SOFTWARE-SKI ALATI ZA ODRŽAVANJE RAČUNARSKIH SISTEMA

SOFTWARE TOOLS FOR MAINTENANCE OF COMPUTER SYSTEMS

M.Sc. Suad Sućeska CCNA™
Sarajevo

REZIME

Održavanje računarskih sistema obuhvata održavanje hardware-a i održavanje software-a. Novije informatičke tehnologije omogućavaju dobivanje podataka o hardware-u i software-u bilo koje komponente računarskog sistema. Iz dobivenih podataka se može odrediti stanje računarskog sistema u cjelini, kao i njegovih pojedinih komponenti. Redovno dobivanje i pregled ovih podataka predstavlja redovni nadzor. Dijagnostika se primjenjuje kada je problem prisutan u računarskom sistemu i treba ga odrediti i rješiti. Članak prezentira software-ske alate za nadzor i dijagnostiku za održavanje računarskih sistema.

Ključne riječi: održavanje, računarski sistem, nadzor, dijagnostika, software-ski alat

SUMMARY

Computer systems maintenance includes maintenance of hardware and maintenance of software. New informatics technologies enable getting data of hardware and software any computer system component. From those data condition of all computer system could be determined, as well as condition of any of its particular components. Getting and monitoring these data regularly is called regular maintenance (structured tasks). Diagnostics is applied when a problem is present in computer system which should be determined and solved. The article introduces the software tools for monitoring and diagnostics for computer systems maintenance.

Keywords: maintenance, computer system, monitoring, diagnostics, software tool.

1. UVOD

Održavanje računarskih sistema obuhvata održavanje hardware-a i održavanje software-a. Novije informatičke tehnologije omogućavaju dobivanje podataka o hardware-u i software-u bilo koje komponente računarskog sistema. Iz dobivenih podataka se može odrediti stanje računarskog sistema u cjelini, kao i njegovih pojedinih komponenti. Redovno dobivanje i pregled ovih podataka predstavlja redovni nadzor. Dijagnostika se primjenjuje kada je problem prisutan u računarskom sistemu i treba ga odrediti i rješiti. Održavanje obuvata i: planiranje proširenja računarske mreže, dokumentiranje mreže i bilo kakvih izmjena na mreži, kontrolu slaganja sa utvrđenom politikom, osiguravanje mreže od internih i eksternih prijetnji. Članak prezentira software-ske alate za nadzor i dijagnostiku koji se koriste za održavanje računarskih sistema. Jedan dio ovih alata dolazi sa operativnim sistemom (MS Windows), drugi dio su posebni programi koje je potrebno instalirati na računar.

U literaturi se mogu naći već urađeni modeli održavanja na kojima se može bazirati i spostveni model, a to su:

1) FCAPS (Fault, Configuration, Accounting, Performance, Security) – je ISO (International Organization for Standardization) model održavanja mreže.
2) ITIL (IT Infrastructure Library) – je skup preporuka iz prakse koji omogućavaju obavljanje poslovnih zadataka.
3) TMN (Telecommunications Management Network) – je model vođenja mreže od ITU-T (International Telecommunication Unon – Telecommunications Standardization Sector). Namjenjen je za vođenje telekomunikacijskih mreža.
4) Cisco Livecycle Services – je Cisco model održavnja koji definira slijedeće faze u životu Cisco-ve tehnologije na mreži: pripremanje, planiranje, dizajn, implementiranje, rad i optimiziranje.

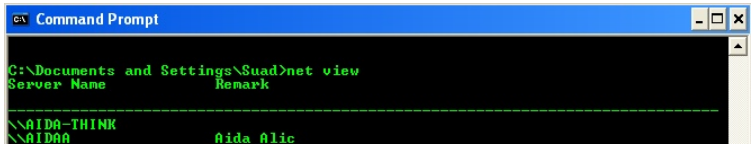
Za održavanje i dijagnostiku mreže je potrebno koristiti software-ske, pa i hardware-ske alate. Ovaj članak navodi i daje kratak opis slijedećih software-skih alata za održavanje računarske mreže: Net View, EventViewer, TaskList, TaskManager, Performance, System Information, Power Shield, Wire Shark, Symantec SEP, Ping, Tracert i Telnet.

2. **CLI** (Command Line Interface) **ALATI**

2.1. NetView

Net View je CLI (Command Line Interface) program pomoću kog se može dobiti spisak računara na domenu ili nekoj radnoj grupi (workgroup). Nepokazivanje ostalih računara ili dijela računara koji su priključeni na neki switch ukazuje na problem povezivosti na mreži koji treba dalje rješavati. Dobiveni listing se za analizu i dokumentiranje može eksportirati u fajl sa nekom od slijedećih ekstenzija: txt, doc, xls, csv. Sintaksa za korištenje ovog programa je:
NET VIEW [\\computername [/CACHE] | /DOMAIN[:domainname]]

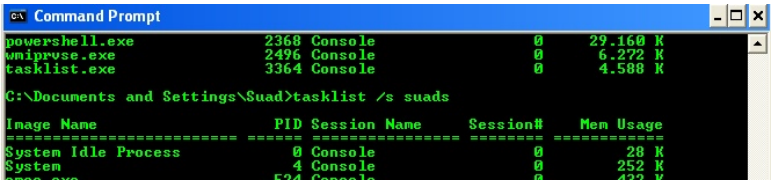
Za dobivanje računara domena u kojem je i lokalni računar nije potrebno navoditi nikakve parametre.



Slika 1: Net View

2.2. TaskList

TaskList je CLI program koji daje listu aplikacija i servisa koji rade na lokalnom ili udaljenom računaru. Sintaksa je :
tasklist [.exe] [/s computer] [/u domain\user [/p password]] [/fo {TABLE|LIST|CSV}] [/nh] [/fi FilterName [/fi FilterName2 [...]]] [/m [ModuleName] | /svc | /v]



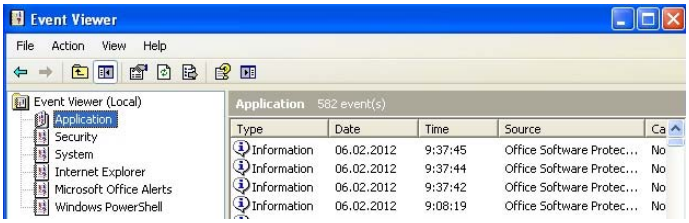
Slika 2: TaskList

Ovaj program omogućava da se iz dobivenog spiska aplikacija i servisa koji trenutno rade na nekom računaru utvrdi da li u pozadini na računaru radi neki maliciozni program, da se taj program odmah zatvori kako ne bi ometao rad računara i širio na druge računare u mreži.

3. PROGRAMI SA KORISNIČKIM SUČELJEM

3.1. Event Viewer

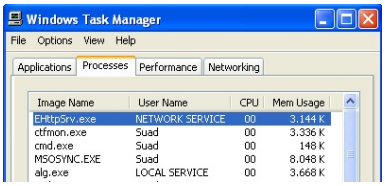
EventViewer je dnevnik (logger) koji se instalira sa Microsoft-ovim operativnim sistemima Windows. On ima grafičko sučelje i bilježi sve aktivnosti računara. Program dolazi sa osnovnim dnevnicima za aplikacije (Application), sigurnost (Security) i sistem (System). Pojedini programi instaliraju svoje dodatne dnevnike: Internet Explorer, Microsoft Office, Power Shell. Korisnik može kreirati i svoj sopstveni dnevnik. Sa odgovarajućim pravima na mreži program omogućava pregledanja dnevnika i na drugim računarima na mreži. Omogućena su brza pretraživanja i filtriranja postojećih podataka dnevnika. Prednost ovog programa je da omogućava nalaženje događaja koji je bitnije uticao na rad računara.



Slika 3: Event Viewer

3.2. Task Manager

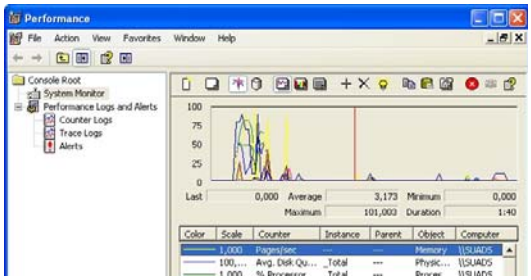
Zgodan program sa grafičkim sučeljem za pregledanje programa i procesa na lokalnom računaru je Task Manager. Ovaj program omogućava pregledanje i zatvaranje programa i procesa koji trenutno rade na računaru, resurse koje oni koriste na računaru (procesor – CPU, page file, ukupnu memoriju, fizičku memoriju, memoriju za kernel), procentualno opterećenje raznih mrežnih konekcija (LAN, Wireless), kao i korisnike koji pristupaju računaru sa stanjem i nazivima njihovih sesija.



Slika 4: Task manager

3.3. Performance

Za detaljno pregledanje zauzetosti resursa lokalnog ili udaljnog računara može se koristiti Performance (Perfmon, Performance Monitor). Program se instalira sa Windows-ima, ima grafičko korisničko sučelje, ali se može koristiti i sa CLI. Ovaj program omogućava grafičko praćenje sistemskih resursa, ali i kreiranje tekstualnih dnevnika (Counter i Trace) i upozorenja (Alerts).

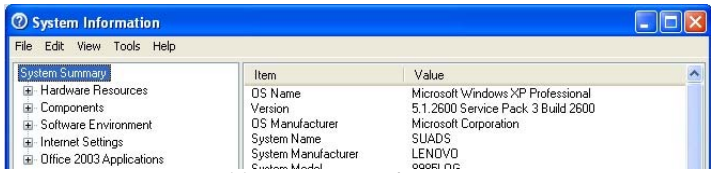


Slika 5: Performance

Ovaj program se može koristiti za kreiranje baseline-a koji treba da sadrži uobičajne karakteristike određenih brojača. Grafikoni baseline-a se mogu koristiti za poređenje sa graficima ili logovima kreiranim za vrijeme nekog neuobičajeneog stanja mreže. Obično se izvodi na serverima. Najčešće korišteni brojači za opis stanja računara su: Memory\Page/sec (default), PhysicalDisk\Avg. Disk Queue Length (default), Processor\% Processor Time (default), Physical Disk\Disk Reads/sec, Physical Disk\Disk Writes/sec, Physical Disk\Current Disk Queue Length, Physical Disk\% Disk Time, LogicalDisk\% Free Space, Processor\% Processor Time, Processor\Interrupts /sec, Processor\% Interrupt Time, Processor\% User Time, Processor\%Privilege Time, Processor\%DPC Time, Process\% Processor Time, System\Processor Queue Length, System\System Calls/sec, System\% Total Processor Time, System\% Total User Time, System\% Total Privledge Time, System\% Total Interrupt Time, Thread Object\% Processor Time, Thread Object\ID Thread, Thread Object\Priority Base, Process\Process ID, Process\% Processor Time, Process\% User Time.

3.4. System Information

Za dobivanje detaljnih podataka o lokalnom ili udaljenom računaru na mreži može se koristiti program System Information. Ovaj program se nalazi u:
Start/AllPrograms/Accessories/System Tools/System Information.
Program se može koristiti sa korisničkim sučeljem ili sa CLI. Ovim programom se mogu dobiti slijedeći podaci: pregled sistema (System Summary), hardware-ski resursi (Hardware Resources), komponente (Components), operativni sistem (Software Environment), parametri za Internet (Internet Settings), MS Office aplikacije (Office Applications). Program se može korisititi i sa CLI, a sintaksa je:
SYSTEMINFO [/S system [/U username [/P [password]]]] [/FO format] [/NH]

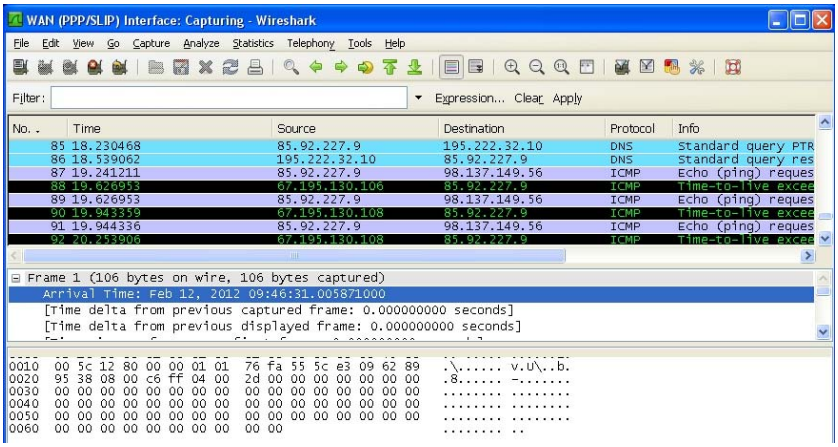


Slika 6: System Information

3.5. WireShark

Za pregled saobraćaja na mreži potrebno je koristiti neki od programa iz vrste network protokol analajzera (MS Network Monitor, WireShark). Ovo su besplatni programi sa korisničkim sučeljem koje je potrebno instalirati na računar. Za preuzimanje svih paketa sa mreže u nekom vremenskom intervalu potrebno je parametre programa posebno podesiti, inače se preuzimaju samo paketi poslati na računar. WireShark je open source software.

Radna ploča je podjeljena u tri dijela: Packet List, Packet Details, Packet Bytes. Packet List daje listu uhvaćenih paketa sa podacima: vrijeme, pošiljalac, odredište, protokol i dodatne informacije. Paket Details daje više podataka o poljima paketa odabranog u okviru Packet List. Packet Bytes daje podatke u heksadecimalnoj formi o paketu odabranom u okviru Packet List. Program omogućava kreiranja filtera koji mogu uzimati samo određene pakete sa mreže i time čuvati buffer od nepotrenih paketa. Za uhvaćene pakete se takođe mogu kreirati filteri za pregledanje samo određenih podataka. Filteri mogu biti postavljeni na: adresu pošiljaoca, odredišnu adresu i/ ili protokol.



Slika 7: WireShark

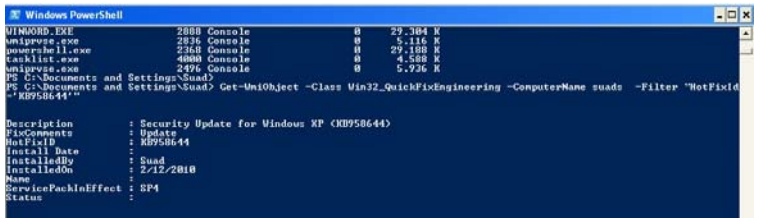
Program je korisno koristiti zato jer se mogu odrediti paketi sa malicioznim sadržajem, a iz njih i podaci o zaraženom računaru, web site-u sa kojeg se dobiva maliciozni sadržaj, itd. Takođe ga je dobro koristiti za uklanjanje nepotrebnog saobraćaja na mreži.

3.6. Symantec SEP

Administratorske kozole antivirusnih programa (Symantec SEP, ESET NOD32) su vrlo korisni alati za nadzor i polazno rješavanje problema na mreži koje izazivaju razne sigurnosne prijetnje. Ovi alati daju spisak svih računara na mreži sa označenim zaraženim računarima. Takođe su omogućena razna grupiranje računara, kreiranja raznih profila, udaljena instalacija i update, automatsko ažuriranje definicija virusa, i drugo.

4. POWER SHIELD

Power Shield sa novom ljuskom koja bazira na .Net-u proširuje mogućnosti CLI programa za administriranje lokalnih i udaljenih računara. Novosti u odnosu na CLI koje ovaj program daje su: kreiranje skripti u fajlovima sa .ps1 ekstenzijom, pipe line, selektiranja, filtriranja, i mnogo granularniji pristup bilo kakvim podacima sa lokalnog ili udaljenog računara. Programi koji rade u CLI se mogu pokrenuti i iz ovog sučelja.

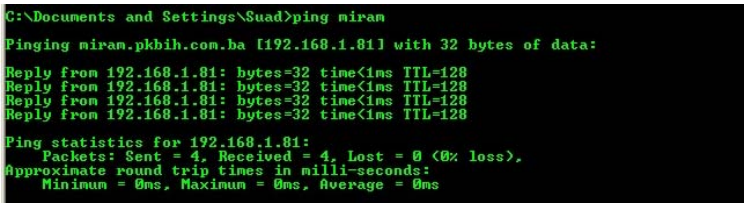


Slika 7: Power Shield

5. CLI PROGRAMI NA RAČUNARIMA, SWITCH-EVIMA I ROUTER-IMA

5.1. Ping

Ping je CLI program kojim se kontrolira IP povezivost na drugi host. Program bazira na ICMP (Internet Control Message Protocol) protokolu. Jedan host drugom šalje ICMP Echo Request, a od njega dobiva ICMP Echo Reply poruku. Sintaksa za korištenje programa je:
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] target_name
Pristup drugom host-u može biti zaustavljen firewall-om ili sistemskim postavkama na nekom od router-a između njih. Program se može koristiti na računarima, router-ima i switch-evima. Na router-ima i switch-evima može se koristiti i prošireni ping (extended).

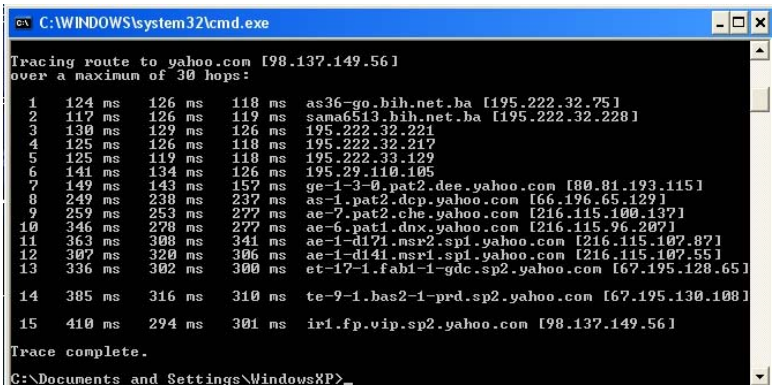


Slika 8: Ping

5.2. Tracert

Tracert je CLI program kojim se može pratiti put do odredišnog host-a. Program također bazira na ICMP protokolu, tj. na Echo Request i Echo Reply porukama, ali stalno povećava TTL (Time To Live) poruke za 1. Sintaksa je:
tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

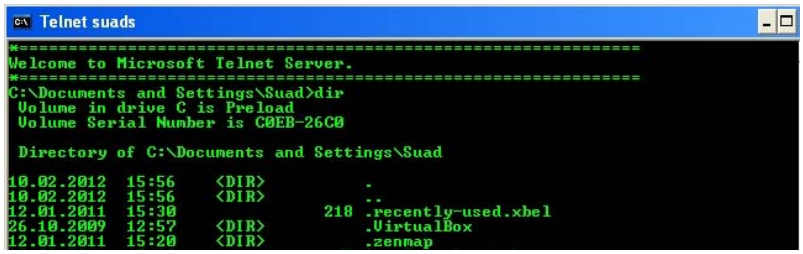
Program je vrlo koristan kada treba odrediti na kojem router-u se prekida konekcija na drugi host. Program se može koristiti na računarima, router-ima i switch-evima. Na router-ima i switch-evima se koristi naredba traceroute.



Slika 9: Tracert

5.3. Telnet

Telnet je program koji omogućava konektovanje sa jednog na drugi host i rad na njemu u okviru terminala sa lokalne konzole. Sastoji se iz Telnet Client-a i Telnet Server-a. Client se može konektovati na Server i na njemu pokretati aplikacije u character modu. To znači da se sa host-a (računar, router, switch) može pristupiti drugom udaljenom hostu i na njemu raditi sa aplikacijama koje se mogu pokrenuti u okviru terminala. Na ovaj način se mogu dobiti podaci sa drugog host-a, ali takođe i izmjeniti njegova konfiguracija. Sintaksa je:
telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]



Slika 10: Telnet

Veliki nedostatak Telnet-a je što se sav saobraćaj između dva hosta prenosi kao tekst. Zato se u novije vrijeme koristi SSH, program koji koristi istoimeni protokol, a koji enkriptira sav saobraćaj koji se prenosi između dva hosta. Ovaj tekst nije lako pročitati. Za korištenje SSH potrebno je dodatno kofigurirati host-ove.

5.4. Naredbe za dobivanje trenutne konfiguracije router-a i switch-eva

Treba navesti i nekoliko dodatnih naredbi za dobivanje podataka sa router-a i switch-eva radi kontrole njihove konfiguracije:

1) show ip interface brief : daje kratak pregled uključenosti interfejsa i njima dodjeljenih ip adresa
2) show ip route – daje ip routing tabelu router-a
3) show ip protocols – daje podatke o uključenim dinamičkim ip protokolima za rout-iranje

Navedeni programi se koriste za nadzor i dijagnostiku računara i konekcija između računara. Neki od nevedenih programa se mogu koristiti i za otklanjanje problema na računarima i konekcijama između računara.

6. ZAKLJUČAK

Redovni nadzor računarskih sistema je važan za njihovo pravilno funkcioniranje. Na računarskim sistemima se pojavljuju i problemi. Probleme je potrebno prvo dijagnosticirati, a zatim riješiti. Održavanje računarskih sistema obuhvata i redovni nadzor i potrebnu dijagnostiku i rješavanje problema računarskih sistema. Održavanje sistema se, dobrim dijelom, može vršiti pomoću software-skih alata. Neki software-ski alati mogu biti instalirani sa operativnom sistemom, dok je druge potrebno posebno instalirati. Neki software-ski alati rade u CLI, ili novijem Powe Shell okruženju, dok su drugi imaju grafičko sučelje. Software ske alate treba koristiti na računarima, ali i na switch-evima i router-ima.

7. REFERENCE

[1] Windows Power Shell™ Primer, Microsoft Corporation, September 2006

[2] Wallace Kevin: CCNP TSHOOT 642-832 Official Certification Guide, Cisco Press, Indianapolis, Mart 2011