Manteniment

Jordi Serra Ruiz

PID_00204284

Universitat Oberta de Catalunya

Índex

Introducció

Tan important és la bona instal·lació i configuració dels servidors i les aplicacions que tenen, com el manteniment que se n'ha de fer durant tot el període de vida del sistema informàtic.

El programari i els sistemes tant de Microsoft com de GNU/Linux s'actualitzen constantment, sia amb pedaços que s'han d'instal·lar damunt del sistema operatiu o amb noves versions d'aquests sistemes, reben noves versions dels diferents mòduls amb noves versions millorades i més segures que fan més difícil poder atacar els sistemes.

És molt important revisar i instal·lar les actualitzacions que creen els fabricants del programari en general, ja que normalment són motivades per forats de seguretat que s'han descobert en el sistema operatiu.

La filosofia de "Ja funciona, no toquem res" no és bona, ja que hi pot haver un error del sistema que desconeguin els administradors però que se solucioni instal·lant un simple pedaç o una actualització.

Un altre aspecte important que s'ha de tenir en compte és el monitoratge dels esdeveniments o del sistema operatiu. En aquests *logs* queden guardats tots els esdeveniments que es produeixen en el sistema. Per exemple, l'accés extern d'un usuari al servidor.

Objectius

En aquest mòdul pretenem que es conegui la manera de tenir un sistema informàtic en general actualitzat i protegit. Amb aquesta finalitat us plantegem els objectius següents:

1. Conèixer els mètodes d'actualització que tenen els sistemes operatius.

2. Conèixer els sistemes d'emmagatzematge d'esdeveniments o *logs* dels sistemes.

3. Aprendre els mecanismes d'automatització de tasques.

1. Actualitzacions

Una de les màximes dels administradors de sistemes és que "si una cosa funciona bé, no la toquis". Actualment aquesta màxima no és aplicable, ja que ens podem trobar que, malgrat que tenim un sistema estable i que funciona de manera correcta, l'hàgim d'actualitzar. Aquesta actualització no la duem a terme per capritx, ni per oferir un servei més bo als usuaris, ni perquè l'usuari sempre estigui a l'última moda. El motiu principal d'aplicar les actualitzacions del programari és la seguretat.

Avui dia hi ha molta gent que indaga totes les versions de programari que hi ha en actiu amb la finalitat de trobar una vulnerabilitat per a explotar-la i, d'aquesta manera, aconseguir entrar en una màquina. De la mateixa manera, hi ha molts programadors d'aplicacions que es dediquen a intentar trobar vulnerabilitats en les seves aplicacions per a millorar-ne les versions i fer-les més robustes a possibles vulnerabilitats. Quan en troben una que pot comprometre la màquina que fa servir el programari, emeten un advertiment de seguretat en què indiquen que actualitzen la versió de programari que ha estat compromesa a una versió superior, en la qual ja s'ha solucionat la vulnerabilitat.

Si volem, ens podem subscriure a aquesta llista, o consultar les vulnerabilitats que han sortit mitjançant l'URL, i fer diferents tipus de cerques, fins i tot per mesos o anys.

En el moment en què un fabricant de programari, el que sigui, distribueix un pedaç per ser aplicat en una part d'aquest, directament està publicant quin problema té si no s'aplica el pedaç. Això és aprofitat per les persones que programen els *exploits*, que estudien amb enginyeria inversa els pedaços que es publiquen i ataquen tots els sistemes que no estan actualitzats perquè apliquen la premissa de "no tocar res, que deixarà de funcionar".

1.1. GNU/Linux

Si volem actualitzar tots els paquets de la nostra distribució Debian instal·lada en l'ordinador, hem d'executar les ordres:

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

Una vegada acabada la instal·lació executem:

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

Ens mostra tots els paquets que s'instal·laran i ens demana si volem continuar l'actualització. Hem de dir que sí. Llavors baixa tots els paquets que s'han d'actualitzar, els instal·la i, si cal, els configura. Depenent dels paquets que actualitzem, ens demana dades de configuració.

Tot i que aquesta manera de fer una actualització del sistema és molt còmoda per a l'administrador, hem d'anar molt amb compte quan la utilitzem en servidors de producció, és a dir, en els servidors que ofereixen algun servei, ja que molts cops, en fer l'actualització caldrà parar el servei, o la configuració dels programes que per defecte hi ha en aquests serveis farà que deixi de funcionar. Per això en gairebé tots els casos, en el moment d'actualitzar, el sistema pregunta si es vol fer o no el canvi dels fitxers de configuració pels que vénen per defecte. Fins i tot es pot mirar quines són les diferencies entre els dos fitxers de configuració i decidir quin serà el que funcionarà millor.

A més pot passar que en algunes versions de programari el canvi de versions no sigui compatible amb altres programes que es tinguin en l'equip, o dit d'una altra manera, el que funcionava en la versió que tenim instal·lada no funcionarà en la versió que volem actualitzar. Això passa perquè en la nova versió:

- S'utilitzen components nous.
- S'utilitzen fitxers de configuració diferents.
- S'han afegit paràmetres nous.

Per evitar aquestes situacions podem procedir de dues maneres diferents:

1) Actualitzar només les aplicacions que sabem que tenen fallades greus en la seguretat, i fer-ho de manera manual. Per a això, en primer lloc hem de baixar la versió de l'aplicació que ens interessa actualitzar i després instal·lar-la manualment. En aquest cas, podem fer la instal·lació via compilació o via paquet Debian.

2) Fer l'actualització del sistema en una màquina de proves, comprovar que tot continua funcionant i després fer l'actualització en el servidor. Això s'acostuma a conèixer com a sistema en preproducció. Són equips idèntics, amb el mateix programari, que serveixen de prova per a fer actualitzacions i canvis sobre el sistema real, que en cas que tinguin èxit, o no donin problemes, es passaran a l'equip en producció.

1.2. Windows Server 2012

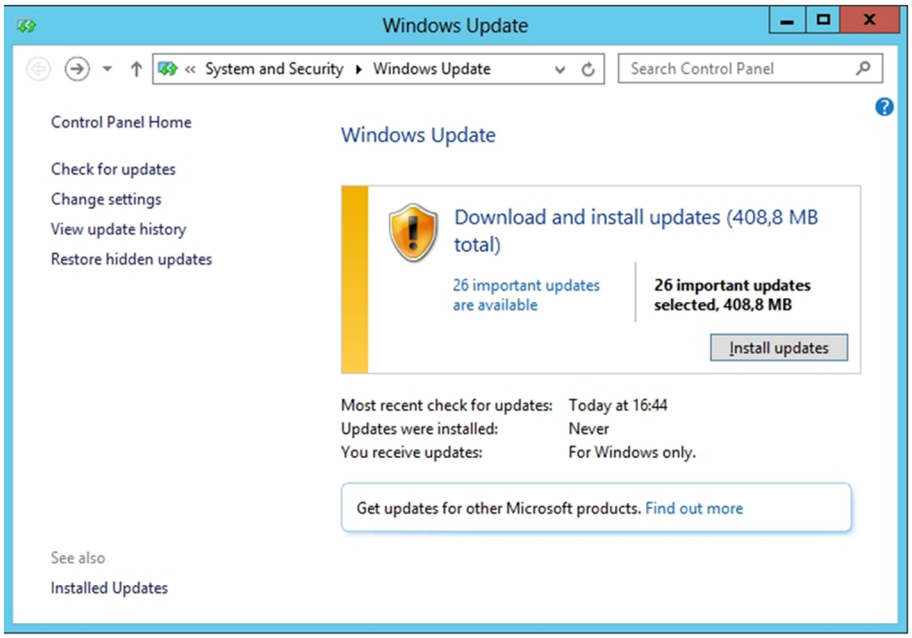
1.2.1. Actualitzacions de Windows Update

Quan es descobreix una d'aquestes fallades del sistema operatiu, Microsoft corregeix el codi font del sistema operatiu per esmenar l'error. No obstant això, tots els sistemes que ja hi ha instal·lats continuen tenint aquest error. Per això és molt important tenir el sistema actualitzat.

Per a facilitar l'actualització del sistema operatiu, Microsoft disposa d'un lloc web d'actualització des del qual es poden obtenir gratuïtament i de manera automàtica totes les actualitzacions necessàries per a tenir el sistema al dia. En les darreres versions de Windows Update, es requereix instal·lar un connector o *plug-in* de Microsoft en accedir a l'URL de Windows Update per a baixar correctament les actualitzacions.

El procés d'actualització es resumeix en uns quants passos. En primer lloc, es dóna a l'usuari l'opció de seleccionar entre dues maneres de fer-ho: la ràpida o la personalitzada. En tots dos casos, es mostren les actualitzacions de sistema, però l'opció personalitzada també mostra possibles actualitzacions de programari i maquinari (programes controladors o *drivers* d'impressió, de targetes de xarxa, de vídeo, etc.), a més de permetre no seleccionar alguna de les actualitzacions si no es vol instal·lar. En el cas dels servidors, és millor decidir què és el que s'instal·la i sobretot quan s'instal·la, ja que això permet tenir un control més acurat del que passa en el servidor.

Windows Update



Una vegada seleccionada l'opció d'instal·lació de les actualitzacions, el sistema escaneja l'equip per localitzar les actualitzacions que falten per instal·lar. Quan acaba, el sistema mostra una pantalla (figura anterior) amb totes les actualitzacions disponibles. Cal fer clic al botó "Instal·lar les actualitzacions" i acceptar el contracte de llicència per a continuar l'actualització.

Una vegada completada la instal·lació, el sistema queda completament actualitzat. És possible que per a instal·lar alguns pedaços faci falta reiniciar el servidor. Per això s'aconsella instal·lar pedaços en horaris de poc accés al servidor (potser a la nit o després de les còpies de seguretat o *backups*).

Les actualitzacions de Windows Update es poden automatitzar de manera que el sistema comprovi periòdicament si n'hi ha cap i la baixi i instal·li sense que l'usuari hi hagi d'intervenir. Per a configurar la baixada automàtica d'actualitzacions, obrim l'eina "Actualitzacions automàtiques" del tauler de control.

En aquesta eina podem seleccionar o no l'opció de fer baixades automàtiques i podem triar un dels quatre mètodes següents:

1) Baixar automàticament les actualitzacions recomanades per a l'equip i instal·lar-les. Aquí es pot indicar a quina hora es vol que es baixin i s'instal·lin les actualitzacions.

2) Baixar les actualitzacions nosaltres mateixos, però permetre'ns triar quan les volem instal·lar. Les actualitzacions queden baixades en el servidor, però pendents d'instal·lar.

3) Notificar-nos les actualitzacions, però no baixar-les automàticament ni instal·lar-les. Ens informa d'actualitzacions noves però no les baixa ni les instal·la.

4) Desactivar actualitzacions automàtiques.

1.2.2. Windows Server Update Services

En una xarxa d'una empresa amb molts clients connectats i diferents versions de sistemes operatius és difícil mantenir tots els equips al dia. Per això és important mantenir activada la baixada automàtica d'actualitzacions en tots els equips.

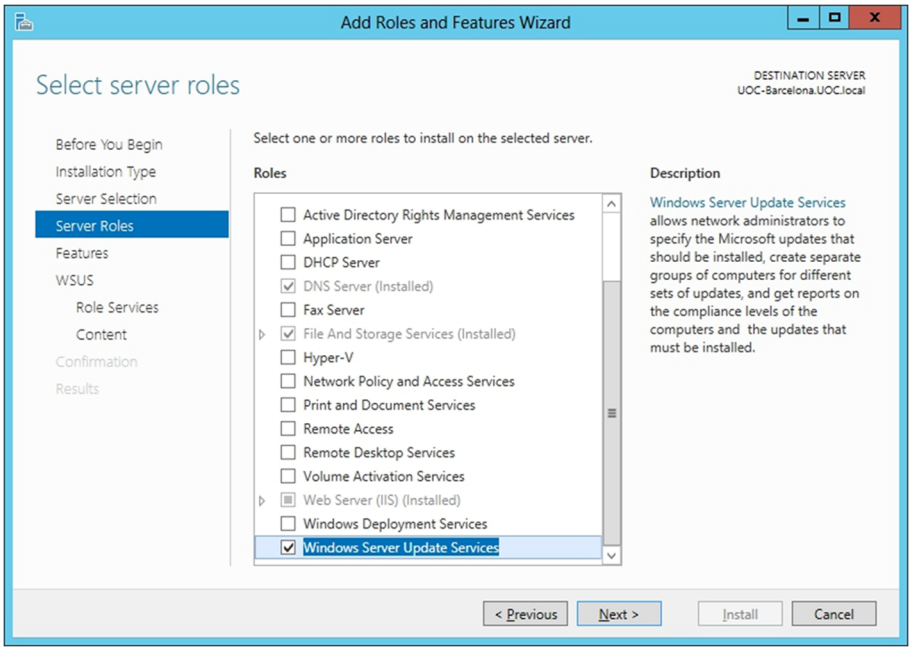
No obstant això, si cada equip hagués de baixar els centenars de megabytes d'informació de totes les actualitzacions, provocaria un descens important del rendiment de la xarxa.

Windows Server Update Services (WSUS) és una aplicació que permet als administradors baixar una única vegada les actualitzacions disponibles per als sistemes operatius de la xarxa, emmagatzemar aquestes actualitzacions en un servidor i permetre que els clients baixin les actualitzacions directament d'aquest servidor en comptes de fer-ho del servidor de Windows Update. Amb això s'aconsegueix velocitat en la baixada, ja que es fa servir la xarxa local, i també facilitat per a configurar i actualitzar els pedaços en els clients des del servidor.

Per instal·lar aquest component, hem de tenir instal·lat IIS (el servidor de pàgines web) en el servidor, ja que els clients consulten i actualitzen els pedaços consultant una pàgina web, en comptes del web de Microsoft Windows Update. Per a instal·lar IIS cal anar al tauler de control, a l'administrador del servidor i afegir el rol, com ja s'ha explicat anteriorment.

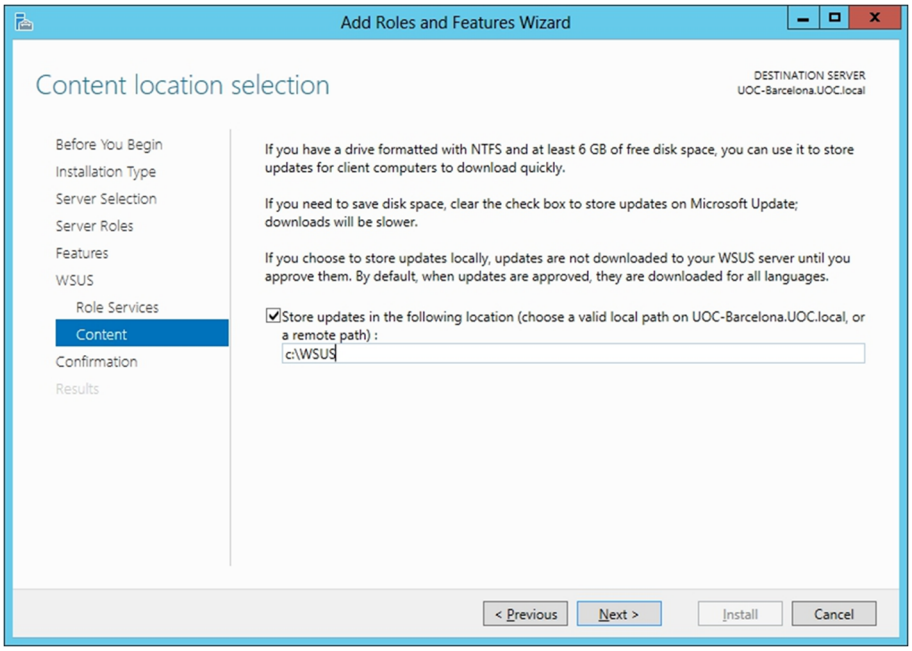
A més, per a gestionar les actualitzacions, també s'ha d'instal·lar el servidor d'actualitzacions en el servidor, per tant el rol de WSUS (*Windows Server Update Services*) també s'haurà de seleccionar i instal·lar-lo.

WSUS



El servei WSUS ha de gestionar les actualitzacions pròpies i de la resta dels equips del domini, i per a fer això necessita una base de dades. En el procés d'instal·lació ja es pot fixar una base de dades per defecte, WID data base. I ja únicament queda seleccionar un directori on anar guardant totes les actualitzacions, que es pot crear en un disc local del servidor o en algun altre recurs compartit de la xarxa.

Directori WSUS

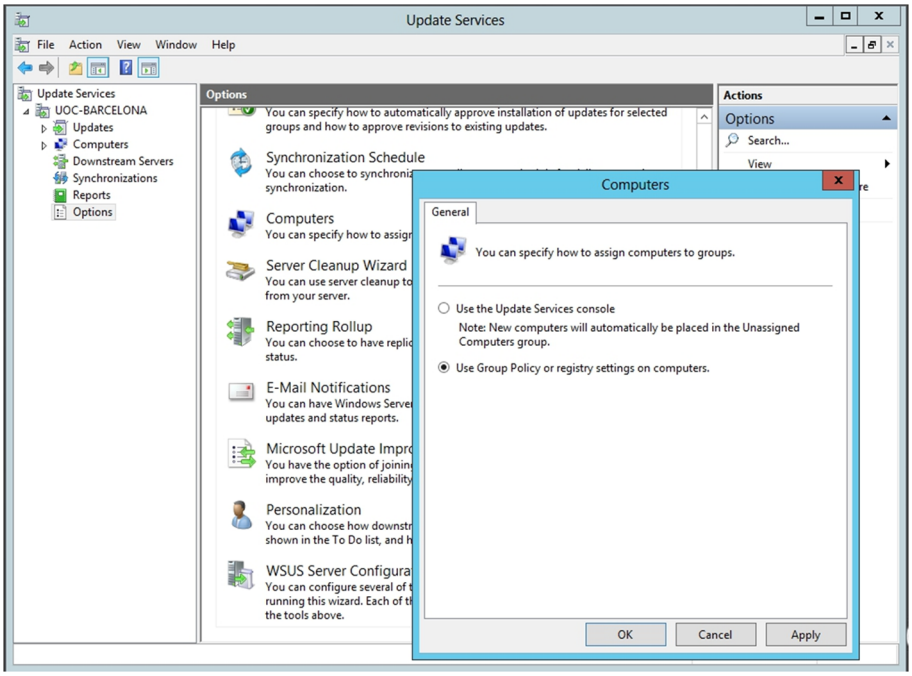


Un cop acabada la instal·lació, cal executar el configurador (que es pot fer des de la pantalla de l'administrador del servidor). Anirem seleccionant i connectant-nos al servidor de Microsoft per acabar configurant correctament el servei.

Es poden seleccionar els idiomes que siguin necessaris, i també el programari amb el qual es vol donar el servei de les actualitzacions. Es mostra un desplegable on es pot anar seleccionant tot allò a què es vol donar servei, com per exemple el sistema operatiu dels ordinadors client (Windows 7), quan es volen aplicar les actualitzacions als equips connectats, si es vol fer manualment o automàticament a una hora determinada.

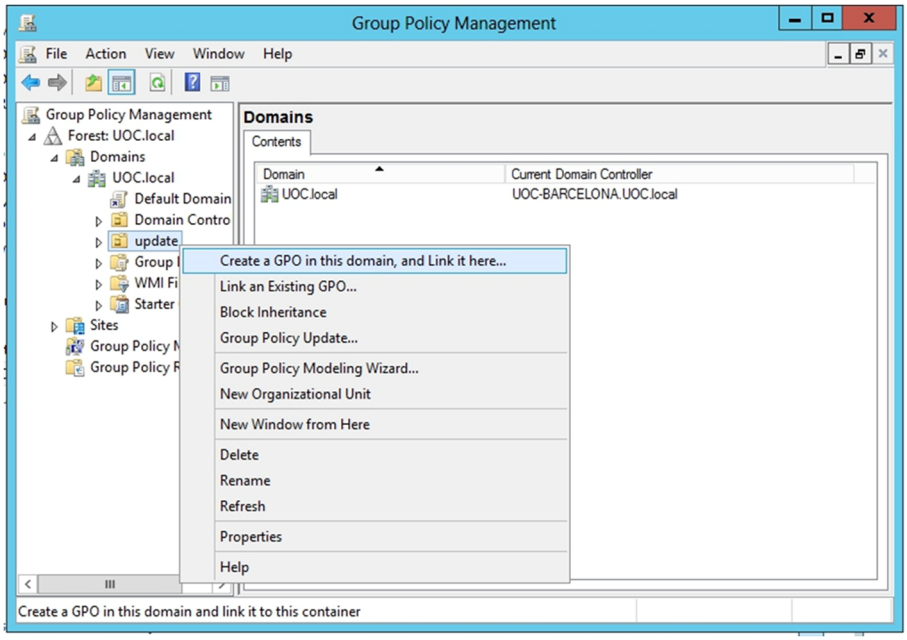
Dins el desplegable de l'esquerra del configurador del WSUS, hi ha els equips, i s'hi haurà d'afegir una altra subcategoria, que pot ser, per exempleen el nostre cas, `/UOC-Barcelona/Computers/updates`, a més també estarà declarada (`updates`) en el directori actiu com una unitat organitzativa nova, on seran tots els ordinadors dels quals es volen gestionar remotament les actualitzacions, només farà falta moure els equips a aquesta nova UO, a més a les opcions del WSUS que hi ha en l'arbre de l'esquerra, en les quals s'ha de triar el menú d'equips i seleccionar que es vol fer servir la GPO (les polítiques de grup) per a administrar les actualitzacions dels equips connectats al domini.

Configuració WSUS



A partir d'aquí cal anar al configurador de les polítiques de grup i crear una nova GPO per a administrar els equips les actualitzacions dels quals es volen controlar des del servidor. Hem d'anar col·locant aquests equips dins d'aquesta unitat organitzativa del directori actiu. S'han de moure de la unitat organitzativa "equips" cap a la nova unitat organitzativa.

Creació de la GPO dins de la UO nova

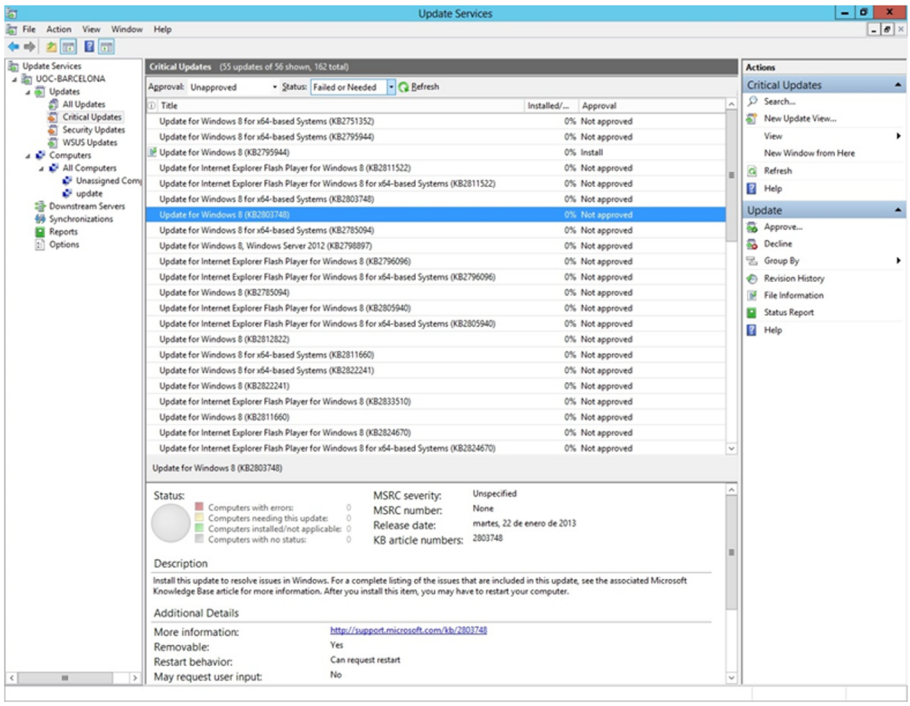


Normalment la comunicació es fa pel port 80 cap als servidor per consultar la llista de les actualitzacions, però en versions antigues i en algunes configuracions, aquesta comunicació es fa pel port 8530.

Un cop instal·lat el servidor d'actualitzacions, només cal entrar al servidor, des de les eines de l'administrador del servidor o des de la pàgina d'inici, on hi ha un accés al WSUS, i configurar la llista d'actualitzacions que hi ha per als sistemes que s'han definit inicialment i aprovar aquestes actualitzacions perquè siguin transmeses als ordinadors client.

La figura següent mostra un conjunt d'actualitzacions preparades per a ser acceptades des del servidor.

Llista d'actualitzacions pendent de ser aprovades



1.2.3. Microsoft Technical Security Notification

Per a mantenir sempre actualitzats els sistemes pel que fa a possibles fallades de seguretat, convé estar registrat en la llista de correu electrònic, o butlletí de seguretat, o en els comptes de Twitter de Microsoft. Els usuaris registrats en aquesta llista reben un butlletí de seguretat en què s'anuncia el descobriment de nous errors o *bugs* en la seguretat del sistema, i també enllaços a les pàgines on hi ha solucions a aquests problemes o la baixada corresponent de l'actualització que corregeix l'error.

1.2.4. Seguretat millorada d'Internet Explorer

Els atacants aprofiten vulnerabilitats del navegador per a executar aplicacions no volgudes sobre l'equip, a l'hora d'accedir a certes pàgines web i de manera inadvertida.

No és recomanable utilitzar el navegador d'Internet des d'un servidor en producció, ja que hi ha aplicacions malicioses que es poden instal·lar en el servidor i ocasionar un desperfecte general del servidor. Per tot plegat, Windows Server 2012 està configurat de tal manera que, en obrir el navegador d'Internet, Internet Explorer bloqueja l'accés a pàgines web desconegudes.

Per defecte, l'accés a webs de "desconfiança" està bloquejat. En accedir a una de les pàgines web que no surt en la llista de "Llocs de confiança", surt una finestra d'avís.

En instal·lar el servidor, només s'afegeixen a "Llocs de confiança" els URL de Microsoft. És recomanable afegir els URL necessaris a la llista de "Llocs de confiança". Per exemple, hi podem afegir l'URL d'actualització del servei antivirus perquè no torni a bloquejar l'accés a l'URL i que acabarà essent una mica molest per a la navegació. Per seguretat, és recomanable comprovar que no tenim cap URL desconegut en aquesta llista de llocs permesos a causa d'un error, ja que pot provocar la instal·lació de programari "malintencionat".

Ja s'ha dit que no és recomanable navegar per Internet des del servidor en producció, però si ho hem de fer, pot arribar a semblar molesta l'eina de seguretat d'Internet Explorer. Es pot deshabilitar des de l'administrador del servidor, a administració del servidor local; en les propietats que surten just al mig es pot canviar el paràmetre *IE Enhanced Security Configuration* a *off*, i d'aquesta manera deixarà de preguntar cada cop per la pàgina web segura.

2. Monitoratge d'esdeveniments

Les màquines que exerceixen de servidors (tant en sistemes GNU/Linux com en sistemes Microsoft Windows) tenen un registre dels esdeveniments que es produeixen en els diferents serveis. Aquests registres s'anomenen *esdeveniments* en sistemes Microsoft Windows i *logs* en sistemes GNU/Linux. Deixant de banda la denominació que tenen, la funció que fan és la mateixa: anotar en un fitxer de text tots els esdeveniments que es produeixen en els serveis. Segons el nivell de *log* que hem definit, s'anoten en el registre més o menys incidències.

2.1. GNU/Linux

A GNU/Linux els *logs* es configuren amb el fitxer `/etc/syslog.conf`. En aquest fitxer es configuren les regles de registre. Cada regla consta de dues parts, el selector i l'acció, i totes dues estan separades per espais o tabulacions.

El selector, al seu torn, es divideix en dos paràmetres: el primer ens indica quin tipus de servei afecta (*facility*); el segon, el nivell (*priority*) de *log* que volem registrar. La separació entre les dues parts del selector es fa amb un punt (`.`).

Els tipus de *facility* que hi ha són els següents:

1) `authpriv`: missatges de seguretat o autorització.
2) `cron`: missatges de les utilitats de rellotge (`cron` i `at`).
3) `daemon`: missatges dels dimonis (`daemons`) del sistema.
4) `kern`: missatges del nucli (*kernel*).
5) `lpr`: missatges del sistema d'impressores.
6) `mail`: missatges del sistema de correu.
7) `news`: missatges del tauler d'anuncis (*Usenet* o *News*).
8) `syslog`: missatges interns del sistema *syslog*.
9) `user`: missatges genèrics d'usuaris.

Els tipus de seguretat (ordenats en ordre decreixent d'importància) són els següents:

1) `emerg`: el sistema està inutilitzat.

2) `alert`: fallades greus en el sistema. S'han de prendre mesures correctores de manera immediata.

3) `crit`: condicions crítiques del sistema.

4) `err`: errors del sistema.

5) `warning`: avisos del sistema.

6) `notice`: esdeveniments que, malgrat que són normals, són significatius.

7) `info`: missatges informatius.

8) `debug`: missatges de depuració del sistema.

L'acció que s'ha de fer és sempre la mateixa: emmagatzemar la informació en un fitxer. El que podem configurar és el tipus de fitxer que volem fer servir. Aquest fitxer ha de ser en el servidor i tenir privilegis d'escriptura.

Els tipus de fitxer que hi són compatibles són els següents:

1) Fitxers regulars: fitxers de text normals. El camí fins a aquest fitxer ha d'estar indicat amb *path* absolut (el camí que s'ha de seguir des del directori arrel).

2) *Terminal console*: els missatges surten en la pantalla del servidor. El dispositiu utilitzat és `/dev/console`.

3) Llistes d'usuaris: els missatges crítics, a part de ser emmagatzemats, poden ser enviats en forma de correu electrònic a l'usuari arrel del servidor. Si volem que aquest tipus de missatges els rebi més d'un usuari, hem d'afegir els noms d'usuaris de tots ells, separats per comes.

4) Tots els usuaris connectats: els missatges d'emergència poden aparèixer en la consola dels usuaris connectats (sia en local o mitjançant consola remota) i indicar el motiu pel qual s'ha bloquejat el sistema.

5) Màquines remotes: els fitxers de *log* poden ser fora del servidor, en una màquina remota.

Aquesta última opció és molt interessant per a l'administrador de sistemes operatius, principalment per dos motius.

El primer d'aquests motius té a veure amb la seguretat. Les persones que ataquen una màquina, si aconsegueixen entrar-hi amb privilegis de *root*, una de les primeres coses que fan és esborrar els fitxers de *log* per a amagar la intrusió. Si aquests fitxers són enviats a una màquina remota regularment, disminueix la possibilitat que siguin esborrats, ja que per a fer-ho l'atacant ha de vulnerar també la segona màquina. És clar que si no es controlen aquests *logs* tampoc no serveixen de gaire, ja que per molta informació que es guardi de manera segura, si no es controla el que es fa regularment i el que està passant no la podrem aprofitar. Per exemple, un atacant aconsegueix explotar una vulnerabilitat del servidor de la base de dades, i el primer que fa és parar l'enviament

dels *logs* a una altra màquina. En conseqüència, no es disposarà de dades en els *logs*, i a més si ningú no s'adona que no s'estan enviant els fitxers de *log*, de poc servirà tenir-lo configurat així.

El segon motiu és per una qüestió d'administració: si tenim tots els fitxers de *log* concentrats en una màquina, només ens hem de fixar en els registres d'una màquina per adonar-nos de tots els esdeveniments que han passat.

Tot i que tenim tots els esdeveniments de la màquina concentrats en un fitxer de text, la supervisió d'aquest fitxer no és una tasca senzilla, sinó més aviat al contrari. Per a facilitar aquesta supervisió hi ha aplicacions que revisen els *logs* i envien un correu electrònic amb un resum de les incidències que hi ha hagut.

Hi ha diverses aplicacions que controlen els *logs* del sistema, com `metalog`, `syslog-ng`, `logwatch`, `loganalyzer`, etc. En aquests materials mostrem aquesta darrera aplicació. `loganalyzer` és una aplicació que supervisa *logs*. Per instal·lar aquesta eina ens hem de connectar a la pàgina web del fabricant, ja que no es troba en el repositori per defecte, i baixar-ne la darrera versió, en aquest cas la 3.6.3. La pàgina del fabricant és: http://loganalyzer.adiscon.com/downloads.

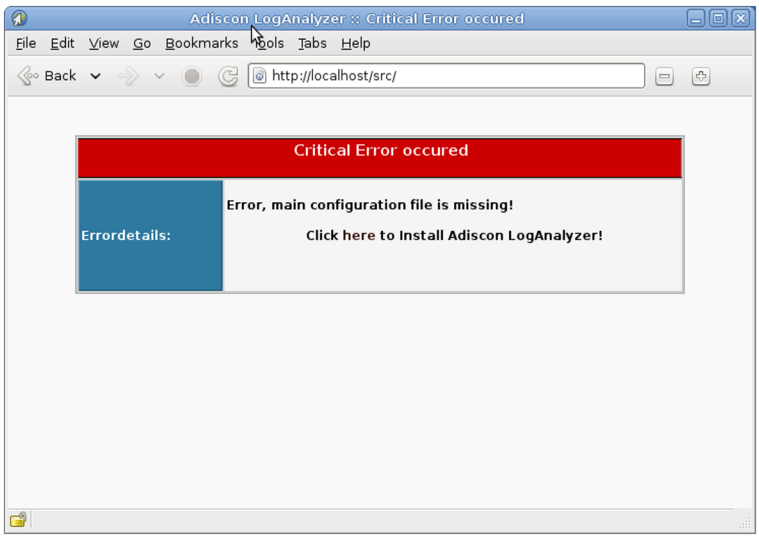
```
root# wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.3.tar.gz
root# tar -xvf loganalyzer-3.6.3.tar.gz
```

Ara cal descomprimir el fitxer i veure que hi ha un fitxer d'instal·lació que explica quins són els requisits necessaris per a poder instal·lar l'aplicació, com pot ser l'`apache`, el `rsyslog` i el `php5`.

Per fer la instal·lació, i seguint els passos que explica el fitxer `INSTALL` que hi ha dins l'aplicació que s'acaba de descomprimir, s'ha de copiar el directori `src` en el directori del servidor web `apache`, copiar també els fitxers `configure.sh` i `secure.sh` del directori `contrib` en el mateix directori `src` que s'acaba de copiar abans, i donar atribut d'execució, és a dir:

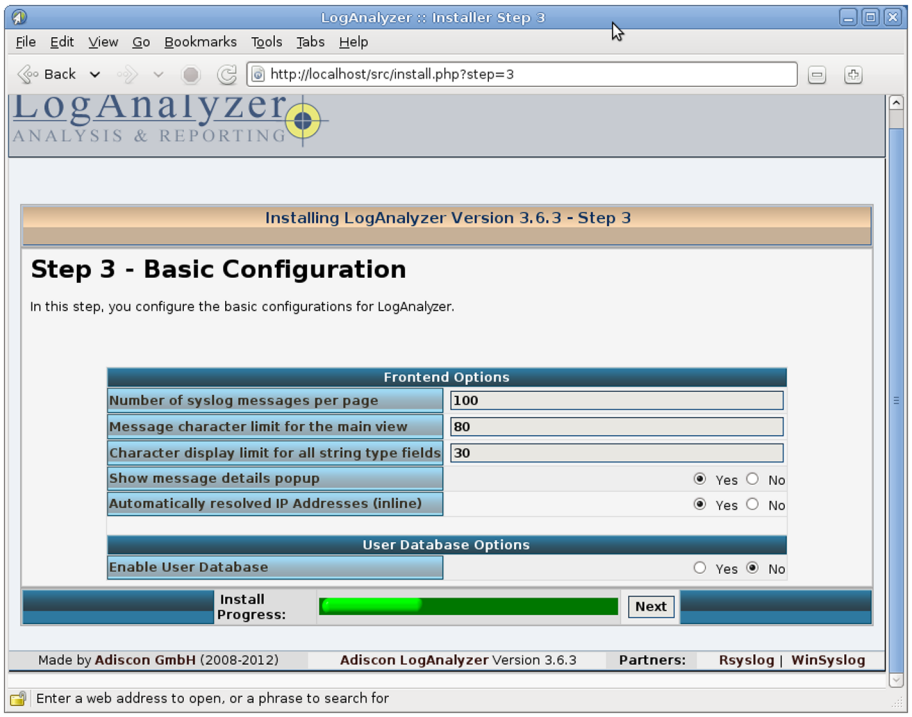
```
root# cp -R /home/jordi/loganalyzer-3.6.3/src/ /var/www/
root# cp /home/jordi/loganalyzer-3.6.3/contrib/*.sh /var/www/src/
root# cd /var/www/src/
root# chmod +x configure.sh secure.sh
```

I ja només queda obrir el navegador d'Internet i accedir a la pàgina web que hi ha dins el directori `/src/` del lloc (*site*), on podrem veure el configurador. La primera vegada ens donarà un error i mostrarà l'enllaç (*link*) per arrencar el configurador.



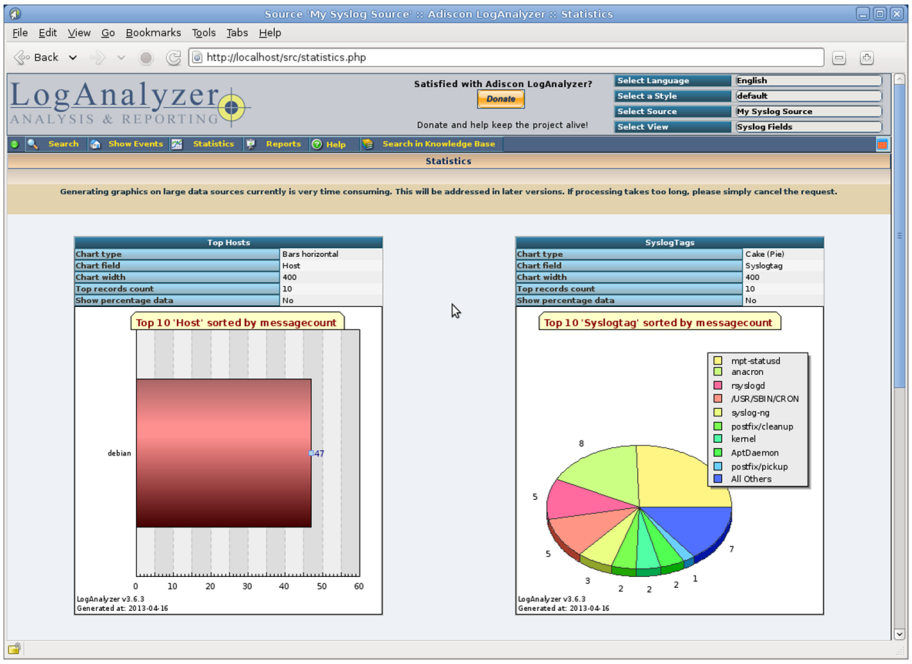
Si entren en l'enllaç, es podrà configurar l'aplicació. En la pàgina web podem trobar molta informació de cada paràmetre.

Paràmetres de configuració



Finalment, podem veure els resultats dels *logs* de l'equip en la mateixa pàgina web que abans donava errors i que ara en mostra el resultat del tractament.

Resultats finals



2.2. Microsoft Windows Server 2012

2.2.1. Monitoratge dels registres d'incidències

Les incidències són accions d'usuaris que queden registrades en el servidor, o qualsevol esdeveniment produït pel sistema operatiu o una aplicació.

A Windows Server 2012 hi ha tres tipus de registres d'incidències:

- Registre del sistema: les incidències registrades les provoca el sistema operatiu; per exemple, una fallada d'un controlador durant l'inici del sistema.

- Registre d'aplicació: conté les incidències provocades per aplicacions del sistema. Problemes en arrencar alguna aplicació, problemes d'accés a registre, problemes de biblioteques, etc.

- Registre de seguretat: guarda incidències relacionades amb la seguretat del sistema, com ara intents d'accessos fallits o un intent d'executar una operació sense privilegis.

A més, hi ha tres tipus d'incidències de sistema o aplicació:

- Informació: registra el funcionament correcte d'una aplicació o un servei.

- Advertiment: registra una incidència que no és problemàtica però que pot comportar un error si no es té en compte.

- Error: és una incidència greu que registra una fallada en una aplicació o un servei.

Els tipus d'incidències de seguretat poden ser els següents:

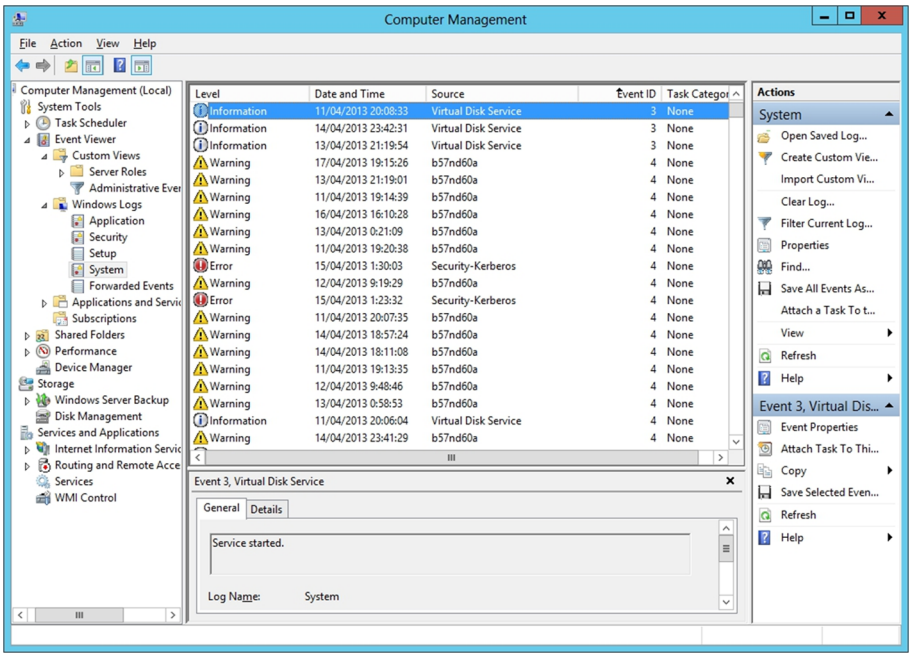
- Auditoria d'encerts: registre d'accessos al servidor amb èxit.

- Auditoria d'errors: registre d'accessos denegats (intents d'accés il·legal o de violació de seguretat).

Per a visualitzar les incidències que hi ha hagut en el sistema, podem utilitzar el visor d'incidències, una eina basada en la consola d'administració que és dins de les eines de l'administrador del servidor.

A l'esquerra veiem una llista dels registres d'incidències. A banda dels registres de què hem parlat abans, hi trobem altres registres d'incidències relacionades amb altres funcionalitats o serveis del servidor com per exemple *Active Directory*.

Esdeveniments del sistema



També hi podem visualitzar els registres d'incidències d'altres equips seleccionant l'opció "Connectar amb un altre equip..." del menú contextual de l'element "Administració de l'equip (local)" de la llista de l'esquerra, i així tenir controlats tots els equips de la xarxa de manera centralitzada en el servidor.

Si fem doble clic sobre una de les incidències, veiem les propietats que té, on es mostra la data, l'hora, el tipus d'incidència, l'origen, etc., que serà útil per a esbrinar què està passant en els diferents equips i en el servidor en concret.

Si seleccionem l'opció "Propietats" del menú contextual d'un dels registres de la llista de l'esquerra, podem configurar algunes propietats de registre d'aquest tipus d'incidències, com per exemple la mida màxima de l'arxiu d'incidències.

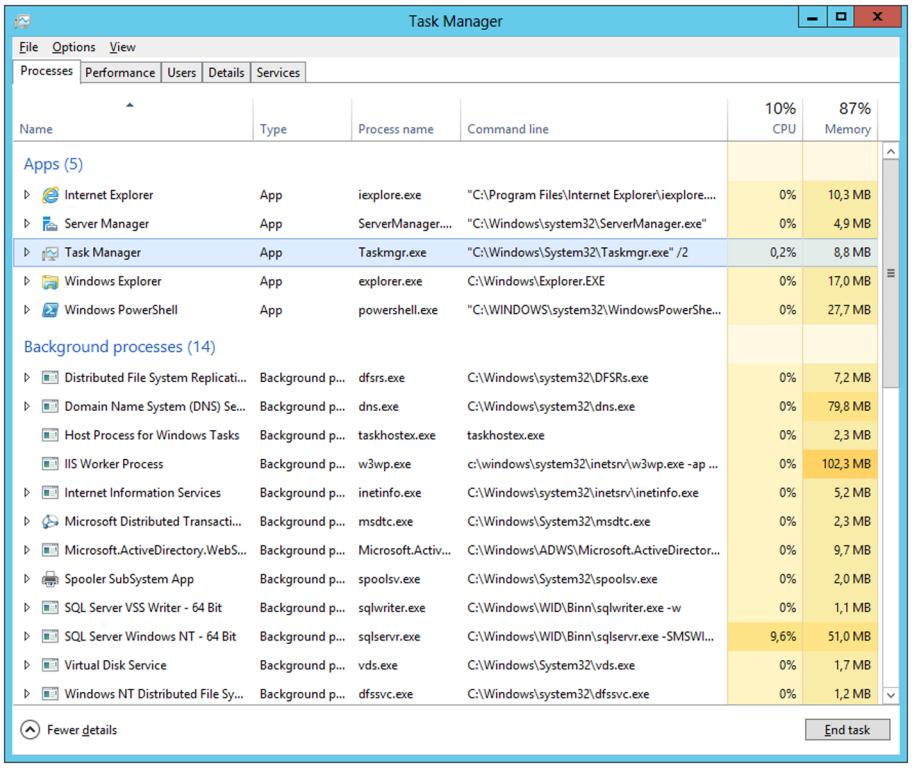
2.2.2. Monitoratge del rendiment del sistema

L'administrador de tasques de Windows permet monitorar i controlar les aplicacions i els processos en execució en el sistema en un moment concret. Per iniciar l'administrador de tasques premem la combinació de tecles "Ctrl + Alt + Supr" i seleccionem l'opció "Administrador de tasques". També s'hi pot accedir directament, prement la combinació de tecles "Ctrl + Majús + Esc", o des de la barra de tasques, amb el botó dret "Administrador de tasques". Hi ha dues versions d'aquesta aplicació: la que únicament mostra el nom de les aplicacions, pensada per a fer servir en entorns amb les pantalles tàctils; i la versió que mostra molts més detalls de tot allò que s'està executant en el sistema. Únicament cal mostrar més detalls per a canviar d'una a l'altra.

En la pestanya "Aplicacions" podem controlar les aplicacions en execució. Si una aplicació no respon, la podem eliminar seleccionant-la i després seleccionant l'opció "Finalitzar tasca". Es perdran totes les dades de l'aplicació, de manera que només es recomana utilitzar aquesta opció si l'aplicació no respon.

Des de la pestanya "Processos" veiem la informació de tots els processos en execució en el sistema:

Llista de processos reals del sistema



Mitjançant l'opció "Acabar procés" s'acaba l'execució d'un procés. Igual que en el cas de les aplicacions, es perden totes les dades del procés, de manera que no és recomanable utilitzar aquesta opció tret que el procés no respongui.

La pestanya "Rendiment", de l'administrador de tasques, mostra l'ús del processador o CPU, la memòria del sistema en un moment concret, l'ús de la xarxa o del disc dur.

La pestanya "Usuaris" permet veure els usuaris connectats al servidor. També es permet des d'aquí la desconnexió, el tancament de sessió i la possibilitat d'enviar un missatge d'avís abans de la desconnexió. Aquí únicament mostra els usuaris que estan connectats directament al servidor, no els que estan treballant des del ordinadors client connectats amb l'*Active Directory* al servidor.

3. Automatització de tasques

3.1. GNU/Linux

Moltes de les tasques que ha de dur a terme l'administrador són rutinàries, és a dir, cada dia fa les mateixes i amb el mateix ordre. Aquestes tasques es poden automatitzar. De fet, les hem d'automatitzar; d'aquesta manera tindrem més temps per a fer altres tasques i només haurem de revisar les rutinàries. Per a això, fem servir la utilitat de rellotge que ens ofereix el sistema. Aquesta utilitat s'anomena `crontab` i està instal·lada per defecte en el sistema operatiu.

Si volem editar el fitxer de configuració de l'aplicació `crontab` per automatitzar una nova tasca, s'ha d'executar l'ordre següent:

```
root# crontab -e
```

Hem de tenir present que per a afegir una tasca a aquest fitxer de configuració s'ha de fer de la manera correcta. La sintaxi que segueix aquest fitxer és la següent:

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

`minutes` accepta valors numèrics de 0 a 59.

`hours` accepta valors numèrics de 0 a 23.

`days` fa referència als dies del mes i accepta els valors numèrics de l'1 al 31.

`month` són els mesos de l'any i, per tant, accepta valors d'1 a 12.

`day_week` accepta valors d'1 a 7.

`path`. Finalment hem de posar l'*script* o ordre que volem executar amb el camí absolut i tots els paràmetres que volem.

Hi ha altres caràcters que també són compatibles amb l'aplicació `crontab`. És el cas de certes cadenes de caràcters: les tres primeres lletres en anglès dels mesos o els dies de la setmana poden substituir els caràcters numèrics. Un altre caràcter compatible amb el `crontab` és el símbol (`*`), que el podem posar a qualsevol lloc i indica que són vàlids tots els possibles valors. Per exemple, un `*` a `day_week` vol dir que s'ha d'executar tots els dies de la setmana.

Un altre exemple és que si volem que s'executi un *script* anomenat `check_disc.sh` cada divendres a les tres de la matinada, la línia que hem de posar dins els fitxers de configuració de l'aplicació `crontab` és la següent:

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

En aquest exemple veiem que la majoria de les tasques que executem en el `crontab` no són ordres amb paràmetres sinó *scripts*. Els llenguatges més utilitzats per a fer *scripts* són *shell script* i PERL. És molt útil per a l'administrador saber utilitzar tots dos llenguatges, ja que tant l'un com l'altre proporcionen maneres diferents de fer les tasques.

El *shell script* està pensat perquè utilitzem les ordres del sistema per a dur a terme determinades tasques, i podem fer servir variables per a guardar resultats. En canvi, el PERL és un llenguatge optimitzat per a treballar amb fitxers de text, manipular-los i imprimir-ne els resultats.

La majoria de les versions de GNU/Linux, quan les instal·lem, tenen diferents *shells* (`zshell`, `tcsh`, `cshell`, `bourne shell`, etc.). Tots són molt semblants però no iguals, i hi podem fer les mateixes coses; el que canvia és la manera de fer servir les variables, les variables d'entorn, l'ús dels paràmetres, etc.

A diferència del *shell*, hi ha moltes versions GNU/Linux que no porten instal·lat el PERL. Per a instal·lar-lo, únicament cal executar l'ordre següent:

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

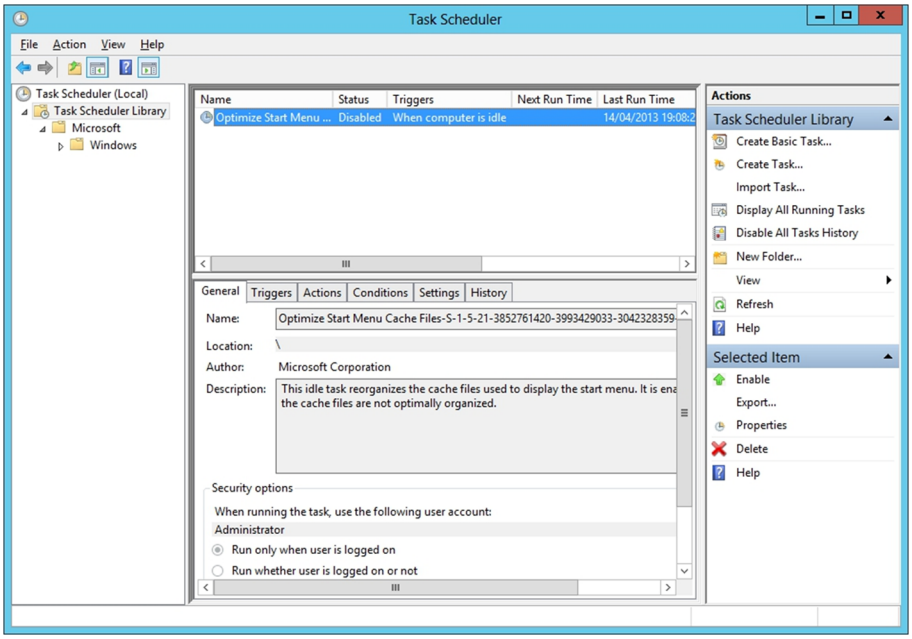
3.2. Windows Server 2012

3.2.1. Tasques programades

Com s'ha comentat, a vegades cal definir algunes tasques rutinàries que s'han de fer periòdicament per a optimitzar el rendiment del sistema, com per exemple compactar els discos durs, fer les còpies de seguretat i netejar les carpetes temporals i arxius d'Internet.

Aquestes tasques es poden programar perquè es facin cada cert temps, preferentment quan el servidor té menys càrrega de feina. Això es pot fer amb el programador de tasques, que es pot obrir seleccionant-lo dins el menú d'eines de l'administrador del servidor.

Programador de tasques



La finestra que hi surt mostra les icones corresponents a les tasques programades actualment. Per programar una nova tasca premem "Crear tasca".

En la pantalla següent ens mostren totes les opcions possibles per programar una nova tasca, temporització, usuari amb què s'executa, etc. En principi es pot executar qualsevol programa instal·lat en el sistema.

Possibles aplicacions que es poden automatitzar perquè no tenen interacció amb les persones i per tant es poden arrencar quan no hi ha ningú fent servir l'ordinador:

- Netejar espai en el disc dur.
- Escanejar els discos durs en busca d'errors.
- Compactar els discos durs.
- Fer una anàlisi antivirus.
- Actualitzar el sistema.
- Fer còpies de seguretat.

En la primera pantalla es mostren les dades relacionades amb la seguretat, on podem seleccionar els usuaris i si ha de ser visible o no aquesta tasca.

3.2.2. Scripting. Windows Management Instrumentation (WMI)

Algunes tasques d'administració poden resultar costoses sobretot si s'han de fer repetidament. N'hi ha algunes que es poden parametritzar i programar per a facilitar la feina dels administradors de sistema.

Windows permet executar arxius de *script* que continguin programes escrits en *visual basic script* (VBScript) o *JScript*, gràcies a l'eina *Windows Script Host* (WSH).

Els *scripts* permeten automatitzar tasques com crear usuaris, assignar permisos d'execució sobre arxius, instal·lar aplicacions, crear *logs* o *reports* de l'estat del sistema. D'aquesta manera es reduiran els errors i els problemes de seguretat, ja que tots els usuaris tindran els mateixos drets i per error no se'n generarà un que tingui més privilegis dels que ha de tenir.

A més, Windows proporciona una sèrie d'objectes utilitzables des dels *scripts*, anomenats *Windows Management Infrastructure* (WMI), que permeten accedir a les propietats internes del sistema operatiu (versió del sistema, maquinari instal·lat, processos, accés al registre, etc.).