

Pràctica 3: Monitorització del rendiment del sistema i dels recursos utilitzats per processos i dispositius. Registres d'esdeveniments del sistema (log). Auditoria.

Objectius

Aquesta pràctica té com a objectiu:

- a) Estudiar el concepte de: **rendiment, eficàcia, eficiència, recurs, rendiment del sistema, esdeveniment del sistema, registre, monitorització i auditoria del sistema.**
- b) Estudiar les eines per poder **monitoritzar el rendiment del sistema** en Linux i Windows.
- c) Estudiar les eines per poder **monitoritzar els recursos utilitzats pels processos del sistema** en Linux i Windows.
- d) Estudiar les eines per poder **monitoritzar els recursos utilitzats pels dispositius** en Linux i Windows.
- e) Estudiar les eines per poder visualitzar i treballar amb els registres d'esdeveniments del sistema (Logs).
- f) Estudiar les eines per realitzar auditories de sistema.

Documentació

- a) Llegeix les pàgines 1 i 2 del document que trobaràs [aquí](#).
- b) Llegeix el document que trobaràs [aquí](#).
- c) Llegeix el document que trobaràs [aquí](#).
- d) Llegeix <http://www.thegeekstuff.com/2011/08/linux-var-log-files/>
- e) Llegeix <http://askubuntu.com/questions/26237/difference-between-var-log-messages-var-log-syslog-and-var-log-kern-log>
- f) Documentació sobre logs i monitorització del sistema que trobaràs [aquí](#).
- g) Informació sobre el rendiment d'un equip: [aquí](#).
- h) Informació sobre auditoria: [aquí](#)

Exercici 1 - Conceptes teòrics (20%)

- 1- Quina és la diferència entre **eficiència** i **eficàcia**?
- 2- Quines característiques ha de tenir un sistema informàtic perquè es consideri que el seu **rendiment** és alt?
- 3- Què és un **recurs** del sistema. Dóna 4 exemples.
- 4- Què és un **esdeveniment** del sistema?
- 5- Què és **monitoritzar**?
- 6- Què són els **registres d'esdeveniments** del sistema?
- 7- En què consisteix una **auditoria** del sistema?

Exercici 2 - Monitorització i auditoria. Registre d'esdeveniments (30%)

1- Posa en marxa l'eina de **monitorització de recursos** de **Windows**. Des de **PowerShell** executa **resmon.exe**. Indica:

- a) Quina és la memòria total del sistema, la disponible i la utilitzada.
- b) Visualitza El % d'utilització de la CPU.

2- Posa en marxa l'eina de **monitorització del rendiment** de **Windows**. Des de **PowerShell** executa **perfmon.exe**. Visualitza una gràfica amb el % de bytes utilitzats, el % de temps d'utilització del processador i d'utilització del disc.

3- Accedeix a l'**índex d'experiència Windows** des de Tauler de control --> Sistema i seguretat --> Centre d'activitats. Si no està instal·lat, descarrega l'eina per calcular l'**índex d'avaluació d'experiència de Windows** des d'[aquí](#). Instal·la-ho. Executa-ho des de Powershell. Executa: **control /name**

Microsoft.PerformanceInformationAndTools. Realitza un càlcul de l'índex i comprova si els valors són satisfactoris.

4- Crea una auditoria d'accés a objectes

- A l'arrel del sistema crea una carpeta de nom **C:\Auditoria**.
- Volem saber quan la carpeta ha estat accedida per l'usuari **alumne00**:
 - Amb l'eina **gpedit.msc** activa l'auditoria d'accés a objectes (Directiva Equipo Local → Configuración del equipo → Configuración de Windows → Directivas locales → Directiva de seguridad → Auditar el acceso a objetos (Correcto/Incorrecto)
 - **Sobre la carpeta auditar selecciona** → **Propiedades** → **Seguridad** → **Opciones avanzadas** → **Auditoria** → **Editar** → **Agregar i selecciona l'usuari alumne00. Aplica la directiva per qualsevol cas d'accés.**

5- Registres d'esdeveniment o logs de Windows: Des del Tauler de control, accedeix a Sistema i seguretat, i selecciona Ver registre d'esdeveniments. Mostra el contingut d'un esdeveniment d'error de sistema.

6- Obre l'administrador de tasques de Windows. Mostra el rendiment de la CPU, memòria i xarxa.

Indicacions

Forma de lliurament de l'informe

1- Treball individual

2- El nom del fitxer ha de tenir el següent format **asix2_cognom_nom_m01uf4pr3.pdf**

3- Envieu la solució proposada per correu electrònic:

Adreça: **cf@collados.org**

Assumpte: **asix2_cognom_nom_m01uf4pr3**

4- La **data límit** de lliurament de la pràctica és el dia **29/04/14** a les **23.59 hores**.

5- Format Lletra: **Arial 10**

6- Marges (superior, inferior, esquerra, dreta): **2cm**

7- Numeració de pàgina: **Peu de pàgina a la dreta**.