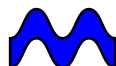


LOG MANAGEMENT



Strudsemetoden

Vi definerer strudsemetoden som den brug af logs, hvor man sent i et forløb opdager et problem og derefter manuelt går tilbage på en server / switch og søger igennem loggen for at se om man kan finde et problem.

Eller lader sine switches (og måske også servere) sende alle logs ind i en fælles base og så glemmer alt om dem. Denne fælles "skraldespand" gør det meget besværligt efterfølgende at søge i logs, og der er ingen proaktiv korrelering. Med andre ord: **Vi stikker hovedet i sandet og bruger ikke logs aktivt.**

Om Logning

De fleste IT afdelinger bruger logs efter strudsemetoden. Det betyder ingen aktiv indsamling, ingen proaktiv anvendelse og kun en reaktiv brug af logs ved at dykke ned i devices logs for at finde nålen i høstakken, som måske kan give et fingerpeg om en driftsforstyrrelse eller en sikkerhedsbrist.

Alternativt bruges logs ved at pege alle dine enheder hen på en samlet base hvor du gemmer logs i hvad der bedst kan beskrives som en skraldespand. Det nemmeste er at trykke "delete all" - meget nemmere end at bruge disse logs aktivt.

Men **logs er den ultimative kilde til information** om tilstanden, fejl og sikkerhedsbrister i alle dine IT systemer og **du går derfor glip af muligheden for en bedre IT-drift, hvis du ikke bruger dine logs aktivt:**

- **Aktiv indsamling** af logs fra dine servere, routere, switches, firewalls, access punkter, applikationer, m.fl. til én fælles database. Logs forwardes normalt som syslogs og typisk omformes dine windows

eventlogs til syslogs vha. en lokal agent på den enkelte server.

- **Log korrelering** er en disciplin hvor din logløsning intelligent "smager på" og sammenligner de indkomne logs mht. frekvens og sammenhæng. Det muliggør at systemet automatisk advarer dig, når der er noget i dine logs, du SKAL være opmærksom på. Derved bruger du dine logs proaktivt.
- **Logsøgning** udføres via dit logsystem i et interface, der gør det muligt (og nemt) at søge på tværs af alle dine logs i et bestemt tidsrum efter en bestemt type af information (fx. hvad har en bestemt IP adresse foretaget sig på nettet sidste onsdag mellem 12 og 14?).
- **Compliance og rapportering** er andre store funktioner i en god log løsning, fordi du med de indbyggede funktioner, gør det nemt at holde både revisionen og ledelsen tilfredse med beviselig compliance og indbyggede rapporter på inventory, sikkerhed, driftsfejl, applikationsfejl mm.

Udbytte af aktiv logning

Sporbarhed: Hvem har gjort hvad og hvornår. Du får overblik via rapporter med detaljer om hvem der har haft adgang til dine servere og switches, samt hvad de har lavet og hvornår. Du kan også brug løsningerne til effektiv interaktiv søgning.

Compliance: Lever du op til revisionens krav om logindsamling eller kravene til kommuner under DS484 og ISO27001 standarderne? En god logløsning giver dig den nødvendige compliance.

Forbedret IT sikkerhed: Du ved helt sikkert hvad der er sket på et bestemt tidspunkt og hvem der har været årsag til eventuelle problemer. Via log korrelering får du proaktivt besked om eventuelle problemer, så du kan nå at gribe ind overfor fx sikkerhedsbrister. Desuden kan du nemt lave en baseline over mængden

Praktiske eksempler

Større driftsforstyrrelse: Du står pludselig med en større driftsforstyrrelse og ved ikke hvad eller hvem, der forårsagede den, men du ved, at der står 500 brugere og triller tommelfingre - inklusive chefen! Med en proaktiv anvendelse af dine logs ville du være blevet advaret om manglende diskplads på den primære DC. Herefter røg mail systemet og alle DC accounts kunne ikke længere logge på domænet...

Revisionskrav: Revisionen kræver, at du kan dokumentere, at du aktivt indsamler og arkiverer dine logs. Det kræver en masse manuelt arbejde og det kan du slippe for ved at automatisere processen med en log management løsning.

Sikkerhedsbrud: Problemer med sikkerhedsbrud kan være af større eller mindre omfang, men hvis du ikke

af sikkerhedslogs og ved at se på variationen dag for dag opdage eventuelle sikkerhedsproblemer på en nem og enkel måde.

Forbedret drift og hurtigere

problemløsning: Ved at bruge dine logs proaktivt, bliver du alarmeret om eventuelle problemer, når de opstår, og du kan derfor hurtigere rette dem, så de får minimal indflydelse på driften. Det gælder fx. applikationer som fejler, hardware der svigter, DOS angreb, ressourceforbrug, fejlsøgning på kritiske applikationer og ændringer af rettigheder.

Tids- og ressourcemæssig besparelse:

Bruger du tid på at lave manuelle rapporter over logs eller ad hoc søgninger i dine logs på forskellige maskiner, så er der væsentlige tidsmæssige besparelser at hente ved at bruge en rigtig log management løsning.

indsamler og analyserer (og korrelerer) dine logs, så bruger du strudsemetoden og ved derfor ikke om der er sikkerhedsmæssige problemer og navnlig hvor store de er. Følgende er eksempler på områder, der ofte kan give sikkerhedsmæssige problemer:

- Brug af konti fra tidligere medarbejdere
- Ændring af brugerrettigheder
- Uautoriserede trafikmønstre (fx Skype, FTP, Youtube mm)
- Uautoriseret adgang til filer og foldere
- Identifikation af malware og orme
- Identifikation af sårbarheder
- Intrusion og direkte hacker angreb. Husk, at det første en hacker vil gøre er at slette sine spor. Hvis du ikke samler dine logs aktivt ind, så er de helt sikkert slettet, når du skal bruge dem.