

Cambiar la contraseña del Administrador local en remoto

Problemática


Cuando se tiene un importante parque de servidores a administrar y se desea garantizar a su empresa un grado de seguridad mínima, será necesario cambiar periódicamente las contraseñas de las cuentas con privilegios de administración. Cuando se trata de cambiar la contraseña de una cuenta del dominio, es fácil, ya que se hace el cambio una vez en un sólo lugar. Pero cuando se trata de cambiar la contraseña de la cuenta Administrador local de cada servidor miembro del dominio, la cosa cambia!

Solución

Vamos a comenzar por escribir una pequeña función que constará de dos parámetros: un nombre de máquina y una contraseña. Esta función se conectará a la base de cuenta local de una máquina remota y le cambiará su contraseña.

```
Function Set-AdminPassword
{
    param ($equipo = $(Throw "¡ Nombre de equipo obligatorio !"),
          $password = $(Throw "¡ Contraseña obligatoria !"))

    $objAdminUser = [ADSI]"WinNT://$equipo/Administrador,user"
    $objAdminUser.SetPassword($password)
    if ($?)
    {
        Write-Host "$equipo: La contraseña se ha modificado"
    }
}
```

 Este script funciona para sistemas operativos en español ya que hemos indicado el nombre de una cuenta de usuario llamado «Administrador» en la consulta ADSI. Si tiene sistemas operativos en inglés deberá cambiar «Administrador» por «Administrator».

Ahora, creamos un archivo de texto que contendrá la lista de servidores en los que queremos cambiar las contraseñas. Supongamos que tenemos una unidad organizativa con los servidores miembros, llamada «Servidores miembros». En este caso, será muy sencillo listar las máquinas y generar un archivo de texto mediante el script siguiente:

```
# Get-ServerList.ps1
# Lista los equipos contenidos en la UO Servidores miembros
$sadsPath = 'LDAP://OU=Servidores miembros,' + ([ADSI]'').distinguishedName
$objDominio = [ADSI]$sadsPath
$objBusqueda = New-Object
                System.DirectoryServices.DirectorySearcher($objDominio)
$consulta = '(&(sAMAccountType=805306369)(name=*))'
$objBusqueda.Filter=$consulta
$equipos = $objBusqueda.FindAll()

foreach ($equipo in $equipos) {
    $equipo.Properties.cn >> .\servidores_miembros.txt
}

PS > Get-Content .\servidores_miembros.txt

ServidorArc1
ServidorArc2
ServidorWeb
```



Es una buena práctica crear una unidad organizativa para clasificar los servidores miembros ya que si no lo hace así, estos estarán perdidos en medio de todos sus puestos clientes en el contenedor Computers. Además, no se pueden aplicar políticas de grupo en un contenedor «builtin» como es el caso de la UO Computers. Por consiguiente, le recomendamos también mover todas sus máquinas cliente a un contenedor que usted haya creado. Como por ejemplo «Equipos de dominio».

He aquí todo lo que hay que hacer para cambiar la contraseña de administrador local de las máquinas presentes en el archivo creado anteriormente:

```
PS > $password = 'Azerty123*'
PS > $equipos = Get-Content ./servidores_miembros.txt
PS > $equipos | Foreach {Set-AdminPassword -Equipo $_ -Password
$password}
```

```
ServidorArc1: La contraseña se ha modificado.
ServidorArc2: La contraseña se ha modificado.
ServidorWeb: La contraseña se ha modificado.
ServidorSQL: La contraseña se ha modificado.
ServidorImpresion: La contraseña se ha modificado.
```

Es posible modificar también con este script la contraseña de Administrador local de todos sus puestos cliente. Sin embargo, deberá hacer frente a otra dificultad: los puestos pueden estar desconectados o haber desaparecido de la red (de ahí la necesidad de una buena administración de las cuentas de equipos, véase Estudio de caso nº 1). No trataremos esta problemática en el estudio del caso, pero no olvide la funcionalidad «Wake On Lan» que hemos visto como ejemplo a lo largo del capítulo .NET, sección Manipular los objetos .NET.