# Windows: Reset password administrador del dominio

Especialmente en sistemas heredados, nos podemos encontrar con la necesidad de tener que cambiar el password de administrador del dominio sin poder iniciar sesión previamente en el controlador o controladores de dominio.

Veamos la ubicación donde se guarda la contraseña:

- En entornos de Active Directory, el password de administrador del dominio queda guardado en la base de datos de Active Directory, por defecto en: `C:\Windows\NTDS\NTDS.dit`. La ruta de la base de datos es definida en el proceso de promoción del equipo a controlador de dominio.

- En entornos de workgroup o cuentas locales, el password de administrador queda guardado en el registro de Windows en la rama de seguridad.

Existen herramientas de terceros de Windows para realizar un reset del password.

Este tipo de herramientas puede que no funcionen sobre sistemas con Active Directory, ya que estas herramientas, conectan con el registro de Windows y eliminan el hash correspondiente al password de una cuenta de usuario.

De todas formas, como norma general: Hemos de entender que cualquier sistema operativo donde disponemos de acceso local al mismo, siempre podremos restablecer el acceso de una forma o de otra.

Veamos un procedimiento para realizar un reset del password de administrador del dominio:

* Este procedimiento será valido tanto para realizar un reset del password de cuentas de usuario locales como para cuentas de usuario de dominio, incluida la cuenta de administrador.

Idea: Acceder al sistema de ficheros NTFS de un controlador de dominio (DC), substituir el fichero de la lupa (`magnify.exe`): "opciones de accesibilidad" por el `cmd.exe`, reiniciar normalmente y antes de iniciar sesión, ejecutar la lupa.

Dispondremos de una shell de CMD con permisos de `SYSTEM`, con los servicios de Active Directory levantados. A partir de aquí, podremos hacer un reset del password de administrador del dominio.

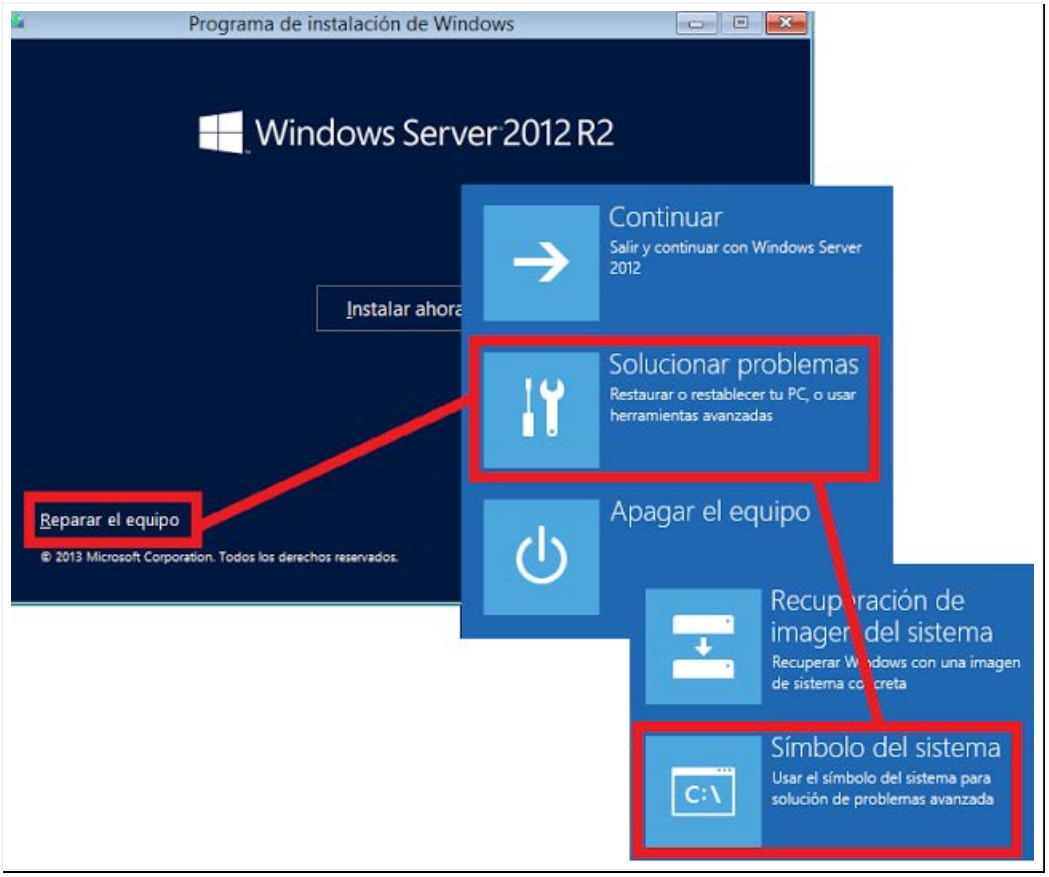
1) Accedemos al sistema de ficheros NTFS:

Una de las formas para acceder al sistema de ficheros NTFS es iniciar el equipo desde un DVD/ISO de Windows Server o Windows cliente.

No es necesario que el DVD/ISO sea la misma versión de sistema Windows que la que tenemos instalada en el controlador de dominio (DC), ya que tan solo necesitamos poder escribir en el sistema de ficheros NTFS.

Veamos como iniciar desde el DVD/ISO de Windows Server 2012 R2 y obtener una consola de CMD:

Iniciamos el DVD, seleccionamos idioma, seleccionamos "Reparar equipo", "Solucionar problemas", "Símbolo del sistema":




Una vez disponemos de una ventana de CMD, accederemos a la unidad donde está instalado Windows Server.

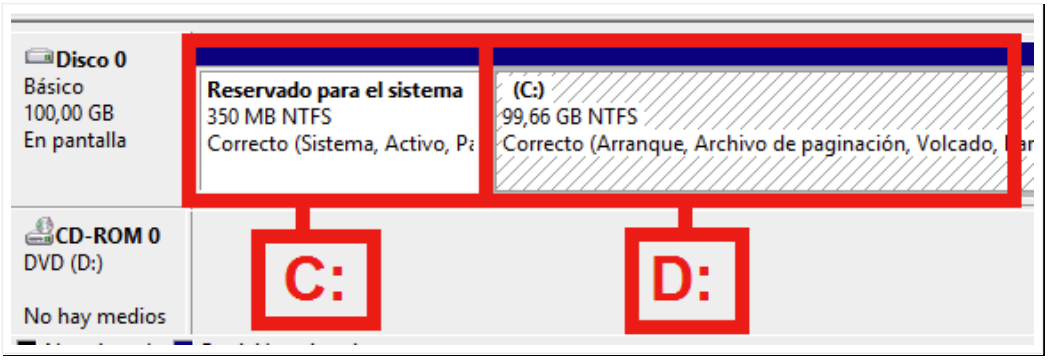
La unidad asignada no tiene por que ser la unidad `C:`

El bootCD asignará de forma secuencial, las letras de unidad a todos los volúmenes NTFS que encuentre.

Recordemos que el volumen "Reservado para el sistema", también dispone del sistema de ficheros NTFS.

Por ejemplo: Si disponemos de la instalación por defecto que realiza Windows Server (a partir de Windows Server 2008), la unidad donde residirá la instalación de Windows, corresponderá a la unidad `D:`

Ejemplo, vista del administrador de discos (`diskmgmt.msc`):

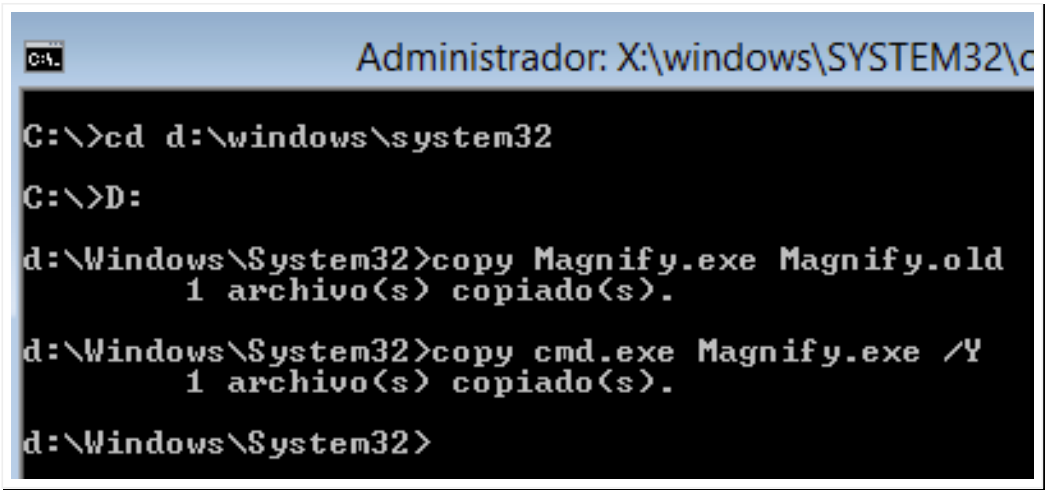



2) Substituimos el fichero de lupa por un `cmd.exe`

Realizamos el procedimiento descrito a continuación, suponiendo que los ficheros donde está instalado Windows Server están ubicados en la unidad `D:`

Nos situamos en el directorio, realizamos una copia de seguridad del fichero `magnify.exe` y lo substituimos por el fichero `cmd.exe`

```
cd d:\windows\system32
D:
copy magnify.exe magnify.old
copy cmd.exe magnify.exe /y
```

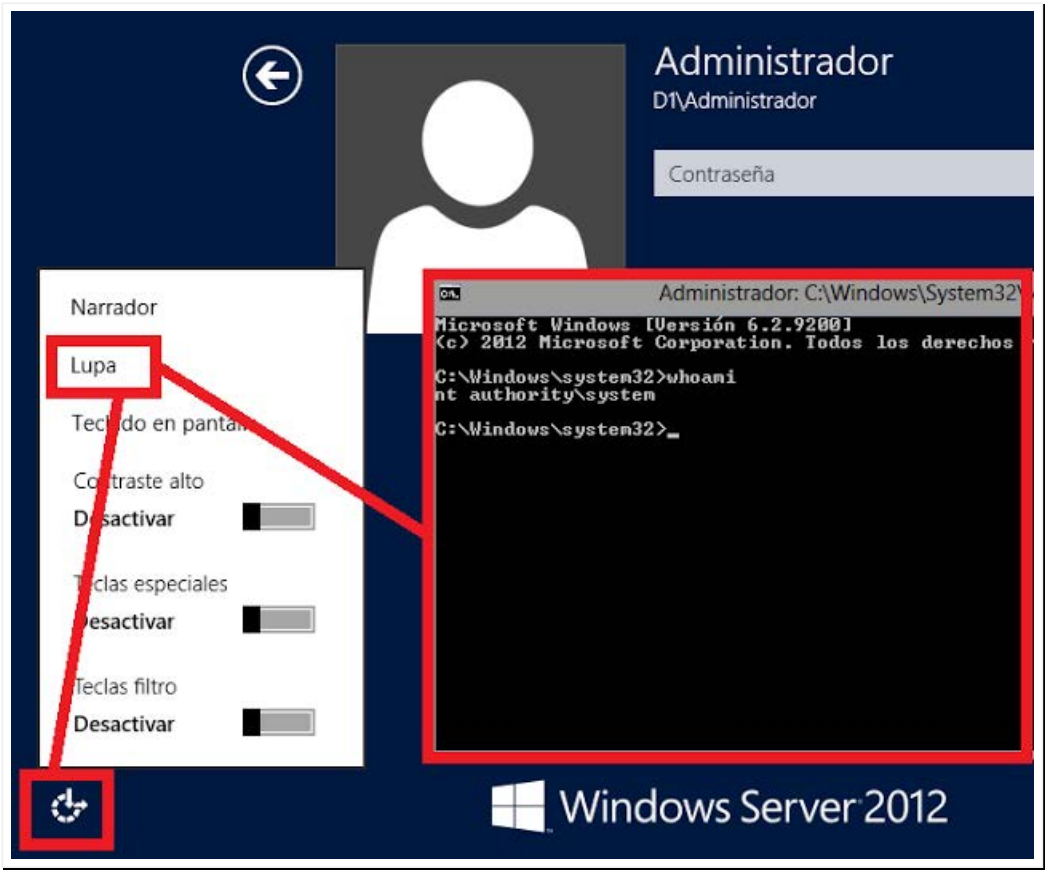



Apagamos el equipo, e iniciamos normalmente Windows Server.

3) Abrimos un CMD antes de iniciar sesión:

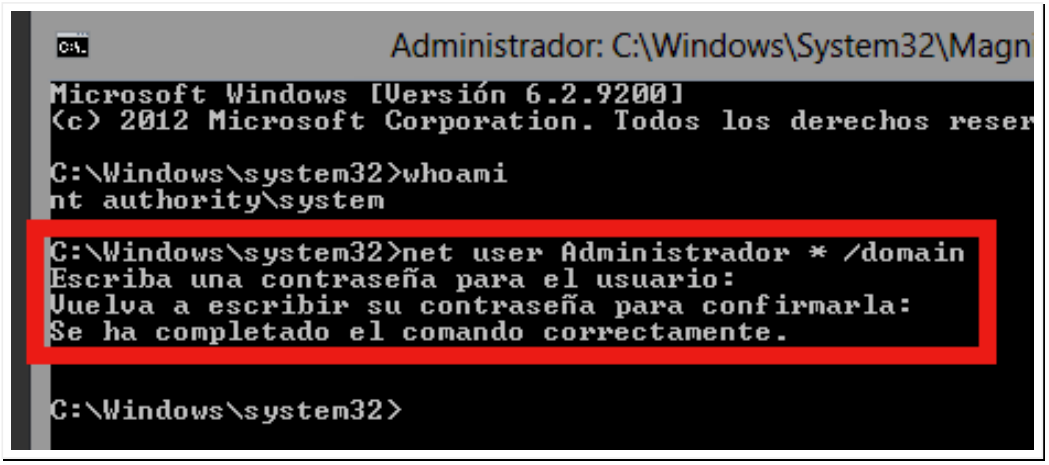
Al iniciar Windows Server, en la pantalla de inicio de sesión, abrimos la lupa.

Vemos que obtenemos una ventana de CMD con permisos de SYSTEM:




4) Realizamos el reset del password de administrador del dominio:

```
Net User Administrador * /domain
```




* Si no se tratase de un equipo controlador de dominio (DC) de Active Directory y quisiéramos cambiar el password de una cuenta local, bastaría con ejecutar:

```
Net User Administrador *
```

5) Cerramos la ventana de CMD, e iniciamos sesión en el dominio con normalidad.

6) Dejamos los ficheros como estaban: Recordemos volver a realizar el procedimiento de iniciar con el DVD/ISO y volver a restaurar el fichero `magnify.exe` por el original:

```
cd d:\windows\system32
D:
copy magnify.old magnify.exe /y
```