

Microsoft windows server 2008 (página 2)

[Tweet](#) Enviado por [Daniel Ricardo S♦nchez Jaramillo](#)

[Anuncios Google:](#)

[בכר יאלמשח שפחמ?](#)

דחא מוקמב עדימה לכ תא ונזכיר הלמרב בכר יאלמשח אצמ | www.b144.co.il

[ISA](#)

Encuestas de opinión pública Estudios electorales y de gobierno | www.isa.org.mx

[Cirugía Plástica México](#)

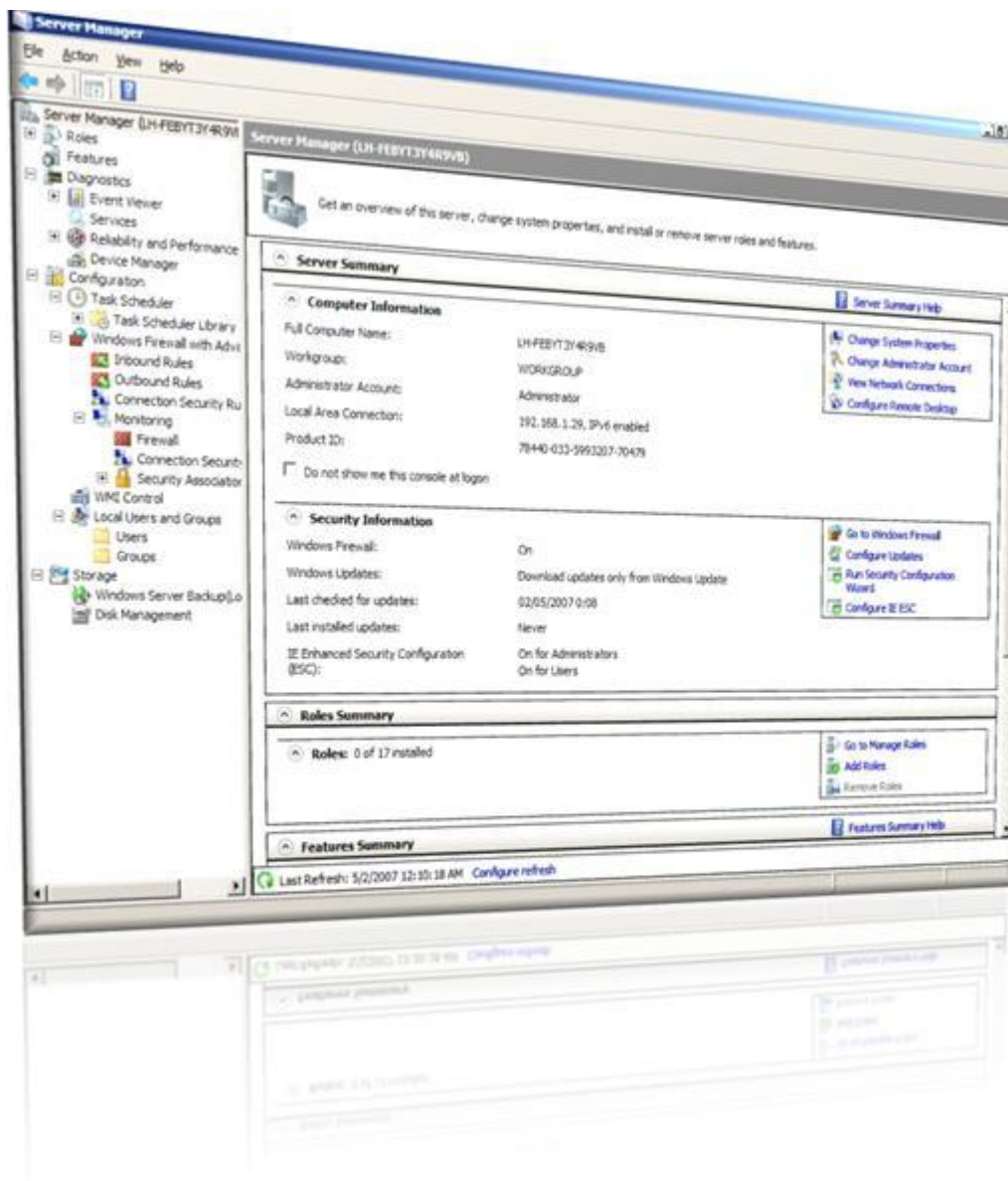
Manos realmente esecialistas manejamos costos accesibles | www.cirugia-plastica-mexico.com/

Partes: [1](#), [2](#)

En [Windows](#) 2003 disponíamos de la herramienta "Administración de equipos". Sin embargo se echaba en falta que en la misma [consola](#) se pudiesen instalar aplicaciones, extensiones, features, administrar el [firewall](#), etc... Para todas estas tareas era necesaria la apertura de otras ventanas, y en algunos casos incluso, necesitábamos otras aplicaciones. Es por ello que en determinados momentos la tarea de administrar varios elementos a la vez podía resultar, cuanto menos, pesada.

Con "Server Manager" se resuelve positivamente esta circunstancia, ya que la herramienta se integra en las nuevas consolas de administración MMC. De éste modo, en una misma consola, estamos capacitados para administrar una parte muy importante de nuestro [sistema operativo](#), como [son](#) por ejemplo la administración de usuarios y [grupos](#), Windows Server Backup, tareas de particionamiento, administración y redimensionado de discos, Firewall de Windows con [seguridad](#) avanzada, Tareas programadas, [herramientas](#) de diagnóstico, [servicios](#), roles, features, log de sucesos, junto a otras.

Todo ello, como podemos observar en la [imagen](#) inferior, aparece ahora en una misma consola, sin necesidad de abrir otras aplicaciones o ventanas. Sustituimos así las consolas de Añadir o quitar complementos, Configura tu [servidor](#) o Administrar Servidor. De igual modo, desde esta consola de [trabajo](#), podremos redimensionar nuestros discos, a la vez que añadimos reglas a nuestro Firewall, pasando por la creación de tareas programadas o verificar que la realización de las copias de seguridad se está llevando a efecto de la forma adecuada.



Firewall Windows con Seguridad Añadida

Uno de los aspectos más notables a destacar en [materia](#) de seguridad, ha sido la incorporación del nuevo Firewall de Windows con seguridad añadida. De sus características novedosas enunciamos ahora algunas de considerable interés: soporte nativo para IPV6, la posibilidad de controlar el tráfico tanto entrante como saliente, NAP (Network [Access](#) Protect), Hardening de servicios, la integración con IPSEC, reglas aplicables a perfiles determinados, reglas basadas en directorio activo, usuarios, grupos y [computadoras](#), etc..

De nuevo, y al estar integrada en su totalidad en las nuevas consolas de administración MMC, se mejora bastante la administración del mismo, pudiéndose crear, mediante asistentes gráficos, reglas tanto de entrada como de salida, y pudiendo llegar a la personalización de estas reglas hasta el más mínimo detalle.

Dependiendo de las reglas que queramos aplicar, podremos implementarlas en función de diversos factores:

- Nombre de aplicación.- Es posible restringir o permitir a una aplicación la conexión con el exterior.
- Puertos.- Es posible restringir o permitir a todos o a un número determinado de puertos la conexión.

- Direcciones [IP](#).- Es posible restringir o permitir a una dirección IP o un rango entero de direcciones la conexión con algún tipo de aplicación o [servicio](#).
- ICMP o ICMPV6.- Es posible restringir o permitir algún servicio de este tipo, como por ejemplo ping.
- Configuración del protocolo
- Servicios.- Es posible restringir o permitir la conexión al exterior de algún servicio.
- Usuarios AD, locales, grupos o máquinas.- Es posible restringir o aplicar reglas para un determinado [grupo](#) de usuarios, usuarios de directorio activo o locales.
- Tipos de Interface.- Es posible aplicar o restringir las reglas en función del tipo de interface que tengamos en el equipo, ya sea [Wireless](#), [Ethernet](#), u otros. En la parte derecha de la consola del Firewall, disponemos de varias opciones también de interés para el [administrador](#). Estas nos van a suministrar la oportunidad de exportar/importar directivas, así como el establecimiento de filtros en función del perfil, del [estado](#) de la conexión o de la pertenencia a grupos.

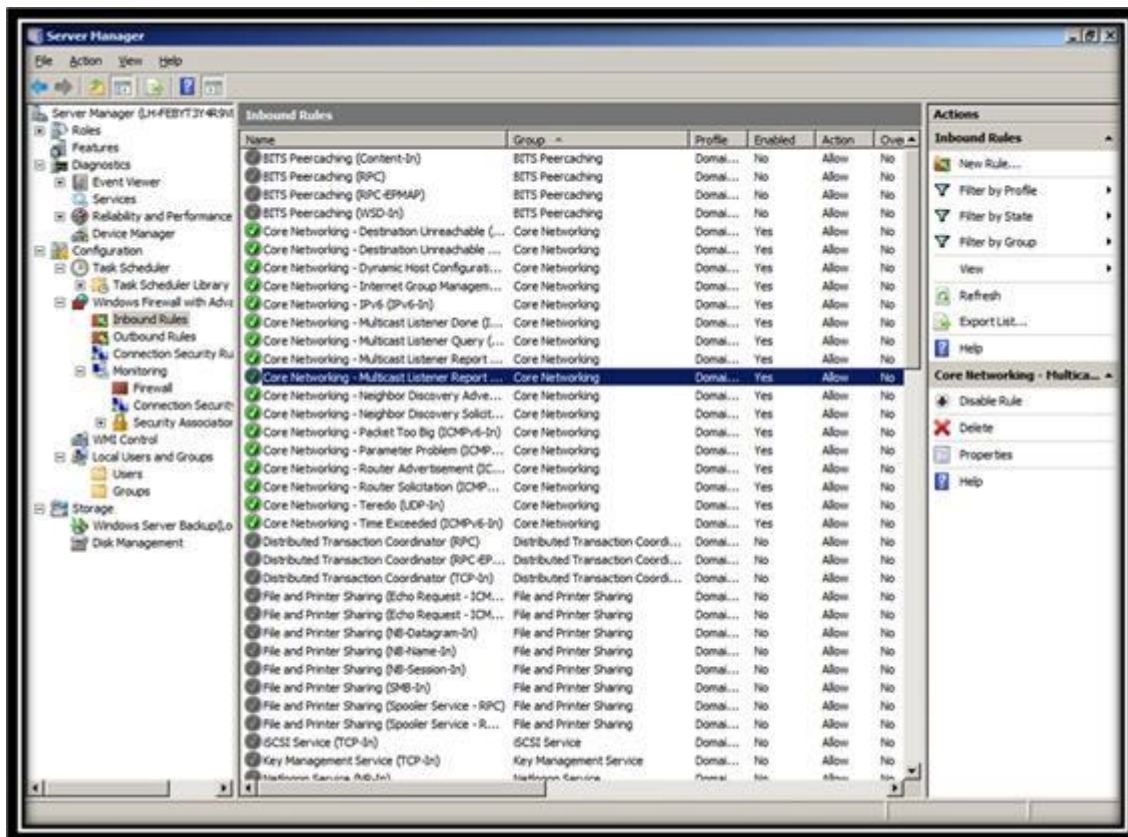
Igualmente en la parte izquierda de la consola se nos presentan las opciones de configuración y monitorización de reglas. Estas no van a permitir configurar tanto las reglas de entrada como las de salida, y monitorizar [el estado](#) de conexiones y actividad del Firewall.

Finalmente en la parte [central](#), podremos ver en todo momento el estado en que se encuentra nuestro Firewall. Siendo posible visualizar también los perfiles de conexión que nos proporciona por defecto Windows: Perfil de [dominio](#), perfil privado y perfil público, así como los accesos para la creación de reglas de entrada o salida y un apartado de [recursos](#) y documentación. Si pulsamos en la parte izquierda sobre las opciones de reglas de entrada y reglas de salida, éstas se nos mostrarán en el centro de la consola.

En las propiedades es posible la visualización de los 3 tipos de perfiles:

- Perfil de Domino: Equipo que se conecta a [una red](#) corporativa, formando parte del directorio activo.
- Perfil privado: Equipo que se conecta a una [LAN](#) privada, como puede ser una [red](#) doméstica por ejemplo.
- Perfil público: Equipo que se conecta a una red sobre la que no disponemos de [control](#) alguno. Cibercafés, aeropuertos, y otros escenarios similares son claros ejemplos de ello. Refiriéndonos a [servidores](#) podría servirnos como ilustrativa la instalación de uno de ellos en una [zona](#) DMZ.

En el momento de incorporar un servidor LongHorn a una red, automáticamente se lleva a efecto la detección del tipo de red a la que nos estamos conectando. Por defecto, se activa automáticamente el perfil público. En función de la configuración de nuestro Firewall, pasarán a aplicarse las reglas establecidas para el perfil en [concreto](#) seleccionado. Por ejemplo, si disponemos de una aplicación a la que conectamos libremente desde casa pero no desde la [oficina](#), podemos llevar a efecto la creación de una regla que determine que es posible la conexión libremente a [internet](#) cuando estemos operando bajo el perfil privado, pero que no sea posible la misma cuando operemos a través de un perfil de dominio. Con ello se facilita considerablemente la labor a los administradores, creando la misma regla pero con ámbitos de acción diferentes en función del perfil.



Cada perfil es totalmente configurable, pudiendo desactivarlo o activarlo a nuestro gusto, creando [archivos](#) de log para cada uno de ellos, mostrando notificaciones de bloqueo, etc. lo cuál evidentemente facilita y mejora las posibilidades de administración asociadas.

Es interesante indicar en este momento que en función del ámbito de red que escojamos, las reglas configuradas por defecto serán más o menos estrictas. El perfil más restrictivo es el perfil público. Este debería ser el seleccionado si la instalación de nuestro servidor se va a realizar en áreas no controladas por nosotros al 100%, con una superficie de ataque amplia. Por el contrario, el perfil menos restrictivo es el de dominio. En este escenario la administración más centralizada y segura nos permite que las restricciones en función del perfil sean menores sin por ello menoscabar el nivel de seguridad deseado.

Adicionalmente, y como todo complemento de Windows, el Firewall es también administrable 100% a través de la línea de [comandos](#). Para ello disponemos de la herramienta netsh. Esta es una aplicación que opera bajo línea de comandos y que nos permite administrar la configuración de red de un equipo. Este tipo de administración es posible realizarla tanto de forma local como remota.

No olvidemos sin embargo que Netsh no sólo sirve para administrar el Firewall de Windows, sino que no capacita también para la administración al 100% de nuestra configuración de red. Pudiendo así, y a través de ella, administrar NAP, [HTTP](#), RPC, configuraciones IP, solucionar [problemas](#) de WinSock, y otras funcionalidades y características propias del entorno de red, operando bien en remoto o local. La sintaxis del comando en cuestión es la siguiente:

Netsh advfirewall firewall

Desarrollemos un ejemplo ilustrativo asociado. Ante la necesidad de tener que implantar una aplicación que cumpla las siguientes condiciones:

- Salida al exterior de la [intranet](#) corporativa.
- Regla sólo aplicable al perfil público.
- El Firewall debe permitir esta conexión, siendo transparente al resto de los perfiles.

La sintaxis completa del comando sería la siguiente:

```
Netsh advfirewall firewall add rule name=" Permitir aplicación Contabilidad" dir=out  
program="C:\Archivos de programa\Aplicación de Contabilidad\Contabilidad.exe" profile=public  
action=allow
```

En donde, el apartado dir refleja la [naturaleza](#) de la regla (si es de entrada o de salida), el apartado profile refleja el ámbito de la regla (perfil público, privado o de dominio) y el apartado action refleja la acción del firewall (permitir o denegar).

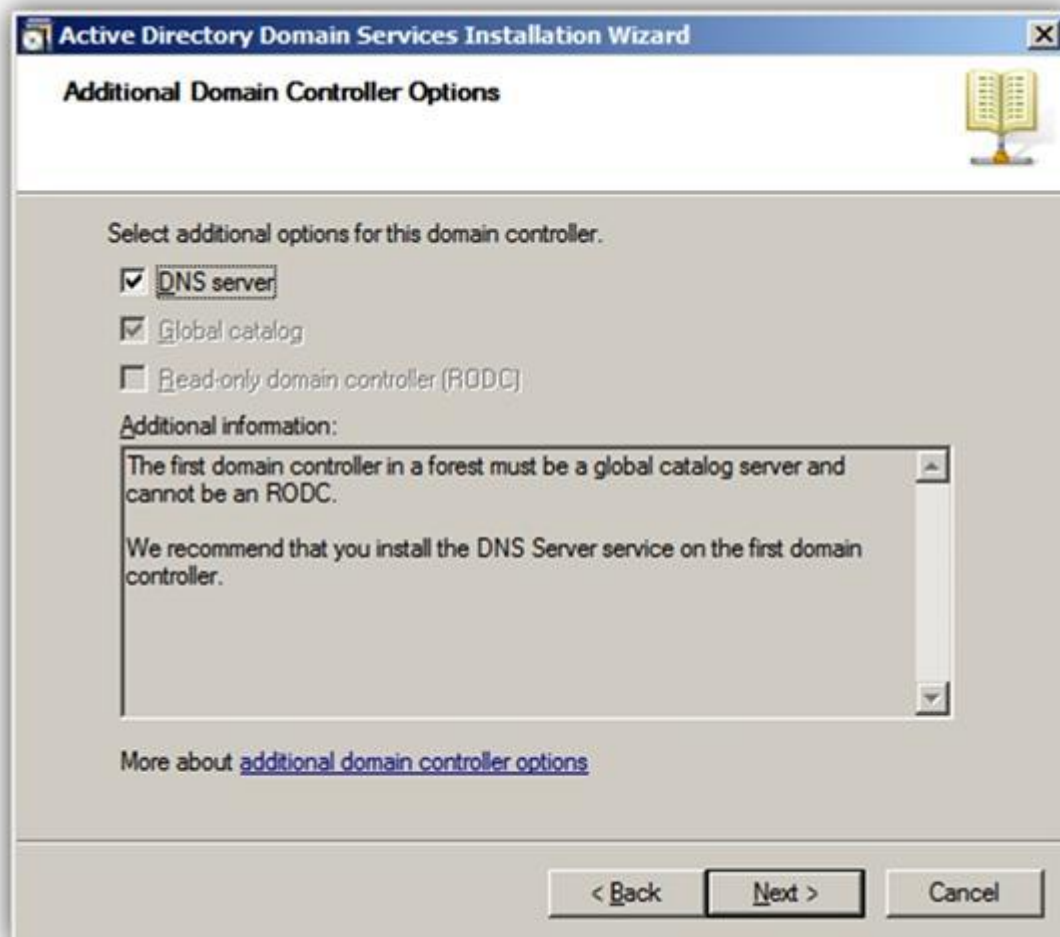
Con netsh podremos crear y eliminar reglas, hacer backups de las mismas, etc... Otra característica novedosa del Firewall Windows es que su total integración con el [protocolo seguro](#) IPSEC. Basándose, como ya indicábamos, toda la administración en una consola única.

En versiones anteriores de Windows, los administradores teníamos que lidiar con el firewall y las reglas de IPSEC en consolas diferentes. Recuerdo cuando a veces creaba reglas IPSEC que luego me bloqueaba el Firewall. Me volvía loco... Ya no sabía si era del Firewall, las reglas, el equipo, el cable, etc... La diversidad de las consolas de trabajo era sin lugar a dudas una posible interferencia en la operativa del administrador que ahora ha sido subsanada.

La total integración del Firewall Windows con IPSEC en el nuevo [sistema](#) operativo no permite ver en una única consola como se están aplicando nuestras reglas, pudiendo ver con mayor detalle si ésta se está efectuando correctamente, y reducir así la superficie de error.

Nuevas Características de Seguridad en Directorio Activo: Controladores de Dominio de Sólo Lectura

Me gustaría abordar en este punto otra cuestión que creo que puede tener intrigados a muchos técnicos, y que planteo desde una pregunta que me hicieron no hace mucho. La pregunta era "Un Controlador de Dominio puede aumentar la seguridad de una corporación, si éste es administrado correctamente, pero ¿qué pasa con los controladores a los que no podemos garantizar una seguridad física?." La respuesta es evidente e incluso inquietante. Bastaría que un [hacker](#) comprometiese el controlador de dominio para [poder](#) tener acceso a información sensible de toda la corporación. LongHorn se ha pensado y diseñado para ser implementado en muchos entornos, entre ellos el mismo escenario que planteábamos en el párrafo anterior. Una corporación que necesita tener un DC (Domain Controller) replicando y situado en una ubicación de la que no podemos garantizar su seguridad ni física, ni lógica. Para atender a esta circunstancia nace una nueva figura, el Controlador de Dominio de solo [lectura](#) (RODC Read Only Domain Controller) Este nos permite que podamos implementar un DC con una [base de datos](#) del dominio de solo lectura.



Un RODC mantiene los mismos atributos y objetos que un controlador de dominio de [escritura](#), con la excepción de no poder hacer cambios en la base de [datos](#). En su lugar, si alguna operación necesita escribir en la base de datos, ésta hace la replicación en un controlador de dominio de escritura que a su vez, replica en el RODC. De este modo evitamos varios problemas, entre ellos dos importantes que anteriormente quedaban expuestos: La replicación indebida a nuestro bosque, y una posible exposición de ataque.

Adicionalmente reducimos la carga de replicación a otros servidores, ya que como en un RODC no es posible escribir en la base de datos, éste no puede replicar. Es decir, en un RODC la replicación siempre es única y exclusivamente unidireccional. En la [arquitectura](#) de un RODC también se ha pensado en el [almacenamiento](#) de credenciales. Por defecto, en un sistema basado en Windows, se guardan los 10 últimos inicios de sesión. Se diseñó así para poder iniciar una sesión en un equipo miembro de un dominio, incluso si éste fallase por cualquier circunstancia. En escenarios donde no se puede garantizar una seguridad física ni lógica, esta cuestión puede representar un serio problema de seguridad. Aplicaciones como cachedump pueden ser utilizadas para recuperar las contraseñas almacenadas en la caché del sistema. La opción de caché del sistema se podía y se puede configurar de forma sencilla en cualquier Windows. Observando lo anterior un RODC no guarda credenciales de usuarios ni de equipos (establecido por defecto), salvo la de sus [cuentas](#) locales y la cuenta de sistema que se utiliza para la autenticación [kerberos](#) (krbtgt), buscando de este modo eliminar o al menos minimizar los [riesgos](#) expuestos.

Sin embargo en estas como en otras cuestiones no siempre llueve al gusto de todos y nos podemos encontrar con que esta limitación respecto de la caché no sea la más correcta en determinadas circunstancias. Es por ello que se ha pensado en la posibilidad de asignar caché para aquellas cuentas que precisemos oportunas. Si tenemos un RODC en una [oficina](#) externa, y ésta oficina tiene 20 usuarios, podremos asignar caché a esos 20

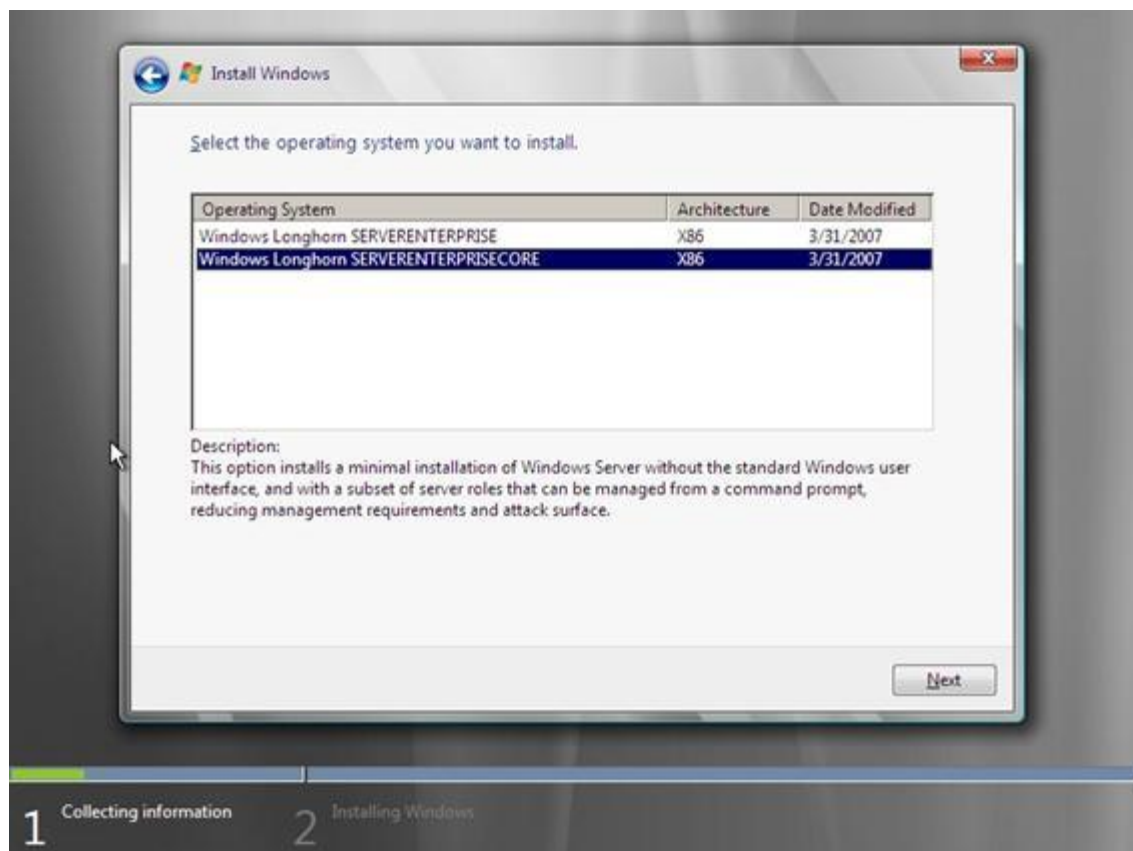
usuarios y denegar al resto. Si por alguna razón, el RODC es comprometido o robado físicamente, sólo tendremos que restablecer las contraseñas de estas cuentas. Al tener total seguridad de qué cuentas pueden ser comprometidas, reducimos el [tiempo](#) de acción de un administrador para solucionar la brecha de seguridad. Incluso podríamos permitirnos el lujo de asignar una cuenta administrativa sólo para manejar el RODC, pero sin acceso a los DC centrales con permiso de escritura. Server Core. Windows también puede operar sin ventanas.

Pasamos en esta apartado a valorar otra novedad de LongHorn. El sistema nos aporta la posibilidad de llevar a efecto una instalación mínima de servidor, también conocida como Server Core. El [proceso](#) en este caso es sumamente sencillo. Tan sólo tendremos que seleccionar la opción de Server Core, y se instalará el sistema base sin entorno gráfico. Nada de instalaciones complicadas. Toda la instalación a sólo un clic de ratón. Con Server Core podremos realizar la instalación mínima de un servidor, con sólo [funciones](#) o roles necesarios que nos permitan desempeñar aquellas funcionalidades específicas para las que estemos generando el nuevo servidor.

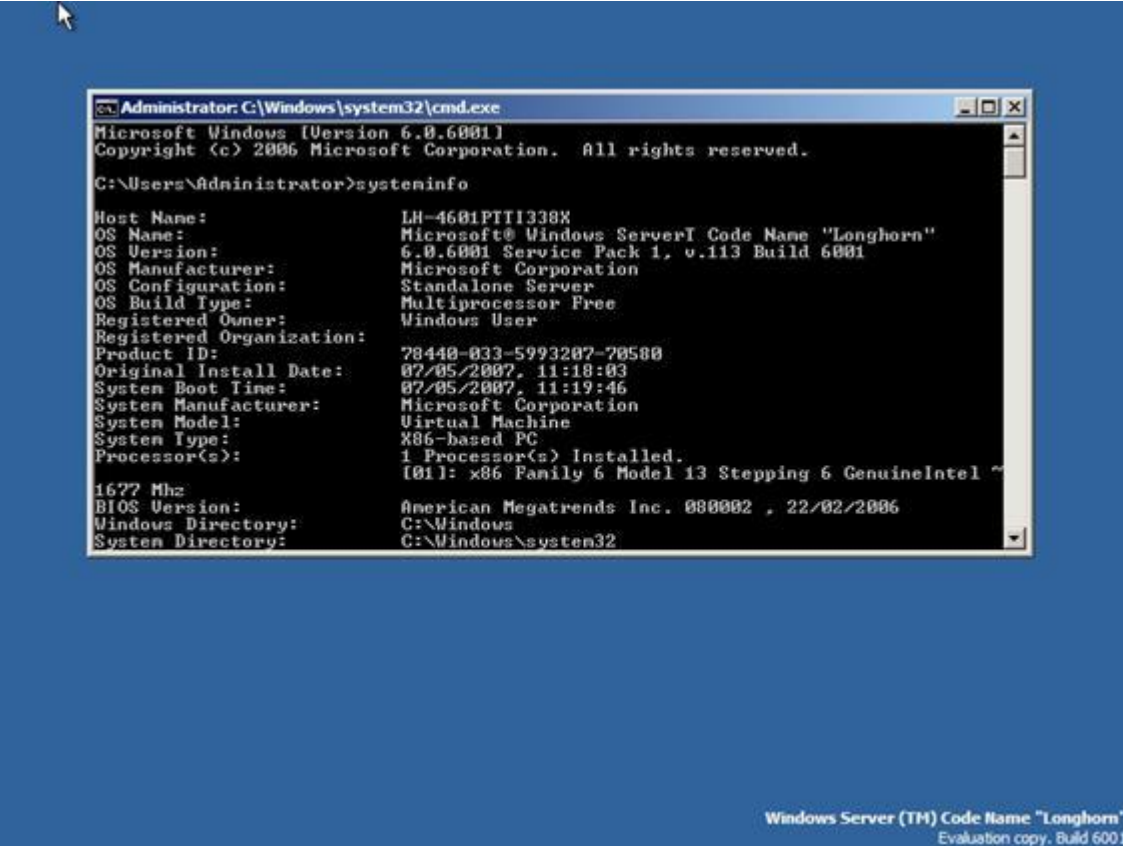
Evidentemente la metodología en esta ocasión es básica y se ocupa únicamente de atender los mínimos necesarios. La instalación es mínima, ocupándose exclusivamente del sistema base, y el rol o roles que necesitemos que adicionalmente desempeñe el equipo. Todo ello sin sistema gráfico, operando íntegramente través de la Shell. Nuestro sistema Windows se ha quedado en esta ocasión sin ventanas.

Supongamos, a modo de ejemplo, un escenario en el que necesitamos que un servidor adopte exclusivamente las funciones como DHCP y [DNS](#). En una instalación Server Code, ésta se limitará al sistema base y una Shell de comandos. Posteriormente, a través de ésta, completaremos la instalación con los servicios adicionales necesarios. Como ya indicábamos, un Windows sin Windows que sin embargo cubre las necesidades que se le demandan.

Una vez instalado el sistema base, nos encontramos con un entorno de trabajo básico. A muchos administradores puede parecerles incluso un tanto hostil, ya que carece de componentes gráficos. Como veremos a continuación, mantener y administrar un servidor de estas características no es, ni mucho menos, tan complejo como puede parecernos. A los más veteranos de la administración les resultará incluso familiar.



Abordemos un ejemplo práctico en mayor detalle para ilustrar este apartado. Una vez instalado el servidor en un modo Server Code, éste presenta una configuración básica no operativa y en nuestro ejemplo tendremos que desarrollar por lo tanto todos los [procesos](#) manualmente, sin apoyarnos en ningún asistente. De este modo modificaremos la password de administrador, cambiaremos el nombre de equipo, configuraremos la red, activaremos Windows, pasando posteriormente a actualizarlo. Finalmente instalaremos un rol y un complemento. A los más antiguos del lugar les traerá recuerdos sin lugar a dudas.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>systeminfo

Host Name:                LH-4601PTI1338X
OS Name:                   Microsoft® Windows Server™ Code Name "Longhorn"
OS Version:                6.0.6001 Service Pack 1, v.113 Build 6001
OS Manufacturer:          Microsoft Corporation
OS Configuration:         Standalone Server
OS Build Type:              Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                 78440-033-5993207-70500
Original Install Date:      07/05/2007, 11:18:03
System Boot Time:          07/05/2007, 11:19:46
System Manufacturer:       Microsoft Corporation
System Model:               Virtual Machine
System Type:                X86-based PC
Processor(s):               1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 13 Stepping 6 GenuineIntel ~
                           1677 Mhz
BIOS Version:               American Megatrends Inc. 080002 , 22/02/2006
Windows Directory:         C:\Windows
System Directory:           C:\Windows\system32
```

Windows Server (TM) Code Name "Longhorn"
Evaluation copy. Build 6001

Para cambiar la password de la cuenta Administrator, utilizaremos el comando:

Net user Administrator *

El comando nos solicitará que introduzcamos una password, y posteriormente nos la volverá a pedir para su verificación. El asterisco se suele poner para no tipear la password en [texto](#) plano. Con esto evitamos a posibles "voyeur" que estén intentando visualizar lo que escribamos en [pantalla](#).

Posteriormente pasamos a modificar el nombre de equipo de la máquina, ya que tal vez el nos haya asignado la instalación, no corresponda a la política corporativa de [nomenclatura](#) de máquinas. Cambiar el nombre de máquina es tan sencillo como formular adecuadamente el comando cuya sintaxis reflejamos a continuación:**Netdom renamecomputer /newname:**

Ejemplo:**Netdom renamecomputer QFGPH-345P /newname: Sevw2k3prb01**

Una vez que la password se ha modificado y el nombre de equipo se encuentra dentro de la política de nomenclatura de [la empresa](#), procederemos a comprobar si el [cliente](#) DHCP y el cliente DNS están en funcionamiento. Para ello bastará con teclear un query de servicios con el comando SC.

Sc query DHCP

Sc query DNS

Comprobado que tenemos estos servicios iniciados y en funcionamiento, es hora de asignar una dirección IP a nuestro adaptador Ethernet. Para ello utilizaremos el comando netsh.

Primeramente tendremos que averiguar el nombre de nuestra interfaz. Para hacerlo teclearemos el siguiente comando:

```
Netsh int show interface
```

Este comando nos devolverá el nombre de interface, información necesaria si posteriormente tuviésemos que modificar su dirección IP.

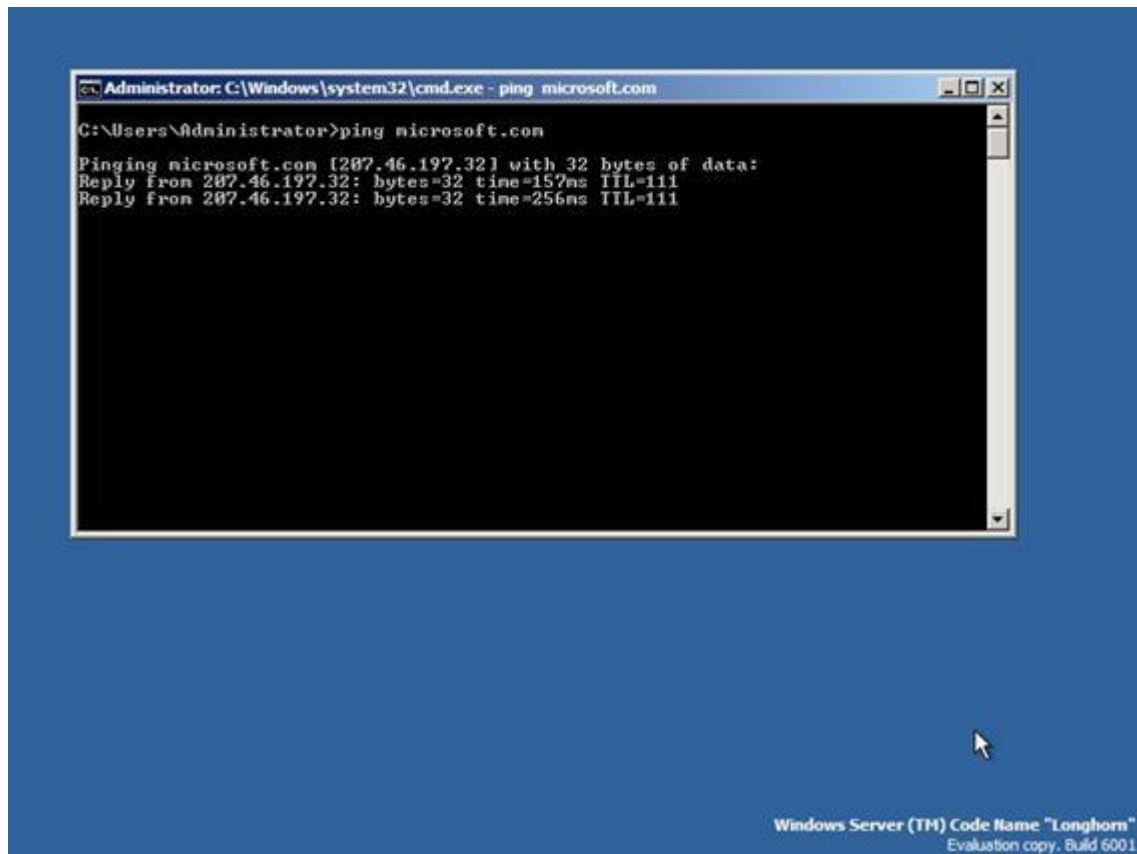
Para establecer la dirección IP de un adaptador, existen dos posibilidades: direccionamiento dinámico (DHCP) o direccionamiento estático. La operativa para recibir la dirección IP desde un servidor DHCP es bien sencilla. Simplemente tendremos que teclear el comando siguiente:

```
Netsh int ip set address name="Local Area Connection" source=d.C.
```

Para direccionamiento estático, imaginemos que necesitamos asignar la dirección IP 192.168.4.120/[Clase C](#) y la puerta de enlace 192.168.4.250 a nuestro servidor. El nombre de la interfaz es Local Area Connection. El comando resultante sería el siguiente:

```
Netsh int ip set address name="Local Area Connection" source=static address=192.168.4.120  
mask=255.255.255.0 gateway=192.168.4.250 1 gwmetric=1
```

Una vez configurada la red, debemos realizar una comprobación de conectividad que verifique que el proceso de configuración se ha finalizado con éxito.



Una vez realizado el [test](#) de conectividad procederemos a activar Windows. Para realizarlo, utilizaremos el siguiente comando:

Slmgr.vbs –ato

Una vez activado Windows Server LongHorn, el sistema nos presenta una ventana informativa mostrándonos el estado de la actualización.



Avanzando en nuestro proceso de configuración, y antes de instalar cualquier rol, podemos actualizar nuestro Windows Server LongHorn con las últimas actualizaciones de seguridad. Para ello debemos de seguir una serie de pasos, que detallamos a continuación:

Lo primero que debemos hacer es configurar nuestro servidor para que se descargue actualizaciones cada cierto tiempo. En nuestro caso cada 3 horas. Estos términos podemos establecerlos con el comando siguiente:

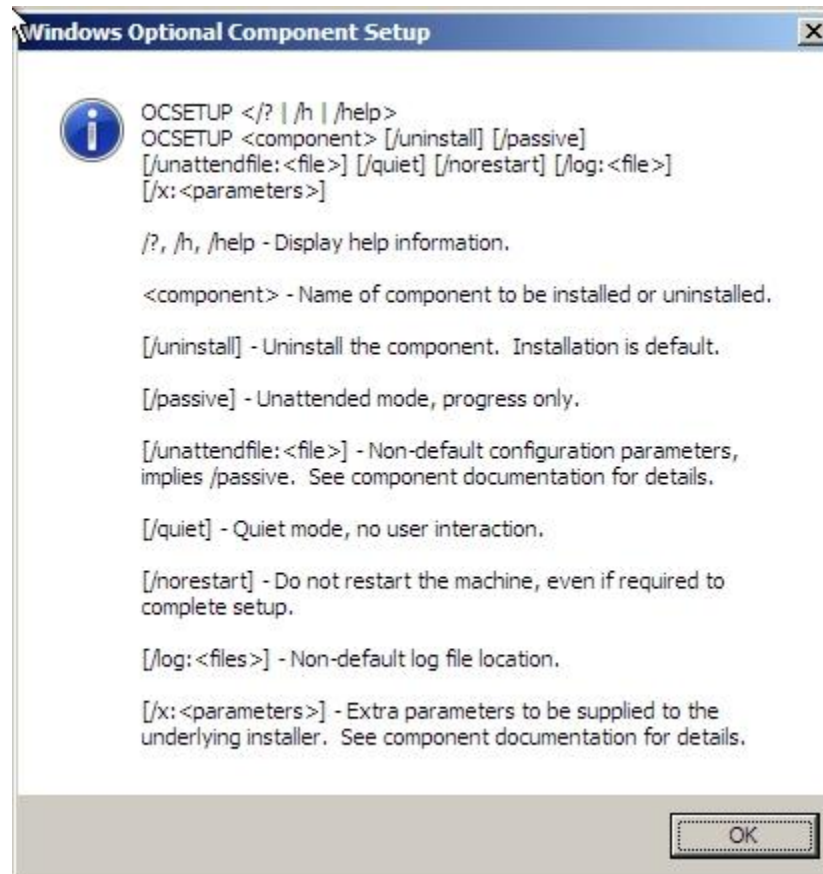
Cscript C:\windows\system32\scregedit.wsf /AU /4

Una vez que hayamos configurado las actualizaciones, procederemos a parar y reiniciar el servicio de actualizaciones, para que éste recoja el [cambio](#). Teclearemos los siguientes comandos:

Net stop Wuauserv

Net start Wuauserv

Existen multitud de comandos que podemos emplear a través de la Shell de Windows. Las posibilidades son amplias. Los límites son nuestra imaginación y conocimientos. Instalar un componente o algún rol no es muy distinto de lo que ya hemos explicado. La operativa a través de la línea de comandos es la misma, siendo la única particularidad que tendremos que hacerlo a través de una aplicación denominada ocsetup.exe.



Si por ejemplo necesitásemos instalar un servidor DHCP en nuestro Windows Server LongHorn, ejecutaríamos el siguiente comando:

Ocsetup.exe DHCPServerCore

Automáticamente el sistema instalaría un servidor DHCP en nuestro equipo. Actualmente la herramienta ocsetup es sensible a mayúsculas y minúsculas, con lo que tendríamos que escribir el comando exactamente como ha sido reflejado con anterioridad.

BitLocker. Cifrado de Datos

Windows Server LongHorn incorpora una nueva funcionalidad en el campo de cifrado de datos. BitLocker. Este nuevo sistema garantiza la seguridad y la confidencialidad de los datos almacenados en el disco mediante cifrado.

BitLocker va a ser el encargado de realizar los procesos de cifrado y descifrado de una forma totalmente transparente. Adicionalmente y a diferencia de Windows Vista, podemos extender el cifrado de datos a otros volúmenes que utilicemos para tal fin.

Este mismo mecanismo interviene también cuando el equipo entra en el modo de hibernación o para garantizar también la seguridad del fichero de paginación, los ficheros temporales y todos aquellos elementos que puedan contener información sensible.

Los mecanismos de seguridad implementados por BitLocker se complementan mediante unas nuevas especificaciones de seguridad [hardware](#) llamada Trusted Platform Module (TPM). Este nuevo chip TPM proporciona una plataforma segura para el almacenamiento de claves, password o certificados, haciendo más difícil el ataque contra las mismas. Una vez que el mecanismo de cifrado ha sido puesto en marcha, la clave de cifrado es eliminada del disco y posteriormente almacenada en el Chip TPM.

Con objeto de defendernos de un posible ataque al sistema hardware que intente explotar posibles vulnerabilidades, se proporcionan mecanismos de autenticación mediante [sistemas](#) adicionales tales como el uso de Token (llave [USB](#)) o una password (PIN) para evitar esta posibilidad.

Cabe decir en este punto que aunque nuestros equipos no dispusieran de este mecanismo de seguridad, las especificaciones de BitLocker admiten su funcionalidad sin el chip TPM.

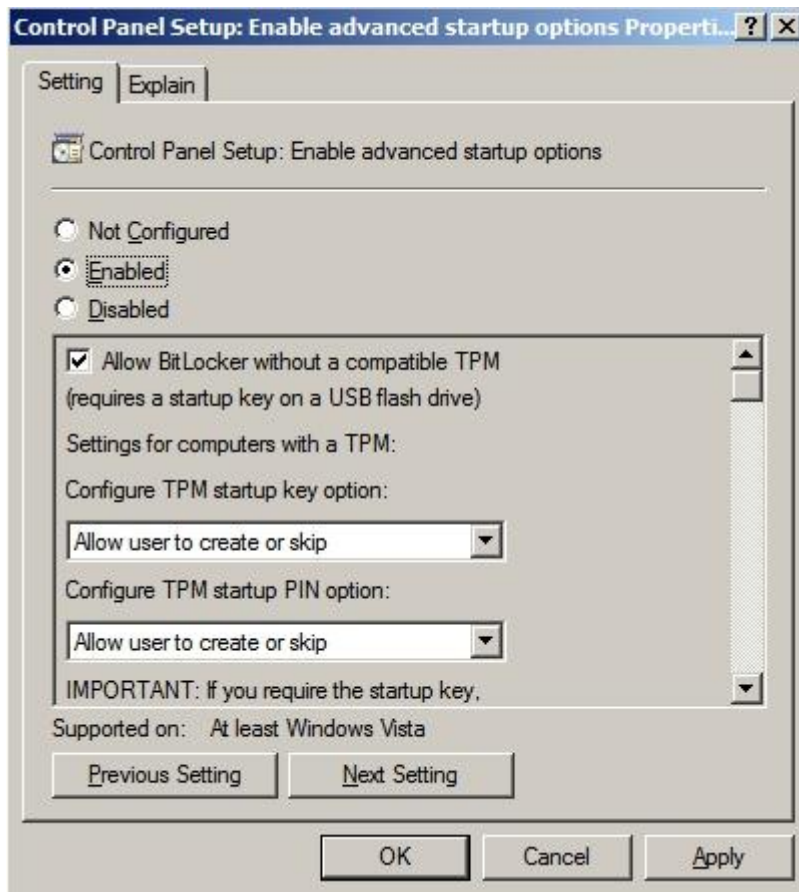
El uso combinado de mecanismos hardware y [software](#) aumenta sensiblemente el porcentaje de posibilidades de éxito a la hora de protegernos de aquellos ataques que tengan como [objetivo](#) la modificación o alteración de datos. Estos aunque cifrados podrían ser manipulados mediante la explotación de vulnerabilidades para poder posteriormente acceder a ellos.

La implementación de BitLocker requiere de la existencia de condiciones determinadas para poderla llevar a efecto. Un factor a considerar es que el sistema debe disponer al menos de dos particiones NTFS. Una de ellas, la partición activa, albergará el sistema de arranque y no se encontrará cifrada. Es por ello que BitLocker también proporciona mecanismos para garantizar que no se han producido modificaciones en el sistema de arranque del sistema, tales como los que pueden provenir de ataques tipo malware que pudieran producir un ataque colateral o el control del acceso al sistema.

Los mecanismos de implementación pueden variar en función del escenario que necesitemos implantar. Dependiendo del mismo son diversas las posibilidades. De este modo podremos utilizar BitLocker sólo con TPM, con algún dispositivo de validación (USB), TPM más PIN, o TPM con dispositivo de validación (USB).

La implementación de esta tecnología dependerá fundamentalmente si nuestro hardware presenta o no el chip TPM. Si no lo llevase, la única opción posible sería el almacenamiento de clave bajo dispositivo USB.

Para todos aquellos que necesiten utilizar el cifrado y no posean el Chip TPM, Windows Server LongHorn presenta una directiva de seguridad bajo la cuál podemos condicionar el uso de BitLocker sin el citado Chip. Por defecto el sistema sólo admite la configuración de BitLocker si el equipo cuenta con el Chip.



NAP (NetWork Access Protection)

Sin lugar a dudas podemos afirmar que en la actualidad las [redes](#) corporativas y las no corporativas son cada día más complicadas de administrar y securizar. Los escenarios presentan cada vez circunstancias de mayor dificultad: comerciales que conectan sus PDAs a los portátiles o equipos de sobremesa, conexión permanente por parte de los usuarios de [dispositivos de almacenamiento](#) externo, usuarios que presentan necesidades operativas en distintas redes de forma habitual son, junto a otros, claros ejemplos de ello.

Desgraciadamente estas circunstancias incrementan considerablemente las múltiples amenazas de seguridad posibles como pueden ser malware, exploits, spyware, DOS, Script-Kiddies y otros. Estas aplicaciones pueden tomar el control de nuestro sistema, realizando [acciones](#) malévolas de forma totalmente transparente. Lo peor de todo, aún así, es que además pueden utilizar el sistema comprometido como puerta de entrada de otras amenazas.

La característica NAP (NetWork Access Protection) es otra de las novedades que nos ofrece Windows Server Longhorn en cuanto a la securización del sistema. Podemos utilizar NAP para paliar el impacto de situaciones como las antes indicadas, y optimizar el nivel de protección de la red corporativa y la información contenida en la misma. Esta tecnología se pensó en un principio para que estuviese presente en [Microsoft](#) Windows Server 2003 R2, pero finalmente en su lugar apareció NAQS (Network Access Quarantine Control) integrándose con IAS (Internet Authentication Service) como solución de control de acceso para [clientes](#) de acceso remoto. Esta implementación a través de una validación del [modelo](#) de seguridad vía vbscripting, fue algo que más tarde apareció integrado en la solución de Microsoft ISA Server 2004 a través de una característica conocida como [VPN](#) Quarantine. En el siguiente enlace podemos encontrar más información al respecto: <http://go.microsoft.com/fwlink/?LinkId=56447>.

La implementación de NAP en Windows Server Longhorn nos permite especificar cuál es la política de [salud](#) de nuestra red. De este modo se establecen una serie de condiciones que ayudarán a los administradores a determinar que equipos de los que se conecten a nuestra red desde cualquier medio (VPN, Internet, Wireless junto a otros) cumplen con una política de salud aceptable y acorde a las directrices de la seguridad corporativa.

Si para nosotros una buena política de salud pasa por defendernos de las [enfermedades](#), hacer ejercicio de forma constante, una buena alimentación, etc., para un equipo una buena política de salud pasaría por disponer de un [antivirus](#) a pleno funcionamiento y con las firmas actualizadas, tener instaladas todas las actualizaciones de seguridad, junto a otras medidas de securización que puedan considerarse como imprescindibles. Para los equipos que no cumpliera con la política de seguridad establecida, podrían ser dos las circunstancias: en primer lugar que no fuese posible la conexión a nuestra red corporativa o como alternativa que esta fuese limitada. En este segundo caso la conexión se realizaría pero en una red aislada de toda la corporación, con acceso sólo a algunos recursos, y a la espera de poder cumplir con los mínimos requisitos de salud. Con NAP podremos:

- Asegurar una política de salud en nuestros equipos que se configuren para DHCP, equipos que se conecten a través de mecanismos de autenticación 802.1X, VPN, y equipos que tengan una política de seguridad NAP IPSEC aplicadas a sus [comunicaciones](#).
- Reforzar la política de seguridad y de salud en equipos portátiles, cuando éstos vuelvan a conectarse a nuestra red
- Restringir el acceso a nuestra red a todo equipo que no cumpla con la política de salud de la compañía NAP también incluye una API (Application Programming Interface) para desarrolladores. A través de ella será posible la generación de componentes de seguridad realizados a medida de las necesidades del sistema corporativo. Una infraestructura NAP requiere de un servidor Windows Server LongHorn para su despliegue, y los clientes soportados son Windows Server LongHorn, Windows Vista y [Windows XP](#) SP2. Para éste último, necesitamos instalar el cliente NAP para Windows XP, y que actualmente se puede descargar desde la [Web](#) <http://connect.microsoft.com/>. Estas tecnologías pueden ser utilizadas de forma independiente o junto a otras en función del modelo de seguridad y la infraestructura a utilizar. La implementación de políticas de salud se realiza a través de un NPS (Network Policy Server) disponible en Microsoft Windows Server LongHorn, y que reemplaza a IAS (Internet Authentication Service) presente en Microsoft Windows Server 2000/2003. NAP se va a responsabilizar de llevar a efecto una serie de acciones:

- Validación de la política
- Aplicación de NAP
- Restricción (cuando ésta es necesaria)
- Establecer las pautas para adecuar el nivel de salud de un cliente
- Supervisión

NPS (Network Policy Server) utiliza SHVs (System Health Validators) para analizar el estado de salud del equipo. SHVs viene incorporado dentro de las políticas de red, y determina la acción a tomar basándose en el estado de salud del equipo que se conecta. Como indicábamos las acciones que se pueden desencadenar son varias: conceder el acceso a toda la red en aquellas situaciones en que se cumplen las demandas de seguridad establecidas o por el contrario denegar el acceso o limitar el mismo a una red de cuarentena en caso contrario.

El estado de salud de un equipo es monitorizado por una parte del cliente NAP, denominada SHAs (System Health Agent). La protección de acceso a la red utiliza en definitiva SHAs y SHVs para monitorizar, reforzar y remediar la configuración de seguridad-salud de un equipo.

Windows Security Health Validation y Windows Security Health Agent se encuentran incluidos en Windows Server LongHorn y Windows Vista. Ellos refuerzan las siguientes configuraciones en un entorno NAP protegido:

- El PC cliente tiene el Firewall instalado y en funcionamiento
- El PC cliente tiene el antivirus instalado y en funcionamiento
- El PC cliente tiene las últimas bases de [virus](#) instaladas
- El PC cliente tiene el software anti-spyware instalado y en funcionamiento
- El PC cliente tiene las últimas bases anti-spyware instaladas
- El PC cliente tiene habilitado Microsoft Update Services

Si a todo esto añadimos un servidor WSUS, el cliente NAP puede verificar que las últimas actualizaciones de seguridad están instaladas en el equipo, basándose en uno de los cuatro niveles de seguridad establecidos por la plataforma Microsoft Security Response Center (MSRC).

Como mencionábamos con anterioridad NAP puede ser configurado para denegar totalmente el acceso a la red, o permitir acceso sólo a una red de cuarentena. En una red de cuarentena podremos encontrar servicios NAP, tales como servidores de certificados de salud (HRA), necesarios para la obtención de certificados provenientes de una entidad certificadora (CA) o remediation servers (RS). Estos últimos disponen los recursos necesarios para que aquellos clientes que no tengan un nivel de salud óptimo, puedan realizar ciertas tareas. Como opción podemos disponer también en la red de cuarentena de recursos que permitan actualizar los equipos con las últimas actualizaciones de seguridad, bases de virus, bases anti-spyware, y otros. Una breve descripción del proceso sería la siguiente. El agente de salud del sistema (SHAs) contiene la información de salud de los equipos. Éste pasa la información a un servidor NPS. El validador de salud (SHVs) del servidor de políticas de red (NPS) realiza el proceso de validación de la política de salud del equipo cliente, y determina si cumple los requisitos para poder conectarse a la red. Si no los cumple, manda a este equipo a una red de cuarentena, en donde dispondrá de los recursos necesarios para que se pueda actualizar acorde a la política de salud de la red corporativa. Con NAP también nos es posible configurar los servicios de remediación, para que éstos automáticamente actualicen los equipos en función de la política de salud de la [empresa](#). Analicemos un ejemplo de posible intervención de estos servicios. En una política de seguridad donde los equipos deban disponer del Firewall Windows activado, si habilitamos la opción en automático (servicios de remediación), aquel cliente que no tenga disponible el firewall de Windows activado, sería enviado a un segmento de red de cuarentena, y los componentes NAP del cliente habilitarían el firewall de Windows sin intervención del usuario.

La operativa de NAP es posible en diversos escenarios. Algunas posibilidades podrían ser los siguientes: tráfico protegido con IPSEC, 802.1X, VPN con acceso remoto, DHCP IPV4 (tanto para renovación como concesión de direcciones). Describamos con algo más de detalle estos escenarios.

- NAP para entornos IPSEC. Para la implementación de NAP en entornos con IPSEC es necesario implantar una entidad certificadora de salud (HRA Server), un NPS Server y un cliente IPSEC. El HRA publica los certificados de salud X.509 para los clientes NAP. Estos certificados son utilizados para autenticar los clientes NAP cuando éstos inician una comunicación basada en IPSEC con otros clientes NAP de la intranet. Este es el método más seguro de aplicar NAP.
- NAP para entornos 802.1X. Para implementar esta solución, necesitamos desplegar un servidor NPS y un componente (EAP). El servidor NPS envía la autenticación basada en 802.1X a un punto de acceso de la red

interna. Si el equipo cliente no cumpliera con alguna regla establecida, el servidor NPS limitaría el acceso al cliente mandando al punto de acceso un filtro basado en dirección IP o identificador virtual.

- NAP para entornos VPN (Virtual Private Network). En esta ocasión necesitamos de un servidor y un cliente VPN. Usando NAP para entornos VPN, los servidores VPN pueden forzar el cumplimiento de la política de salud de la empresa cuando los clientes externos se conecten a nuestra intranet. Esta solución proporciona los mecanismos necesarios para establecer una comunicación segura entre un cliente externo y la red interna.
- NAP para entornos de configuración dinámica de direcciones (DHCP). Para implementar esta solución, necesitamos el componente NAP de un servidor DHCP y un servidor NAP. Usando DHCP, podemos cumplir con la política de salud de la empresa a través de NPS y DHCP. Cuando un equipo intente renovar o solicitar una dirección IP (IPv4). El servidor limitaría el acceso a los equipos que no cumplieran con la política de salud de la empresa asignando direcciones IP reservadas para tal fin. Cada uno de estos métodos de implementación NAP tiene sus ventajas e inconvenientes, por lo que implantar una plataforma de este tipo en una corporación dependerá en gran medida de las necesidades de servicio y condiciones operativas de ésta. NAP adicionalmente proporciona una API para desarrolladores que necesiten integrar su software a las necesidades de la empresa. Con ello las posibilidades de personalización de las [soluciones](#) es aún mucho mayor.

Windows Deployment Services

Respecto al despliegue de sistemas, en anteriores versiones de Windows disponíamos de la herramienta RIS (Remote Installation Services). Con Windows Server LongHorn, esta herramienta se ha actualizado, denominándose ahora Windows Deployment Services. Se nos presenta como una serie de componentes que podremos utilizar para llevar a efecto con éxito un despliegue masivo de equipos. Estos componentes están organizados en tres categorías:

- Componentes de servidor: Estos incluyen un entorno de pre-arranque (Pre-Boot Execution Environment o PXE) y un TFTP (Trivial File Transfer Protocol), componentes que necesitaremos para poder arrancar un cliente con soporte de red, y posteriormente instalar el sistema operativo. También se incluyen directorios compartidos, repositorio de imágenes y los ficheros necesarios para poder realizar un despliegue.
- Componentes de cliente: Estos componentes incluyen un interfaz gráfico que arranca con el Windows Preinstallation Environment (Windows PE). Éste se comunica con el servidor de componentes para poder seleccionar e instalar la imagen del sistema operativo.
- Componentes de [mantenimiento](#): Son una serie de herramientas que nos ayudarán a mantener el servidor, las imágenes de los [sistemas operativos](#), junto a otras posibilidades.

Gracias a esta tecnología de despliegue podemos mantener e instalar equipos a través de la red, sin que tengamos que estar físicamente en el equipo. Al poder automatizar estas tareas, la corporación gana en tiempo, mejora el mantenimiento y reduce el esfuerzo humano, con las consiguientes ventajas económicas que ello supone. Si antiguamente, para implantar una oficina de 100 equipos con Windows XP, necesitábamos 3 administradores y 25 [CD](#) de instalación, gracias a estas soluciones, ahorraríamos coste humano y dejaría de ser una necesidad el disponer de soporte de [medios](#) para el almacenamiento de esos [sistemas operativos](#).

Algunas Notas sobre Servicios en Windows Server LongHorn

En el campo de los servicios, Windows Server LongHorn amplía su uso del principio del mínimo privilegio mediante una reducción, aún mayor, de los privilegios y el acceso a los archivos y claves del [Registro](#). Windows Server LongHorn crea una nueva cuenta de grupo, denominada Identificador de seguridad del servicio (SID), la cual es exclusiva de cada servicio. Un servicio puede establecer permisos en todos sus

recursos, pero de forma que sólo tenga acceso su SID de servicio. Esto impide que los servicios que se ejecutan bajo la misma cuenta de usuario puedan tener acceso si un servicio se ve en peligro. El SID de un servicio lo podemos ver tecleando en el intérprete de comandos o en Windows PowerShell el comando `sc showsid` seguido del nombre del servicio. Los SID de servicio protegen el acceso a los recursos que son [propiedad](#) de un servicio específico, aunque de manera predeterminada los servicios continúan pudiendo acceder a todos los objetos para los que la cuenta de usuario en la que se ejecutan tenga privilegios.

Windows Server LongHorn introduce un nuevo tipo de servicio restringido denominado servicio restringido de escritura, que concede un acceso de escritura de servicio sólo a aquellos objetos accesibles a su SID de servicio, al grupo Todos y al SID asignado a la sesión de inicio. Para ello se utilizan SID restringidos, un tipo de SID introducido en [Windows 2000](#). Cuando el proceso que abre un objeto es un servicio restringido de escritura, el [algoritmo](#) de comprobación de acceso cambia para que un SID que no se haya sido asignado a un proceso, no se pueda usar para conceder al proceso acceso de escritura a un objeto.

Ahora, con Windows Server LongHorn, es más sencillo que un servicio impida que otros servicios que se ejecutan en la misma cuenta tengan acceso a los objetos que éste servicio crea. En versiones anteriores de Windows, el autor de un objeto es también propietario de él, y como propietario del mismo, es capaz de leer y cambiar los permisos de sus objetos, concediendo acceso completo a sus propios objetos. Windows Server LongHorn introduce el nuevo SID de [derechos](#) de propietario, el cual, si existe en los permisos de un objeto, puede limitar los accesos que un propietario tiene a su propio objeto, incluso eliminando el derecho de establecer y consultar los permisos. Cuando el Administrador de control de servicio inicia un proceso que hospeda uno o varios servicios de Windows, éste crea un token de seguridad (que incluye la cuenta de usuario de un proceso, las pertenencias a grupos y los privilegios de seguridad) para el proceso que contiene sólo los privilegios necesarios para los servicios del proceso. Si un servicio especifica un privilegio que no está disponible para la cuenta en que se ejecuta, el servicio no se puede iniciar. Si ninguno de los servicios que se ejecutan en un proceso de cuenta de servicio local necesita algún tipo de privilegio, el Administrador de control de servicio elimina dicho privilegio del token de seguridad del proceso. Un código malicioso no podrá utilizar los privilegios no solicitados por los servicios que se ejecutan en el proceso. En Windows Server LongHorn, la elevación de privilegios mediante inyecciones dll o suplantación de tokens, es todavía, si cabe, mucho más difícil.

Mantener el control de los servidores en una corporación, y que los clientes puedan acceder a los recursos alojados en los servidores en una red, son prioridades fundamentales para los administradores. Partiendo de esta premisa, Windows Server LongHorn actualiza su área de funcionalidad Internet Information Services 7.0 (IIS 7.0), que nos va a ayudar a los administradores a maximizar el control sobre los accesos a los servidores de red.

Windows Server LongHorn ofrece una plataforma unificada para la publicación web que integra IIS 7.0, [ASP](#) .NET, Windows Communication Foundation, Windows Workflow Foundation, y Windows SharePoint Services 3.0.

Podemos presentar IIS 7.0 como una de las principales mejoras que se han introducido en esta nueva versión de sistema operativo servidor Windows. Juega un papel clave en la integración de tecnologías Web. Ayuda a los desarrolladores y administradores a maximizar el control sobre las interfaces de Internet y de red. Para ello hace uso de sus potentes características, como son la administración delegada, una seguridad mejorada, un área de superficie menor para un posible ataque, aplicación integrada y gestión del rendimiento para servicios web, así como herramientas mejoradas de administración. Para aquellas [empresas](#) que tengan usuarios remotos, Windows Server LongHorn añade una serie de mejoras e innovaciones en los servicios de terminal (Terminal Services Web Access y Terminal Services Gateway). Con ello se facilita la integración de aplicaciones remotas y locales en los equipos cliente, el acceso a estos mismos [programas](#) a través de un navegador web, y el acceder a terminales y aplicaciones remotas a través de firewalls.

Esta nueva funcionalidad de Terminal Services Web Access ofrece una gran flexibilidad en el acceso a aplicaciones remotas a través de un navegador web, aceptando una amplia variedad de formas en que el usuario puede hacer uso de los programas desde terminales remotos. Por su parte, Terminal Services Gateway permite al usuario acceder a terminales remotos y a programas de terminales remotos de una manera tipo firewall. Y todo ello sin tener que configurar nada en el cliente.

Son otras muchas las novedades y mejoras que incorpora Windows Server LongHorn. Evidentemente no es posible analizarlas íntegramente en un simple artículo. Una mayor flexibilidad a la hora de controlar dominios que se encuentren en localizaciones no seguras, el uso y facilidad de integración de aplicaciones de negocio junto a otros son claros ejemplos de ello y que por el momento no abordaremos de forma directa en el presente artículo. .

Hemos pretendido con estas breves líneas en [torno](#) a Windows Server LongHorn realizar un breve acercamiento a alguna de las nuevas características y funcionalidades del sistema tanto en el ámbito de la seguridad, como en el nivel de aplicación. Hemos simplemente destacado y mencionado alguna de las muchas innovaciones que hemos considerado de especial interés. En ningún término nuestro planteamiento ha sido generar con el presente artículo información técnica de referencia, y bajo esta panorámica deben ser asimilados los datos aquí recogidos. Será necesario que administradores y técnicos del sistema sigan trabajando y estudiando características y funcionalidades del nuevo entorno servidor Windows. Pero sin lugar a dudas este nuevo sistema les proporcionará mejores condiciones y herramientas para el correcto [desarrollo](#) de sus tareas habituales.

Autor:

Ing. Daniel Ricardo S?nchez Jaramillo