Comprovador d'arxius del sistema per a Windows Vista o 7

Utilitza l'eina comprovador d'arxius del sistema (System File Checker) sfc.exe per a determinar quin arxiu està causant el problema, i després reemplaçar el fitxer.

1. Obre una consola del sistema amb permisos d'administrador.

   Inici / Tots els programes / Accessoris. Clica amb el botó dret del ratolí a sobre d'Indicador d'ordres i tria Executa'l com a administrador.
   (Si et demana una contrasenya d'administrador o una confirmació, escriu la contrasenya o fes clic a permet.)

2. En la consola escriu l'ordre següent:

   ```
   sfc /scannow
   ```

   L'ordre sfc /scannow examina tots els arxius protegits de sistema i reemplaça les versions incorrectes per versions correctes de Microsoft.

Determina quins fitxers no podrien ser reparats mitjançant l'eina comprovador d'arxius de sistema (sfc).

1. Obre una consola del sistema amb permisos d'administrador
2. En la consola escriu l'ordre següent:

   ```
   findstr /c:"[SR]" %windir%\Logs\CBS\CBS.log > "%userprofile%\Desktop\sfcdetalls.txt"
   ```

   L'arxiu sfcdetalls.txt conté detalls de cada vegada que l'eina sfc s'ha executat en l'equip. L'arxiu inclou informació sobre els arxius que no seran reparats per l'eina sfc. Comprova les entrades de data i hora per determinar els arxius problemàtics que es van trobar l'última vegada que es va executar l'eina.

Si el comprovador d'arxius de sistema no pot reparar un arxiu reemplaça'l amb una còpia bona coneguda

1. Obre una consola del sistema amb permisos d'administrador
2. En la consola escriu l'ordre següent:

   ```
   takeown /f camí_i_nom_de_l'arxiu
   ```

   Per exemple, `takeown /f c:\windows\system32\mfc42u.dll`

3. Concedeix als administradors accés total a l'arxiu

   ```
   icacls camí_i_nom_de_l'arxiu /GRANT ADMINISTRATORS:F
   ```

   Per exemple, `icacls c:\windows\system32\mfc42u.dll /grant administrators:F`

4. Reemplaça el fitxer amb una còpia bona coneguda de l'arxiu

   ```
   copy camí_i_nom_de_l'arxiu_origen camí_i_nom_de_l'arxiu_destinació
   ```

   Per exemple, `copy D:\mfc42u.dll c:\windows\system32\mfc42u.dll`

SFC

```
Comprobador de recursos de Microsoft (R) Windows (R) versión 6.0
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.

Examina la integridad de todos los archivos de sistema protegidos y reemplaza
las versiones incorrectas por las correctas de Microsoft.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<archivo>] [/VERIFYFILE=<archivo>]
    [/OFFWINDOWS=<directorio de Windows sin conexión> /OFFBOOT=<directorio
    de arranque sin conexión>]

/SCANNOW        Examina la integridad de todos los archivos protegidos del
                sistema y repara los archivos con problemas siempre que es
                posible.
/VERIFYONLY     Examina la integridad de todos los archivos protegidos del
                sistema, pero no realiza ninguna reparación.
/SCANFILE       Examina la integridad del archivo al que se hace referencia y lo
                repara si se detectan problemas. Debe especificarse la ruta de
                acceso completa de <archivo>.
/VERIFYFILE     Comprueba la integridad del archivo con la ruta de acceso
                completa de <archivo>, pero no realiza ninguna reparación.
/OFFBOOTDIR     Para la reparación sin conexión, indica la ubicación del
                directorio de arranque sin conexión.
/OFFWINDIR      Para la reparación sin conexión, indica la ubicación del
                directorio de Windows sin conexión.

Ejemplos:

        sfc /SCANNOW
        sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
        sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows
        sfc /VERIFYONLY
```

FINDSTR

```
Busca cadenas en los archivos.

FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/P]
        [/F:archivo] [/C:cadena] [/G:archivo] [/D:lista_directorios]
        [/A:atrib_color] [/OFF[LINE]] cadenas [[unidad:][ruta]archivo[ ...]]

  /B          Hace coincidir los modelos si están al principio de la línea.
  /E          Hace coincidir los modelos si están al final de la línea.
  /L          Literalmente usa cadenas de búsqueda.
  /R          Usa cadenas de búsqueda como expresiones regulares.
  /S          Busca archivos que coinciden en el directorio actual y en todos
              los subdirectorios.
  /I          Especifica que la búsqueda no distingue mayúsculas de minúsculas.
  /X          Imprime líneas que coinciden con exactitud.
  /V          Sólo imprime líneas que no contienen una correspondencia.
  /N          Imprime el número de la línea antes de la línea que coincide.
  /M          Sólo imprime el nombre de archivo si el archivo contiene una
              correspondencia.
```

```
  /O          Imprime un carácter de desplazamiento antes de las líneas que
              coinciden.
  /P          Omite archivos con caracteres que no son imprimibles
  /OFFLINE    No omite archivos con el atributo "sin conexión" establecido.
  /A:atr      Especifica atributos de color con dos dígitos hexadecimales.
              Consulte "color /?"
  /F:archivo  Lee la lista de archivos desde el archivo especificado
              (/ significa consola).
  /C:cadena   Usa una cadena especificada como una búsqueda de cadena
              literal.
  /G:archivo  Toma la búsqueda de archivos desde el archivo especificado
              (/ significa consola).
  /D:dir      Busca un signo de punto y coma de la lista delimitada de
              directorios
  cadenas     Texto que se va a buscar.
  [unidad:][ruta]archivo
              Especifica el archivo o archivos que se van a buscar.

Usa espacios para separar múltiples cadenas de búsqueda a no ser que
el argumento lleve un prefijo con /C.  Por ejemplo, 'FINDSTR "qué tal" x.y'
busca "qué" o "tal" en el archivo x.y.  'FINDSTR /C:"qué tal" x.y' busca
"qué tal" en el archivo x.y.

Expresión regular de referencia rápida:
  .        Comodín: cualquier carácter
  *        Repetir: cero o más ocurrencias de un carácter previo o de clase
  ^        Posición de línea: comienzo de la línea
  $        Posición de línea: fin de línea
  [clase]  Clase de carácter: cualquier carácter en la serie
  [^class] Clase inversa: cualquier carácter que no esté en la serie
  [x-y]    Intervalo: cualquier carácter que esté dentro del intervalo
           especificado
  \x       Escape: uso literal de un metacarácter x
  \<xyz    Posición de palabra: principio de palabra
  xyz\>    Posición de palabra: fin de palabra

Para obtener una información más completa sobre expresiones regulares de
FINDSTR referirse al Comando de referencia Command en línea.
```

TAKEOWN

```
TAKEOWN [/S sistema [/U nombre_usuario [/P [contraseña]]]]
        /F nombre de archivo [/A] [/R [/D pregunta]]

Descripción:
    Esta herramienta permite que el administrador recupere el acceso a un
    archivo denegado mediante la reasignación de la propiedad del archivo.

Lista de parámetros:
    /S    sistema             Especifica el sistema remoto con el
                              que se va a conectar.

    /U    [dominio\]usuario   Especifica el contexto de usuario
                              el que el comando se debe ejecutar.
```

```
    /P    [contraseña]         Especifica la contraseña para el
                               contexto de usuario dado.
                               Pide la entrada si se omite.

    /F    nombreArchivo        Especifica el nombre de archivo o nombre de
                               directorio patrón. Puede usarse el comodín "*"
                               para especificar el patrón. Permite
                               nombre de recurso compartido\nombre de archivo.

    /A                         Concede la posesión al grupo de
                               administradores en vez del usuario actual.

    /R                         Recurse: le indica a la herramienta que opere en
                               archivos en el directorio especificado y todos
                               los subdirectorios.

    /D    pregunta             Respuesta predeterminada usada cuando el
                               usuario actual no tiene el permiso "listar
                               carpeta" en un directorio. Esto ocurre al
                               trabajar de manera recursiva (/R) con
                               subdirectorios. Son valores válidos "S" para
                               tomar posesión y "N" para omitir.

    /?                         Muestra este mensaje de ayuda.

    NOTA: 1) Si no se especifica /A, la propiedad del archivo se concederá al
             usuario conectado en ese momento.

          2) No se admiten los modelos combinados que usan "?" y "*".

          3) /D se usa para suprimir la pregunta de confirmación.

Ejemplos:
  TAKEOWN /?
  TAKEOWN /F archivo_perdido
  TAKEOWN /F \\sistema\recurso_compartido\archivo_perdido /A
  TAKEOWN /F directorio /R /D N
  TAKEOWN /F directorio /R /A
    TAKEOWN /F *
    TAKEOWN /F C:\Windows\System32\acme.exe
    TAKEOWN /F %windir%\*.txt
  TAKEOWN /S sistema /F recurso\Acme*.doc
  TAKEOWN /S sistema /U usuario /F recurso\foo.dll
  TAKEOWN /S sistema /U dominio\usuario /P contraseña /F
  recurso_compartido\nombre_de_archivo
  TAKEOWN /S sistema /U usuario /P contraseña /F Doc\Report.doc /A
  TAKEOWN /S sistema /U usuario /P contraseña /F recurso\*
  TAKEOWN /S sistema /U usuario /P contraseña /F Principal\Inicio_de_sesión /R
  TAKEOWN /S sistema /U usuario /P contraseña /F Recurso\directorio /R /A
```

ICACLS

```
ICACLS nombre /save archivoACL [/T] [/C] [/L] [/Q]
    almacena las DACL para los archivos y carpetas cuyos nombres coinciden
```

```
    en archivoACL para su uso posterior con /restore. Tenga en cuenta que no
    se guardan las SACL, el propietario ni las etiquetas de identidad.

ICACLS directorio [/substitute SidOld SidNew [...]] /restore archivoACL
                  [/C] [/L] [/Q]
    aplica las DACL almacenadas a los archivos del directorio.

ICACLS nombre /setowner usuario [/T] [/C] [/L] [/Q]
    cambia el propietario de todos los nombres coincidentes. Esta opción
    no fuerza un cambio de propiedad; use la utilidad takeown.exe
    con esta finalidad.

ICACLS nombre /findsid Sid [/T] [/C] [/L] [/Q]
    busca todos los nombres coincidentes que contienen una ACL
    que menciona el SID de forma explícita.

ICACLS nombre /verify [/T] [/C] [/L] [/Q]
    busca todos los archivos cuya ACL no está en formato canónico o cuyas
    longitudes no son coherentes con los recuentos de la ACE.

ICACLS nombre /reset [/T] [/C] [/L] [/Q]
    reemplaza las ACL con ACL heredadas predeterminadas para todos
    los archivos coincidentes.

ICACLS nombre [/grant[:r] Sid:perm[...]]
       [/deny Sid:perm [...]]
       [/remove[:g|:d]] Sid[...]] [/T] [/C] [/L] [/Q]
       [/setintegritylevel nivel:directiva[...]]

    /grant[:r] Sid:perm concede los derechos de acceso al usuario
        especificado. Con :r, los permisos reemplazan cualquier permiso
        explícito concedido anteriormente. Sin :r, los permisos se agregan a
        cualquier permiso explícito concedido anteriormente.

    /deny Sid:perm deniega de forma explícita los derechos de acceso al
        usuario especificado. Se agrega una ACE de denegación explícita
        para los permisos indicados y se quitan los mismos permisos de
        cualquier concesión explícita.

    /remove[:[g|d]] Sid quita todas las repeticiones del SID en la ACL. Con
        :g, quita todas las repeticiones de derechos concedidos a ese SID. Con
        :d, quita todas las repeticiones de derechos denegados a ese SID.

    /setintegritylevel [(CI)(OI)]nivel agrega de forma explícita una ACE de
        integridad a todos los archivos coincidentes. El nivel se debe
        especificar como:
            L[ow] - para bajo
            M[edium] - para medio
            H[igh] - para alto
        Las opciones de herencia para la ACE de integridad pueden preceder al
        nivel y se aplican sólo a los directorios.

    /inheritance:e|d|r
        e - habilita la herencia
        d - deshabilita la herencia y copia las ACE
        r - quita todas las ACE heredadas

Nota:
    Los SID pueden tener un formato numérico o de nombre descriptivo. Si se da
    un formato numérico, agregue un asterisco (*) al principio del SID.
```

/T indica que esta operación se realiza en todos los archivos o
directorios coincidentes bajo los directorios especificados en el
nombre.

/C indica que esta operación continuará en todos los errores de archivo.
Se seguirán mostrando los mensajes de error.

/L indica que esta operación se realiza en el vínculo simbólico en sí
en lugar de en su destino.

/Q indica que icacls debe suprimir los mensajes de que las operaciones
se realizaron correctamente.

ICACLS conserva el orden canónico de las entradas ACE:
Denegaciones explícitas
Concesiones explícitas
Denegaciones heredadas
Concesiones heredadas

perm es una máscara de permiso que puede especificarse de dos formas:
una secuencia de derechos simples:
N - sin acceso
F - acceso total
M - acceso de modificación
RX - acceso de lectura y ejecución
R - acceso de sólo lectura
W - acceso de sólo escritura
D - acceso de eliminación
una lista separada por comas entre paréntesis de derechos específicos:
DE - eliminar
RC - control de lectura
WDAC - escribir DAC
WO - escribir propietario
S - sincronizar
AS - acceso al sistema de seguridad
MA - máximo permitido
GR - lectura genérica
GW - escritura genérica
GE - ejecución genérica
GA - todo genérico
RD - leer datos/lista de directorio
WD - escribir datos/agregar archivo
AD - anexar datos/agregar subdirectorio
REA - leer atributos extendidos
WEA - escribir atributos extendidos
X - ejecutar/atravesar
DC - eliminar secundario
RA - leer atributos
WA - escribir atributos
los derechos de herencia pueden preceder a cualquier forma y se
aplican sólo a directorios:
(OI) - herencia de objeto
(CI) - herencia de contenedor
(IO) - sólo herencia
(NP) - no propagar herencia
(I) - permiso heredado del contenedor principal

Ejemplos:

```
icacls c:\windows\* /save archivoACL /T
- Guardará todas las ACL para todos los archivos en c:\windows
  y sus subdirectorios en archivoACL.

icacls c:\windows\ /restore archivoACL
- Restaurará todas las ACL para cada archivo dentro de
  archivoACL que exista en c:\windows y sus subdirectorios.

icacls file /grant Administrador:(D,WDAC)
- Concederá al usuario permisos de administrador para eliminar y
  escribir DAC en el archivo.

icacls file /grant *S-1-1-0:(D,WDAC)
- Concederá al usuario definido por el SID S-1-1-0 permisos para
  eliminar y escribir DAC en el archivo.
```

COPY

```
Copia uno o más archivos en otra ubicación.

COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/L] [/A | /B ] origen [/A | /B]
     [+ origen [/A | /B] [+ ...]] [destino [/A | /B]]

  origen       Especifica el archivo o archivos que deben copiarse.
  /A           Indica un archivo de texto ASCII.
  /B           Indica un archivo binario.
  /D           Permite que el archivo de destino se cree sin cifrar.
  destino      Especifica el directorio y/o el nombre de archivo de los
               nuevos archivos.
  /V           Comprueba si los nuevos archivos están escritos
               correctamente.
  /N           Si está disponible, usa un nombre de archivo corto al copiar
               un archivo cuyo nombre no tiene el formato 8.3.
  /Y           Suprime la solicitud de confirmación antes de
               sobrescribir un archivo de destino existente.
  /-Y          Solicita confirmación antes de sobrescribir un archivo de
               destino existente.
  /Z           Copia archivos de red en modo reiniciable.
  /L           Si el origen es un vínculo simbólico, copia el vínculo al
               destino en lugar del archivo real al que apunta el vínculo.

El modificador /Y puede preestablecerse en la variable de entorno COPYCMD.
Esto puede anularse con el modificador /-Y en la línea de comando.
La confirmación del usuario se solicita de forma predeterminada antes de
sobrescribir algo, excepto si el comando COPY se ejecuta desde un script por
lotes.

Para anexar archivos, especifique un único archivo de destino pero
varios archivos de origen (con caracteres comodines o el formato
archivo1+archivo2+archivo3).
```