HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Osiris alata za provjeru integriteta datotečnog sustava

CCERT-PUBDOC-2003-11-50

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Provjera integriteta datotečnog sustava jedan je od osnovnih načina na koji se može uočiti bilo kakva izmjena, brisanje ili dodavanje datoteka na sustav. Iako ih ne može spriječiti, ova metoda pomaže pri detektiranju neovlaštenih radnji na sustavu i u slučaju kompromitiranja sustava olakšava forenzičku analizu.

Osiris je multiplatformski distribuirani sustav za provjeru integriteta datotečnog sustava, koji omogućuje praćenje stanja na više računala istovremeno. Glavna namjena ovog sustava je periodičko pregledavanje ključnih računala na mreži, u svrhu prikupljanja informacija koje bi ukazivale na promjenu stanja sustava.

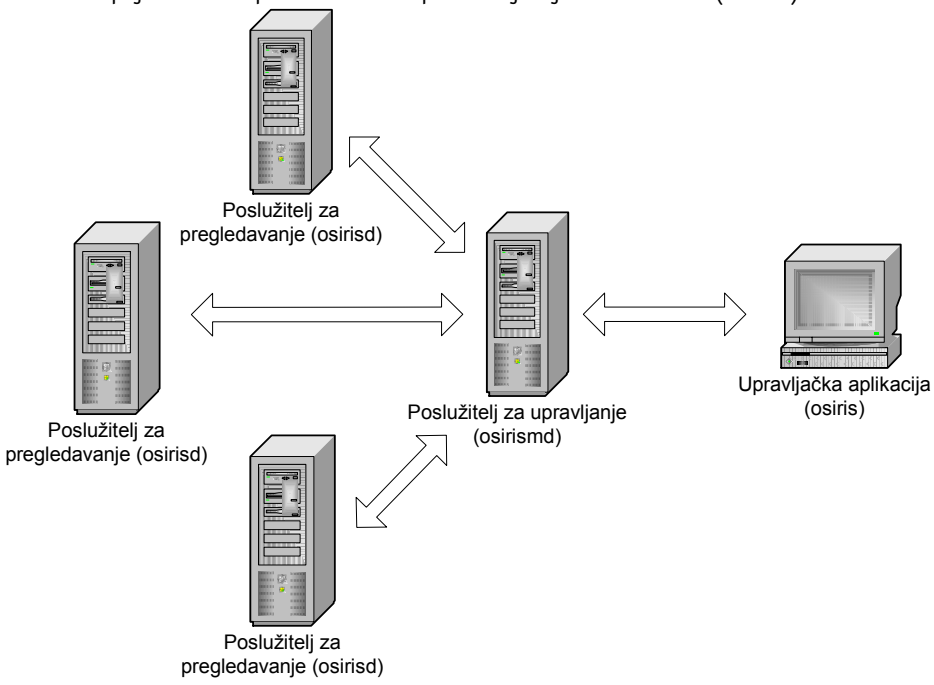
Sve komponente Osiris sustava moguće je koristiti na Windows NT, 2000 i XP operacijskim sustavima, kao i na svim uobičajenim UNIX sustavima uključujući i BSD, Linux, Mac OS X. Na taj način zajamčen je visok stupanj fleksibilnosti i neovisnosti kod implementacije sustava.

2. Princip rada

Osiris sustav se sastoji od tri glavne komponente:

- Poslužitelj za upravljanje (`osirismd`)
- Poslužitelj za pregledavanje (osirisd)
- Upravljačka aplikacija (klijent) (osiris)

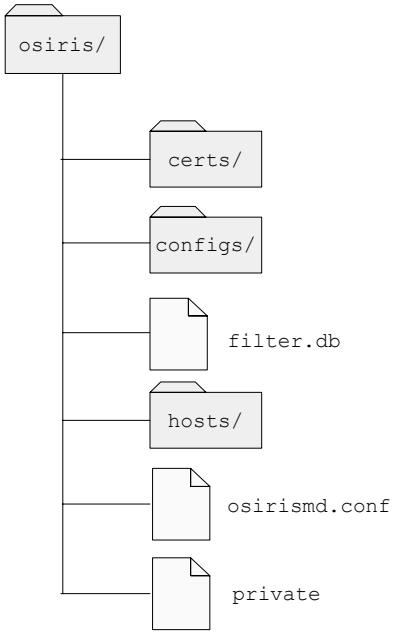
Odnos između pojedinih komponenti sustava prikazan je sljedećom slikom (Slika 1).



Slika 1: *Prikaz komponenata Osiris sustava*

Poslužitelj za pregledavanje je jednostavan proces koji se pokreće na svakom računalu koje se želi nadzirati. Ova komponenta zadužena je za pregledavanje datotečnog sustava na računalu na kojem je pokrenuta i prosljeđivanje prikupljenih podataka poslužitelju za upravljanje. Radi postizanja zadovoljavajuće sigurnosne razine poslužitelj za pregledavanje izveden je tako da nikada ne pristupa datotekama s namjerom pisanja, tj. datoteke se isključivo čitaju.

Poslužitelj za upravljanje prikuplja i čuva sve podatke o pregledanim računalima te ih prezentira klijentu za upravljanje. Na računalu na kojem je instaliran, poslužitelj za upravljanje kreira strukturu direktorija u kojoj se čuvaju svi važni konfiguracijski podaci kao i rezultati provedenog skeniranja.

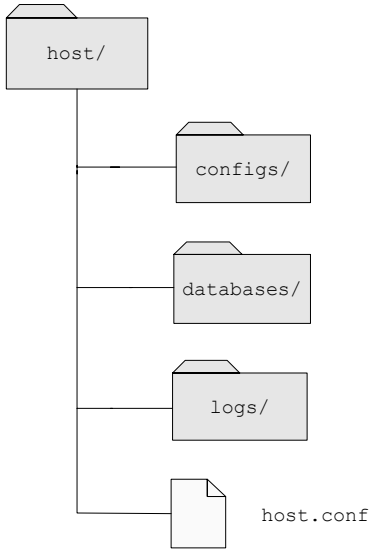


Slika 2 Struktura direktorija poslužitelja za upravljanje

Značenje pojedinih direktorija i datoteka je sljedeće:

- `certs/` - datoteke s certifikatima
- `configs/` - inicijalna konfiguracija i konfiguracijske datoteke za poslužitelje za pregledavanje
- `filter.db` - baza sa filtrima za usporedbu
- `hosts/` - direktoriji s rezultatima pregledavanja računala
- `osirismd.conf` – konfiguracija poslužitelja za upravljanje
- `private` – baza podataka s korisničkim podacima

U slučaju premještanja poslužitelja za skeniranje na neko drugo računalo, dovoljno je cjelokupnu strukturu direktorija prebaciti na novo računalo i ponašanje poslužitelja će ostati isto. Za svako računalo na kojem je instaliran poslužitelj za pregledavanje, upravljački poslužitelj, unutar direktorija `hosts`, otvara sljedeću strukturu poddirektorija (Slika 3) u kojoj se nalaze svi konfiguracijski podaci i podaci prikupljeni pregledavanjem.



Slika 3 Struktura poddirektorija s rezultatima skeniranja

Rezultati skeniranja pohranjuju se u poddirektorij `databases`, dok se rezultati usporedbe dva stanja sustava pohranjuju u poddirektorij `logs`.
Zbog prirode pohranjenih podataka upravljački je poslužitelj poželjno instalirati na "sigurno" računalo, tj. računalo s ograničenim ovlastima pristupa.
Upravljačka aplikacija (klijent) koristi se od strane administratora za pregled rezultata i izvedena je tako da komunicira isključivo s upravljačkim poslužiteljem. Na taj način administrator nema nikakvu interakciju sa pregledavanim računalima.

3. Instalacija i konfiguracija paketa

Kao što je ranije spomenuto, Osiris je multiplatformski orijentiran sustav pa će se o ovom poglavlju opisati postupak njegove instalacije na Windows i Linux računalima. Postupak instalacije na Linux računalima moguće je primijeniti i na bilo koje računalo koje koristi UNIX ili neki njemu sličan operacijski sustav.
Potrebno je napomenuti da Osiris za svoj ispravan rad zahtijeva instaliranu inačicu 0.9.6j (ili noviju) OpenSSL paketa.

3.1. Linux instalacija

Na Linux operacijskim sustavima sve komponente Osiris alata dolaze u jedinstvenom tar.gz paketu. Paket sadrži izvorni kod programa kojeg je potrebno prevesti u izvršnu datoteku. Prvi korak prilikom prevođenja programa je pokretanje Configure skripte kojom će se ispitati parametri sustava potrebni za uspješno prevođenje. U slučaju da Configure skripta nije u mogućnosti automatski locirati komponente OpenSSL paketa potrebne kod prevođenja programa, ispravnu stazu do direktorija u kojem se nalaze OpenSSL biblioteke i datoteke sa zaglavljima potrebno je specificirati opcijom –with-ssl-dir prilikom pokretanja skripte.

```
#./configure

Osiris (c) 2000-2003 The Shmoo Group (TSG)
------------------------------------------------------

 ==> Configuration Complete.
 ==> Osiris has been configured with the following options:

                 Host: i686-pc-linux-gnu
             Compiler: gcc
       Compiler flags: -g -O2
   Preprocessor flags:
         Linker flags:
```

```
            Libraries: -lpthread  -lssl -lcrypto -lresolv
  Privlege Separation: yes
         SSL Location: (system)

 ==> use one of the following targets:

       install: install scanner and management console.
       package: create scanner installation package.
       clean:   remove object files.
```

Nakon konfiguracije paketa, potrebno je instalirati željenu komponentu sustava. Upravljački poslužitelj prevodi se naredbom `make`, a na sustav se instalira naredbom `make install`. Nakon instalacije, poslužitelj je potrebno pokrenuti kako bi se izmijenila njegova inicijalna konfiguracija.

Poslužitelj za pregledavanje i klijentska aplikacija prevode se naredbom `make osirisd`, a naredbom `make package` kreira se poseban instalacijski paket pomoću kojega je poslužitelj za pregledavanje lako moguće distribuirati po ostalim računalima na mreži koja sadrže isti operacijski sustav.

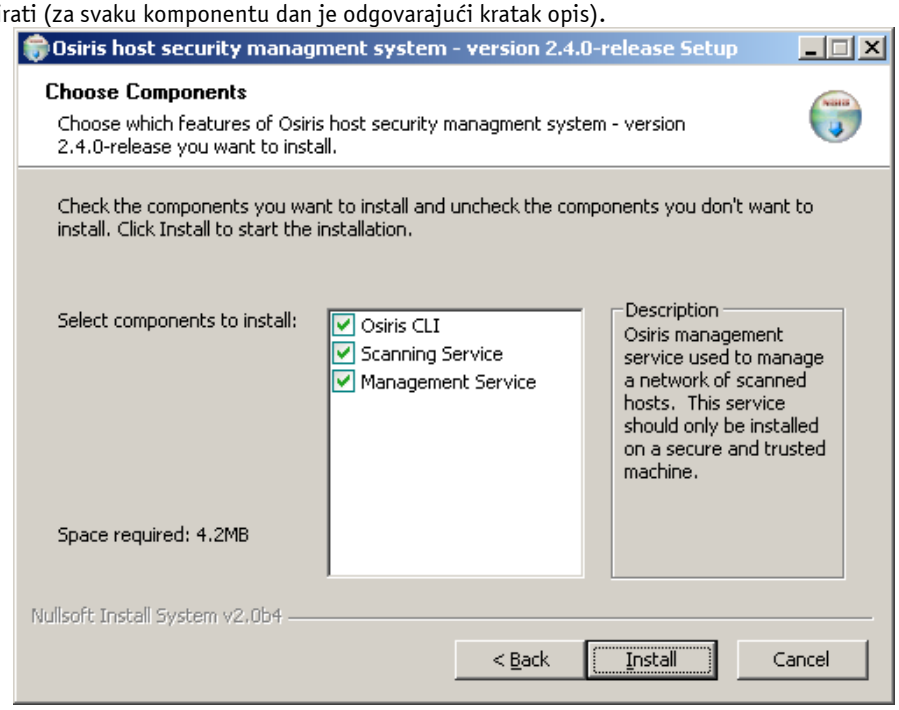
```
# make package
------------------------------------------------------------------------
building release tarball:
installer package contents:
total 144
-rwxr-xr-x    1 spajic   spajic      19332 Sij 14 16:30 install.sh
-rwxr-xr-x    1 spajic   spajic       2828 Sij 14 16:30 LICENSE
drwxr-xr-x    2 spajic   spajic       4096 Sij 14 16:30 linux
-rwxrwxr-x    1 spajic   spajic     108156 Sij 14 16:30 osirisd
-rw-r--r--    1 spajic   spajic         43 Sij 14 16:30 version.h
------------------------------------------------------------------------
installer package created.

Paket osiris-"2.4.0-release"-Linux.tar.gz
```

Na ciljanom računalu paket je potrebno otpakirati i pokrenuti skriptu `install.sh` koja se nalazi u novonastalom direktoriju.

3.2. Windows instalacija

Za razliku od Linux i Unix sustava, na Microsoft Windows NT, 2000 i XP operacijskim sustavima sve komponente Osiris paketa mogu se instalirati pokretanjem jedinstvenog instalacijskog programa osiris-2.4.0-win32.exe. U sučelju prikazanom na slici (Slika 4) označavaju se komponente koje se žele instalirati (za svaku komponentu dan je odgovarajući kratak opis).



Slika 4: *Instalacijsko sučelje Osiris-a za Windows operacijske sustave*

Pritiskom na tipku **Install**, pokreće se instalacija odabranih komponenata u C:\WINNT\osiris direktorij. U slučaju potrebe za deinstalacijom, u isti direktorij će se spremiti i program sa automatsku deinstalaciju.

4. Konfiguracija

4.1. Konfiguracija upravljačkog poslužitelja

Prvi korak u konfiguraciji Osiris sustava je konfiguracija upravljačkog poslužitelja. Upravljački poslužitelj je inicijalno podešen tako da prihvaća konekcije isključivo s računala na kojem je pokrenut,

tako da je u svrhu podešavanja potrebno lokalno pokrenuti klijentsku aplikaciju (`osiris.exe` ili `osiris`). Ukoliko je pokrenuta bez ikakvih dodatnih parametara, klijentska aplikacija će se automatski spojiti na lokalni upravljački poslužitelj.
Prilikom inicijalnog spajanja poslužitelj će od klijentske aplikacije zatražiti potvrdu certifikata upravljačkog poslužitelja.

```
# osiris
Osiris command line management utility - version 2.4.0-release
unable to load root cert for management host:
(/root/.osiris/osiris_root.pem)
fetching root certificate from management host (localhost).

The authenticity of host 'localhost' can't be established.

  [ server certificate ]

      subject = /C=US/CN=Osiris Managment Daemon/OU=Osiris IDS
      issuer  = /C=US/CN=Osiris Managment Daemon/OU=Osiris IDS

            key size: 2048 bit
      MD5 fingerprint: 44:33:36:83:E8:40:68:7F:A3:7F:B2:A4:0F:CC:A3:A4

Verify the fingerprint specified above.
Are you sure you want to continue connecting (yes/no)? yes
authenticating to (localhost)

User: admin
Password:

connected to management daemon, code version (2.4.0-release).
hello.
```

Certifikat je potrebno prihvatiti, nakon čega će se pohraniti u poddirektorij `.osiris/`, unutar korisnikovog korijenskog (home) direktorija. Na sustav se spaja pod korisničkim imenom `admin` i praznom lozinkom, a potvrda uspješnog spajanja na poslužitelj je sljedeći naredbeni prompt (u uglatim zagradama upisano je ime računala na kojem se poslužitelj nalazi).

```
osiris-2.4.0-release:
```

Unutar ovog naredbenog prompta moguće je, izdavanjem posebnih naredbi, upravljati Osiris upravljačkim poslužiteljem. Popis svih naredbi moguće je dobiti izdavanjem naredbe `help`.
Inicijalna konfiguracija upravljačkog poslužitelja sadrži samo jedan korisnički račun pod nazivom `admin`. Zaporka za administratorski (`admin`) korisnički račun podešava se naredbom `passwd admin`. Unutar Osiris sustava ne postoji stroga hijerarhija između korisnika, što znači da će svi eventualno dodani korisnici imati jednake ovlasti kao i administrator. Lista svih korisnika ispisuje se naredbom `users`.
Osnovne postavke upravljačkog poslužitelja mogu se podesiti naredbom edit-mhost, koja pokreće proces u kojem se administratoru sustava nudi odabir vrijednosti konfiguracijskih parametara. Za svaki konfiguracijski parametar ponuđena je i uobičajena vrijednost koja se koristi u slučaju da administrator ne upiše nikakvu vrijednost pod zadani parametar. Objašnjenje pojedinih parametara moguće je pronaći u dokumentaciji Osiris paketa.

4.2. Dodavanje novih poslužitelja za pregledavanje

Unutar upravljačkog poslužitelja potrebno je podesiti i koji će se poslužitelji pregledavati. Pregledavanje je moguće obavljati samo na lokalnom računalu, ali u većini slučajeva pregledava se više kritičnih računala na mreži. Za svako računalo na kojem je instaliran poslužitelj za pregledavanje potrebno je pomoću `new-host` naredbe pokrenuti konfiguracijski proces sličan onome za upravljački poslužitelj.

```
osiris-2.4.0-release: new-host

  [ new host ]

> name this host []:  localhost
> hostname/IP address []: 127.0.0.1
> description []: lokalno_skeniranje
> enable scan logging for this host? (yes/no) [no]: yes
```

```
> archive scan databases for this host?  (yes/no) [no]: yes
> enable admin email notification for this host? (yes/no) [yes]: yes
> send scan notification, even when no changes detected  (yes/no) [no]: no
> notification email (default uses mhost address) []: spajic@localhost
> configure scan scheduling information? (yes/no) [no]: yes

  [ scheduling information for localhost ]

Scheduling information consists of a start time and a frequency value.
The frequency is a specified number of minutes between each scan, starting
from the start time.  The default is the current time.

Specify the start time in the following format: mm/dd/yyyy HH:MM

enter the start date and time
using 'MM/DD/YYYY hh:mm' format: [Dec  6 16:05:17 2004]
enter scan frequency in minutes: [daily (1440)]

> activate this host? (yes/no) [no]: y
```

Nakon prikupljenih informacija, upravljački će poslužitelj generirati strukturu direktorija potrebnu za pohranu podataka prikupljenih pregledavanjem.

Posljednji korak kod dodavanja novog poslužitelja za pregledavanje je njegova inicijalizacija.

```
the new host (localhost) was sucessfully created.
initialize this host? (yes/no): y

Initializing a host will push over a config, start a scan, and set the
created database to be the trusted database.

Are you sure you want to initialize this host (yes/no): yes

OS Name: Linux
OS Version: 2.4.19-16mdk
use the default config for this OS? (yes/no): yes
The config: default.linux has been pushed.
perform an initial scan and database for this host? (yes/no): yes
scanning process was started on host: localhost
```

Pokretanjem inicijalizacijskog postupka, upravljački će poslužitelj proslijediti konfiguracijske parametre poslužitelju za pregledavanje i pokrenuti inicijalno pregledavanje udaljenog računala. Rezultate tog inicijalnog pregleda tretirati će kao relevantne prilikom usporedbe sa rezultatima svakog sljedećeg pregleda.

5. Rad s alatom

Inicijalizirani poslužitelji za pregledavanje će prosljeđivati rezultate upravljačkom poslužitelju koji će ih pohraniti u posebne datoteke. Za zapis ovih datoteka koristi se Berkeley DB format zapisa za baze podataka. Baze su formatirane tako da se mogu bez poteškoća prenositi sa jednog operacijskog sustava ili računala na drugi sustav ili računalo. Na taj način, migracija upravljačkog poslužitelja na drugo računalo prilično je jednostavna, kao i naknadna forenzička analiza prikupljenih podataka koju je u ovom slučaju moguće provoditi na bilo kojem operacijskom sustavu ili računalu.

5.1. Zakazivanje pregledavanja

Upravljački poslužitelj sadrži interni mehanizam za automatsko pokretanje zakazanih pregledavanja. U zakazanom trenutku, on će poslužitelju za pregledavanje proslijediti konfiguracijske parametre identične onima korištenima kod inicijalnog pregledavanja i pokrenuti ponovni postupak pregledavanja.

Po završenom pregledavanju, rezultati se uspoređuju sa rezultatima inicijalnog pregledavanja i eventualne razlike se prijavljuju administratoru. Ovisno o konfiguraciji poslužitelja, neki rezultati usporedbe i ne moraju biti prijavljeni.

Kako bi se izbjegla mogućnost pogreške zbog krivo konfiguriranog poslužitelja za pregledavanje, upravljački poslužitelj prilikom svakog novog postupka pregledavanja prosljeđuje poslužitelju za pregledavanje inicijalnu konfiguraciju.

5.2. Uočavanje promjena na pregledavanom sustavu

Budući da su određene promjene na operacijskom sustavu neminovne, redovito pokretanje pregledavanja i usporedba rezultata dovesti će do upozorenja koja se prosljeđuju administratoru. Ukoliko se ne poduzmu odgovarajuće mjere korekcije, uočene promjene konstantno će se prijavljivati, sve dok stanje ne bude identično stanju sustava u trenutku inicijalnog pregledavanja. Budući da velik broj nepotrebnih upozorenja vrlo lako može odvući pažnju administratora sa uočenih ozbiljnih propusta na sustavu, naredbom set-base-db u naredbenom promptu Osiris upravljačkog poslužitelja moguće je posljednju bazu u nizu pregledavanja proglasiti inicijalnom. Ovu opciju korisno je upotrijebiti nakon nadogradnje sustava ili sličnih promjena koje uzrokuju velik broj upozorenja, a zapravo ne predstavljaju opasnost po integritet sustava.
Osim promjene inicijalne baze pregledavanja, Osiris omogućuje i korištenje posebnih filtara za usporedbu rezultata. Ovi filtri dozvoljavaju određene promjene na sustavu bez slanja upozorenja administratoru, omogućujući na taj način eliminiranje nepotrebnih upozorenja. Njihova upotreba vrlo je korisna kod praćenja datoteka čiji su određeni parametri podložni stalnim promjenama. Tako je na primjer kod log datoteka sasvim normalna promjena njihove veličine, ali ostali parametri (npr. vlasnik i dozvole nad datotekom) ne bi se smjeli mijenjati.

5.3. Log datoteke

Za obavještavanje administratora o trenutnom stanju Osiris sustava upravljački poslužitelj prosljeđuje log poruke operacijskom sustavu. Na Linux i Unix sustavima log poruke se šalju Syslog poslužitelju, dok se kod Windows operacijskih sustava za tu svrhu koristi Event Viewer aplikacija. Moguće je koristiti nisku, srednju i visoku razinu obavještavanja. Visoku razinu se preporučuje koristiti kod prvog puštanja sustava u rad, kada se očekuje veći broj grešaka u radu sustava, dok je kod uhodanog sustava sasvim dovoljno koristiti nisku ili srednju razinu obavještavanja.
Radi njihove lakše analize, log poruke pohranjuju se u sljedećem formatu:
[računalo] [tip poruke] *poruka*
Polje koje označava tip poruke može poprimiti sljedeće vrijednosti:

- `Info` – poruka obavijesnog tipa
- `Err` – poruka o pogrešci u radu sustava
- `Warning` – upozorenje
- `Cmp` – poruka o promjeni u radu sustava

U nastavku je dan primjer tipičnog log zapisa iz datoteke `/var/log/messages`.

```
Dec  6 12:56:53 cecilija osirismd[4874]: [*][err]with control server binding
to port: 2266.
Dec  6 12:56:53 cecilija osirismd[4874]: [*][info] halting.
Dec   6  12:56:53  cecilija  osirismd[4874]:  [*][info]  osirismd  servers  shut
down.
Dec  6 12:56:53 cecilija osirismd[4874]: [*][info] osirismd scheduler process
shut down.
```

Potrebno je napomenuti kako se u log datoteke ne zapisuju nikakvi podaci koji bi imali veze sa rezultatima provjere integriteta sustava, već se ove poruke koriste isključivo za obavještavanje o stanju i radu samog sustava.

6. Općenite preporuke za ispravno korištenje

Bilo da se radi o implementaciji Osirisa u stvarnom okruženju sa velikim brojem računala ili o testnom sustavu sa samo nekoliko računala, poželjno je pridržavati se nekih općenitih preporuka kako bi sustav radio brzo i pouzdano. O ispravnoj implementaciji ovisi i efikasnost ovog sustava, tj. jednostavnost praćenja uočenih promjena na računalima.
Jedno od osnovnih pravila kojega se treba pridržavati je da se nikada ne provjeravaju sve datoteke na sustavu (tj. sadržaj cijelog tvrdog diska). Provjeravanje svih datoteka je dugotrajan proces koji nepotrebno troši resurse sustava, a krajnji ishod je redovito velika baza rezultata pregledavanja koja je nepregledna i samim time praktički neupotrebljiva. Poželjno je odrediti kritične datoteke na sustavu i pratiti isključivo njihovu promjenu. Značajna poboljšanja na brzini pregledavanja mogu se postići i korištenjem MD5 umjesto SHA-1 algoritma za provjeru datoteka.

Važan faktor efikasnosti pregledavanja je i broj obavijesti koje prima administrator sustava.
Neiskusnim korisnicima preporučuje se upotreba inicijalne konfiguracije ili pregledavanje isključivo izvršnih datoteka, biblioteka, važnih datoteka sustava i datoteka jezgre sustava. Na taj način broj rezultata pregledavanja biti će sveden na minimum, a ipak će biti moguće uočiti sve prijetnje integritetu sustava.
Učestalost provjera u potpunosti je proizvoljna i ovisi o frekvenciji promjene datoteka koje se provjeravaju. Ipak, razmak između dva pregledavanja ne bi smio biti previše kratak jer bi se na taj način prekomjerno trošili resursi pregledavanog računala. Također, učestalo pregledavanje sa loše konfiguriranim alatom može uzrokovati generiranje iznimno velikog broja upozorenja, pa je prilikom uhodavanja rada Osiris sustava poželjno koristiti veći period između dvije provjere.
Rezultate pregledavanja poželjno je redovito uklanjati s računala kako bi se izbjeglo popunjavanje tvrdog diska nepotrebnim podacima.

7. Zaključak

Osiris je napredan i vrlo fleksibilan alat za provjeru integriteta datotečnog sustava.
Sve komponente Osiris sustava izvedene su tako da jamče maksimalnu sigurnost i integritet pregledavanih sustava. Iz tog razloga rezultati pregledavanja se nikada ne čuvaju na pregledavanim računalima, a za međusobnu komunikaciju i autentikaciju između komponenata koristi se OpenSSL protokol.
Ovaj alat je u potpunosti besplatan i razvija se pod OpenSource licencom, što jamči brz i siguran razvoj koda, te vrlo dobru prilagodbu softvera svim zahtjevima korisnika.