ANTIVIRUS

Functia de baza a unui antivirus este aceea de a scana fisierele de pe discul unei statii de lucru, in scopul de a identifica fisierele "infectate". Un fisier este considerat "infectat" daca el contine secvente considerate "malitioase", adica secvente pe care antivirusul le are inregistrate in baza sa de cunostinte. Antivirusul poate scana diverse tipuri de fisiere cum ar fi fisiere text, fisiere executabile, etc. Un fisier text este considerat infectat daca el contine cel putin un cuvant "malitios", in timp ce un fisier executabil trebuie sa contina cel putin una din secventele binare cunoscute de antivirus (ar putea fi "semnatura" unui virus). Antivirusul realizeaza scanarea fisierelor printr-un ScanManager ce gestioneaza o serie de ScanWorkeri specializati pe diverse tipuri de fisiere (pentru fisiere text, pentru fisiere executabile, etc.).

Astfel, plecand de la o lista de fisiere data, antivirusul, prin intermediul managerului instantiat va genera workeri de scanare, in functie de tipul fisierelor intalnite (tipul fisierului este dat de extensia acestuia: .txt, .exe, ...). Pentru a nu ocupa resursele statiei monitorizate, antivirusul are un numar maxim (o limita) de workeri pe care ii poate genera. Daca lista de fisiere scanate este mai lunga, iar antivirusul a creat deja numarul maxim de workeri, va incepe sa refoloseasca din workerii deja creati.

Scopul operatiei de scanare este aceea de a genera un raport sub forma unui fisier text de jurnalizare (raportare) in care se vor trece fiecare din fisierele scanate, id –ul workerului care realizeaza scanarea, iar pentru cele gasite „infectate", gradul infectiei (cate cuvinte recunoscute sau cati „virusi" detectati). In finalul raportului va fi un sumar care contine numarul total de fisiere scanate si numarul total de workeri care au contribuit la scanare.

Antivirusul are posibilitati de actualizare a bazei sale de cunostinte utilizate pentru scanarea de fisiere (pentru cele text primeste un sir de carcatere cu cuvintele noi „malitioase" pe care le adauga bazei sale de cunostinte, iar pentru cele executabile primeste numele fisierului continand semnatura unui nou virus). La nivelul antivirusului precum si la nivelul clasei (claselor) de gestiune a bazei de cunostinte se vor implementa operatiile necesare in acest sens. De asemenea, se va implementa functionalitatea de a verifica daca antivirusul este „up-to-date" in raport cu o baza de cunostinte data. Aceasta functionalitate verifica daca baza de cunostinte a antiviruslui contine cel putin tot ce contine o baza de cunostinte in raport cu care se face verificarea. In acest sens se vor folosi cel putin un mecanism de supraincarcare de operatori.

Antivirusul poate realiza scanarea si in modul „strict", mod in care workerii se comporta diferit la scanare. In acest mod, recunosaterea unei secvente malitioase (text sau binara) are loc daca secventa este identica cu cea din baza de cunostinte in proportie de P% unde P este transmis ca parametru operatiei de scanare stricte a ScanManagerului.

Indicatii de implementare:
Lista de fisiere ce va fi scanata este transmisa operatiei de scanare a ScanManager –ului ca sir de caractere continand numele fisierelor ce urmeaza a fi scanate, separate prin spatii. Limita maxima de workeri este data la constructia ScanManager-ului.
Fiecare worker de scanare are un id unic (numar intreg) care este autogenerat la crearea workerului. Primul worker are id –ul 0, urmatorul 1, samad.
Pentru gestionarea stringurilor (cum ar fi numele fisierelor) si a operatiilor asociate se va folosi implementare proprie minimala de clasa pentru gestiunea stringurilor.
Cel putin pentru implementarea bazei de cunostinte se va folosi o implementare proprie de lista, operatiile asociate cu aceasta structura fiind realizata printr-o clasa template.
ScanManager –ul trebuie sa fie implementat asa incat sa suporte o singura instantiere per aplicatie (aka Singleton).

Situatiile exceptionale (vor fi tratate prin mecansime bazate pe exceptii):
S-a atins limita maxim admisa de workeri, dar este nevoie de un tip de worker care insa nu exista in lista. Se va distruge un worker existent pentru a se creea workerul necesar.
Sunt probleme de acces la fisiere, se logheaza in fisierul de raportare si se continua scanarea
Baza de cunostinte este goala, se logheaza si se opreste operatia de scanare
Sunt probleme critice (alocare de memorie), se incearca logarea si apoi se inchide aplicatia.