Monitorització de sistemes Windows

Mòdul 0224 - Sistemes Operatius en Xarxa

Supervisió del rendiment, detecció de problemes i manteniment dels sistemes Windows Server i els seus clients en un entorn de domini Active Directory.

Què monitoritzem en un entorn Windows?

Al igual que amb entorns Linux, en un entorn Windows, la monitorització consisteix a observar de manera contínua l'estat dels recursos del sistema per detectar anomalies, prevenir fallades i garantir el bon funcionament dels serveis.

CPU

Percentatge d'ús del processador. Valors alts de forma sostinguda indiquen sobrecàrrega o processos problemàtics.

Memòria RAM

Quantitat de memòria disponible i en ús. La manca de RAM provoca paginació excessiva i lentitud.

Emmagatzematge

Espai lliure al disc i velocitat de lectura/escriptura. Un disc ple pot deixar inoperatiu tot el sistema.

Xarxa

Ample de banda consumit, latència i errors de connexió. Essencial per detectar colls d'ampolla.

Servidor vs. Clients

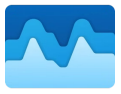
El **servidor** allotja serveis crítics (AD, DNS, DHCP) i requereix monitorització constant. Els **clients** es monitoritzen per detectar problemes d'usuari, malware o consum anormal de recursos.

Per què és important monitoritzar el domini?

- Un servidor sobrecarregat afecta tots els usuaris.
- Els errors d'autenticació es registren centralment.
- Permet detectar intrusions i accessos no autoritzats.
- Facilita la planificació en cas que es vulgui augmentar la capacitat.

Eines de monitorització natives de Windows

Windows Server incorpora un conjunt d'eines integrades que permeten supervisar el sistema sense necessitat d'instal·lar programari addicional. Cada eina té un propòsit específic i un nivell de detall diferent.



Administrador de tasques

Visió ràpida dels processos actius, ús de CPU, RAM, disc i xarxa en temps real. Ideal per a diagnòstics immediats.

Monitor de recursos

Detall per procés i per recurs. Permet identificar quin procés bloqueja un fitxer o utilitza la xarxa de forma intensiva.

Monitor de rendiment

Registra comptadors de rendiment al llarg del temps. Permet crear informes i analitzar tendències per establir una línia base.

Visor d'esdeveniments

Registre centralitzat d'errors, advertències i informació del sistema. Imprescindible per a l'auditoria i la resolució d'incidències.

Eina	Accés ràpid	Què mesura principalment	Nivell de detall
Task Manager	Ctrl+Shift+Esc	CPU, RAM, disc, xarxa, processos	Bàsic
Resource Monitor	resmon.exe	Detall per procés i recurs	Mitjà-Alt
Performance Monitor	perfmon.exe	Comptadors de rendiment en el temps	Alt
Event Viewer	eventvwr.msc	Esdeveniments del sistema, seguretat, aplicacions	Alt

Administrador de tasques (Task Manager)

L'Administrador de tasques és la primera eina a la qual recorrem quan sospitem que el sistema va lent o que un procés consumeix massa recursos. S'obre amb **Ctrl+Shift+Esc** o fent clic dret a la barra de tasques.

Processos

Llista de tots els processos actius amb CPU%, RAM, disc i xarxa consumits.

Rendiment

Gràfics en temps real de CPU, memòria, disc i xarxa.

Usuaris

Sessions d'usuari actives i recursos que consumeix cada una.

Serveis

Estat dels serveis del sistema (en execució, aturat...).

Detalls

Informació avançada: PID, estat, CPU%, memòria per procés.

Columnes clau a la pestanya Detalls

- **CPU%** - Percentatge de processador consumit
- **Memòria** - RAM en ús pel procés (MB)
- **PID** - Identificador únic del procés
- **Estat** - En execució / Suspès

Com identificar i finalitzar un procés problemàtic

1. Obre el Task Manager amb Ctrl+Shift+Esc
2. Ordena per columna **CPU%** o **Memòria** (clic a la capçalera)
3. Identifica el procés que encapçala la llista de forma anormal
4. Fes clic dret sobre el procés → **Finalitza la tasca**
5. Confirma l'acció i comprova que el sistema es recupera

⚠️ Finalitzar un procés del sistema pot causar inestabilitat. Assegura't d'identificar correctament el procés abans d'aturar-lo.

Monitor de recursos (Resource Monitor)

El Monitor de recursos ofereix un nivell de detall molt superior al Task Manager. S'accedeix des de la pestanya **Rendiment** del Task Manager (botó "Obre el Monitor de recursos") o executant `resmon.exe`.

1

Informació general

Resum de CPU, disc, xarxa i memòria en una sola pantalla amb gràfics en temps real.

2

CPU

Detall per procés: cicles de CPU, fils d'execució i serveis associats a cada procés.

3

Memòria

Distribució de la RAM: en ús, en espera, modificada i lliure. Detecta fuites de memòria.

4

Disc

Activitat de lectura/escriptura per procés i per fitxer. Identifica quin procés bloqueja un fitxer.

5

Xarxa

Connexions de xarxa actives per procés, adreces IP remotes i ample de banda consumit.

Avantatge sobre el Task Manager

Mentre el Task Manager mostra dades agregades, el Resource Monitor permet veure **exactament quin procés** fa cada operació:

- Quin procés té obert un fitxer específic
- Quines connexions de xarxa té obertes cada aplicació
- Quina és la velocitat de lectura/escriptura per fitxer

Cas pràctic: procés que bloqueja un fitxer

1. Obre el Resource Monitor → pestanya **Disc**
2. A la secció "Fitxers associats", cerca el nom del fitxer
3. El procés que apareix és el que el té bloquejat
4. Tanca l'aplicació o finalitza el procés per alliberar el fitxer

Monitor de rendiment (Performance Monitor)

El Monitor de rendiment (`perfmon.exe`) és l'eina més potent per a l'anàlisi de rendiment a llarg termini. Permet enregistrar **comptadors** durant intervals de temps i analitzar els resultats posteriorment.

Conceptes clau

Comptador (Counter): Mètrica específica que es vol mesurar, com ara el percentatge d'ús del processador o els megabytes de memòria disponibles.

Data Collector Set: Conjunt de comptadors que s'enregistren junts durant un interval de temps definit. El resultat es desa en un fitxer per a anàlisi posterior.

Comptadors clau recomanats

Comptador	Descripció
`Processor\% Processor Time`	% d'ús de la CPU
`Memory\Available MBytes`	RAM disponible en MB
`LogicalDisk\% Free Space`	Espai lliure al disc
`Network Interface\Bytes Total/sec`	Tràfic de xarxa total

Com crear un Data Collector Set

01

Obre perfmon.exe

Executa `perfmon.exe` com a administrador. Navega a **Conjunts de recollida de dades → Definit per l'usuari**.

02

Crea un nou conjunt

Fes clic dret → Nou → Conjunt de recollida de dades. Tria "Crear manualment" i selecciona "Comptadors de rendiment".

03

Afegeix comptadors

Fes clic a "Afegeix" i selecciona els comptadors desitjats de la llista. Configura l'interval de mostreig (ex: cada 5 segons).

04

Inicia l'enregistrament

Fes clic dret al conjunt creat → Iniciar. Deixa-ho enregistrant durant el temps necessari (minuts o hores).

05

Analitza el gràfic

Atura l'enregistrament i obre l'informe generat. Analitza els pics i valors mitjans per identificar problemes de rendiment.

Visor d'esdeveniments (Event Viewer)

El Visor d'esdeveniments (`eventvwr.msc`) és el registre centralitzat de tot el que passa al sistema. És imprescindible per a l'auditoria de seguretat, la resolució d'incidències i el seguiment de l'activitat del servidor.

Estructura del Visor d'esdeveniments

Windows Logs

- **Application**: Errors d'aplicacions i programes
- **Security**: Auditoria d'accessos i autenticació
- **System**: Esdeveniments del sistema operatiu

Applications and Services Logs

Registres específics de rols i serveis com Active Directory, DNS, DHCP i altres components de Windows Server.

Nivells de gravetat

- 🔵 **Information**: Operació completada correctament
- 🟡 **Warning**: Situació que pot derivar en error
- 🔴 **Error**: Fallada que afecta la funcionalitat
- ⛔ **Critical**: Fallada greu que requereix atenció immediata

Event IDs importants que cal conèixer

Event ID	Log	Significat
4624	Security	Inici de sessió correcte: Un usuari s'ha autenticat amb èxit
4625	Security	Error d'autenticació: Intent d'inici de sessió fallit (possible atac de força bruta)
6005	System	Inici del servei Event Log: Indica que el sistema ha arrencat
6006	System	Aturada del servei Event Log: Indica que el sistema s'ha apagat correctament
7034	System	Un servei s'ha aturat de forma inesperada: Pot indicar un problema crític

Com filtrar per Event ID

1. Obre el Visor d'esdeveniments → selecciona el log (ex: Security)
2. Al panell dret, fes clic a **"Filtra el registre actual..."**
3. Al camp "ID d'esdeveniment", escriu el número (ex: 4625)
4. Fes clic a Acceptar per veure només els esdeveniments filtrats

Com exportar el log

1. Selecciona el log que vols exportar
2. Fes clic dret → **"Desa tots els esdeveniments com..."**
3. Tria el format: `.evtx` (natiu) o `.csv` (per a Excel)
4. Desa el fitxer en una ubicació segura per a anàlisi posterior

Monitorització de clients des del servidor

En un entorn de domini, l'administrador pot supervisar els equips clients de forma remota sense necessitat de desplaçar-se físicament. Això permet detectar problemes, auditar l'activitat i fer diagnòstics de manera centralitzada.

Visor d'esdeveniments remot

Des del Visor d'esdeveniments, fes clic dret a "Visor d'esdeveniments (local)" → **Connecta a un altre equip**. Introdueix el nom o IP del client del domini per consultar els seus logs de forma remota.

PsExec (Sysinternals)

Permet executar comandes en equips remots com si fossis davant d'ells. Exemple: `psexec \\NomEquip cmd` obre una consola remota al client per fer diagnòstics avançats.

Process Explorer (Sysinternals)

Versió avançada del Task Manager amb informació detallada sobre processos, DLLs carregades i jerarquia de processos. Ideal per detectar malware o processos sospitosos.

Comandes per supervisar sessions i recursos compartits

Comandes CMD / net

`net session` - Mostra les sessions actives connectades al servidor (usuari, equip, temps de connexió).

`net statistics server` - Estadístiques del servidor: bytes enviats/rebuts, errors, sessions obertes des de l'últim reinici.

PowerShell remot

`Get-EventLog -ComputerName NomEquip -LogName System -Newest 20`

Consulta els 20 últims esdeveniments del log System d'un equip remot del domini directament des del servidor, sense necessitat d'eines addicionals.

Bones pràctiques

Una bona administració de sistemes no es limita a reaccionar davant els problemes: cal anticipar-se, documentar i establir rutines de monitorització que garanteixin la salut del sistema a llarg termini.

→ Revisa els logs regularment

Consulta el Visor d'esdeveniments almenys un cop al dia. Presta especial atenció als errors (Error, Critical) i als intents d'autenticació fallits (Event ID 4625).

→ Estableix una línia base (*baseline*)

Enregistra el rendiment del sistema en condicions normals amb el Performance Monitor. Aquesta línia base et permetrà detectar desviacions anormals en el futur.

→ Documenta les incidències

Registra cada problema detectat, la seva causa i la solució aplicada. Aquesta documentació és valuosa per a futures incidències similars i per a l'equip tècnic.

Comparativa final d'eines

Característica	Task Manager	Resource Monitor	Performance Monitor	Event Viewer
Detall per procés	Mitjà	Alt	Alt	No aplica
Dades històriques	No	No	Sí	Sí
Auditoria seguretat	No	No	Parcial	Sí
Ús recomanat	Diagnòstic ràpid	Anàlisi detallada	Tendències i baseline	Errors i seguretat