Monitorizarea log-urilor într-o o rețea de calculatoare

Gabriel Neagu

Rezumat

Monitorizarea log-urilor într-o rețea de calculatoare este o temă de mare actualitate în domeniul asigurării securității informaționale în cadrul companiilor şi instituțiilor. Proiectul de față își propune dezvoltare a unei aplicații open-source (eng. "cu sursa deschisa"- practica de a produce sau dezvolta permițând accesul utilizatorului sa acționeze liber asupra procesului de producție sau dezvoltare) şi distribuite care să permită colectarea şi analiza log-urilor (eng. colecție de evenimente) emise de către stațiile de lucru prezente într-o rețea locală.

În cadrul acestui demers, entitățile de bază considerate sunt :

- ***aplicația de tip server*** care acționează ca un sistem de colectare a log-urilor emise de către stațiile monitorizate;
- ***aplicația de tip client*** care colectează informațiile de pe stațiile unde este present şi le trimite către server;
- ***interfața cu utilizatorul*** care permite urmărirea informațiilor colectate pe server.

Funcționarea aplicației de monitorizare a log-urilor parcurge următorii paşi:

1. serverul trimite cereri de conectare către toate stațiile de lucru care sunt specificate în fişierul său de configurare;
2. stațiile de lucru care primesc cererea şi au instalată aplicația de tip client vor efectua un proces de confirmare şi stabilire a legăturii (*eng.Handshake – proces automat de negociere care seteaza parametrii de comunicare*) cu serverul, după care primesc sarcinile pe care trebuie să le execute;
3. în momentul în care un client, prin procesul de monitorizare, recepționează o informație cerută, acesta trimite log-ul către server;
4. serverul colectează log-ul şi îl stochează;
5. informațiile adunate de către server pot fi vizualizate prin intermediul aplicației cu rol de interfață grafică.

Scopul principal al proiectului este monitorizarea log-urilor şi managementul lor, aşa cum reiese şi din modul de funcționare al aplicației descrise anterior.

Tematica urmărită de proiect a fost aleasă pentru a cumula un număr cât mai mare de arii de interes pentru formarea ca inginer în domeniul calculatoare şi tehnologia informației. În cadrul proiectului sunt utilizate noțiuni, tehnici şi tehnologii din domenii cum ar fi:

- rețele de calculatoare;
- securitatea informației;
- programare în Python/C# ;
- proiectarea arhitecturilor software;
- servicii Linux;
- testare software.

Log managementul este procesul care generează, adună, transmite, stochează, analizează şi şterge evenimentele de tip log primite de la diverse surse [National Institute of Standards and Technology, 2006]. Din punct de vedere architectural, log managementul se împarte în 3 nivele, [3]:

Nivelul 1:Generarea log-urilor

Include sistemul, rețeaua şi aplicațiile care generează date.

Nivelul 2: Analiza şi stocarea log-urilor

Acesta este compus din serverele de log, cunoscute sub denumirea de colectori de log-uri (eng. *log collectors)* care primesc datele de la primul nivel.

Nivelul 3: Monitorizarea log-urilor

Compus din aplicații administrative care au rolul de a monitoriza şi analiza datele colecționate.

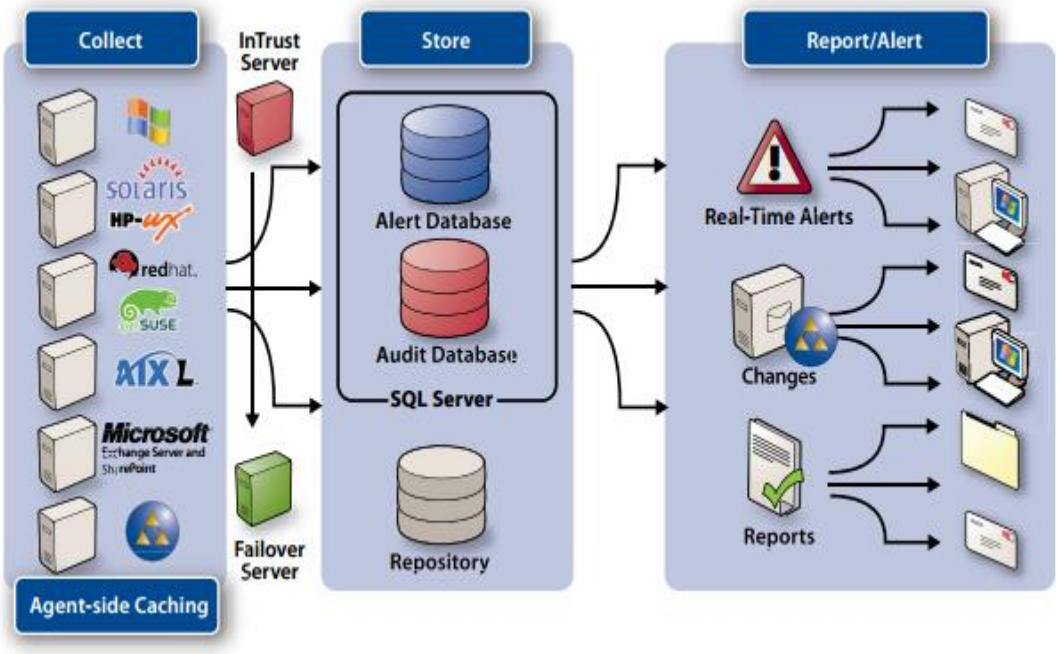

Figura** Error! No text of specified style in document.**.1.Nivelele din care este compusă o aplicație de log management

Modulele de bază folosite în dezvoltarea aplicației de log management sunt :

- **Protocolul de control al transmisiei** (*eng. Transmission Control Protocol, TCP*)
  Este un protocol de bază al suitei de protocoale de tip Internet. Efectuează o conectare virtuală full duplex intre două puncte terminale, fiecare punct fiind definit de către o adresa IP (*eng. Internet Protocol, IP*) şi de către un port TCP. Protocolul TCP este elementul de bază pentru comunicarea între stațiile de lucru, astfel fiind foarte important pentru dezvoltarea aplicației de management al log-urilor.
- **Sistemul de operare** (*eng. Operating System, OS*)
  Sistemul de operare vizat pentru dezvoltarea aplicației este Linux. Alegerea acestui sistem de operare a fost determinată în primul rând de faptul că acesta este preferat în rândul companiilor şi firmelor din ce în ce mai mult datorită avantajelor pe care le prezintă față de larg răspânditul sistem de operare Windows, şi anume costul, stabilitatea, securitatea ș.a.m.d. Pe de altă parte, experiența dobândită la materia *Sisteme de operare* a contribuit la luarea deciziei.
- **Python**
  Limbajul de programare Python a fost ales ca mediul principal de dezvoltare a aplicației deoarece se găseşte pe orice distribuție de Linux, conține biblioteci specializate pentru comunicații de tip server-client şi are o documentație completă. De asemenea, experiența de a lucra în Python dobândită pe parcursul studierii disciplinei *Rețele de calculatoare* a contribuit la luareadeciziei.