Modul 11 – Lab: Monitorovanie výkonu a prehliadač udalostí

Príprava
Prihláste sa na PC1 ako užívateľ ADMIN s heslom Pa$$w0rd.

Skúmanie správcu úloh a monitorovanie zdrojov

- Stlačte kombináciu kláves ľavý Ctrl+Shift+Esc
- V okne správcu úloh si prezrite záložku aplikácie.
- V hornom menu kliknite na Options – a zrušte zaškrtnutie Always on top
- Kliknite na Start a do poľa vyhľadávania zadajte cmd.exe a potvrďte stlačením Enter
- Na príkazovom riadku spustite programy calc.exe a write.exe
- Prezrite si zoznam aplikácií v správcovi úloh
- Na záložke Applications kliknite pravým na program „Document-Wordpad" a vyberte voľbu „Go to process"
- Na záložke Processes kliknite pravým na zvýraznený program wordpad.exe a vyberte možnosť End Process
- V zobrazenom dialógu „Windows task manager" potvrďte uzatvorenie procesu voľbou End process
- Všimnite si, že aplikácie príkazového riadku a kalkulačky stále bežia
- V správcovi úloh vyberte záložku applications, pravým kliknutím vyberte aplikáciu s ikonou príkazového riadku a opäť vyberte voľbu „Go to process"
- Na záložke Processes pravým kliknutím vyberte zobrazený príkazový riadok cmd.exe a vyberte voľbu „End process tree" – potvrďte rovnakú voľbu v dialógovom okne
- Všimnite si, že ukončenie stromu procesu cmd.exe spôsobilo i ukončenie dcérskej aplikácie Calc...
- V správcovi úloh v s v processes from all users"
- Prezrite si rozšírený na záhlavie s označením „User name" zoraďte spustené p ateľov)
- Kliknutím na záhlav ých úloh podľa zaťaženia procesora

- V menu View vyberte voľbu „Select columns" a v menu pridajte zaškrtnutie pri PID (Process ID) a potvrďte voľbou OK
- Prezrite si popisy spoustených procesov v stĺpci Description
- Kliknite na ľubovoľný proces pravým tlačítkom a vyberte voľbu Properties. Prezrite si záložku General a Details – uzavrite okno vlastností procesu.
- Kliknite na záložku Services a vyhľadajte službu s názvom Spooler – prezrite si jej popis v stĺpci Description.
- Kliknite pravým na službu Spooler a ukončite bežiacu službu stlačením Stop service
- Prepnite sa na záložku Performance a prezrite si zaťaženie procesora a pamäte v hornej časti a dvojitým kliknutím do grafu si zobrazte hodnoty detailne.
- Stlačte tlačítko „Resource monitor"
- Prezrite si zobrazené grafy pre meranie zaťaženia systému
- V pravej časti Resource overview kliknite na graf CPU a v ľavej časti si prezrite rozbalený výpis v príslušnej sekcii. Zaškrtnite ľubovoľný proces a všimnite si oranžový graf vo výpise, ktorý ukazuje vyťaženie komponentu daným procesom. Zrušte zaškrtnutie pre akýkoľvek proces.
- Kliknutím na jednotlivé záhlavia zoraďte prehľad zaťaženia procesora jednotlivými programami
- Rovnakým spôsobom si prezrite zaťaženie pamäte a disku – pokiaľ sa v nich nič neobjavuje a vidíte len oranžový pruh Filtered by perfmon.exe, potom sa presvedčte, že ste pri sledovaní procesora zrušili všetky zaškrtávatka.
- V ľavej časti okna sa prepnite na záložku CPU. Všimnite si, že môžete vidieť nie len vyťaženie CPU jednotlivými procesmi, ale aj služby, ktoré tieto procesy spúšťajú.
- Na záložke Network si rozkliknite položku Network activity a Listening ports.
- Uzavrite okno Resource monitor

Skúmanie spoľahlivosti a zaťaženia

- Kliknite na Start a pravým kliknutím vyberte Computer a v zobrazenom menu vyberte možnosť Manage
- V konzole Computer management v hornej sade ikon kliknite na ikonu s popisom Show/Hide action pane
- V sekcii System tools rozbaľte uzol Perfmormance – Monitoring tools

- Kliknite na Performance monitor a v pravej časti kliknite pravým do plochy grafu a vyberte voľbu Add counters
- V dolnej časti zaškrtnite voľbu Show description
- V hornej časti rozbaľte skupinu Processor a kliknite na počítadlo % Processor Time
- Prezrite si zobrazenú nápovedu v spodnej časti obrazovky
- Pridajte počítadlo do zoznamu kliknutím na tlačítko Add
- Rovnakým spôsobom si prezrite nápovedu a pridajte počítadlo zo skupiny „Physical disk" s názvom „Average Disk Queue Length" a tiež počítadlo zo skupiny „Memory" s názvom „Available MBytes"
- Potvrďte výber kliknutím na OK a v zobrazenom grafe si prezrite grafy pre jednotlivé pridané položky
- Opakovane stlačte Ctrl+G a prejdite si jednotlivé typy náhľadov na dáta
- V spodnej časti si vyberte ľubovoľné počítadlo a stlačte Ctrl+H pre zvýraznenie grafu
- V spodnej časti obrazovky si zobrazte vlastnosti jednotlivých počítadiel a vhodnou zmenou hodnoty Scale si zmeňte zobrazované veličiny tak, aby sa vošli do zobrazovaného grafu.
- Pravým kliknutím na uzol Performance monitor v ľavej časti vyberte voľbu New – „Data Collector Set", čím si uložíme výber nami nakombinovaných počítadiel
- V poli Name ponechajte východiskový názov a kliknite na Next
- V poli Root directory si prezrite východiskové umiestenie pre dáta zbierané z počítadiel a kliknite na Next
- V časti Run as si všimnite, že vytváranú kolekciu môžete spúšťať pod iným účtom
- Ponechajte východiskové voľby a kliknite na Finish

Skúmanie sady kolekcie dát

- V ľavej časti rozbaľte uzol „Data collector sets" a User defined
- Prezrite si východiskové vlastnosti novo vytvárenej kolekcie „New data collector set"
- Na záložke General si prezrite a poznamenajte východiskové umiestnenie logov s nazbieranými dátami
- Na záložke Stop condition si všimnite, že východiskové nastavenia nikdy neukončia zber dát
- Zaškrtnite voľbu Duration a nastavte limit na 20s

- Potvrďte voľby stlačením Apply a OK
- V ľavej časti okna vyberte pravým kliknutím „New Data Collector Set" a vyberieme voľbu Start – týmto spustíme zber dát našich počítadiel po zvolenú dobu 20s
- Prezrite si zmenu ikony pri „New Data Collector Set" v dobe, keď prebieha zber dát

Prezeranie nazbieraných dát v Monitorovaní výkonu

- Po ukončení zberu dát v ľavej časti kliknite na Reports – User defined – New Data Collector Set a vyberte ikonu logu s nazbieranými dátami
- Prezrite si graf zobrazený v pravej časti
- V spodnej časti si prezrite možnosť obmedziť zobrazené obdobie z doby, keď prebiehal zber dát
- V zobrazenom grafe vyberte určité časové obdobie, v ktorom je pozorovateľná zmena niektorých veličín
- Pravým kliknutím do zvoleného výseku a výberom Zoom To nechajte zobraziť detailné informácie zo zvoleného obdobia – všimnite si znázornenie vybraného úseku na posuvníku pod grafom
- Môžete upraviť vlastnosti jednotlivých počítadiel tak, aby vhodná mierka (scale) umožnila zobrazenie vo vybranom období
- Na posuvníku pod grafom uchopením a pretiahnutím okrajov výseku roztiahnite výber na celé obdobie a pravým kliknutím do plochy grafu vyberte voľbu Zoom To, čím sa zobrazí graf za celú dobu zberu dát

Spustenie vstavaných kolekcií dát

Prezrite si vstavané kolekcie dát pre sledovanie výkonu:

- V ľavej časti vyberte „Data collector sets" – System – „System performance", v pravej časti si zobrazte vlastnosti Performance counter a prezrite si zbierané počítadlá a umiestnenie súborov logu
- Uzavrite vlastnosti Performance counter
- V ľavej časti vyberte pravým kliknutím „System performance" a zvoľte Start
- Behom zberu dát (približne 1 minúta) môžete na virtuálnom počítači vykonávať rôzne akcie a zaťažiť tak systém (pridávanie súborov do ZIP archívu, počítanie v kalkulačke, mnoho paralelných kopírovaní a čítaní a pod.)

- Po uplynutí jednej minúty od spustenia zberu dát rozbaľte v pravej časti uzol Reports – System – System Performance – a kliknite na posledný report
- Prezrite si detailný výpis v pravej časti – hodnotenie zaťaženia jednotlivých komponentov i výpis zaťaženia komponentov jednotlivými programami
- V ľavej časti konzoly vyberte posledný report, pravým kliknutím vyberte View a zvoľte zobrazenie „Performance Monitor"
- V ľavej časti konzoly vyberte posledný report, vyberte pravým kliknutím View a zvoľte zobrazenie Folders
- Prezrite si obsah priečinku s výpisom reportu v HTML formáte

Prezeranie udalostí

- V konzole správy počítača v sekcii System Tools rozbaľte uzol Event Viewer
- V sekcii Windows Logs – System si prezrite jednotlivé udalosti
- Kliknite myšou do oblasti udalostí a stlačte Ctrl+F pre detailné prehľadávanie všetkých zobrazených udalostí a do vyhľadávacieho poľa napíšte: **service was started** a kliknite na voľbu Find
- Prehliadač udalostí prejde všetky udalosti v systémovom logu a zobrazí prvú nájdenú správu
- Dvojitým kliknutím vyberte nájdenú správu a prezrite si detailné informácie v spodnej časti
- Všimnite si zobrazené ID udalosti (EventID): 6005

Pozn.: Uvedená udalosť oznamuje spustenie Logovania a spravidla probieha pri spustení systému.

- V ľavej časti okna vyberte pravým kliknutím System log a vyberte voľbu Filter current log
- V poli EventID uveďte hodnotu 6005 a v dolnej časti potvrďte filtrovanie voľbou OK
- Filtrovanie ukazuje len udalosti 6005 – prezrite si časy, kedy bol Váš systém reštartovaný
- Zrušte filtrovanie zobrazenia pravým kliknutím na System log v ľavej časti okna a vyberte voľbu Clear Filter
- V ľavej časti okna vyberte pravým kliknutím Application log a vyberte voľbu Filter current log
- V hornej časti zvoľte zobrazenie udalostí s úrovňou Critical, Error, Warning a potvrďte OK
- Prezrite si zobrazené chyby aplikácií, ku ktorým došlo na PC1
- V ľavej časti okna vyberte pravým kliknutím Application log a vyberte voľbu Save Filtered log file as ...

- Uložte filtrovaný výpis do dokumentov pod názvom AppErr.txt a v dolnej časti v poli Save type as vyberte typ TXT
- Prezrite si v prieskumníkovi uložený log

Pozn.: Pre podrobnejšiu analýzu je možné log ukladať vo formáte CSV, ktorý sa dá spracovať v Exceli či v databázi.

Vytváranie vlastných pohľadov

- V ľavej časti okna vyberte pravým kliknutím Application log a vyberte voľbu Save Filter to Custom View
- V poli Name napíšte: Chyby aplikácií
- V poli Description napíšte: Prehľad zlyhaní aplikácií na PC1
- V dolnej časti kliknite na voľbu New Folder a napíšte názov: Apps
- Potvrďte voľbou OK
- V ľavej časti okna vyberte pravým kliknutím Application log a vyberte voľbu Clear Filter
- Presvedčte sa, že výpis udalostí v okne je opäť kompletný (zobrazujú sa i správy Information)

Prezeranie a export definície vlastných pohľadov

- V ľavej časti konzoly správy počítača rozbaľte Event viewer – Custom views – Apps – Chyby aplikácií
- Prezrite si filtrovaný pohľad na udalosti aplikácií – tento pohľad je aktualizovaný pri vzniku nových udalostí
- V ľavej časti vyberte pravým kliknutím Chyby aplikácií a voľbu Export custom view
- Uložte XML definíciu svojho pohľadu pod názvom FailedApps.XML
- Prezrite si súbor s definíciou dvojitým kliknutím v prieskumníkovi

Pozn.: Exportovaný pohľad je možné akokoľvek upraviť a potom naimportovať na ľubovoľný počítač.

Prezeranie logov aplikácií a služieb

- V ľavej časti konzoly správy počítača rozbaľte Event viewer – Applications and services logs – Microsoft – Windows – Diagnostics-Performance a prezrite si zoznam udalostí, ktoré sa generovali behom predošlých sledovaní výkonu systému

- Prezrite si log WLAN-Autoconfig s výpisom chýb overovania vo WiFi sieťach a UAC-FileVirtualization s výpisom všetkých presmerovaných zápisov do systémových oblastí a GroupPolicy s výpisom udalostí pri spracúvaní skupinových politík