SISTEMAS INFORMÁTICOS
TEMA 8: GESTIÓN DE RECURSOS EN RED

CFGS - DAW 1

JESUITAS
Sagrado Corazón
Jesuitas · Logroño

Índice

1. LOS PERMISOS Y LOS DERECHOS

- Un **derecho** es un atributo de un usuario (o grupo) que le permite realizar una acción que afecta al sistema en su conjunto (y no a un objeto o recurso en concreto).
  - Existe un conjunto fijo y predefinido de derechos en Windows.
  - Para determinar qué usuarios poseen qué derechos, cada derecho posee una lista donde se especifican los grupos o usuarios que tienen concedido ese derecho.

1. LOS PERMISOS Y LOS DERECHOS

- Un **permiso** es una característica de cada recurso (carpeta, archivo, impresora, etc.) del sistema, que concede o deniega el acceso al mismo a un usuario o grupo concreto.
  - Cada recurso del sistema posee una lista en la que se establece qué usuarios o grupos pueden acceder a dicho recurso y qué tipo de acceso puede hacer cada uno (lectura, modificación, ejecución, borrado, etc.).

1. LOS PERMISOS Y LOS DERECHOS

- Windows distingue dos tipos de derechos:
  - **Los derechos de conexión**: establecen las diferentes formas en que un usuario puede conectarse al sistema (de forma interactiva, a través de la red, etc.).
    - Acceso desde la red al equipo
    - Inicio de sesión local
  - **Los privilegios**: hacen referencia a ciertas acciones predefinidas que el usuario puede realizar una vez conectado al sistema. Entre ellos se encuentran:
    - Hacer copias de seguridad de archivos y directorios:
    - Cambiar la hora del sistema
    - Apagar el sistema

1. LOS PERMISOS Y LOS DERECHOS

- Es importante destacar: en caso de conflicto entre un permiso y un derecho, prima este último.
  - Por ejemplo: Imaginemos que los miembros de un grupo llamado Operadores poseen el derecho de realizar copias de seguridad de todos los archivos del sistema.
  - Sin embargo, es probable, que sobre algunos de los archivos no tengan ningún tipo de permiso.
  - Así al ser el derecho más prioritario, podrán realizar las copias sin problemas.

2. LOS ATRIBUTOS DE PROTECCIÓN DE LOS RECURSOS

- En un sistema de archivos NTFS de Windows cada carpeta o archivo posee los siguientes atributos de protección:
  - El SID del propietario: inicialmente, el propietario es siempre el usuario que lo ha creado (aunque se puede modificar posteriormente).
  - La lista de control de acceso de protección (ACL): incluye los permisos que los usuarios tienen sobre el archivo o carpeta. La lista puede contener un número indefinido de entradas, de forma que cada una de ellas concede o deniega un conjunto concreto de permisos a un usuario o grupo del sistema.
  - La lista de control de acceso de seguridad (SACL): se utiliza para definir qué acciones sobre un archivo o carpeta tiene que auditar el sistema (anotación en el registro del sistema de las acciones que los usuarios realizan sobre los archivos o carpetas).

2. LOS ATRIBUTOS DE PROTECCIÓN DE LOS RECURSOS

A.8.1. Busca y explica, qué es una DACL heredada y una DACL explícita

3. LA ASOCIACIÓN DE LOS PERMISOS A LOS RECURSOS

- Cuando se crea un nuevo archivo o carpeta, éste posee por defecto los permisos heredados de la carpeta o unidad donde se ubica y ningún permiso explícito.
- Cualquier usuario que posea control total sobre el archivo o carpeta (por defecto, su propietario) podrá incluir nuevos permisos (positivos o negativos) en la lista de permisos explícita.
- El control sobre la herencia de permisos (por ejemplo, qué objetos heredan y qué permisos se heredan) se realiza a dos niveles:
  - En cada objeto (archivo o carpeta) se puede decidir si se desea o no heredar los permisos de su carpeta padre.
  - Cuando se define un permiso explícito en una carpeta, se puede también decidir qué objetos van a heredarlo. En este caso, se puede decidir entre cualquier combinación de la propia carpeta, las subcarpetas y los archivos.

3. LA ASOCIACIÓN DE LOS PERMISOS A LOS RECURSOS

- El copiar un archivo o carpeta a otra ubicación se considera una creación, y, por tanto, el archivo copiado recibirá una lista de permisos explícitos vacía y se activará la herencia de la carpeta padre correspondiente a la nueva ubicación.
- En el proceso de mover un archivo se distinguen dos casos:
  - Si se mueve una carpeta o archivo a otra ubicación dentro del mismo volumen (o partición) NTFS, se desactivará la herencia y se mantendrán los permisos que tuviera como explícitos en la nueva ubicación.
  - Si el volumen destino es distinto, entonces se actuará como en una copia (solo se tendrán los permisos heredados de la carpeta padre correspondiente a la nueva ubicación).

4. LA COMPARTICIÓN DE DIRECTORIOS

- Una carpeta compartida es una carpeta similar a las demás pero con la peculiaridad de que usuarios de otros equipos pueden conectarse a ella para ver su contenido y, con los permisos adecuados, copiar archivos o eliminarlos.
- Los permisos de carpetas compartidas que se pueden otorgar son:
  - Sin acceso: cuando no tiene permitido ningún permiso sobre el directorio.
  - Leer: permite ver los nombres de los archivos y subdirectorios, ver datos de los archivos y ejecutar programas.
  - Cambiar: se tienen los mismos permisos que en Leer y, además, permite crear subdirectorios y archivos, modificar datos en archivos, borrar archivos y subdirectorios.
  - Control total: tiene todos los permisos anteriores y, además, modificar los permisos.

4. LA COMPARTICIÓN DE DIRECTORIOS

A.8.2. Crea una carpeta llamada "Iniciales_PUBLICO" (ILF_PUBLICO) y comparte dicho directorio junto con algún fichero con tus compañeros.

A.8.3. Una vez la unidad de tu compañero esté compartida, accede a él y mapéalo a una unidad de red de tu equipo, por ejemplo, mapéalo a la unidad F:.
Comprobar el nuevo icono que aparecerá en "Equipo".

A.8.4. Modifica los permisos de los recursos compartidos en la práctica anterior, para que los usuarios que se conecten a él tengan tan sólo permiso de lectura.

5. LOS RECURSOS COMPARTIDOS ESPECIALES

- Se entiende por recursos compartidos especiales aquellos recursos que ha creado el sistema operativo para tareas administrativas y que, en la mayoría de los casos, no deben ser eliminados ni modificados, aunque también los usuarios pueden crear este tipo de recursos compartidos:
  - ADMIN$: es un recurso que utiliza el sistema durante la administración remota del equipo. Siempre es la raíz del sistema y corresponde al directorio donde se instaló.
  - IPC$: es un recurso que comparte las canalizaciones con nombre esenciales para la comunicación entre programas. Se utiliza durante la administración remota de un equipo y al ver sus recursos compartidos.
  - PRINT$: es un recurso utilizado para la administración remota de impresoras.
  - letra_de_unidad$: es un recurso que permite conectar con el directorio raíz de un dispositivo de almacenamiento (por ejemplo, C$).

6. LAS COPIAS DE SEGURIDAD

- Se dispone de varios métodos:
  - Copia de seguridad diaria: se realiza con los archivos seleccionados que se hayan modificado en el día en que se realiza la copia de seguridad. Los archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.
  - Copia de seguridad diferencial: se realiza con los archivos creados o modificados desde la última copia de seguridad normal o incremental. Los archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.
  - Copia de seguridad incremental: se realiza con los archivos creados o modificados desde la última copia de seguridad normal, incremental o diferencial. Los archivos se marcan como copiados y ya no podrán volver a respaldarse hasta que se modifiquen.
  - Copia de seguridad intermedia: se realiza con todos los archivos seleccionados. Dichos archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.
  - Copia de seguridad normal: se realiza con todos los archivos seleccionados. Dichos archivos se marcan como copiados y ya no podrán volver a respaldarse hasta que se modifiquen.

6. LAS COPIAS DE SEGURIDAD

- En Windows, cuando se realiza una copia del Estado del Sistema (System State), se incluyen los componentes siguientes:
  - Bases de datos del Registro.
  - Bases de datos del Registro de clases COM+.
  - Archivos de inicio (incluidos los archivos del sistema).
  - Los archivos del sistema bajo protección de archivos de Windows.

6. LAS COPIAS DE SEGURIDAD

- Además de las copias de seguridad indicadas anteriormente, se puede realizar:
  - Una imagen del sistema que es una copia exacta de una unidad. Cuando se restaura el equipo a partir de una imagen del sistema, se realiza una restauración completa; no se pueden elegir elementos individuales para restaurar, así que todo el contenido se reemplazará por el contenido de la imagen del sistema.
  - Un disco de reparación del sistema que arranque el sistema operativo en caso de un error grave del sistema que no permita acceder al sistema.
  - Un punto de restauración del sistema que permite devolver el equipo a un punto que se creó anteriormente.

6. LAS COPIAS DE SEGURIDAD

A.8.5. En la máquina virtual de Windows 7 añadir un disco duro virtual de 10GB de capacidad para realizar copias de seguridad.

A.8.6. Hacer una copia de seguridad de un directorio completo .

A.8.7. Restaurar el directorio completo que has creado anteriormente.

6. LAS COPIAS DE SEGURIDAD

A.8.8. ¿Para qué sirve hacer una imagen del sistema? Crea una sobre la VM que estabas trabajando utilizando las herramientas del SO.
Utiliza Acronis True Image 2017 para realizar una imagen del sistema. http://www.acronis.com/es-es/tutorials/ATI2017/

A.8.9. ¿Para qué sirven los puntos de restauración? Crear un punto de restauración del sistema.

A.8.10. Restaurar el sistema al punto de restauración que creaste anteriormente.

7. LA ADMINISTRACIÓN REMOTA

- La administración remota consiste en realizar determinadas acciones desde un equipo local y que las mismas se ejecuten en otro equipo remoto. Entre las herramientas que se pueden utilizar se encuentran:
  - Los servicios de terminal: permiten a los usuarios acceder a los programas que están instalados en un servidor de terminales u obtener acceso a todo el Escritorio de Windows de forma remota, desde una red corporativa o desde Internet (está disponibles desdeWindows Server 2003/2008).
  - Los Escritorios remotos: esta utilidad, conocida anteriormente como el cliente de los Servicios de Terminal Server, permite administrar las Conexiones a Escritorio remoto de los servidores de terminales y los equipos que ejecuten una versión desde Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista o Windows XP y posteriores

7. LA ADMINISTRACIÓN REMOTA

- La asistencia remota (RA) permite al personal del soporte técnico ver el Escritorio de los usuarios en tiempo real para solucionar los problemas que pudieran tener. El usuario que necesite asistencia puede mostrar la naturaleza del problema al personal de soporte técnico.

  Se trata de una forma más rápida y eficaz de comunicar los problemas que pudieran tener los usuarios que por teléfono o correo electrónico.

  Si es necesario, el usuario también puede dar permiso al personal de soporte técnico para tomar el control remoto compartido del equipo del usuario para que pueda mostrarle cómo resolver el problema.

7. LA ADMINISTRACIÓN REMOTA

A.8.11. Entre dos equipos W7.

Enviar una invitación de asistencia remota.

Tramitar la invitación de asistencia remota

7. LA ADMINISTRACIÓN REMOTA

A.8.12. Entre dos W7 realiza una conexión de Escritorio Remoto

8. EL CIFRADO DE ARCHIVOS O DIRECTORIOS

- Solo se pueden cifrar archivos y directorios en volúmenes de unidades formateadas para ser utilizadas por el sistema NTFS.
- Los archivos cifrados se pueden descifrar si se copian o mueven a una unidad que no esté formateada para ser utilizada por el sistema NTFS.
- No se pueden cifrar las carpetas ni los archivos que estén comprimidos ni los archivos del sistema.
- Al mover archivos descifrados a una carpeta cifrada, automáticamente se cifrarán en la nueva carpeta; sin embargo, la operación inversa no se hará automáticamente y se deberá realizar explícitamente el descifrado.

8. EL CIFRADO DE ARCHIVOS O DIRECTORIOS

- Cuando se cifra un directorio, el sistema preguntará si se desea que se cifren también todos los archivos y subcarpetas de dicho directorio.
  - Si se decide hacerlo, se cifrarán todos los archivos y subcarpetas que se encuentren en dicha carpeta, así como los archivos y subcarpetas que se agreguen posteriormente a ella.
  - Si se cifra solo la carpeta, no se cifrarán los archivos ni las subcarpetas que contenga pero se cifrarán todos los archivos y subcarpetas que se agreguen posteriormente a ella.
- Cuando se cifra un archivo, el sistema preguntará si se desea que se cifre también el directorio que lo contiene. Si decide hacerlo así, se cifrarán todos los archivos y subcarpetas que se agreguen posteriormente a la carpeta.

8. EL CIFRADO DE ARCHIVOS O DIRECTORIOS

A.8.13. Poner el atributo cifrar a un archivo de alguno de los directorios de la VM y aplicar el cambio sólo al archivo . Exporta las claves de cifrado.

A.8.14. Poner el atributo cifrar a alguno de los directorios de la VM y aplicar el cambio de atributos a subcarpetas y archivos.

A.8.15. Investiga qué es y para qué sirve la aplicación BitLocker. Utilízala sobre un directorio.