Administratívne nástroje

Server mannager

Nástroj na základnú správu aktuálnej inštalácie windows servera a jej služby  
 Umožnuje prvotnú po inštalačnú úpravu servera

Dashboard – quick start

Dashboard – roles and server groups

Zobrazuje udalosti pre jednotlivé roly bežiace na serveri

Pre každú rolu upozornuje na problémi s:  
 - manažovateľnosťou  
 - kritickými udalosťami  
 - nefunkčními službamy  
 - preťaženie CPU/RAM  
 - výsledky analís BPA

Local server – properties

Computer Name – umožňuje nastaviť meno počítača (platné v celej sieti)  
 Workgroup – umožňuje nastaviť pracovnú skupinu (počítače v skupine sa navzájom  
 vidia a môžu zdieľať priečinky)  
 Windows Firewall – umožňuje meniť nastavenia firewallu  
 Remote management – umožňuje sprístupniť server pre vzdialenú správu cez  
 administračné nástroje a PowerShell  
 Remote desktop – umožňuje vzdialenú správu servera cez vzdialenú plochu  
 NIC teaming – umožňuje zoskupiť viacero fyzických sieťových kariet do jednej  
 logickej sieťovej karty (alternatíva k Etherchannelu/Cisco resp.   
 Bondingu/Linux)  
 Ethernet – umožňuje zobraziť a meniť nastavenia sieťových kariet  
 Last installed update – informácia o poslednej aktualizácii systému   
 Windows Update – umožňuje zmeniť spôsob sťahovania a inštalácie aktualizácií Last   
 checked for updates – informácia o čase poslednej kontroly aktualizácií Windows   
 Defender – umožňuje meniť nastavenia antivírusovej ochrany Feedback & Diagnostics –  
 umožňuje nastaviť, aké informácie sa budú zdieľať so spoločnosťou   
 Microsoft pri riešení problémov so systémom   
 IE Enhanced Security Configuration – umožňuje zapnúť/vypnúť zvýšenú ochranu v   
 internetovom prehliadači Internet Explorer   
 Time zone – umožňuje nastaviť časovú zónu, v ktorej sa server nachádza Product ID –   
 zobrazenie/zmena informácií o aktivácii systému

Local events – events

Udalosti hodné pozretia za posledné časové obdobie na aktuálnom serveri

Local events – services

Zobrazuje stav služieb v systéme (bežiace a zastavené)  
 napr. logy (v linuxe /var/log...)(W c:\windows\system32\winevt\Logs)

Local server – best practices analyzer

zoznam odporúčaní pre jednotlivé bežiace služby pre zachovanie ich najlepšieho výkonu

local server – performance

grafické zobrazenie využitia procesora a voľnej pamäti v serveri

local server – roles and features

zoznam najinštalovanejších rolí a súčastí systému a možnosti ich pridania a   
 odinštalovania

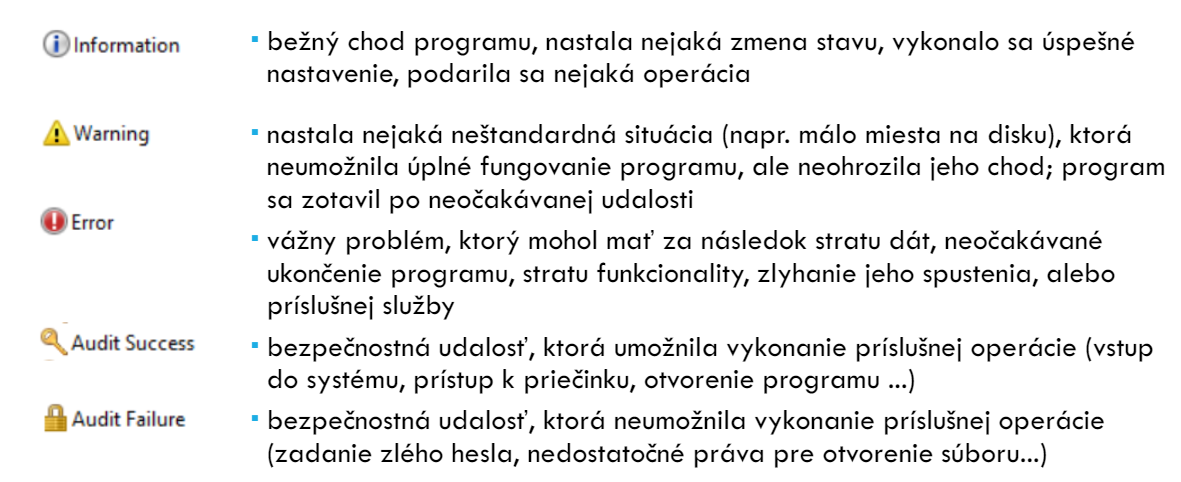
control panel

event viewer

Nástroj na prezeranie udalostí (eventov), ktoré vznikli v systéme

Udalosti zapisujú programy a služby   
(programátori pri ošetrovaní rôznych chýb a udalostí vo svojich aplikáciách využili funkcie operačného systému, ktoré im umožňujú zapisovať tieto udalosti do spoločnej databázy)

* mechanizmus zapisovania denníkov vstavaný do Windows systémov
* Uchováva záznamy z operačného systému
* Uchováva záznamy z aplikácií nainštalovaných do systému
* Je veľmi užitočný pri odhaľovaní problémov
* Je tiež užitočný pre riešenie bezpečnostných incidentov

Úrovne hlásenia  
  
 

Hlavné denniky (logy)

Applications  
 obsahuje info od doplnkových programov windowsu

Security  
 obsahuje info o prístupe k zdrojom, prihláseniach a odhláseniach

Setup  
 info o inštalácií programov, updatov, rolí a súčastí systému

System  
 info o problémoch s hardvérom, ovládačmi, sieťou a iné core súčasti

Aplication and services  
 detailnejšie info od súčasti systému + info o programoch 3tych strán

Počítače môžeme nastaviť tak, aby svoje (vybrané) logy zasielali na centrálny zberný počítač (collector)

To nám umožňuje lepšiu kontrolu nad tým, čo sa na počítačoch v sieti deje, rýchlejšiu detekciu bezpečnostných incidentov, či riešenie problémov

Na zdrojových počítačoch musíme definovať tzv. subscription

Subscription

obsahuje:   
 Meno (a popis)   
 Cieľ, kam sa majú logy ukladať   
 Kto vyvoláva zápis – kolektor alebo zdrojový počítač   
 Zoznam udalostí pre zber (definuje sa rovnako ako filter log)   
 Účet, pod ktorým sa majú kontaktovať vzdialené počítače pre zber logov