Deo I

Administriranje mreža i sistema

U OVOM DELU

U ovom delu se upoznajemo s dužnostima administratora sistema. Opisani su projektovanje mreže, instaliranje operativnog sistema i rad sa sistemom datoteka i konfiguracionim datotekama operativnog sistema Red Hat Linux.

Poglavlje 1
Dužnosti administratora sistema

U OVOM POGLAVLJU

- Administrator sistema
- Instaliranje i podešavanje servera
- Instaliranje i podešavanje aplikacija
- Pravljenje i održavanje korisničkih naloga
- Pravljenje rezervnih kopija i vraćanje datoteka iz kopija
- Nadgledanje i podešavanje performansi
- Konfigurisanje sistema bezbednosti
- Korišćenje alatki za nadgledanje bezbednosti

LINUX JE VIŠEKORISNIČKI, višeprogramski, celovit operativni sistem, i u tom smislu administrator sistema ima slobodu – i dužnost – koje daleko nadmašuju posao administratora drugih operativnih sistema. Distribucija Red Hat donosi mnoge inovacije koje proširuju obaveze čak i iskusnog korisnika Linuxa. U ovom poglavlju opisaćemo te zahteve.

Administrator sistema Linux

Da bi se koristio Linux, potrebno je mnogo više nego sesti za računar i uključiti ga. Često možete da čujete o „strmoj krivoj učenja“, ali ta obeshrabrujuća fraza može da zavara. Zapravo, Linux je na više načina sasvim različit od većine popularnih operativnih sistema i iako nije teži za učenje od drugih operativnih sistema, može delovati vrlo neobično čak i iskusnom administratoru nekog drugog sistema. Sem toga, povećala se složenost mnogih komponenata distribucije Red Hat, pa će verovatno čak i iskusni administratori sistema Linux pronaći mnogo novog i nepoznatog. Na sreću, postoje alatke koje administraciju sistema čine jednostavnijom nego ranije.

Da ne bude zabune: svaki računar na svetu ima administratora sistema. Većina administratora sistema su oni koji su instalirali i podesili softver i periferne uređaje u vreme isporuke računara. Računari često i ostaju u tom stanju jer većina korisnika retko menja unapred zadate parametre. Međutim, kada korisnik odluči da postavi drugu sliku u pozadinu ili da doda program koji nije isporučen zajedno s računarom, on preuzima poslove administratora sistema.

Ta titula donosi i neke obaveze. Nijedan korisnik čiji je računar povezan sa Internetom, nije imun na posledice lošeg administriranja sistema, kao što su to pokazali distribuirani napadi za uskraćivanje usluga (engl. *DDoS*, *Distributed Denial of Service*) i makro virusi koji su potresali Internet poslednjih godina. Posledice tog računarskog vandalizma (a u nekim slučajevima i krađa) bile bi mnogo manje da su administratori sistema bolje razumeli svoje obaveze.

Administrator Linuxa verovatno bolje razume potrebu aktivne administracije sistema nego obični korisnici koji pretpostavljaju da je dovoljno to što je računar pravilno konfigurisan pre isporuke. Korisnik ili firma koji se odluče za Linux, odlučuju se i da preuzmu kontrolu koju taj sistem nudi i obaveze koje iz toga slede.

Kao moderan višekorisnički operativni sistem, Linux zahteva veći stepen administracije nego neki manje robusni sistemi. Čak i ako koristite samo jedan računar koji se modemom i telefonskom linijom povezuje sa Internetom ili se uopšte ne povezujete, imate pogodnosti da koristite isti sistem kao i neke najveće kompanije na svetu i radićete većinu stvari koje rade IT stručnjaci u tim kompanijama. Administracija sistema podrazumeva izvestan stepen učenja, ali znači i da ćete podešavajući sistem ovladati veštinama i time prerasti običnog „korisnika računara". Administrator sistema Linux ne postaje se samom kupovinom računara, već preuzimanjem pune kontrole nad onim šta i kako računar radi.

Možda ćete podešavati male kućne ili male poslovne mreže koje čine dva ili više računara, od kojih neki možda ne rade pod operativnim sistemom Lunux. Možete biti odgovorni za poslovnu mrežu koju čine desetine računara. Administracija Linuxa je iznenađujuće dosledna, bez obzira na veličinu instalacije. Ona uključuje aktiviranje i podešavanje dostupnih sistemskih funkcija.

Po definiciji, administrator sistema Linux je osoba koja ima pun pristup, odnosno osoba koja je superkorisnik (engl. *super user*) ili osnovni korisnik sistema (engl. *root*). Mogućnosti rada običnog korisnika Linuxa ograničene su, dok superkorisnik ima neograničen pristup svemu – svim korisničkim nalozima, njihovim matičnim direktorijumima i datotekama u njima, svim konfiguracijskim parametrima i svim datotekama sistema. Postoji mišljenje da niko ne treba da se prijavljuje za rad kao superkorisnik zato što poslovi administracije sistema mogu da se obave jednostavnije i bezbednije na neki drugačiji način, o čemu će biti reči kasnije. Administrator sistema ima sva prava na sistemu, tako da je prva njegova dužnost da zna šta radi kako ne bi nešto pokvario.

Po definiciji, administrator sistema Linux je osoba koja ima pun pristup, odnosno osoba koja je superkorisnik sistema.

Reč „dužnosti" nagoveštava da se radi o teškom i mukotrpnom poslu. Zapravo, dužnosti administratora su odraz odgovornosti ispravnog instaliranja veoma fleksibilnog sistema. Obavljanjem tih dužnosti, administrator može potpuno da prilagodi instalaciju potrebama sistema. Sve nabrojane dužnosti se, u nekoj meri, javljaju prilikom administracije bilo kog sistema. Pogledajmo ukratko koji su to zadaci.

Instaliranje i podešavanje servera

U svetu Linuxa, reč server ima šire značenje od onog na koje ste možda navikli. Na primer, standardno grafičko okruženje operativnog sistema Red Hat Linux zahteva grafički sloj koji se zove XFree86, a on je server. Taj program se izvršava čak i na neumreženom računaru s jednim korisničkim nalogom, i mora biti pravilno podešen. (Na sreću, taj posao je jednostavan i bezbolan deo instaliranja osim za neuobičajene kombinacije grafičke kartice i monitora; dani mučnog konfigurisanja grafičkog okruženja pripadaju prošlosti.)

Takođe, štampanje će biti moguće tek kada podesite server za štampu. I taj posao je postao jednostavan, gotovo trivijalan.

U nekim oblastima klijentsko-serverska nomenklatura može biti zbunjujuća. Iako ne možete imati grafičko okruženje bez servera, možete pristupati Webu bez Web servera, pristupati FTP uslugama bez FTP servera, čitati i e-poštu bez servera za e-poštu. Možda ćete ipak hteti da koristite te servere, koji su sastavni deo operativnog sistema Red Hat Linux. Kad god je server povezan s drugim računarima van vaše fizičke kontrole, morate razmišljati o bezbednosti. Želite da korisnici jednostavno pristupaju potrebnim uslugama, ali ne želite da sistem koji administrirate otvorite celom svetu.

Kad god je server povezan s drugim računarima van vaše fizičke kontrole, morate razmišljati o bezbednosti. Želite da korisnici jednostavno pristupaju potrebnim uslugama, ali ne želite da sistem koji administrirate otvorite celom svetu.

Nekada su svi serverski programi podrazumevano bili aktivni na distribucijama Linuxa. To je bila posledica ranije ere lepog ponašanja u računarskom svetu, kada ljudi nisu smatrali da je uništavanje tuđih računara dobra zabava. Realnost modernog i opasnijeg sveta zahtevala je da svi serveri sem osnovnih budu isključeni sve dok se ne aktiviraju i ne konfigurišu. To spada u dužnosti administratora sistema. Treba da znate koji serveri vam trebaju i kako da ih primenite. Nepotrebne servere, koje sistem ne koristi, ne treba omogućiti jer to predstavlja rizik po bezbednost. Sledeće strane će pokazati kako da obavite ovaj deo administracije sistema lako i efikasno.

Instaliranje i podešavanje aplikacija

Ovo može da izgleda suvišno, ali je izuzetno važno da novi administratori Linuxa razumeju dve karakteristike po kojima se Linux razlikuje od popularnih komercijalnih operativnih sistema: prva je postojanje korenskog korisnika ili superkorisnika, a druga je višekorisnički rad. Svaki korisnik ima svoj (ili koristi tuđi) nalog na sistemu, bez obzira na to da li se radi o zasebnom računaru ili jednom računaru s više korisničkih naloga.

Jedan razlog zašto je ovaj koncept tako bitan nalazi se u administraciji aplikativnog softvera.

Iako je moguće da individualni korisnici instaliraju aplikacije u svoje matične direktorijume (prostor na disku namenjen za njihove datoteke i parametre) te aplikacije neće moći da koriste drugi korisnici bez intervencije administratora sistema. Ako sa

aplikacijom treba da radi više korisnika, ona verovatno treba da bude instalirana više u hijerarhiji datoteka, što je posao koji može da uradi samo administrator sistema. (Administrator određuje korisnike koji mogu da rade u nekim aplikacijama i to tako što pravi „grupu“ za tu aplikaciju, a zatim dodaje pojedine korisnike u tu grupu.)

Novi softverski paketi mogu biti instalirani u direktorijum `/opt` ako je verovatno da će se ažurirati nezavisno od distribucije Red Hat; ako uradite tako, biće jednostavno da zadržite staru verziju sve dok ne budete sigurni da nova verzija radi na očekivani način. Neki paketi moraju da se instaliraju u direktorijum `/usr/local` ili čak `/usr` ako su nadogradnje paketa iz distribucije Red Hat. (Na primer, nekada postoje bezbednosne nadogradnje postojećih paketa.) Lokacija instalacije je važna samo ako aplikaciju prevodite iz izvornog koda; ako koristite RPM paket, aplikacija se automatski smešta tamo gde treba.

Podešavanje i prilagođavanje aplikacija je u izvesnoj meri posao korisnika, ali ne sasvim. Kostur konfiguracije (engl. *skeleton*) su podrazumevani parametri koje definiše administrator. Oni postavljaju osnovu za korišćenje aplikacije. Ako postoje određeni obrasci koji se koriste u čitavom preduzeću, administrator sistema treba da ih postavi ili bar da ih učini dostupnim dodajući ih u kostur konfiguracije. Isto važi i za podešavanje korisnikove radne površine, čak i za spisak aplikacija u meniju korisnikove radne površine. Vaša kompanija možda ne dozvoljava da igre, koje se isporučuju uz modernu distribuciju Linuxa, budu dostupne korisnicima, a možda ćete hteti da dodate stavke menija za instalirane ili naručene aplikacije. Sve to treba da omogući administrator sistema.

Pravljenje i održavanje korisničkih naloga

Ne može svako da se prijavi na računar pod Linuxom. Za svakog korisnika mora da postoji korisnički nalog – i pogađate – niko sem administratora sistema ne može da napravi takav nalog.

Ali to uključuje odluke koje vi ili vaša kompanija morate da donesete. Možete dozvoliti korisnicima da izaberu lozinke koje će lako pamtiti, ali koje će se lako i provaljivati. Teorijski je bezbednije da vi odredite lozinke, ali to će povećati verovatnoću da korisnici zapišu svoju lozinku na parčetu papira – što predstavlja rizik ako više ljudi ima pristup prostoriji u kojoj se računar nalazi. Ili možete podesiti da Linux zahteva od korisnika da povremeno menjaju svoje lozinke.

A šta raditi sa starim korisničkim nalozima? Možda je neko napustio kompaniju. Šta se dešava s njegovim korisničkim nalogom? Verovatno ne biste tom korisniku dozvolili da i dalje koristi mrežu kompanije. S druge strane, ne želite da obrišete korisnički nalog i da naknadno otkrijete da ste uništili bitne podatke.

Čemu mogu da pristupe pojedini korisnici? Možda postoje aspekti posla koji zahtevaju pristup Webu, ali ne želite da svako provodi radno vreme pretražujući Web. Ako se radi o kućnom računaru, možda ćete hteti da deci ograničite pristup Webu i zabranite lokacije kojima nijedan roditelj ne želi da izloži svoju decu.

Donošenje ovih i nekih drugih odluka, deo je dužnosti administratora sistema u upravljanju korisničkim nalozima. Bez obzira na to da li ova pravila utvrdi administrator ili uprava preduzeća, njih svakako treba propisati radi zaštite svih zainteresovanih. U preduzeću je dobro to uraditi u pisanoj formi.

Pravljenje rezervnih kopija i vraćanje datoteka iz kopija

Dok oprema ne postane savršena i dok ljudi ne izgube želju da uništavaju vlasništvo drugih (i istini za volju, dok administratori sistema ne postanu savršeni), postojaće potreba za pravljenjem rezervnih kopija važnih datoteka. U slučaju greške u hardveru, bezbednosti ili administraciji, prekid u radu sistema može biti minimalan ako postoji rezervna kopija. Samo administrator sistema može da napravi takve kopije. (Zbog ugrađenih bezbednosnih funkcija Linux može da zabrani korisnicima da prave rezervne kopije svojih datoteka na disketama.)

Dalje, saznanje da je pravljenje rezervnih kopija datoteka vaš posao, nije dovoljno. Treba da definišete strategiju da biste bili sigurni da sistem nije ranjiv i podložan velikim ispadima. I to nije uvek očigledno. Ako imate uređaj za trake velikog kapaciteta i nekoliko dobrih skupova sistemskih disketa za oporavak, možete da pravite rezervnu kopiju čitavog sistema svakih nekoliko dana. Ukoliko upravljate sistemom s mnogo korisnika, verovatno ćete smatrati da ima više smisla praviti rezervne kopije korisničkih naloga i konfiguracionih datoteka sistema jer se brže i jednostavnije instaliraju sa distribucionog CD-a nego što se vraćaju s trake. (Ne zaboravite aplikacije koje ste instalirali nezavisno od distribucije Red Hat, naročito one koje imaju mnogo parametara!)

Prvo odlučite *šta* treba čuvati u rezervnim kopijama, a zatim *koliko često* treba da pravite kopije i da li ćete praviti serije inkrementalnih rezervnih kopija, dodajući samo one datoteke koje su se promenile od poslednjeg pravljenja rezervne kopije ili ćete praviti više potpunih rezervnih kopija. Odlučite i *kada* treba praviti rezervne kopije. Da li imate poverenja u automatsko pravljenje rezervnih kopija, bez nadzora? Da li želite da, pored rezervnih kopija, koristite redundantne nizove nezavisnih diskova (engl. *redundant array of independent disks*, *RAID*), sisteme više diskova sa istim podacima kao obezbeđenje od kvara diska. (RAID nije dovoljan zato što kvar diska nije jedini problem koji može zaustaviti sistem.)

S druge strane, ne želite da postanete samozadovoljni ili da ohrabrujete takav stav korisnika. Pravljenje rezervnih kopija treba da bude deo strategije, bez obzira na to da li će vam one ikada zatrebati. To znači da treba da podstičete korisnike da i sami prave više kopija sopstvenih važnih datoteka u svojim korisničkim direktorijumima da ne biste morali da povezujete rezervnu kopiju za vraćanje datoteke koju je oštetio korisnik. (Ako računar nije povezan na mrežu, vi kao administrator sistema možete da uvedete praksu pravljenja rezervnih kopija konfiguracionih i drugih važnih datoteka.)

Velika je verovatnoća da, čak i ako radite za kompaniju, sami donosite ove odluke – sve što šefovi hoće jeste da sistem radi savršeno – i stalno. Pravljenje rezervnih kopija je samo deo priče. Treba da napravite plan za oporavak sistema ako on otkaže. Taj plan je van oblasti koje obrađuje ova knjiga. Ponekad su hardverski kvarovi toliko ozbiljni da je jedino rešenje zamena diska, zamena svega *osim* diska, ili čak restauriranje sistema na nov računar.

Pravljenje rezervnih kopija je samo deo priče. Treba da napravite plan za oporavak sistema ako on otkaže.

Nadgledanje i podešavanje performansi

Podrazumevana instalacija Red Hat Linuxa dobro koristi postojeće sistemske resurse. Ipak ne postoji konfiguracija koja svima odgovara i Linux se može beskrajno podešavati.

Na modernim računarima koji nisu povezani u mrežu, Linux bi trebalo da bude prilično brz. Ako nije, nešto nije u redu i to treba da razreši administrator sistema. Ali možda hoćete da iscedite i najmanji delić performansi iz hardvera. U slučaju višekorisničkog servera datoteka, servera za e-poštu, ili sličnog sistema, poboljšanja performansi mogu mnogo da znače, iako su su na prvi pogled mala.

Podešavanje sistema je stalan proces u kome se koriste razne dijagnostičke alatke i alatke za nadgledanje. Neke odluke vezane za performanse donose se u vreme instaliranja, a druge se sprovode kasnije. Dobar primer je uslužni program `hdparm`, koji može znatno da poveća brzinu pristupa IDE diskovima. Ako koristite neispravne ili nekvalitetne kablove, a disk optimizujete programom `hdparm`, u sistemskim zapisnicima pronaći ćete velik broj grešaka.

Pravilno nadgledanje omogućava da otkrijete aplikacije koje se čudno ponašaju, koje možda troše više resursa nego što bi trebalo ili ne uspevaju da oslobode zauzete resurse kada završe s radom. Korišćenjem alatki za upravljanje performansama možete da odredite kada treba da se nadogradi hardver, na primer memorija, dodatan disk, ili čak složeniji elementi poput hardverskog RAID-a, da bi korišćenje računara u preduzeću bilo isplativije ili da bi se obavljali komplikovani poslovi kao što je trodimenzionalna grafička obrada.

Verovatno je najznačajnije to što pažljivo nadgledanje sistema i dijagnostičke alatke upozoravaju na prve znake da će otkazati neka komponenta sistema, pa se moguće vreme prekida rada može smanjiti. U kombinaciji sa resursima za određivanje najboljih komponenata za Red Hat Linux, nadgledanje performansi može da ukaže na to da određenu komponentu treba zameniti drugom, mnogo robusnijom i ponekad efikasnijom.

U svakom slučaju, pažljivo nadgledanje sistema uz mudro podešavanje Linuxa, omogućava da izvučete maksimum iz opreme koju posedujete, od prilagođavanja upravljačkog programa za grafičku karticu, preko primene specijalnih zakrpa (engl. *patch*), do isključivanja nepotrebnih usluga, oslobađanja memorije i procesora.

Da biste postigli najbolje performanse s postojećom opremom, pažljivo nadgledajte sistem i mudro koristite ugrađene alatke za podešavanja.

Obezbeđivanje sistema

Ako postoji zajednička nit u administraciji sistema Linux, nešto što je prisutno u svemu što radite, to je bezbednost računara i integritet podataka.

Šta to znači? Pa, skoro sve. Prvi i najvažniji zadatak administratora sistema jeste da obezbedi da se nijedan podatak s računara ili mreže ne ošteti, bilo da otkaže hardver, nestane struja, bilo greškom u podešavanju ili greškom korisnika (u obimu koji kasnije može biti izbegnut) ili zlonamernim ili nepažljivim upadom spolja. To znači obavljanje svih poslova opisanih u ovom poglavlju pažljivo i s punim razumevanjem njihovih posledica, ali znači i mnogo više.

Svako ko ima veze s računarima sigurno je čuo o uspešnim i izuzetno ozbiljnim napadima na računare koji su povezani sa Internetom. Većina pogođenih računara nisu bili Linux sistemi, ali to ne znači da je Linux u potpunosti otporan, bilo na direktne napade, bilo na efekte napada na računare koji rade pod drugim operativnim sistemima. U jednom DDoS napadu, žrtve su bile nekoliko kompanija na Internetu, a veliki broj zombi računara, koji su iskorišćeni da bi vandali mogli istovremeno da napadnu, radili su pod operativnim sistemom Linux na koji nisu bile primenjene zakrpe za zaštitu od poznatih bezbednosnih propusta. U raznim napadima crva Code Red 2001. godine, Linux računari nisu bili ranjivi, ali velika količina saobraćaja generisana ovim crvom ipak je nedeljama sprečavala mnogo Linux računara da pružaju usluge Weba. Retki su korisnici e-pošte koji nisu dobili virus SirCam u – besmislenim porukama nepoznatih pošiljalaca sa nasumično pridruženim datotekama. Iako ova zaraza nije pogodila Linux računare koliko one koji rade pod drugim operativnim sistemima, svako ko je morao da preuzme više megabajta elektronske pošte telefonskom linijom, teško da nije bio pogođen napadom.

U zavisnosti od toga kako i sa čim je Linux računar povezan, od osetljivosti podataka koje sadrži i potreba za koje se koristi, obezbeđivanje sistema može da se svede na jednostavno isključivanje nepotrebnih usluga i nadgledanje bezbednosne liste slanja kompanije Red Hat. Međutim, to može biti i posao koji zahteva puno radno vreme i koji uključuje definisanje nivoa bezbednosnih dozvola unutar sistema i dozvola za pristup preko mreže, razmatranje i postavljanje barijere za zaštitu i Linux računara i računara koji koriste drugi softver i mnogo su ranjiviji. Obezbeđivanje podrazumeva i fizičku bezbednost – obezbedite da niko ne može da ukrade ceo računar!

Za bilo koji računar u mreži, bezbednost znači dobru odbranu od napada i obezbeđivanje da niko ne koristi vaš računar kao platformu za napad na druge računare. Ako izvršavate servere za Web, FTP ili e-poštu, to znači da dajete pristup jednoj grupi korisnika i zabranjujete pristup svima ostalima. Treba da budete sigurni da se lozinke ne mogu lako otkriti ili odati neovlašćenim osobama, da nezadovoljni bivši zaposleni nemaju više pristup sistemu i da neovlašćene osobe ne mogu da kopiraju datoteke sa vašeg ili vaših računara.

Sprovođenje bezbednosnih mera je trajan proces – neko je rekao da je jedini potpuno bezbedan računar onaj koji ne sadrži podatke, nije uključen u mrežu, nije priključen na električno napajanje, nema priključenu tastaturu i zaključan je u podrumu. Iako je to teorijski tačno, to takođe znači da je sprovođenje mera bezbednosti ukinulo i sve koristi od računara, zar ne? Posao administratora sistema jeste da pronađe pravu meru između maksimalne koristi i najstrože bezbednosti, sve vreme imajući na umu da poverenje u bezbednost računara danas ne znači ništa za bezbednost računara sutra.

Na stranama koje slede, naučićete o mnogim alatkama Red Hat Linuxa za zaštitu od upada, čak i od upada u računare s drugim operativnim sistemima, koji možda postoje u vašoj mreži. Linux je od samog početka projektovan tako da se imala na umu bezbednost, pa u svim poslovima koje obavljate treba da zadržite svest o pitanjima bezbednosti.

Posao administratora sistema je da pronađe pravu meru između maksimalne koristi i najstrože bezbednosti, sve vreme imajući na umu da poverenje u bezbednost računara danas ne znači ništa za bezbednost računara sutra.

Korišćenje alatki za nadgledanje bezbednosti

Zlonamernici, koji iz bahatosti ili zabave vole da provaljuju u tuđe računare, lukavi su ljudi. Ako sistem ima neku slabost, oni će je pronaći. Na sreću, grupa za razvoj operativnog sistema Linux brzo pronalazi moguće probleme i nalazi načina da provalnicima zalupi vrata. Takođe, kompanija Red Hat marljivo objavljuje nove, zakrpljene verzije paketa u kojima su otklonjeni potencijalni nedostaci sistema. Dakle, prvi i najbolji savet za bezbednost jeste da redovno preuzimate i instalirate ispravljene pakete. To može biti zamorno, ali je zanemarljivo u odnosu na ponovno podizanje oštećenog sistema.

Koliko god da su dobri programi za traženje grešaka, oni nekad imaju suprotan efekat. Zadatak administratora je da spreči da se računar koristi u nedobronamerne svrhe i da ga odbrani od upada. Red Hat Linux sadrži alatke za otkrivanje i razmatranje neovlašćenog pristupa raznih vrsta. Naučićete kako da instalirate i podesite te alatke i kako da razumete njihove poruke. Obratite pažnju na odeljke o tome i radite prema datim uputstvima. Ako je računar povezan sa Internetom, iznenadiće vas broj pokušaja provale i shvatićete značaj pitanja bezbednosti.

Sažetak

Dok čitate ovu knjigu, imajte na umu da su poslovi administratora trajni i da ne postoji računar koji je potpuno podešen, u potpunosti aktuelan i sasvim bezbedan na duže vreme. Brzina razvoja Linuxa oduzima dah i važno je da redovno pratite te promene. Ova knjiga vam daje najbolje informacije o distribuciji Red Hat Linux i objašnjava sve što treba da znate o tome kako dobiti najbolje rezultate od njega. Treba da je čitate usvajajući tačku gledišta administratora Linuxa, razumevajući kako radi sistem, a ne samo zasebne alatke. I kao što će vam reći najbolji administratori, administracija sistema je stanje svesti.