KÜRT
INFORMÁCIÓMENEDZSMENT

logdrill
MAKE YOUR DATA WORK

LogDrill termékleírás

v 3.1

LogDrill alkalmazás bemutatása

A naplóállományok elemzésében az egyik legnehezebb feladatot a nagy adatmennyiségek hatékony kezelése jelenti. Az informatikai rendszerek naplóállományok formájában óriási mennyiségű nyersadatot generálnak saját működésükről. A napjaink logelemző alkalmazásaiba épített, általánosan elterjedt módszerek használatával ennek az adatmennyiségnek a feldolgozása még a legegyszerűbb logelemző műveleteknél is hosszas várakozást eredményezhet. A rendszermeghibásodások, az incidenseket jelző információk időben történő feltárása ilyen módon szinte lehetetlen. A naplóállományok elemzésének ezt a sarkalatos és jellemző problémáját küszöböli ki a LogDrill alkalmazás, amely a terület legújabb kutatási eredményeinek felhasználásával kifejlesztett, speciális adatbázis-motort alkalmaz.

1.1.1 A termék főbb előnyei és jellemzői

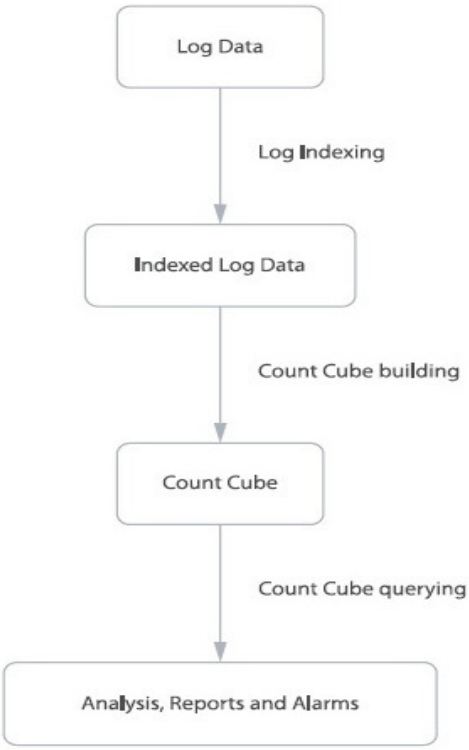
- **Korszerű, „state-of-the-art" technológia:** A szoftver az adatbázis elméletek területén végzett kutatások legfrissebb eredményeit alkalmazza. A LogDrill kétlépcsős adattömörítési módszere segítségével birkózik meg a nagyobb adatmennyiségekkel. Az eredeti naplófájlokból leválogatott, az elemzés szempontjából releváns információt tartalmazó számosság-kocka a nyers naplóállományoknál nagyságrendekkel kisebb lehet, jelentősen megkönnyítve és meggyorsítva ezzel az elemzői munkát.
- **Normalizáció:** A naplóállományok jellemzően strukturálatlan vagy félig strukturált formában állnak elő. A LogDrill nagy sebességgel strukturálja ezen adatokat és hozza egységes, így együttesen elemezhető formátumra. A LogDrill számos logformátumot beépítetten ismer, mely jelentősen segíti a feldolgozási szabályok, szabályszettek elkészítését.
- **Intuitív elemzés:** A legkézenfekvőbb, ha az első elemzési lépésként az eseményszámosságok változását vizsgáljuk meg. Ez az esetek több mint 80%-ban segít lokalizálni a rendszerekben felmerült anomáliákat. A LogDrill ezen módszertant támogatja az eseményszámosságok széleskörű vizsgálatát lehetővé tevő, interaktív „drag-and-drop" lekérdezés-szerkesztőjével.
- **Vizualizáció:** Az alkalmazás a lekérdezések eredményeit grafikus felhasználói felületének (Dashboard) segítségével az elemző igényeinek megfelelően, többféleképpen (grafikonok, diagramok, táblázatok) vizualizálja a hatékony munkavégzés támogatása érdekében. Létrehozhatók olyan mátrixok is, amelyek más adatelemzési platformokkal is feldolgozhatóak.
- **Erőforrás-hatékonyság:** Az elemzési folyamat akár egy átlagos laptopon is elvégezhető: 1 TB nyers tömörítetlen naplóállományból, kb. 100 GB tömörített log állítható elő. Az ebből épített belső modell akár 1 GB-ra tömörítve egy egyszerű gép memóriájában is elfér.
- **Biztonság:** A felhasználók csak olyan projekteken dolgozhatnak, melyekhez jogosultságot kaptak, és ezekhez kizárólag a szükséges erőforrásokat vehetik igénybe. A rendszeradminisztrátor egyedi feladatköröket rendelhet hozzá az egyes felhasználókhoz, ami tovább növeli a LogDrill biztonságosságát és sokoldalú felhasználhatóságát.
- **Integrálhatóság:** A LogDrill könnyen integrálható más rendszerekkel, input és output oldalon egyaránt. Bemeneti oldalon: a LogDrill bármilyen, félig strukturált szöveges adat (naplófájl) feldolgozására képes, mert rugalmasan konfigurálható. Kimeneti oldalon: a LogDrill szabványos CSV-formátumban is exportálhatóvá teszi az adatokat, hogy azok akár az Excel számára is feldolgozhatóak legyenek. Emellett a rendszerbe épített riasztási („alerting") funkció lehetővé teszi az alkalmazás eseménykezelő rendszerekbe integrálását.

Korábbi projektjeink során szerzett tapasztalataink azt mutatják, hogy az alkalmazás a következő területeken nyújt kimagasló támogatást felhasználói számára:

- biztonsági események műszaki vizsgálata, a bekövetkezési körülmények elemzése, kivizsgálása („forensics" célú elemzés);
- az informatikai rendszerek működésével, rendelkezésre állásával kapcsolatos információk szolgáltatása, incidensek felismerése;
- elemzések alapján az IT rendszerek karbantartása és működésük optimalizálása (üzemeltetéstámogatás).

1.1.2 A Logdrill működése

A LogDrill a feldolgozásra kijelölt, előzetesen összegyűjtött naplóállományokat indexálja annak érdekében, hogy a logsorok az elemzési munka későbbi szakaszaiban gyorsan elérhetőek legyenek. Ezt követően történik a normalizálás, amikor a szövegelemzési szabályok alapján a félig strukturált adatokból strukturált adat készül, majd az aggregációt követően a logokból egy számosság-kocka áll elő. Mivel az eredeti logsorokból így az elemző számára lényegtelen adatok kikerülnek, a számosság-kocka nagyságrendekkel kisebb az eredeti logállománynál.



1. ábra LogDrill: a logfeldolgozási folyamat fő lépései

A lekérdezéseket a program a számosság-kockában futtatja le. Ehhez egy, az MDX-hez (lekérdező nyelv OLAP-adatbázisokhoz) hasonló szintaxisú lekérdezési nyelvet használ. A lekérdezések interaktív módon történnek, minimális várakozási idővel. A találatok – a lekérdezés tartalmától függően – többdimenziós adatállományok. A lekérdezések eredményei kényelmesen megjeleníthetők jelentések, táblázatok és grafikonok formájában.