como mínimo, un valor cero en este campo indica que pueden dejarse las contraseñas en blanco.
* Vigencia máxima de la contraseña. Las contraseñas de los usuarios caducan y dejan de ser validas después del número de días indicados en esta configuración, y el sistema obligará al usuario a cambiarlas. (Recordemos que al crear una cuenta de usuario podemos indicar que la contraseña nunca caduca para esa cuenta).
* Vigencia minina de la contraseña. Indica cuanto tiempo debe transcurrir desde que un usuario se cambió la contraseña, hasta que puede volver a cambiarla.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**GESTIÓN DE CONTRASEÑAS**

* Desde la Configuración de seguridad local (secpol.msc) también podemos gestionar el comportamiento de las cuentas de usuario relacionado con las contraseñas, y por ejemplo bloquear las cuentas si se intenta acceder al sistema con las mismas, pero usando contraseñas incorrectas.
* Esta configuración la encontramos en Configuración de Seguridad – Directivas de Cuenta – Directivas de Bloqueo de Cuentas) **InicioHerramientas Administrativas Directiva de Seguridad local Directivas de bloqueo de cuentas.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Aquí podemos configurar:

* Duración del bloqueo de cuenta. (Durante cuanto tiempo permanecerá una cuenta bloqueada si se supera el umbral de bloqueo. Un valor cero indica que la cuenta se bloqueará hasta que un Administrador la desbloquee).
* Restablecer la cuenta de bloqueos después de. (Indica cada cuanto tiempo se pone el contador de intentos erróneos a cero).
* Umbral de bloqueo de la cuenta. (Indica cuantos intentos erróneos se permiten antes de bloquear la cuenta).

SID:

El DNI que usa el sistema para referirse a las cuentas de usuario se denomina SID. (Security IDentifier o Identificador de Seguridad). Es posible ver los SID que se le asignan a nuestros usuarios y grupos con la orden **whoami.exe** y tiene que ser único. RID es el último numero de 4 cifras.

RUNAS /USER:ANA CMD

Ponemos CMD porque es la aplicación que queremos ejecutar como fulanito, pero podría ser otra aplicación la que quisiéramos ejecutar.

Who: quien tiene sesión iniciada.

WHOAMI /GROUPS.

**AUTOMATIZAR LA CREACIÓN DE USUARIOS**

Se hace para evitar trabajo.

**For /F:** Se utiliza para que acuda a un archivo, y se ejecute tantas veces como líneas tenga el archivo (bucle).

**Do**: detrás del do se le dice lo que queremos que ejecute con cada uno de los valores.

**Tokens**: se indican los campos que hay definidos en el fichero de datos de contrataciones.

**Delims**: le indicamos que carácter vamos a utilizar para separar un campo de otro, en este caso para separar el apellido del nombre, de la contraseña, del departamento… utilizo un \*.

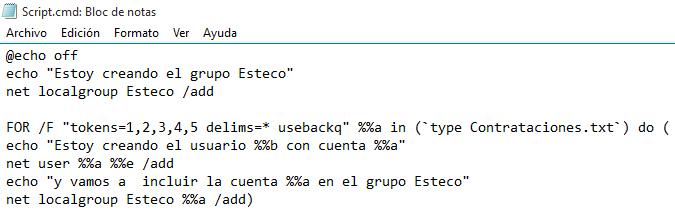
**Usebackq**: este delimitador es para decirle que en el type se van a utilizar las comas invertidas.

**Type:** contrataciones.txt = le decimos que nos visualice el contenido del fichero indicado.

**Net localgroup /add**: se utiliza para gestionar los grupos locales en un equipo, si añadimos el nombre del grupo y el nombre del usuario, añadiremos ese usuario a ese grupo respectivo. Por el contrario, si ponemos solo el nombre con el parámetro /add únicamente crearemos ese grupo.

**Net user /add**: se utiliza para gestionar usuarios locales. Con el parámetro /add crearemos ese usuario además de poder añadirle más opciones como la contraseña (como en el script que hemos realizado).

**echo:** es un comando que se utiliza para la impresión de un texto en pantalla.

**@echo off**: se usa para evitar que todos los comandos del archivo se muestren en la pantalla.

@echo off

echo "VAMOS A CREAR USUARIOS"

for /f "tokens=1,2,3,4 delims=; useback" %%i in (`type AltaDpto.txt`) do (

if "%%l" == "chapa" (

net user %%i %%k /add)

**For /L %%i in (10,1,30) do (net user usuario%%i P@ssw0rd /add)**

For /L sirve cuando ya sabes como se van a llamar los usuarios y quieres que lleven un cierto orden (usuario1, usuario2, usuario3).

(10,1,30)

comienzo, pasos que quieres dar (de uno en uno), hasta el 30.

Se van a crear 20 usuarios.

ACL Lista de Control de Acceso:

Cuando un usuario intenta acceder a un recurso, pide autorización al recurso para hacerlo. El recurso comprobará entonces si en su ACL aparece el SID del usuario, y en caso contrario, comprobará si en su ACL aparece el SID de algún grupo al que pertenezca el usuario.

Si aparece en la ACL algún SID del usuario, el recurso comprueba si la acción que quiere realizar el usuario (leer, borrar, escribir, etc.) está permitida para ese SID en su ACL, si lo está le autoriza para hacerlo, en caso contrario se lo impide.

Explícitos: Son aquellos que se establecen de forma predeterminada, cuando se crea el objeto.

Heredados: Son aquellos que se propagan a un objeto desde un objeto principal. Los permisos heredados facilitan la tarea de administrar permisos y garantizar la coherencia de los permisos entre todos los objetos. (Quitar la herencia y lo pones explícitos)

**Permisos de compartición y de seguridad (ntfs):**  
Primero actúa el permiso de compartir antes que el de seguridad (ntfs)

Los permisos de Compartición son el máximo de permisos concedidos, pero tenerlos en compartición no significa poder llevarlos a cabo, tienes que tenerlos también en permisos de seguridad o NTFS. Si tienes un permiso en compartición, pero no lo tienes en seguridad no lo puedes realizar y viceversa...

Los primeros permisos que se ven siempre son los de compartición.

Si perteneces a varios grupos los permisos se sumarán al menos que alguien lo deniegue

Para administrar una red Windows, todos los equipos deben de estar en el mismo grupo de trabajo.

Si somos admin de una red Windows, y en todos los equipos tenemos creado el usuario Administrador con la misma contraseña, no tendremos problema para entrar desde otro equipo y podrá ver todos los recursos compartidos.

Para poder ver los recursos que se comparten desde un ordenador tenemos que conocer el usuario y la contraseña.

Todos los Windows hacen una validación en local, cada base de datos tiene los usuarios y contraseñas. Los únicos que no tienen esa base de datos son los servidores, tienen una base de datos global donde están creados todos los usuarios del dominio.

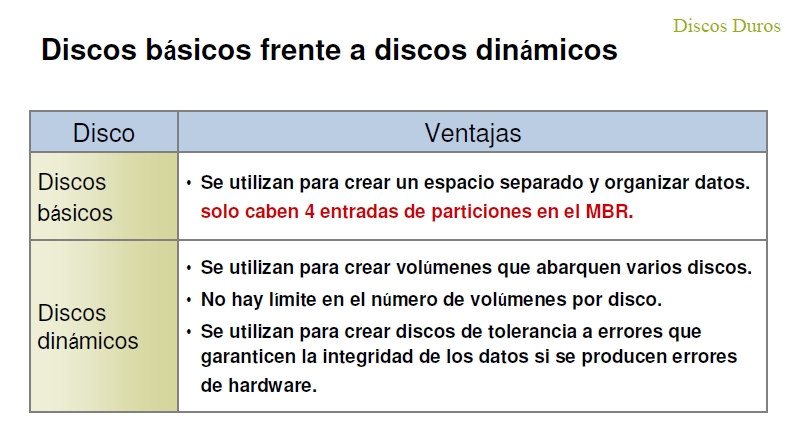
Los permisos de compartición: Solo nos afectan cuando intentamos conectarnos a través de la red

Permisos de seguridad o ntfs: Nos afectan cuando iniciamos sesión local en ese equipo y cunado nos conectamos a través de la red.

Tipo de discos:

Básico: También se conocen como volúmenes, y es un disco físico que contiene particiones primarias, particiones extendidas. Las particiones y las unidades lógicas de los discos básicos se conocen como volúmenes, también llamadas volúmenes básicos.

* Los discos básicos utilizan la tabla de particiones. MBR=4 particiones primarias o 3 primarias y extendida. GPT=128
* Dinámicos: Principal beneficio es que se puede crear volúmenes con diferentes discos. Y sin límite de particiones primarias.



Volumen

Se refiere a un área accesible de almacenamiento como una partición en un disco duro, cada volumen tiene una letra o una unidad y existen varios tipos de volúmenes.

Como el simple:

Se compone por espacio libre de un único disco dinámico Este tipo de volumen permite ser reflejado, aunque no es tolerante a errores (adiós) y tiene que ser continuo.

Volumen distribuido

Es la forma de repartir el espacio no asignado en un sistema con varios discos en una única unidad lógica.

-Más eficiente.

-Se puede redimensionar.

-No hay tamaño fijo y al final será como uno único.

-No tiene seguridad.

-Se aprovecha el espacio.

-Tienes cuatro discos con huecos, entre todos podrás hacer un espacio útil.

Volumen seccionado (RAID0)

Es una variante del volumen distribuido, ya que también utiliza el espacio de varios discos y los convierte en una única unidad lógica.

-Más rendimiento.

- Las secciones de los discos tienen que ser todas del mismo tamaño.

-No se pueden redimensionar

-Reparte los datos

-Si pierdes un disco pierdes los datos de ese disco.

Tienes 3 discos de tamaños de 10GB, 20GB y 30GB el volumen podrá ser de 10GB por disco un total de un volumen de 30GB.

Suma de los 3.

**Ventajas**: proporciona alto rendimiento, tiempos de acceso muy bajos y posibilidad de acceso en paralelo.

No tiene coste adicional. Se emplea toda la capacidad del disco.

**Inconvenientes**: no es verdaderamente un disco *RAID* ya que no presenta integridad de los datos. Un error enuno de los discos implica la pérdida total de los datos.

Volumen reflejado (RAID1)

Es una copia exacta de un disco en otro, tienen que ser pares.

-Mismo fabricante, tiene que tener el mismo tamaño

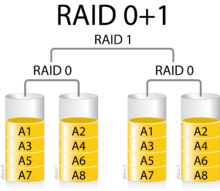
– Hay redundancia de datos al duplicar dos volúmenes idénticos

(espejos) (si una unidad falla, se trabaja con la otra)

-Solo es tolerante al fallo de un disco no a la perdida de datos o eliminación de archivos (si se borra un archivo de uno, se borra del otro)

-No se puede redimensionar.

-Romper volumen reflejado: Separa el volumen reflejado en dos volúmenes simples manteniendo en ambos todos los datos, al romper el volumen reflejado los datos ya no son tolerantes a fallos, pero los datos siguen estando, el disco maestro se queda con la letra del volumen y se le asigna una nueva al otro volumen simple

[](http://commons.wikimedia.org/wiki/File:Raid0mas1.png?uselang=es)Quitar reflejo: elimina el espacio de uno de los discos que formaban parte del volumen reflejado dejando solo un volumen simple con los datos.

Creas dos volúmenes seccionados y lo unes por un volumen reflejado.

Creas dos volúmenes reflejados y lo unes por un volumen seccionados.

[](http://commons.wikimedia.org/wiki/File:Raid10.png?uselang=es)

RAID 4

Un RAID 4, Necesita un mínimo de 3 discos físicos. Esto permite que cada miembro del conjunto funcione independientemente cuando se solicita un único bloque. Con el disco de la paridad se podría calcular si algún disco se estropeara. Y aquí pierdes un disco entero para la paridad.



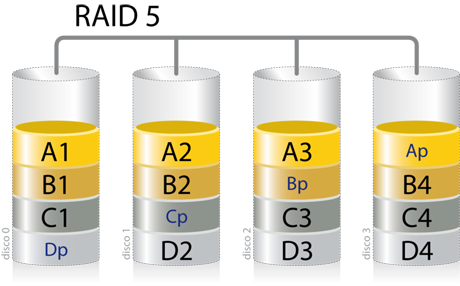
RAID5:

Usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia... RAID 5 necesitará un mínimo de 3 discos para ser implementado.

**Ventajas**: alto rendimiento en aplicaciones con gran demanda de velocidad. No se desaprovecha ningún disco exclusivamente para almacenar códigos de paridad. Se pueden recuperar los datos.

**Inconvenientes**: bajo rendimiento en escrituras (por el algoritmo tiene bajo rendimiento). Se requiere un mínimo de tres discos.

La paridad no se puede recuperar si se estropean 2. Pierdes 5GB si tuvieras 15. (más lento) por los algoritmos.



Discos Duros:

* Tiempo de búsqueda: Tiempo que tarda la cabeza en situarse en una pista
* La Latencia: tiempo que tarda la cabeza en colocarse en un sector de la pista. Depende de las revoluciones del disco (7200 revoluciones)
* Tiempo de transferencia: tiempo que tarda en leer o escribir un dato en el disco duro. Depende el bus del sistema.

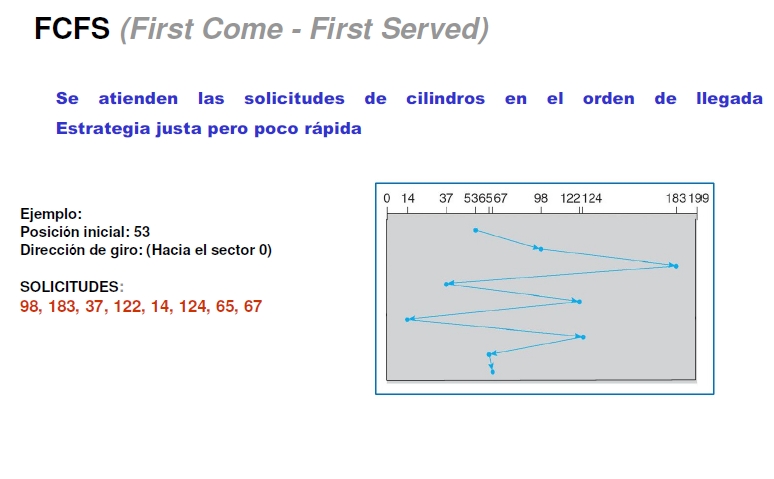
Depende del algoritmo es menor el tiempo de búsqueda.

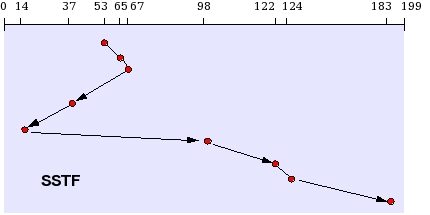
**FCFS**: Atiende las peticiones según el orden de llegada. La primera petición que llega es la primera que se sirve

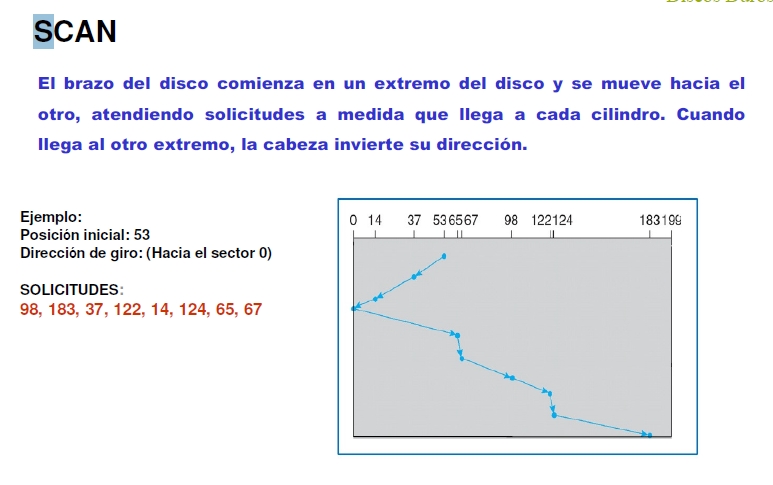
-ventajas Fácil de implementar.

-InconvenientesNo optimiza el rendimiento del disco duro, la cabeza del disco que puede romper con más facilidad.

Es el peor porque viene las peticiones desordenadas, si entrara ordenadas sería el mejor.

 **SSTF**: Atiende a la petición que más cerca este de la cabeza. Atiende los pedidos por menor tiempo de búsqueda. Se atiende la petición que requiere el menor movimiento de la cabeza de lectura/escritura desde su posición actual

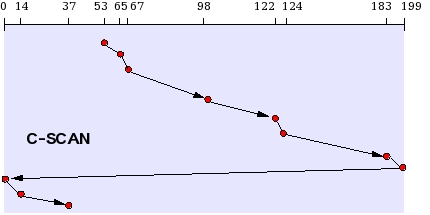
Siempre mira la pista más cercana por eso es rápido, de menor a mayor

Desde la posición en la que está ira en dirección al 0 pasando por todos los números que se encuentren a su paso, llegara hasta el 0 aunque no tenga peticiones. Después va en sentido ascendente barriendo todo lo que se encuentra y llega hasta la última 199 aunque no tenga petición.

**C-Scan**: El brazo del disco se mueve de un extremo al otro del disco. Suponiendo que este tiene 200 posiciones, arrancara desde el primer pedido, avanzando hasta el 199, cuando llegue a este, sea pedido o no, hará un salto hasta la posición 0 y comenzara nuevamente el recorrido del disco, todas las veces yendo de 0 a 199 y tocando los extremos.

El C-Scan funciona igual que el SCAN, pero cuando la cabeza llega al final no vuelve para atrás, sino que se coloca otra vez al principio

Va siempre en un sentido solo y después en el otro.



Atiende las peticiones en un solo sentido de forma ascendente y regresa al 0 sin atender peticiones en el regreso, partiendo del 0 otra vez independientemente de cuál sea la petición menor siempre parte de 0.

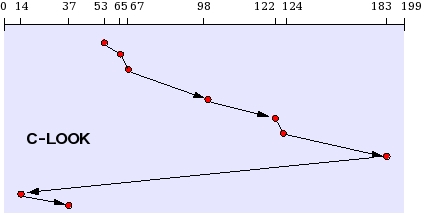
Diferencia entre C-SCAN y SCAN

Scan lee en las dos direcciones barriendo lo que se encuentra y C-SCAN solo lee en dirección ascendente si leer a la vuelta.

-LOOK: variante de SCAN, sino hay peticiones pendientes en la

Dirección actual se cambia el sentido del movimiento (siempre va a ser el mejor) Vuelve sin llegar al final ni al inicio lo que hace que sea la mejor.

- C-Look: Igual que el C-Scan, con la diferencia de que este no toca los bordes del disco a menos que estos sean explícitamente pedidos (mejor que c-scan)



¿Diferencia entre LOOK y C-LOOK?

Look va hacia el 0 pero solo hasta la petición mas pequeña sin llegar al 0 y vuelve atendiendo las peticiones, pero solo hasta la mayor sin necesidad de llegar al 199.

Y C-Look atiende solo de forma ascendente hasta la mayor sin necesidad de llegar al 199 y vuelve atendiendo las peticiones hasta la mas pequeña sin necesidad de llegar al 0.

Se suma la diferencia

11+2+31+24+2+59+169+23=321/9 peticiones=35,69min

Copia de seguridad:

## Copia normal o copia total o completa

Una copia de seguridad normal es una copia de seguridad total de todos los archivos y directorios seleccionados.

**Diferencial o acumulativa**

Es la copia de todos los archivos nuevos o modificados desde la última copia total. Ejemplo, si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad diferencial el resto de los días, cada copia diferencial guardará los archivos que se hayan modificado desde el día 1.

**Incremental**

En un proceso de copia de seguridad incremental, se hace una copia de seguridad sólo de los archivos que han cambiado desde la última copia de seguridad realizada.

Ejemplo, si hacemos copia de seguridad total el día 1 de cada mes y copia de seguridad incremental el resto de los días, cada copia incremental solo guardará los archivos que se hayan modificado ese día. Si tenemos que realizar la restauración de archivos ante un desastre, debemos disponer de la copia total y de todas las copias incrementales que hayamos realizado desde la copia total.

Es la copia de todos los archivos nuevos o modificados desde la última copia realizada.

|  |  |  |  |
| --- | --- | --- | --- |
| Tipo de copia de seguridad | Descripción | Ventajas | Desventajas |
| Total | Copia completa de todos los datos | Más segura y fácil de restaurar | Requiere más espacio y tiempo |
| Diferencial | Solo copia los archivos que han cambiado desde la última copia total | Requiere menos espacio y tiempo que una copia total | Se necesita la copia total original y la última copia diferencial para restaurar |
| Incremental | Solo copia los archivos que han cambiado desde la última copia total o incremental | Requiere menos espacio y tiempo | Se necesita la copia total original para restaurar |

Términos:

Gestor de discos (DISKMGMT.MSC).

Memoria Virtual: PAGEFILE.SYS (ESTA OCULTO)

Consola Especial: NETPLWIZ: Crear usuarios.

Entorno gráfico del administrador de usuarios y grupos locales: LUSRMGR.MSC

Fichero de hibernación: Hiberfil.sys: Guarda el contenido de la RAM durante el proceso de hibernación.

Este archivo es usado para cambiar el nuevo estilo de aplicación de Microsoft llamadas aplicaciones “universales” de Windows: Swapfile.sys

Configuración de Directivas de Seguridad Local: **SECPOL.MSC**