Algebra

visoka škola za
primijenjeno računarstvo

Napredni nadzor i pracenje rada sustava – I.dio

www.racunarstvo.hr

Uobičajeni pristup, I.dio

- **pregledavati log zapise na udaljenim serverima ne smije biti iterativan posao:**
  - ulogirati se na udaljeni server kroz SSH
  - pregledavati lokalne log zapise
  - *Repetitio est mater studiorum*
- **postoji li možda neki efikasniji način za obavljanje ovog posla?**

Uobičajeni pristup, II.dio

- napraviti skriptu koja će se u petlji SSH-om spajati na udaljene servere i koristiti isti princip kao prije
- svaki put kad trebamo pretražiti zapise, morati ćemo pokrenuti skriptu, dok mi pokrenemo skriptu, log zapisi će se već promijeniti
- kako sve te log zapise držati sinhroniziranima?

Rješenje 1. – konfiguracija rsyslog poslužitelja i klijenta

- iskoristimo rsyslog servis da bismo jedan server *„proglasili"* rsyslog serverom, na koji će ostali slati log zapise
- ostale servere ćemo *„proglasiti"* klijentima u ovom sustavu

Algebra
visoka škola
za primijenjeno
računarstvo

Demo – konfiguracija rsyslog poslužitelja i klijenta

Algebra
visoka škola
za primijenjeno
računarstvo

Rješenje 2. – konfiguracija rsyslog poslužitelja i klijenta za pohranu u MySQL bazu

- rsyslog ima mogućnost pohrane direktno u bazu podataka
- minimalna promjena u konfiguraciji servera:

```
[root@OOS2 ~]# vi /etc/rsyslog.conf
$ModLoad ommysql
*.*       :ommysql:db-server,db-name,db-userid,db-password
```

- slijedeći korak bio bi izrada php/MySQL aplikacije za analizu

Algebra
visoka škola
za primijenjeno
računarstvo

Rješenje 3. – Korištenje gotovog sustava

- **Primjer: Adiscon Log Analyzer**
  - ima mogućnost korištenja web-sučelja za pregled log zapisa koji su sakupljeni sa više servera
  - ima dodatne module za spajanje na Windows računala (komercijalni modul)

Algebra
visoka škola
za primijenjeno
računarstvo

Demo – Adiscon Log Analyzer

- Možemo kroz regularne izraze tretirati i znakove kao što su:

\n - nova linija

\t - tab

\w - bilo koji alfanumerički znak, kao [a-zA-Z0-9_]

\W - bilo koji non-alfanumerički znak, kao [^a-zA-Z0-9_]

\d - bilo koji broj, kao [0-9]

\D - bilo koji non-broj, kao [^0-9]

\s - bilo koji *whitespace* znak - space, tab, newline, itd.

\| - traženje *pipe* znaka

\[- traženje lijeve uglate zagrade

Algebra

visoka škola
za primijenjeno
računarstvo

?