GHID GENERAL DESPRE ANALIZA LOG-URILOR

CE ESTE UN LOG

Este un jurnal digital al unui eveniment sau a unei activități generate de un software, sistem de operare sau aplicație.

Tipuri de log-uri:

- Event log
- Server log
- Application log
- Database log
- Security log
- System log
- Audit log.

Event logs

- Un jurnal de evenimente este o înregistrare cronologică a acțiunilor, sau modificărilor care au loc într-un sistem sau într-un proces. Este folosit pentru monitorizarea și înregistrarea activităților importante pentru analiză, audit sau urmărire a istoricului.

Exemplu log entry (Security Event)

Logon Type: 3
User: NT AUTHORITY\SUSTEM
Source: Security
Event ID: 4624
Description: An account was succesfully logged on.

System logs

- Jurnalele de sistem urmăresc funcționarea sistemului de operare și a componentelor hardware. Ele includ informații despre pornirea sistemului, închiderea acestuia și problemele hardware.

Exemplu

Log Type: Error
Source: Disk
Event ID: 7
Description: The device, \Device\Harddisk0\DR0, has a bad block.

Security logs

- Jurnalele de securitate sunt înregistrări detaliate care urmăresc evenimentele legate de securitatea unui sistem informatic sau a unei rețele. Ele conțin informații despre accesul la resurse, încercările de intruziune, erorile de autentificare și alte activități care pot afecta securitatea.

Exemplu

Log Type: Information
Source: Security
Event ID: 4624
Description: An account was sucessfully logged on.
Logon Type: 3
User: DOMAIN\User

Application log

- Jurnalele de aplicație sunt fișiere sau înregistrări digitale care documentează activitățile și evenimentele care au loc în cadrul unei aplicații software. Aceste înregistrări includ informații detaliate despre erori, avertismente, solicitări de servicii, trasee de execuție și alte aspecte relevante pentru funcționarea și diagnosticarea corectă a aplicației.

Exemplu

Log Type: Error
Source: Application Error
Event ID: 1000
Description: Faulting application<Application Name>, version <Version>, faulting module <Module Name>, version <Module Version>, fault address <Memory Address>.

Audit log

- Jurnalele de audit înregistrează informații despre activitățile utilizatorilor și despre schimbările ce țin de configurarea sistemului. Sunt esențiale pentru conformitate și evidență.

Exemplu

Log Type: Success Audit
Source: Security
Event ID: 638
Description: User Account Management: User Account Created.
New account: DOMAIN\NewUser

Debug logs

- Jurnalele de depanare sunt înregistrări detaliate care conțin informații relevante pentru diagnosticarea și remedierea erorilor și a altor probleme într-un software sau sistem informatic. Aceste înregistrări conțin de obicei informații despre acțiunile și stările sistemului, mesaje de eroare, valori ale variabilelor și alte date relevante pentru procesul de depanare.

Exemplu

Log Type: Debug
Source: MyApp
Event ID: 638
Message: Entering function <Function Name>.
Variable1=<Value1>, Variable2=<Value2>

Transaction logs

- Jurnalele de tranzacții urmăresc modificările efectuate într-o bază de date pentru a asigura integritatea și recuperabilitatea datelor în caz de eșecuri de sistem.

Exemplu

Log Type: Information
Source: SQL Server
Event ID: 9002
Description: The transaction log for database <Database Name>is full due to <'Reason'>.
Trasaction log entries: ...

COMPONENTELE UNUI LOG

Componentele unui jurnal digital, pot include diferite date și elemente precum:

- Timestamp sau Marcajul temporal
- Hostname sau Identificatorul Sursei
- Aplicația sau Identificatorul Procesului
- Nivelul de Severitate
- Mesajul log
- User sau Informația entității
- Event ID sau Identificator unic
- Status/ Outcome
- Metadate (adițional)
- Alte câmpuri

Timestamp

- Acesta indică data și timpul când a avut log evenimentul;
- Este esențial și obligator în ordonarea cronologică a evenimentului și corelarea activităților.

Exemplu

2024-12-17 18:20:55 (An-Luna-ZI Ora:Minute:Secunde)

Hostname

- Identifică sursa de înregistrare a log-ului, deseori este vorba de dispozitivul sau sistemul ce generează înregistrarea.
- Ajută la identificarea originii evenimentului în mediul de rețea.

Exemplu

web-server-01 sau 192.168.1.100

Process Identifier

- Specifică aplicația sau procesul relaționat cu evenimentul înregistrat.
- Facilitează categorizarea și identificarea rapidă a sursei.

Exemplu

sshd (SSH daemon) , apache (Apache Web Server)

Nivelul de severitate

- Indică severitatea sau importanța evenimentului înregistrat;
- Asistă la prioritizarea și filtrarea evenimentelor bazată pe impactul acestora.

Exemplu

INFO, ERROR, WARNING

Log Message

- Conține informații detaliate despre eveniment sau activitate;
- Oferă context și specifică mai concret ce s-a întîmplat.

Exemplu

Accepted publickey for user123 from 192.168.1.100 port 22 ssh2

Informația despre utilizator

- Specifică utilizatorul sau entitatea asociată cu evenimentul;
- Ajută în urmărirea activității utilizatorului și securitatea investigațiilor.

Exemplu

user123, admin

Event ID sau Identificator unic

- O valoare unică asignată fiecărei noi înregistrări la intrare;
- Facilitează referința și urmărirea unui eveniment specific.

Exemplu

EventID: 1234-5678-ABCD

Status

- Descrie etapa curentă sau rezultatul final al evenimentului;
- Indică dacă evenimentul a fost desfășurat cu succes sau a întâmpinat dificultăți.

Exemplu

Failure, Success

Metadata (informații adiționale)

- Informații adiționale ce oferă mai mult context evenimentului;
- Permite o mai bună înțelegere a înregistrărilor (log-urilor).

Exemplu

Session ID, Source IP, Destination IP

Cîmpuri personalizate

- Cîmpuri adiționale adăugate particular de organizații pentru mai multe informații specifice necesităților proprii.
- Personalizarea unor intrări pentru corespunderea unor formate sau cerințe.

Exemplu

CustomField1: value1, CustomField2: value2

FORMATUL LOG-URILOR

Formatul log-urilor se referă la structura în care înregistrările sau log-urile sunt prezentate în fișiere log. Acestea pot fi cu structurate fie pentru o mai bună interoperabilitate fie pentru citire mai ușoară.

Formatele comune includ:

- Syslog
- JSON
- CSV
- XML
- Format personalizat

SYSLOG

- Syslog este un standard pentru logging-ul mesajelor, oferind un mod pentru dispozitive de a produce și consuma log-uri.
- Fiecare intrare syslog constă din: timestamp, hostname, application, severity level, și log message.

Exemplu

<13> Jan 25 08:31:45 web-server-01 sshd[1234]: Accepted publickey for user123 from 192.168.1.100 port 22 ssh2

JSON

- JSON (JavaScript Object Notation) este un format de schimb de date ușor, lizibil pentru oameni și ușor de generat și interpretat de mașini. Este folosit frecvent pentru transmiterea datelor în aplicațiile web.
- Oferă un format structurat și ușor de citit.

Exemplu

```
{
“timestamp”: “2023-01-25T08:31:45”,
“hostname”: “web-server-01”,
“application”: “sshd”,
“hostname”: “web-server-01”,
“severity”: “INFO”,
“message”: “Accepted publikey for user123 from 192.168.1.100
port 22 ssh2”,
}
```

CSV

- CSV (Comma-Separated Values) este un format simplu de fișier folosit pentru stocarea datelor tabelare, unde fiecare linie a fișierului reprezintă un rând de date, iar valorile din fiecare rând sunt separate prin virgule.

Exemplu

2023-01-25 08:31:45, web-server-01,sshd,web-server-01,INFO, Accepted publikey for user123 from 192.168.1.100 port 22 ssh2

XML

- XML (eXtensible Markup Language) este un format de fișier folosit pentru a descrie datele într-o manieră structurată și lizibilă pentru oameni și mașini. Este utilizat pe scară largă pentru schimbul de date între sisteme diferite și pentru stocarea datelor.

Exemplu

```
<log>
<timestamp>2023-01-25T08:31:45</timestamp><hostname>web-server-
01</hostname>,<application>sshd</application><severity>INFO</severity><message>
Accepted publikey for user123 from 192.168.1.100 port 22 ssh2</message>
</log>
```

Format personalizat

- Organizațiile pot folosi model personalizat de elaborare a formatului log-urilor derivat din necesitățile ei.

Exemplu

[2023-01-25 08:31:45] [INFO][web-server-01][ssh] Accepted publikey for user123 from 192.168.1.100 port 22 ssh2

ANALIZA LOG-URILOR

Analiza jurnalelor este procesul de interpretare și revizuire a jurnalelor de evenimente generate de computer pentru identificarea proactivă a erorilor, amenințărilor de securitate sau altor riscuri.

Analiza jurnalelor este de obicei realizată în cadrul unui Sistem de Gestionare a Jurnalelor, o soluție software care adună, sortează și stochează datele jurnalelor și jurnalele de evenimente dintr-o varietate de surse. De exemplu: ELK Stack (Elasticsearch, Logstash, Kibana), Splunk, Graylog.

PAȘI DE ANALIZA

01
Colectarea datelor

02
Indexarea datelor

03
Analiza

04
Monitorizarea

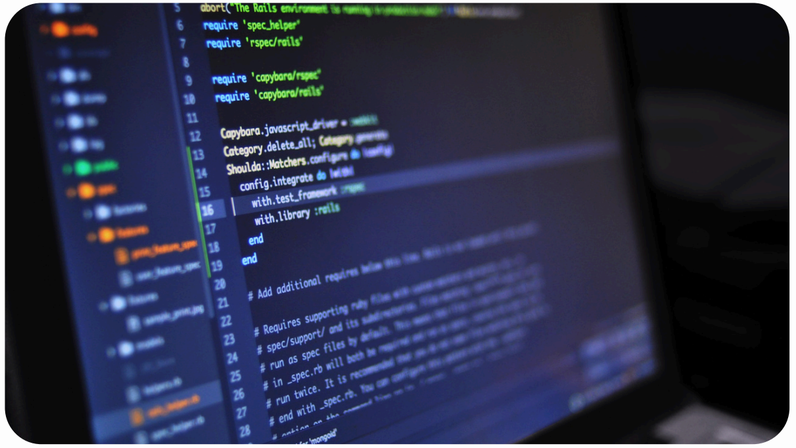
05
Raportarea

METODE DE COLECTARE A LOG-URILOR

Agents

Componentele software instalate pe sistemele individuale care colectează și transmit jurnale către un depozit central.

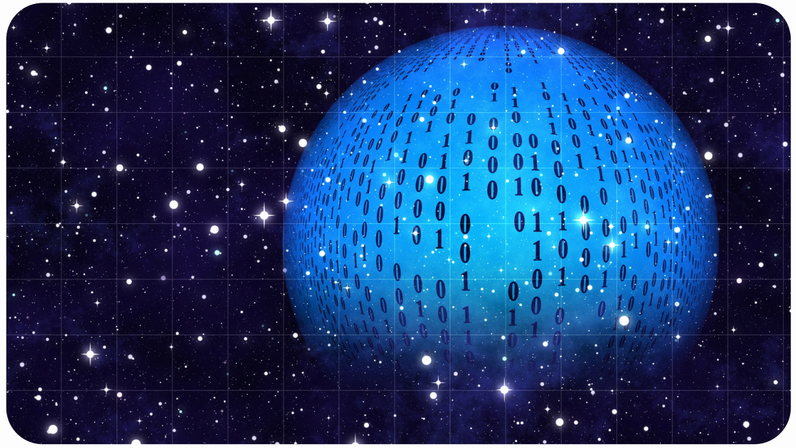
- Colectare în timp real
- Ușor
- Potrivit pentru sistemele la distanță sau dezactivate
- Necesită instalare pe fiecare sistem
- Consum potențial de resurse



Syslogs

Un protocol standard pentru transmiterea mesajelor de jurnal în cadrul unei rețele IP.

- Standardizat
- Atât UDP și TCP
- Folosit pe scară largă în sistemele bazate pe UNIX
- Funcționalități de securitate limitate în protocolul syslog original

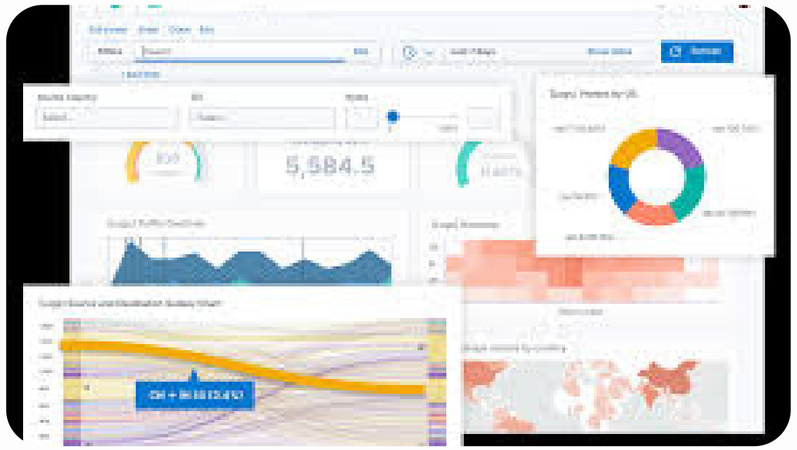


Log forwarder

Instrumente specializate care colectează jurnale din diverse surse și le transmit către sisteme centralizate de gestionare a jurnalelor.

- Agregarea jurnalelor din multiple surse
- Funcționalități de securitate îmbunătățite
- Suprasarcină de configurare și întreținere

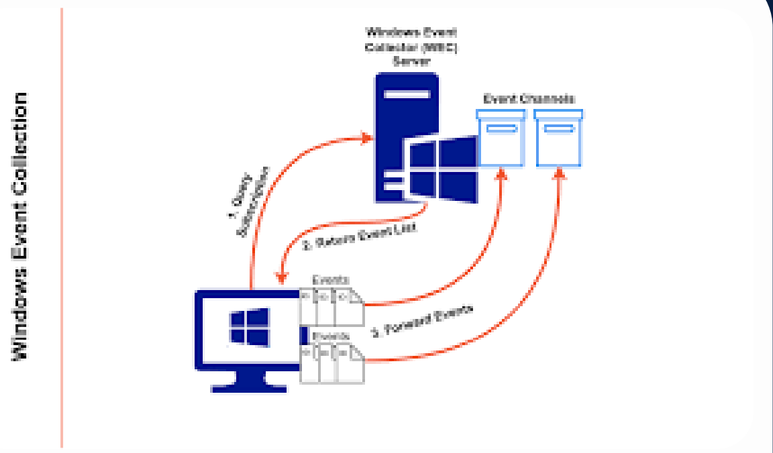
METODE DE COLECTARE A LOG-URILOR



CENTRALIZED LOGGING SOLUTIONS

Platforme complete care centralizează stocarea, analiza și vizualizarea jurnalelor.
exemplu: ELK Stack, Splunk, Graylog

- Scalabilitate
- Capabilități puternice de căutare și analiză
- Unelte de vizualizare
- Cost (unele soluții pot fi costisitoare)
- Consum intensiv de resurse



WINDOWS EVENT FORWARDING

Mecanism specific Windows pentru colectarea și transmiterea jurnalelor de evenimente.

- Caracteristică integrată în Windows
- Susține abonamente și transmitere personalizată a evenimentelor
- Limitat la medii Windows

PACKET SNIFFING

Capturarea și analizarea traficului de rețea pentru a extrage informații similare cu cele din jurnale.

- Oferă perspective asupra activităților la nivel de rețea
- Detalii limitate la nivelul aplicației
- Potențiale considerații etice și legale

FACTORI DE LUAT ÎN CONSIDERARE ÎN COLECTAREA JURNALELOR

Scalabilitatea

Metoda aleasă ar trebui să se poată scala odată cu volumul de date de jurnal.

Securitatea

Asigurați confidențialitatea și integritatea jurnalelor colectate.

Compatibilitatea

Compatibilitate dintre sursele de jurnale și instrumentele de analiză utilizate.

SURSE COLECȚII DE LOG-URI

- Windows Event Logs
- Linux/Unix Syslogs
- Routers and Switches
- Firewalls
- Apache Access and Error
- Logs
- Nginx Access and Error
- Logs
- Java Application Logs
- .NET Application Logs
- Database Server Logs
- AWS CloudWatch Logs
- Azure Monitor Logs
- Syslog Aggregation)
- Splunk, ELK Stack (Elasticsearch, Logstash, Kibana)
- Docker Logs
- Kubernetes Events and Logs
- Application-specific logs
- Active Directory Logs
- LDAP Logs
- Custom Application Logs
- Terraform Logs
- Antivirus and Anti-malware
- Logs
- VMware/Hyper-V Logs
- Logs from MDM Systems

TEHNICI DE ANALIZĂ

- CĂUTARE ȘI FILTRARE
- CORELAREA
- DETECTARE ANOMALIE
- NORMALIZAREA

Căutare și filtrare

- Expresii regulate (Regex) - Utilizați expresii regulate pentru a căuta și filtra intrările de jurnal bazate pe modele și criterii.

  Exemplu: Căutarea adreselor IP, a codurilor de eroare specifice sau a numelor de utilizatori.

- Instrumente command-line -Valorificați comenzile precum grep și awk pentru căutarea și filtrarea eficientă a jurnalelor în interfața de linie de comandă.

  Exemplu: Utilizarea comenzii grep pentru filtrarea liniilor care conțin cuvinte cheie specifice.

CORELAREA

- Analiștii pot combina jurnalele din multiple surse pentru a ajuta la descifrarea unui eveniment care nu este ușor vizibil cu datele dintr-un singur jurnal.
- Acest lucru este util în timpul și după atacurile cibernetice, unde corelarea între jurnalele de la dispozitive de rețea, servere, firewall-uri și sisteme de stocare ar putea indica date relevante pentru atac și ar putea evidenția modele care nu erau evidente dintr-un singur jurnal.
- Alinierea evenimentelor pe baza marcajelor temporale pentru a înțelege secvența de activități.
- Identificarea și conectarea evenimentelor relevante din surse de jurnale diferite pentru a stabili o vedere cuprinzătoare a unui incident.

Detectarea anomaliei

- Stabilirea comportamentului de bază și utilizarea metodelor statistice pentru a detecta abateri care indică anomalii potențiale.

Exemplu: Identificarea unei creșteri bruște în traficul de rețea sau a unei creșteri semnificative în încercările eșuate de autentificare.

- Aplicarea algoritmilor de învățare automată pentru a învăța modele normale și pentru a detecta abateri.

Exemplu: Antrenarea unui model pentru a recunoaște modele neobișnuite în comportamentul utilizatorilor.

Normalizarea

- Conversia datelor diverse din elementele jurnalelor într-un format standard poate ajuta la asigurarea că comparările pot fi făcute și că datele pot fi stocate și indexate central, indiferent de sursa jurnalului.

Luați în considerare în analiză factorii

Înțelegeți contextul în care au fost generate jurnalele pentru o analiză precisă.

Implementați măsuri pentru a reduce rezultatele pozitive false în detectarea anomaliilor.

Utilizați script-uri și automatizare pentru a eficientiza sarcinile repetitive de analiză.

Documentați metodologiile și constatările analizei pentru referințe viitoare.