
Mantenimiento

PID_00204294

Jordi Serra Ruiz



Los textos e imágenes publicados en esta obra están sujetos –excepto que se indique lo contrario– a una licencia de Reconocimiento-NoComercial-SinObraDerivada (BY-NC-ND) v.3.0 España de Creative Commons. Podéis copiarlos, distribuirlos y transmitirlos públicamente siempre que citéis el autor y la fuente (FUOC. Fundación para la Universitat Oberta de Catalunya), no hagáis de ellos un uso comercial y ni obra derivada. La licencia completa se puede consultar en <http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.es>

Índice

Introducción.....	5
Objetivos.....	6
1. Actualizaciones.....	7
1.1. GNU/Linux	7
1.2. Windows Server 2012	9
1.2.1. Actualizaciones de Windows Update	9
1.2.2. Windows Server Update Services	10
1.2.3. Microsoft Technical Security Notification	14
1.2.4. Seguridad mejorada de Internet Explorer	14
2. Monitorización de acontecimientos.....	16
2.1. GNU/Linux	16
2.2. Microsoft Windows Server 2012	20
2.2.1. Monitorización de los registros de incidencias	20
2.2.2. Monitorización del rendimiento del sistema	22
3. Automatización de tareas.....	24
3.1. GNU/Linux	24
3.2. Windows Server 2012	25
3.2.1. Tareas programadas	25
3.2.2. Scripting. Windows Management Instrumentation (WMI)	27

Introducción

Tan importante es la buena instalación y configuración de los servidores y las aplicaciones que tienen, como el mantenimiento que se tiene que hacer durante todo el periodo de vida del sistema informático.

Tanto los sistemas de Microsoft como GNU/Linux se actualizan constantemente, el software y los sistemas operativos, sea con parches que se tienen que instalar sobre el sistema operativo o con nuevas versiones de estos sistemas, reciben nuevas versiones de los diferentes módulos, mejoradas y más seguras, que hacen más difícil poder atacar los sistemas.

Es muy importante revisar e instalar las actualizaciones que crean los fabricantes del software en general, puesto que normalmente son proporcionadas por agujeros de seguridad que se han descubierto en el sistema operativo.

La filosofía de “Ya funciona, no toquemos nada” es buena, puesto que puede haber un error del sistema que desconozcan los administradores pero que se solucione instalando un simple “parche” o una actualización.

Otro aspecto importante que hay que tener en cuenta es la monitorización de los acontecimientos o del sistema operativo. En estos *logs* quedan guardados todos los acontecimientos que se producen en el sistema. Por ejemplo, el acceso externo de un usuario al servidor.

Objetivos

En este módulo pretendemos que se conozca la manera de tener actualizado y protegido un sistema informático en general. A tal efecto os planteamos los objetivos siguientes:

- 1.** Conocer los métodos de actualización que tienen los sistemas operativos.
- 2.** Conocer los sistemas de almacenamiento de acontecimientos o *logs* de los sistemas.
- 3.** Aprender los mecanismos de automatización de tareas.

1. Actualizaciones

Una de las máximas de los administradores de sistemas es que “si una cosa funciona bien, no la toques”. Actualmente esta máxima no es aplicable, puesto que nos podemos encontrar con que, a pesar de que tenemos un sistema estable y que funciona de manera correcta, lo tengamos que actualizar. Esta actualización no la llevamos a cabo por capricho, ni para ofrecer un servicio mejor a los usuarios, ni para que el usuario esté siempre a la última moda. El motivo principal de aplicar las actualizaciones del software es la seguridad.

Hoy en día hay mucha gente que investiga todas las versiones de software que hay en activo con el fin de encontrar una vulnerabilidad para explotarla y, de este modo, conseguir entrar en una máquina. Del mismo modo, hay muchos programadores de aplicaciones que se dedican a intentar encontrar vulnerabilidades en sus aplicaciones para mejorar sus versiones y hacerlas más fuertes ante posibles vulnerabilidades. Cuando encuentran una que puede comprometer la máquina que usa su software, emiten una advertencia de seguridad, en la que indican que actualizan la versión de software que se ha visto comprometida a una versión superior, en la que ya se ha solucionado la vulnerabilidad.

Si queremos, nos podemos suscribir a esta lista, o consultar las vulnerabilidades que han salido mediante la URL, y hacer diferentes tipos de buscas, incluso por meses o años.

En el momento en que un fabricante de software, el que sea, distribuye un parche para ser aplicado en una parte de su software, directamente está publicando qué problema existirá en su software si no se aplica el parche. Esta información la aprovechan las personas que programan los *exploits*, que estudian con ingeniería inversa los parches que se publican para atacar todos aquellos sistemas que no están actualizados, ya que aplican la premisa de “no tocar nada, que dejará de funcionar”.

1.1. GNU/Linux

Si queremos actualizar todos los paquetes de nuestra distribución Debian instalada en el ordenador, tenemos que ejecutar las órdenes:

```
root# apt-get clean  
root# apt-get update
```

Una vez acabada, ejecutamos:

```
root# apt-get upgrade
```

Nos muestra todos los paquetes que se instalarán y nos pide si queremos continuar la actualización. Tenemos que decir que sí. Entonces baja todos los paquetes que se tienen que actualizar, los instala y, si es necesario, los configura. Dependiendo de los paquetes que actualizamos, nos pide datos de configuración.

A pesar de que esta manera de llevar a cabo una actualización del sistema es muy cómoda para el administrador, tenemos que ir con mucho cuidado cuando la utilizamos en servidores de producción, es decir, en los servidores que están ofreciendo algún servicio, puesto que muchas veces, al hacer la actualización, esta será necesaria para el servicio, o la configuración de los programas por defecto que hay en estos servicios harán que deje de funcionar. Por eso, en casi todos los casos, en el momento de actualizar, el sistema pregunta si se quiere hacer o no el cambio de los ficheros de configuración por los que venden por defecto. Se puede incluso mirar cuáles son las diferencias entre los dos ficheros de configuración y decidir cuál será el que mejor funcione.

Además puede pasar que en algunas versiones de software el cambio de versiones no sea compatible con otros programas de los que disponga el equipo, o dicho de otro modo, el que funcionaba en la versión que tenemos instalada no funcionará en la versión que queremos actualizar. Esto pasa porque en la nueva versión:

- se utilizan componentes nuevos,
- se utilizan ficheros de configuración diferentes,
- se han añadido parámetros nuevos.

Para evitar estas situaciones, podemos proceder de dos maneras diferentes:

1) Actualizar solo las aplicaciones que sabemos que tienen fallos graves en la seguridad, y hacerlo de manera manual. Para lo cual, primero tenemos que bajar la versión de la aplicación que nos interesa actualizar y después instalarla manualmente. En este caso, podemos hacer la instalación vía compilación o vía paquete Debian.

2) Hacer la actualización del sistema en una máquina de pruebas, comprobar que todo continúa funcionando y después hacer la actualización en el servidor. Esto se acostumbra a conocer como sistema en preproducción. Son equipos idénticos, con el mismo software, que sirven de prueba para hacer actualizaciones y cambios sobre el sistema real, que en el caso de que tenga éxito o no den problemas, se pasarán al equipo en producción.

1.2. Windows Server 2012

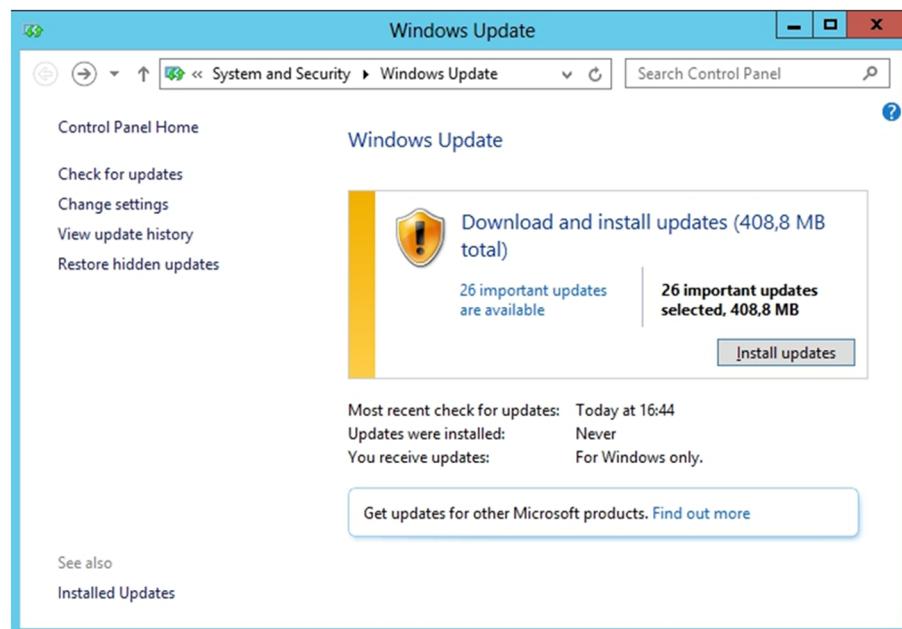
1.2.1. Actualizaciones de Windows Update

Cuando se descubre uno de estos fallos del sistema operativo, Microsoft corrige el código fuente del sistema para enmendar el error. Sin embargo, todos los sistemas que ya están instalados continúan teniendo este error. Por eso es muy importante tener el sistema actualizado.

Para facilitar la actualización del sistema operativo, Microsoft dispone de un sitio web de actualización desde el cual se pueden obtener gratuitamente y de manera automática todas las actualizaciones necesarias para tener el sistema al día. En las últimas versiones de Windows Update, se requiere instalar un conector o *plug-in* de Microsoft al acceder a la URL de Windows Update para bajar correctamente las actualizaciones.

El proceso de actualización se resume en unos cuantos pasos. Primero, se da al usuario la opción de seleccionar entre dos maneras de hacerlo: la rápida o la personalizada. En los dos casos se muestran las actualizaciones de sistema, pero la opción personalizada también muestra posibles actualizaciones de software y hardware (programas controladores o *drivers* de impresión, de tarjetas de red, de vídeo, etc.), además de permitir no seleccionar alguna de las actualizaciones si no se quiere instalar. En el caso de los servidores, es mejor decidir cuál es el que se instala y, sobre todo, cuándo se instala, puesto que esto permite tener un mejor control de lo que está pasando en el servidor.

Windows Update



Una vez seleccionada la opción de instalación de las actualizaciones, el sistema escanea el equipo para localizar las actualizaciones que falta por instalar. Cuando acaba, el sistema muestra una pantalla (figura anterior) con todas las actualizaciones disponibles. Hay que hacer clic en el botón “Instalar las actualizaciones” y aceptar el contrato de licencia para continuar la actualización.

Una vez completada la instalación, el sistema queda completamente actualizado. Es posible que para instalar algunos parches haya que reiniciar el servidor. Por eso se aconseja instalar parches en horarios de poco acceso al servidor (quizás por la noche o después de las copias de seguridad o *backups*).

Las actualizaciones de Windows Update se pueden automatizar de manera que el sistema compruebe periódicamente si hay alguna y la baje e instale sin que el usuario tenga que intervenir. Para configurar la bajada automática de actualizaciones, abrimos la herramienta “Actualizaciones automáticas” del panel de control.

En esta herramienta podemos seleccionar o no la opción de hacer bajadas automáticas y podemos elegir uno de los cuatro métodos siguientes:

- 1) Bajar automáticamente las actualizaciones recomendadas para el equipo e instalarlas. Aquí se puede indicar a qué hora se quiere que se bajen y se instalen las actualizaciones.
- 2) Bajar las actualizaciones nosotros mismos, pero permitirnos elegir cuándo las queremos instalar. Las actualizaciones quedan bajadas en el servidor, pero pendientes de instalar.
- 3) Notificarnos las actualizaciones, pero no bajarlas automáticamente ni instalarlas. Nos informa de actualizaciones nuevas pero no las baja ni las instala.
- 4) Desactivar actualizaciones automáticas.

1.2.2. Windows Server Update Services

En una red de una empresa con muchos clientes conectados y diferentes versiones de sistemas operativos, es difícil mantener todos los equipos al día. Por eso es importante mantener activada la bajada automática de actualizaciones en todos los equipos.

Sin embargo, si cada equipo tuviera que bajar los centenares de megabytes de información de todas las actualizaciones, provocaría un descenso importante del rendimiento de la red.

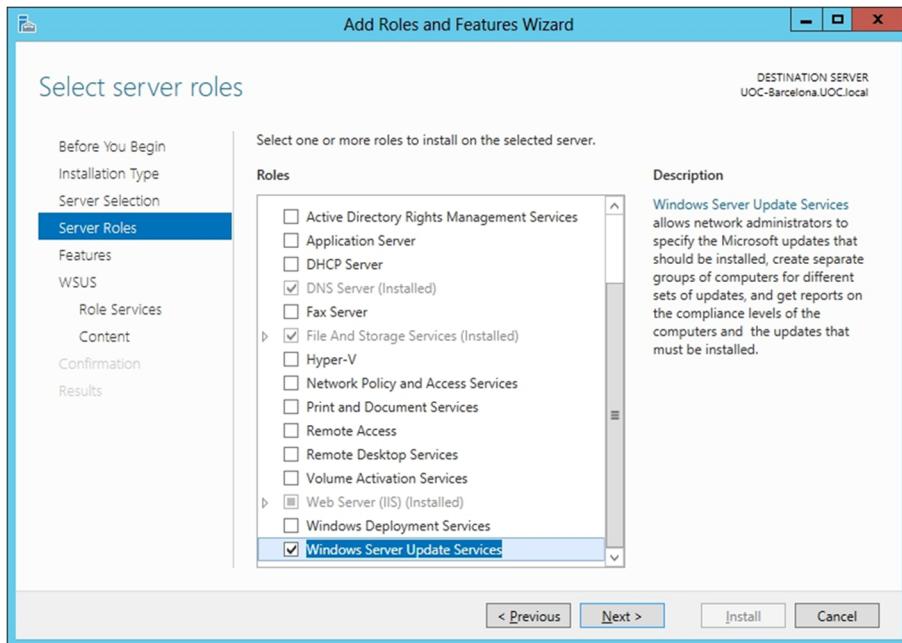
Windows Server Update Services (WSUS) es una aplicación que permite a los administradores bajar una única vez las actualizaciones disponibles para los sistemas operativos de la red, almacenar estas actualizaciones en un servidor y

permitir que los clientes bajen las actualizaciones directamente de este servidor en lugar de hacerlo del servidor de Windows Update. Con esto se consigue velocidad en la bajada, puesto que se usa la red local, y también facilidad a los clientes para configurar y actualizar los parches desde el servidor.

Para instalar este componente tenemos que tener instalado IIS (el servidor de páginas web) en el servidor, puesto que los clientes consultan y actualizan los parches consultando una página web, en lugar de la web de Microsoft Windows Update. Para instalar IIS hay que ir al panel de control, al administrador del servidor y añadir el rol, como ya se ha explicado anteriormente.

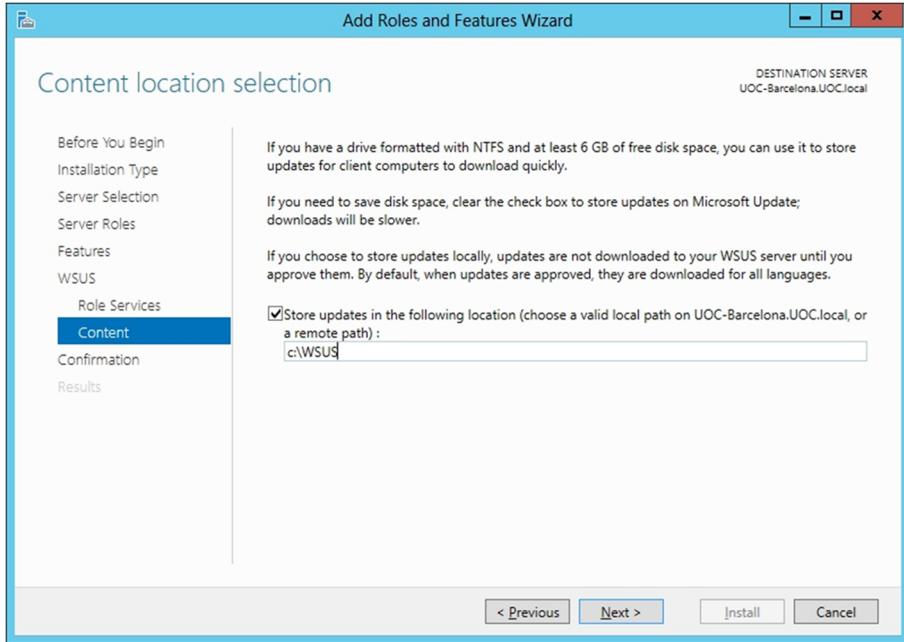
Además, para gestionar las actualizaciones, se tiene que instalar también el servidor de actualizaciones en el propio servidor, por lo tanto, el rol de WSUS (*Windows Server Update Services*) también se tendrá que seleccionar para instalarlo.

WSUS



El servicio WSUS tiene que gestionar las actualizaciones propias y del resto de los equipos del dominio, y para hacer esto necesita una base de datos. En el propio proceso de instalación ya se puede fijar una base de datos por defecto, WID data base. Y ya únicamente queda seleccionar un directorio donde ir guardando todas las actualizaciones, que se puede crear en un disco local del servidor o en algún otro recurso compartido de la red.

Directorio WSUS

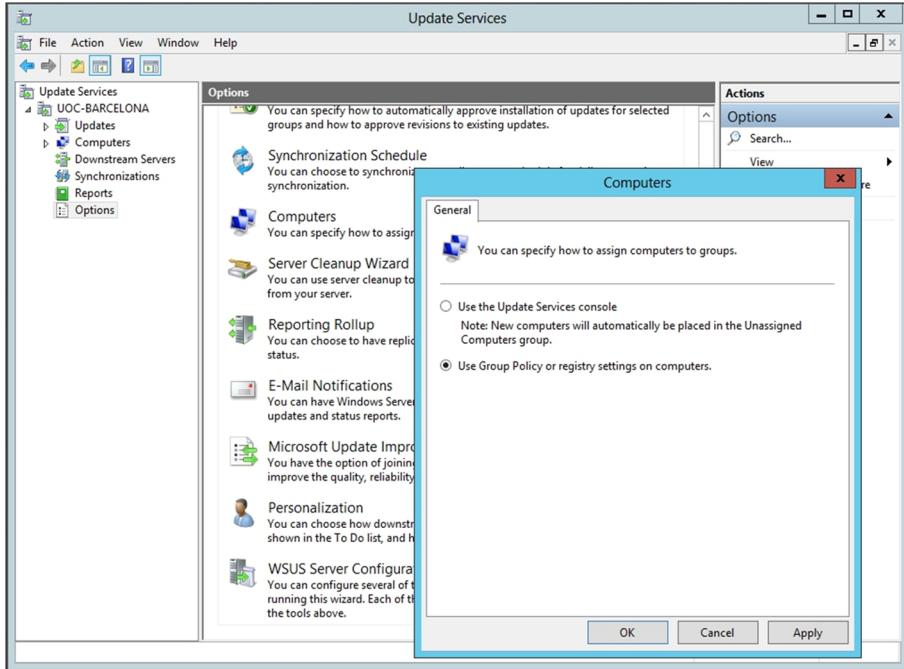


Una vez acabada la instalación, requiere que se ejecute el configurador (que se puede hacer desde la misma pantalla del administrador del servidor). Iremos seleccionando y conectándonos al servidor de Microsoft para acabar configurando correctamente el servicio.

Se pueden seleccionar los idiomas que sean necesarios, así como el software con el que se quiere dar servicio a las actualizaciones. Se muestra un desplegable donde se puede ir seleccionando todo aquello a lo que se quiere dar servicio, como por ejemplo: el sistema operativo de los ordenadores clientes (Windows 7), cuándo se quiere aplicar las actualizaciones a los equipos conectados, si se quiere hacer manualmente o automáticamente, y a una determinada hora.

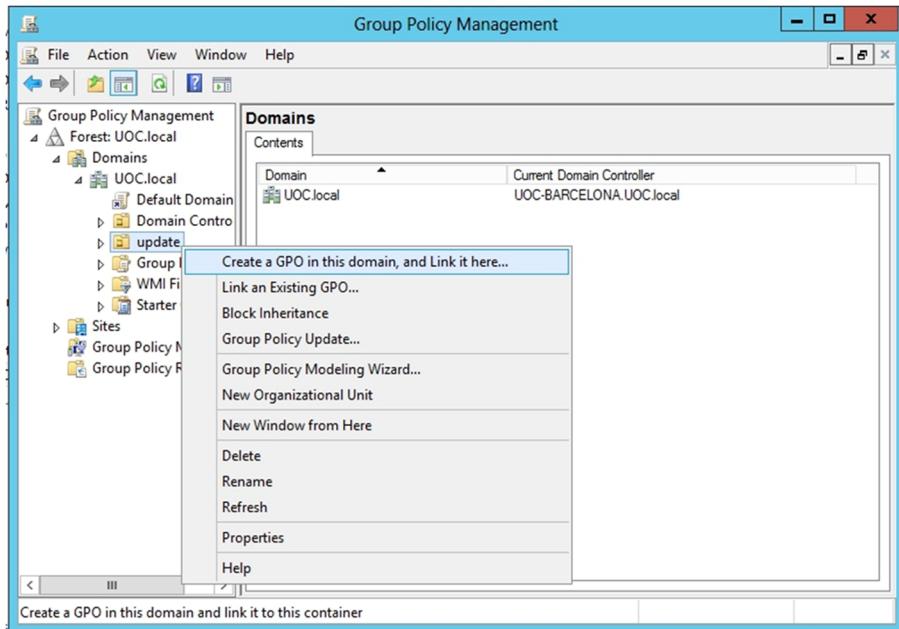
Dentro del desplegable de la izquierda del configurador del WSUS, están los equipos, y se tendrá que añadir otra subcategoría, que puede ser, por ejemplo en nuestro caso, /UOC-Barcelona/Computers/updates, además también estará declarada (updates) en el directorio activo como una unidad organizativa nueva, donde estarán todos aquellos ordenadores de los que se quiere gestionar remotamente las actualizaciones, solo hará falta mover los equipos a esta nueva UO, además de las opciones del WSUS que están en el árbol de la izquierda, en las que se tiene que seleccionar el menú de equipos y pulsar que se quiere usar la GPO (las políticas de grupo) para administrar las actualizaciones de los equipos conectados al dominio.

Configuración WSUS



A partir de aquí hay que ir al configurador de las políticas de grupo y crear una nueva GPO para administrar los equipos de los que se quiere controlar las actualizaciones desde el servidor. Debemos ir colocando estos equipos dentro de esta unidad organizativa del directorio activo. Se tienen que mover de la unidad organizativa “equipos” hacia la nueva unidad organizativa.

Creación de la GPO dentro de la UO nueva

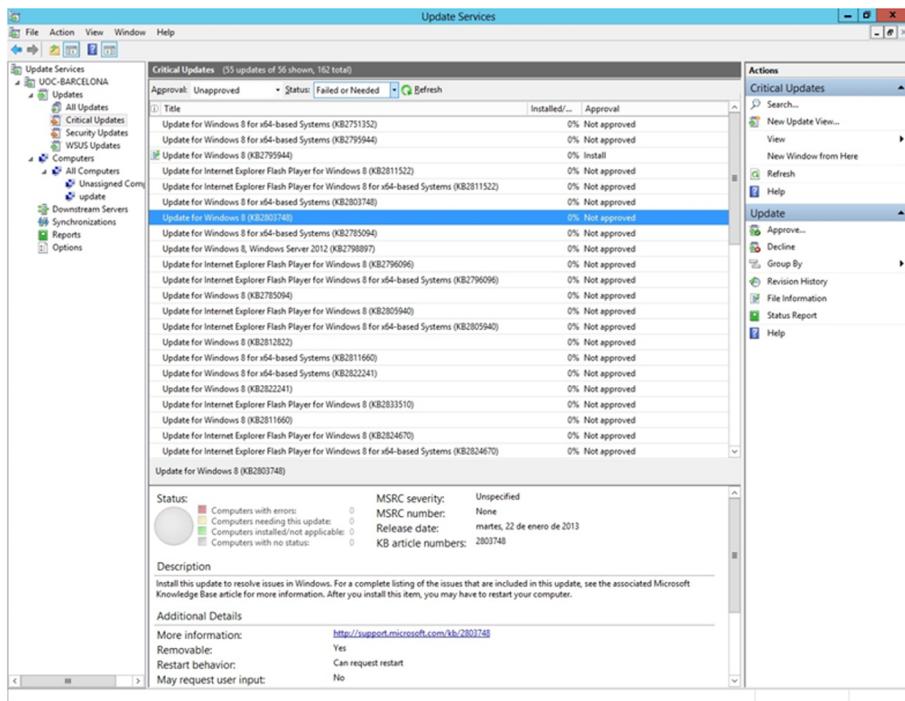


Normalmente la comunicación se hace por el puerto 80 hacia el servidor para consultar la lista de las actualizaciones, pero en versiones antiguas, y en algunas configuraciones, también se puede encontrar que esta comunicación se haga por el puerto 8530.

Una vez instalado el servidor de actualizaciones, solo hay que entrar en el propio servidor, desde las herramientas del administrador del servidor o desde la página de inicio, donde hay un acceso al WSUS, y configurar la lista de actualizaciones que hay para los sistemas que se han definido inicialmente, y aprobar estas actualizaciones para que sean transmitidas a los ordenadores clientes.

La siguiente figura muestra un conjunto de actualizaciones preparadas para ser aceptadas desde el servidor.

Listado de actualizaciones pendientes de ser aprobadas



1.2.3. Microsoft Technical Security Notification

Para mantener siempre actualizados los sistemas en cuanto a posibles fallos de seguridad, es conveniente estar registrado en la lista de correo electrónico, o boletín de seguridad, o en las cuentas de Twitter de Microsoft. Los usuarios registrados en esta lista reciben un boletín de seguridad en el que se informa de nuevos errores o *bugs* en la seguridad del sistema, y también enlaces a las páginas donde hay soluciones a estos problemas o la correspondiente bajada de la actualización que corrige el error.

1.2.4. Seguridad mejorada de Internet Explorer

Los atacantes aprovechan vulnerabilidades del navegador para ejecutar aplicaciones no deseadas sobre el equipo, a la hora de acceder a ciertas webs y de manera inadvertida.

No es recomendable utilizar el navegador de Internet desde un servidor en producción, puesto que hay aplicaciones maliciosas que se pueden instalar en el servidor y ocasionar un desperfecto general del mismo. Por todo ello, Windows Server 2012 está configurado de tal manera que, al abrir el navegador de Internet, Internet Explorer bloquea el acceso a webs desconocidas.

Por defecto, el acceso a webs de “desconfianza” está bloqueado. Al acceder a una de las webs que no está en la lista de “lugares de confianza”, sale una ventana de aviso.

Al instalar el servidor, solo se añaden a “lugares de confianza” las URL de Microsoft. Es recomendable añadir las URL necesarias a la lista de “lugares de confianza”. Por ejemplo, podemos añadir la URL de actualización del servicio antivirus para que no vuelva a bloquear el acceso a la URL y que acabará siendo un poco molesto para la navegación. Por seguridad, es recomendable comprobar que no tenemos ninguna URL desconocida en esta lista de lugares permitidos debido a un error, puesto que puede provocar la instalación de software “malintencionado”.

Ya se ha dicho que no es recomendable navegar por Internet desde el servidor en producción, pero si lo tenemos que hacer, puede llegar a parecer molesta la herramienta de seguridad de Internet Explorer. Esta se puede deshabilitar desde el administrador del servidor, al administrador del servidor local; en las propiedades que salen justo en medio se puede cambiar el parámetro *IE Enhanced Security Configuration* a off, dejando de preguntar cada vez por la web segura.

2. Monitorización de acontecimientos

Las máquinas que ejercen de servidores (tanto en sistemas GNU/Linux como en sistemas Microsoft Windows) tienen un registro de los acontecimientos que se producen en los diferentes servicios. Estos registros se denominan acontecimientos en sistemas Microsoft Windows y *logs* en sistemas GNU/Linux. Dejando de lado la denominación que tienen, la función que hacen es la misma: anotar en un fichero de texto todos los acontecimientos que suceden en los servicios. Según el nivel de *log* que hemos definido, se anotan en el registro más o menos incidencias.

2.1. GNU/Linux

En GNU/Linux los *logs* se configuran con el fichero `/etc/syslog.conf`. En este fichero se configuran las reglas de registro. Cada regla consta de dos partes, el selector y la acción, y las dos están separadas por espacios o tabulaciones.

El selector, a su vez, se divide en dos parámetros: el primero nos indica a qué tipo de servicio afecta (*facility*); el segundo, el nivel (*priority*) de *log* que queremos registrar. La separación entre las dos partes del selector se hace con un punto (.).

Los tipos de *facility* que hay son los siguientes:

- 1) authpriv: mensajes de seguridad o autorización.
- 2) cron: mensajes de las utilidades de reloj (cron y at).
- 3) daemon: mensajes de los demonios (daemons) del sistema.
- 4) kern: mensajes del núcleo (kernel).
- 5) lpr: mensajes del sistema de impresoras.
- 6) mail: mensajes del sistema de correo.
- 7) news: mensajes del tablón de anuncios (*Usenet* o News).
- 8) syslog: mensajes internos del sistema *syslog*.
- 9) user: mensajes genéricos de usuarios.

Los tipos de seguridad (ordenados en orden decreciente de importancia) son los siguientes:

- 1) emerg: el sistema está inutilizado.
- 2) alert: fallos graves en el sistema. Se tienen que tomar medidas correctoras de manera inmediata.
- 3) crit: condiciones críticas del sistema.
- 4) err: errores del sistema.
- 5) warning: avisos del sistema.

- 6) notice: acontecimientos que, a pesar de que son normales, son significativos.
- 7) info: mensajes informativos.
- 8) debug: mensajes de depuración del sistema.

La acción que se tiene que hacer es siempre la misma: almacenar la información en un fichero. Lo que podemos configurar es el tipo de fichero que queremos usar. Este fichero tiene que estar en el servidor y tener privilegios de escritura.

Los tipos de fichero que son compatibles son los siguientes:

- 1) Ficheros regulares: ficheros de texto normales. El camino hasta este fichero tiene que estar indicado con *path* absoluto (el camino que se tiene que seguir desde el directorio raíz).
- 2) *Terminal console*: los mensajes salen en la pantalla del servidor. El dispositivo utilizado es `/dev/console`.
- 3) Listas de usuarios: los mensajes críticos, aparte de ser almacenados, pueden ser enviados en forma de correo electrónico al usuario raíz del servidor. Si queremos que este tipo de mensajes los reciba más de un usuario, tenemos que añadir los nombres de usuarios de todos ellos, separados por comas.
- 4) Todos los usuarios conectados: los mensajes de emergencia pueden aparecer en la consola de los usuarios conectados (sea en local o mediante consola remota), e indicar el motivo por el cual se ha bloqueado el sistema.
- 5) Máquinas remotas: los ficheros de *log* pueden estar fuera del servidor, en una máquina remota.

Esta última opción es muy interesante para el administrador de sistemas operativos principalmente por dos motivos.

El primero de estos motivos tiene que ver con la seguridad. Las personas que atacan una máquina, si consiguen entrar en esta máquina con privilegios de *root*, una de las primeras cosas que hacen es borrar los ficheros de *log* para esconder la intrusión. Si estos ficheros son enviados a una máquina remota regularmente, disminuye la posibilidad de que sean borrados, puesto que para hacerlo el atacante tiene que vulnerar también la segunda máquina. Claro que si no se controlan estos *logs*, tampoco sirven de mucho, pues por mucha información que se guarde de manera segura, si no se controla que se lleva a cabo regularmente y que está haciéndose, no la podremos aprovechar. Por ejemplo, un atacante consigue explotar una vulnerabilidad del servidor de la

base de datos, y lo primero que hace es parar el envío de los *logs* a otra máquina, no se dispondrá de datos en los *logs*, y además, si nadie se da cuenta de que no se están enviando los ficheros de *log*, de poco servirá tenerlo configurado así.

El segundo motivo es por una cuestión de administración: si tenemos todos los ficheros de *log* concentrados en una máquina, solo nos tenemos que fijar en los registros de esta para darnos cuenta de todos los acontecimientos que han pasado.

A pesar de que tenemos todos los acontecimientos de la máquina concentrados en un fichero de texto, la supervisión de este fichero no es una tarea sencilla, sino más bien al contrario. Para facilitar esta supervisión, hay aplicaciones que revisan los *logs* y envían un correo electrónico con un resumen de las incidencias que ha habido.

Existen varias aplicaciones que controlan los *logs* del sistema, como `metalog`, `syslog-ng`, `logwatch`, `loganalyzer`, etc. En estos materiales mostramos esta última aplicación. `loganalyzer` es una aplicación que hace la supervisión de *logs*. Para instalar esta herramienta tenemos que conectarnos a la página web del fabricante, puesto que no se encuentra en el repositorio por defecto, y bajar la última versión, en este caso la 3.6.3. La página del fabricante es: <http://loganalyzer.adiscon.com/downloads>.

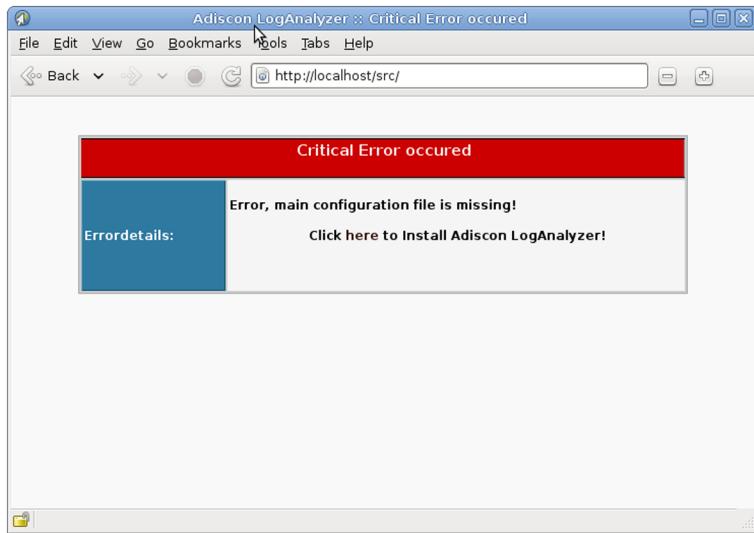
```
root# wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.3.tar.gz
root# tar -xvf loganalyzer-3.6.3.tar.gz
```

Ya solo hay que descomprimir el fichero y ver que hay un fichero de instalación que explica cuáles son los requisitos necesarios para poder instalar la aplicación, como puede ser el `apache`, el `rsyslog` y el `php5`.

Para realizar la instalación, y siguiendo los pasos que explica el fichero `INSTALL` que hay dentro de la aplicación que se acaba de descomprimir, se tiene que copiar el directorio `src` en el directorio del servidor web `apache`, copiar también los ficheros `configure.sh` y `secure.sh` del directorio `contrib` en el mismo directorio `src` que se acaba de copiar antes, y dar atributo de ejecución, es decir:

```
root# cp -R /home/jordi/loganalyzer-3.6.3/src/ /var/www/
root# cp /home/jordi/loganalyzer-3.6.3/contrib/*.sh /var/www/src/
root# cd /var/www/src/
root# chmod +x configure.sh secure.sh
```

Y ya solo queda abrir el navegador de Internet y acceder a la página web que hay dentro del directorio `/src/` del *site*, donde podremos ver el configurador. La primera vez nos dará un error y mostrará el enlace para arrancar el configurador.

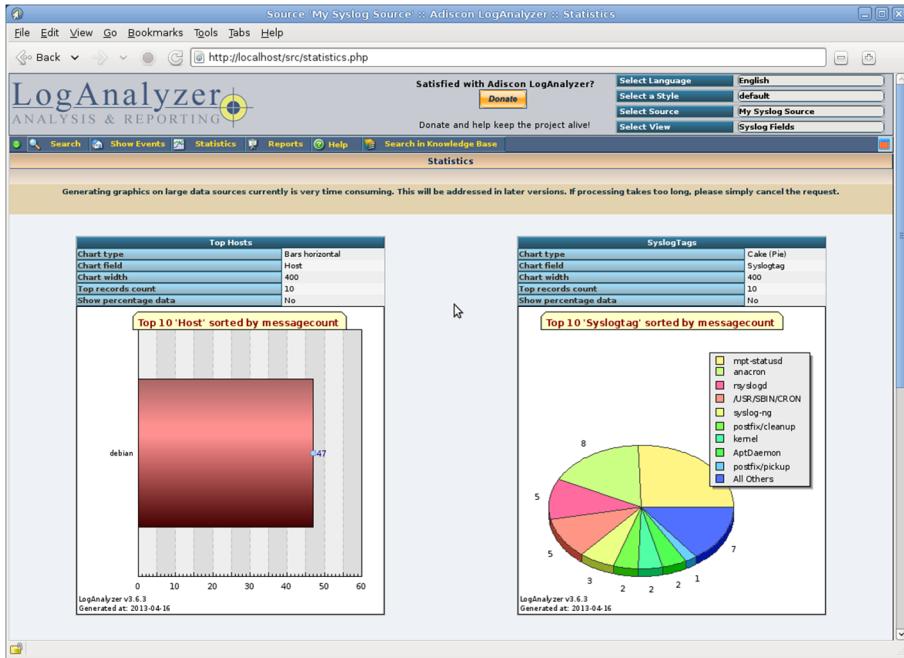


Si entran en el enlace, se podrá configurar la aplicación. En la página web podemos encontrar mucha información de cada parámetro.

Parámetros de configuración

Finalmente, podemos ver los resultados de los *logs* en la misma página web que antes daba errores y que ahora muestra el resultado del tratamiento de los *logs* del equipo.

Resultados finales



2.2. Microsoft Windows Server 2012

2.2.1. Monitorización de los registros de incidencias

Las incidencias son acciones de usuarios que quedan registradas en el servidor, o cualquier acontecimiento producido por el sistema operativo o una aplicación.

En Windows Server 2012 hay tres tipos de registros de incidencias:

- Registro del sistema: las incidencias registradas las provoca el sistema operativo; por ejemplo, un fallo de un controlador durante el inicio del sistema.
- Registro de aplicación: contiene las incidencias provocadas por aplicaciones del sistema. Problemas al arrancar alguna aplicación, problemas de acceso a registro, problemas de bibliotecas, etc.
- Registro de seguridad: guarda incidencias relacionadas con la seguridad del sistema, como por ejemplo intentos de accesos fallidos o un intento de ejecutar una operación sin privilegios.

Además, hay tres tipos de incidencias de sistema o aplicación:

- Información: registra el funcionamiento correcto de una aplicación o un servicio.

- Advertencia: registra una incidencia que no es en sí problemática pero que puede llevar a un error si no se tiene en cuenta.
- Error: es una incidencia grave que registra un fallo en una aplicación o un servicio.

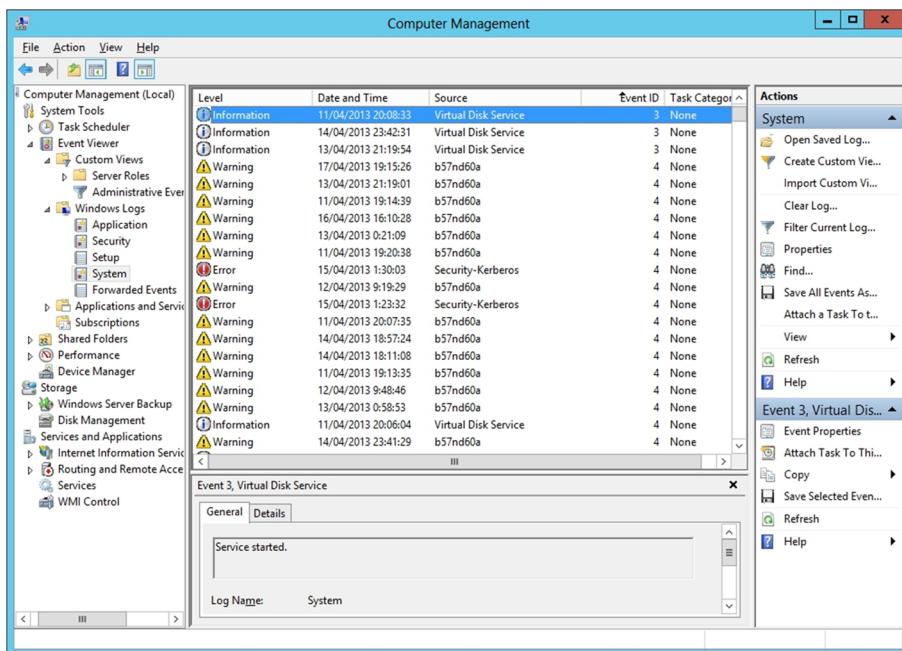
Los tipos de incidencias de seguridad pueden ser los siguientes:

- Auditoría de aciertos: registro de accesos al servidor con éxito.
- Auditoría de errores: registro de accesos denegados (intentos de acceso ilegal o de violación de seguridad).

Para visualizar las incidencias que ha habido en el sistema, podemos utilizar el visor de incidencias, una herramienta basada en la consola de administración que está dentro de las herramientas del administrador de los servidores.

A la izquierda vemos una lista de los registros de incidencias. Aparte de los registros de los que hemos hablado antes, encontramos otros registros de incidencias relacionadas con otras funcionalidades o servicios del servidor, como por ejemplo *Active Directory*.

Eventos del sistema



También podemos visualizar los registros de incidencias de otros equipos seleccionando la opción “Conectar con otro equipo...” del menú contextual del elemento “Administración del equipo (local)” de la lista de la izquierda, y así tener controlados todos los equipos de la red de manera centralizada en el servidor.

Si hacemos doble clic sobre una de las incidencias, vemos las propiedades que tiene, dónde se muestra la fecha, la hora, el tipo de incidencia, el origen, etc., que será útil para averiguar qué es lo que está pasando en los diferentes equipos y en el servidor en concreto.

Si seleccionamos la opción “Propiedades” del menú contextual de uno de los registros de la lista de la izquierda, podemos configurar algunas propiedades de registro de este tipo de incidencias, como por ejemplo, el tamaño máximo del archivo de incidencias.

2.2.2. Monitorización del rendimiento del sistema

El administrador de tareas de Windows permite monitorizar y controlar las aplicaciones y los procesos en ejecución en el sistema en un momento concreto. Para iniciar el administrador de tareas, pulsamos la combinación de teclas “Ctrl + Alt + Supr” y seleccionamos la opción “Administrador de tareas”. También se puede acceder directamente, pulsando la combinación de teclas “Ctrl + Majús + Esc”, o desde la barra de tareas, con el botón derecho “Administrador de tareas”. Hay dos versiones de esta aplicación, la que únicamente muestra el nombre de las aplicaciones, pensada para usar en un entorno de pantallas táctiles, y la versión donde muestra muchos más detalles de todo aquello que está ejecutándose en el sistema; únicamente habrá que mostrar más detalles para cambiar de una a la otra.

En la pestaña “Aplicaciones” podemos controlar las aplicaciones en ejecución. Si una aplicación no responde, la podemos eliminar seleccionándola y después seleccionando la opción “Finalizar tarea”. Se perderán todos los datos de la aplicación, de manera que solo se recomienda utilizar esta opción si la aplicación no responde.

Desde la pestaña “Procesos” vemos la información de todos los procesos en ejecución en el sistema:

Listado de procesos reales del sistema

Name	Type	Process name	Command line	10% CPU	87% Memory
Apps (5)					
Internet Explorer	App	iexplore.exe	"C:\Program Files\Internet Explorer\iexplore...."	0%	10,3 MB
Server Manager	App	ServerManager....	"C:\Windows\system32\ServerManager.exe"	0%	4,9 MB
Task Manager	App	Taskmgr.exe	"C:\Windows\System32\Taskmgr.exe" /2	0,2%	8,8 MB
Windows Explorer	App	explorer.exe	C:\Windows\Explorer.EXE	0%	17,0 MB
Windows PowerShell	App	powershell.exe	"C:\WINDOWS\system32\WindowsPowerShe...	0%	27,7 MB
Background processes (14)					
Distributed File System Replicat...	Background p...	dfrs.exe	C:\Windows\system32\DFSRs.exe	0%	7,2 MB
Domain Name System (DNS) Se...	Background p...	dns.exe	C:\Windows\system32\dns.exe	0%	79,8 MB
Host Process for Windows Tasks	Background p...	taskhostex.exe	taskhostex.exe	0%	2,3 MB
IIS Worker Process	Background p...	w3wp.exe	c:\windows\system32\inetsrv\w3wp.exe -ap ...	0%	102,3 MB
Internet Information Services	Background p...	inetinfo.exe	C:\Windows\system32\inetsrv\inetinfo.exe	0%	5,2 MB
Microsoft Distributed Transacti...	Background p...	msdtc.exe	C:\Windows\System32\msdtc.exe	0%	2,3 MB
Microsoft.ActiveDirectory.WebS...	Background p...	Microsoft.Activ...	C:\Windows\ADWS\Microsoft.ActiveDirector...	0%	9,7 MB
Spooler SubSystem App	Background p...	spoolsv.exe	C:\Windows\System32\spoolsv.exe	0%	2,0 MB
SQL Server VSS Writer - 64 Bit	Background p...	sqlwriter.exe	C:\Windows\WID\Binn\sqlwriter.exe -w	0%	1,1 MB
SQL Server Windows NT - 64 Bit	Background p...	sqlservr.exe	C:\Windows\WID\Binn\sqlservr.exe -SMSWI...	9,6%	51,0 MB
Virtual Disk Service	Background p...	vds.exe	C:\Windows\System32\vds.exe	0%	1,7 MB
Windows NT Distributed File Sy...	Background p...	dfssvc.exe	C:\Windows\system32\dfssvc.exe	0%	1,2 MB
Fewer details				<input type="button" value="End task"/>	

Mediante la opción “Acabar proceso” se acaba la ejecución de un proceso. Igual que en el caso de las aplicaciones, se pierden todos los datos del proceso, de manera que no es recomendable utilizar esta opción salvo que el proceso no responda.

La pestaña “Rendimiento”, del administrador de tareas, muestra el uso del procesador o CPU, la memoria del sistema en un momento concreto, el uso de la red o del disco duro.

La pestaña “Usuarios” permite ver los usuarios conectados al servidor. También se permite desde aquí la desconexión, el cierre de sesión y la posibilidad de mandar un aviso antes de la desconexión. Aquí únicamente muestra los usuarios que están conectados directamente al servidor, no los que están trabajando desde los ordenadores clientes conectados con el *Active Directory* al servidor.

3. Automatización de tareas

3.1. GNU/Linux

Hay muchas de las tareas que tiene que llevar a cabo el administrador que son rutinarias, es decir, cada día hace las mismas y en el mismo orden. Estas tareas se pueden automatizar. De hecho, las tenemos que automatizar. Así dispondremos de más tiempo para hacer otras tareas y las rutinarias solo habrá que supervisarlas. Para lo cual, usamos la utilidad del reloj que nos ofrece el sistema. Esta utilidad se denomina `crontab` y está instalada por defecto en el sistema operativo.

Si queremos editar el fichero de configuración de la aplicación `crontab` para automatizar una nueva tarea, se tiene que ejecutar la orden siguiente:

```
root# crontab -e
```

Tenemos que tener presente que para añadir una tarea a este fichero de configuración se tiene que hacer de la manera correcta. La sintaxis que sigue este fichero es la siguiente:

```
minutes hours days month day_week /path/absolute/to/your/script
```

`minutes` acepta valores numéricos de 0 a 59.

`hours` acepta valores numéricos de 0 a 23.

`days` hace referencia a los días del mes y acepta los valores numéricos del 1 al 31.

`month` son los meses del año y, por lo tanto, acepta valores de 1 a 12.

`day_week` acepta valores de 1 a 7.

`path`. Finalmente tenemos que poner el `script` u orden que queremos ejecutar con el camino absoluto y todos los parámetros que queremos.

Hay otros caracteres que también son compatibles con la aplicación `crontab`. Es el caso de ciertas cadenas de caracteres: las tres primeras letras en inglés de los meses o los días de la semana pueden sustituir a los caracteres numéricos. Otro carácter compatible con el `crontab` es el símbolo (*), que lo podemos

poner en cualquier lugar, e indica que son válidos todos los posibles valores. Por ejemplo, un * en `day_week` quiere decir que se tiene que ejecutar todos los días de la semana.

Otro ejemplo, si queremos que se ejecute un *script* llamado `check_disc.sh` cada viernes a las tres de la madrugada, la línea que tenemos que poner dentro del fichero de configuración de la aplicación `crontab` es la siguiente:

```
00 03 * * 5 /root/bin/check_disc.sh
```

En este ejemplo vemos que la mayoría de las tareas que ejecutamos en el `crontab` no son órdenes con parámetros sino *scripts*. Los lenguajes más utilizados para hacer *scripts* son *shell script* y PERL. Es muy útil para el administrador saber utilizar los dos lenguajes puesto que tanto el uno como el otro proporcionan maneras diferentes de hacer las tareas.

El *shell script* está pensado para que utilicemos las órdenes del sistema para llevar a cabo determinadas tareas, y podemos usar variables para guardar resultados. En cambio, el PERL es un lenguaje optimizado para trabajar con ficheros de texto, manipularlos e imprimir los resultados.

La mayoría de las versiones de GNU/Linux, cuando las instalamos, tienen diferentes *shells* (`zsh`, `tcsh`, `csh`, `bourne shell`, etc.). Todos son muy parecidos pero no iguales, y con ellos podemos hacer las mismas cosas; lo que cambia es la manera de usar las variables, las variables de entorno, el uso de los parámetros, etc.

A diferencia del *shell*, hay muchas de las versiones GNU/Linux que no llevan instalado el PERL. Para instalarlo, únicamente hace falta ejecutar la orden siguiente:

```
root# apt-get install perl
```

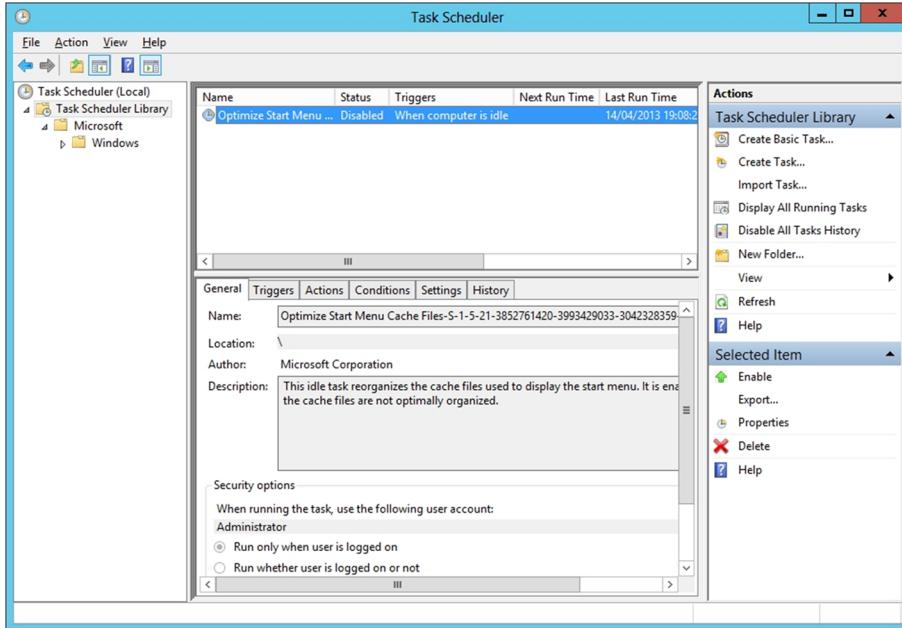
3.2. Windows Server 2012

3.2.1. Tareas programadas

Como se ha comentado, a veces hay que definir algunas tareas rutinarias que se tienen que hacer periódicamente para optimizar el rendimiento del sistema, como por ejemplo, compactar los discos duros, hacer las copias de seguridad y limpiar las carpetas temporales y archivos de Internet.

Estas tareas se pueden programar para que se hagan cada cierto tiempo, preferentemente cuando el servidor tiene menos carga de trabajo. Esto se puede realizar con el Programador de tareas, que se puede abrir seleccionándolo dentro del menú Herramientas del administrador del servidor.

Programador de tareas



La ventana que sale muestra los iconos correspondientes a las tareas programadas actualmente. Para programar una nueva tarea pulsamos “Crear tarea”.

En la pantalla siguiente se nos muestran todas las opciones posibles para programar una nueva tarea, temporización, usuario con que se ejecuta, etc. En principio se puede ejecutar cualquier programa instalado en el sistema.

Posibles aplicaciones a automatizar que no tienen interacción con las personas y por lo tanto se pueden arrancar cuando no hay nadie usando el ordenador:

- Limpiar espacio en el disco duro.
- Escanear los discos duros en busca de errores.
- Compactar los discos duros.
- Hacer un análisis antivirus.
- Actualizar el sistema.
- Hacer copias de seguridad.

En la primera pantalla se muestran los datos relacionados con la seguridad, donde podemos seleccionar a los usuarios y si tiene que ser visible o no esta tarea.

3.2.2. Scripting. Windows Management Instrumentation (WMI)

Algunas tareas de administración pueden resultar costosas sobre todo si se tienen que hacer repetidamente. Hay algunas que se pueden parametrizar y programar para facilitar el trabajo de los administradores de sistema.

Windows permite ejecutar archivos de *script* que contengan programas escritos en *visual basic script* (VBScript) o JScript, gracias a la herramienta *Windows Script Host* (WSH).

Los *scripts* permiten automatizar tareas, como crear usuarios, asignar permisos de ejecución sobre archivos, instalar aplicaciones, crear *logs* o *reports* del estado del sistema. De este modo se reducirán los errores y los problemas de seguridad, puesto que todos los usuarios tendrán los mismos derechos y por error no se generará uno que tenga más privilegios de los que tiene que tener.

Además, Windows proporciona una serie de objetos utilizables desde los *scripts*, denominados *Windows Management Infrastructure* (WMI), que permiten acceder a las propiedades internas del sistema operativo (versión del sistema, hardware instalado, procesos, acceso al registro, etc.).

