Monitorizarea calculatoarelor

19 Aprilie

Cuprins

- Event Viewer
- Reliability and Performance Console
- Audit
- SNMP

Software Logs

- În mod frecvent produsele software generează rapoarte despre activitatea lor
- Salvarea acestor rapoarte se face în fişiere de log
- Care este rolul unor astfel de fişiere?
  - administratori pot analiza activitatea produsului
  - generarea de alerte automate pe baza lor
  - data statistice despre consumul de resurse
  - documentarea atunci când apar erori
- Fişierele de log sunt de obicei fişiere text
- Sistemele de operare windows folosesc aplicaţii grafică pentru vizualizarea lor

Event Viewer

- Componenta sistemului de operare care generează log-uri se numeşte Windows Eventing
  - rolul principal este de a înregistra informaţii despre activitatea sistemului
  - aceste informaţii sunt salvate sub formă de pachete denumite "events"
- Aplicaţia folosită pentru vizualizarea pachetelor se numeşte Event Viewer
- In Windows Server 2008 este o aplicaţie de tip Microsoft Management Console (MMC)

Event Viewer

- Custom views
  - metode de filtrare create de utilizator
- Windows Logs
  - evenimente generate de sistemul de operare
  - principalele trei categorii sunt
    - Application
    - Security
    - System
- Application and Services Logs
  - evenimente generate de serviciile sau aplicatiile instalate

Nivel de log

- Information
  - eveniment ce descrie schimbarea stării unui proces ca fiind parte a unei operaţii normale
- Error
  - un eveniment ce descrie o problemă apăruta pentru un proces
  - această problemă nu afectează procesul în sine, ci poate afecta alte componente ale sistemului de operare
- Warning
  - un eveniment ce anunţă posibila degradare a serviciului
- Critical
  - un eveniment generat la pierderea funcţionalităţiilor sau a datelor unei anumite componente

Tipuri de log-uri

- Admin
  - conţin evenimente destinate unui utilizator ce indică o problemă şi o posibilă soluţie
- Operational
  - conţin evenimente ce reprezintă o schimbare în aplicaţie sau serviciu, precum adăugarea unei imprimante
- Analytic
  - număr mare de evenimente ce raportează activitatea aplicaţiilor
- Debug
  - evenimente folosite de programatori pentru depanare
- Ultimele două sunt ascunse în mod implicit pentru ca de obicei conţin cantităţii mari de informaţi

Monitorizarea performanţelor

- Nivelul de performaţă al unui sistem de operare este în permanenţă schimbare, raportat la operaţiile pe care le execută
- Monitorizarea performanţelor componentelor pentru un anumit interval este singura metodă pentru observarea capabilităţilor sistemului
- Log-uri sunt utile pentru analiza evenimentelor din trecut, este necesară o metodă pentru analiza performanţelor în timp real

Reliability and Performance Monitor

- Resource Overview
- Monitoring Tools
  - Performance Monitor
  - Reliability Monitor
- Data Collector Sets
  - User defined
  - System
- Reports
  - User defined
  - System

Resource Overview

- Afişează grafic informaţii statistice despre cele mai importante patru componente hardware
  - CPU
  - Disk
  - Network
  - Memory
- Fiecare secţiune poate fi extinsă pentru pentru detalii sub formă de grafice, precum resursele utilizate de fiecare proces sau serviciu ce rulează

Performance Monitor

- Folosind pentru afişarea de statistici în timp real
- Poate afişa date salvate intr-un log
- Este foarte configurabil, poate afişa sute de diferite tipuri de statistici (denumite “performance counters”) prin intermediul unui grafic
- Adăugarea de noi date este foarte simplă şi se bazează pe următoarele patru informaţii
  - Calculator
  - Obiectul analizat
  - Particularitate a obiectului ce trebuie analizat
  - Instanţa obiectului ce trebuie analizat

Reliability Monitor

- Este un feature nou pentru Windows Server 2008
- Monitorizează evenimentele ce au un efect negativ asupra sistemului
- Calculează o notă de stabilitate a sistemului pentru fiecare 24 de ore în care sistemul a rulat
- Pentru a putea determina cauza scăderii ratei de stabilitatea, se înregistrează şi principalele puncte referitoare la reconfigurarea sistemului

Resurse de monitorizat – Procesorul

- Processor: % Processor time
  - procent din timp în care procesorul este încărcat
  - trebuie să fie cât mai mic, recomandat sub 85%
  - dacă valoarea este prea mare trebuie determinat care este procesul care are nevoie de mai multe resurse
- System: Processor Queue Length
  - numărul de fire de execuţie ce aşteaptă să fie executate
  - trebuie să fie cât mai mic, recomandat sub 10

Resurse de monitorizat – Procesorul

- Server Work Queues: Queue Length
  - număr de cereri ce trebuie executate de către un procesor
  - valoarea trebuie să fie cât mai mică, recomandat sub 4
- Processor: Interrupts/sec
  - numărul de întreruperi pe care un procesor îl prelucrează la fiecare secundă
  - această valoare poate varia destul de mult
  - trebuie comparată cu o rată prestabilită, calculată atunci când încărcarea pe server nu este foarte mare
  - un echipament hardware ce generează prea multe întreruperi poate monopoliza un procesor

Resurse de monitorizat – Memoria

- Memory leak
  - reprezintă alocarea de memorie de către un program, memorie ce nu a fost eliberată la terminarea rulării programului
  - de cele mai multe ori sunt generate de către aplicaţii, dar există şi astfel de probleme generate de sistemul de operare
  - pot fi foarte rapide, ducând la o "îngheţare" bruscă a sistemului
  - cele lente pot fi foarte greu de observat
- În timp memorie disponibilă se poate micşora foarte mult, ducând chiar şi la "îngheţarea sistemului de operare"

Resurse de monitorizat – Memoria

- Memory: Page Faults/Sec
  - datele sau codul necesar pentru rularea unui program nu se găsesc în memorie
  - valoarea trebuie să fie cât mai mică, recomandare sub 5
  - poate fi cauzată de un număr mare de programe ce rulează şi insuficientă memorie, sau de un program care nu adresează zonele de memorie corespunzător
- Memory: Pages/Sec
  - de câte ori informaţia necesară a fost adusă de pe disk în memorie, sau scrisă pe disk pentru eliberarea de memorie
  - valoarea trebuie să fie cât mai mică, recomandare sub 20

Resurse de monitorizat – Memoria

- Memory: Available Mbytes
  - memorie fizică disponibilă în megabytes
  - valoarea trebuie să fie cât mai mare, nu mai mic de 5%
  - pentru Windows Server 2008 recomandarea este de cel puţin 2 GB
- Memory: Committed Bytes
  - memoria virtuală ce are spaţiu rezervat pe disk
  - valoarea trebuie să fie cât mai mică, sub memoria RAM existentă
- Memory: Pool Non-paged Bytes
  - memoria folosită de sistemul de operare, ce nu poate fi scrisă pe disk
  - acest număr ar trebui să fie o valoare stabilă, creşterea sa este în concordanţă cu creşterea activităţii serverului

Resurse de monitorizat – Hard-disk

- Problemele ce pot apărea sunt de cele mai multe ori strâns legate de defectarea echipamentului
- La selectarea unui hard-disk pentru un server trebuie avut în considerare şi rolul serverului în reţea
  - server de fişiere => spaţiu de stocare mai mare
  - server de AD => viteza de rotaţie mai mare
- Soluţiile în cazul unor probleme pot fi
  - instalarea unui dispozitiv mai rapid
  - instalarea mai multor dispozitive pentru distribuirea modului de acces la date
  - folosirea de sisteme RAID

Resurse de monitorizat – Hard-disk

- PhysicalDisk: Disk Bytes/sec
  - media numărului de biţi transferaţi către/de pe disk per secundă
  - această valoare ar trebui să fie stabilă în cazul în care serverul nu este folosit pentru stocarea de fişiere
  - scăderea acestei valorii poate însemna defectarea hard-disk-ului
- PhysicalDisk: Current Disk Queue Length
  - numărul de cereri de scriere-citire în aşteptare
  - valoarea trebuie să fie cât mai mică, recomandare sub 2 per dispozitiv
  - o valoare ridicată poate însemna defectarea echipamentului, sau o viteză de scriere-citire prea mică în comparaţie cu necesităţile serverului

Resurse de monitorizat – Hard-disk

- PhysicalDisk: % Disk Time
  - procentul de timp în care dispozitivul este ocupat
  - valoarea trebuie să fie cât mai mică, recomandare sub 80%
  - pentru o valoare prea mare verificaţi dacă există "memory leak", sau funcţionalitatea corectă a echipamentului
- LogicalDisk: % Free Space
  - specifică valoarea procentuală a spaţiului liber disponibil pe disk
  - această valoare trebuie să fie cât mai mare, recomandare de peste 20%

Resurse de monitorizat – Reţeaua

- Network Interface: Bytes Total/sec
  - număr de biţi primiţi/trimişi pentru interfaţa specificată
  - această valoare ar trebui să fie constantă
  - creşterea valorii poate reprezenta un atac de tip DDOS; scăderea acestei valori poate reprezenta o defectare a plăcii de reţea
- Network Interface: Output Queue Length
  - specifică numărul de pachete ce asteaptă în memorie să fie trimis pe reţea
  - această valoare trebuie să fie cât mai mică, recomandare de 0
  - un număr mare înseamnă în cele mai multe cazuri defectarea plăcii de reţea
- Server: Bytes Total/Sec
  - numărul total de biţi trimis de server pe toate interfeţele sale
  - valoarea recomandată este de sub 50% din capacitatea totală

Data collector sets

- Pentru salvarea anumitor statistici folosind consola Reliability and Performance Monitor trebuie creat un "data collector set"
- Datele astfel colectate pot veni din diverse surse
  - performance counters
  - event traces
  - Windows registry
- Există predefiniţi collectori pentru
  - LAN Diagnostics
  - System Diagnostics
  - System Performance

Reports

- După definirea unui set de date ce vor fi colectate se execută o analiză a sistemului pentru datele interesante
- Fiecare "data collector set" poate fi executat manual de către administrator, sau poate fi planificat
- După executie se generează un raport, fiecare raport este evidenţiat prin nume şi ora la care a fost generat
- Rapoartele pot fi vizualizate sub formă de tabel, identic cu metodele de afişare din Performance Monitor

Audit

- Procesul prin care un administrator poate monitoriza anumite evenimente
- Implicit este dezactivat
- Activarea se face prin intermediul “Local Security Policy”
- După activare, monitorizarea se realizează folosind Event Viewer
- Pentru auditarea accesului la fişiere trebuie specificat utilizatorul pentru fiecare fişier
  - hard-disk-ul trebuie să fie formatat NTFS

Run a task on event

- Fiecare eveniment generat poate avea un task atasat
- Există trei posibile acţiuni ce se pot rula la generarea unui eveniment
  - Run a program
  - Send a message
  - Display a message
- Toate aceste task-uri pot fi administrate prin intermediul “Task Scheduler” -> Event Viewer Tasks