

Cégep Limoilou

TP1

Travail présenté à :

Patrick Dubois

Dans le cadre du cours :

420-6B6-LI

Sécurité des applications

Par :

Amir Boulmerka, Lawrence Lefebvre et Antoine Fortier

Date : 2024-04-03

## Introduction :

Sécurité des logs, des journaux et de la gestion des erreurs.

Un log, événement ou journal, est simplement la notification d'un événement d'une importance plus ou moins élevée envoyée par un service, un système, un élément réseau ou une application. Les journaux d’événement permettent en administration systèmes, réseaux et en sécurité de retracer les actions et la vie d'un système. Les logs ont un intérêt et une importance cruciale en informatique, car il s'agit là de savoir ce qu'il s'est passé sur un ensemble d'applications ou systèmes.

## Clientèle cible :

Cette présentation est pour les programmeurs qui effectueront des tâches de programmation ou de maintien sur un système.

## Objectifs :

* Informer les utilisateurs sur l’importance des logs dans un système.
* Informer les utilisateurs sur les failles de sécurités possibles liées aux logs d’un système.
* Les impacts
* Informer les utilisateurs sur comment bien sécuriser les logs d’un système.

## Contenu général :

[Quels sont les points et sous-points qui seront traités ?].

Important : "système informatique" peut en effet se référer à une application logicielle

**Importance des logs dans un système :**

1. Débogage et diagnostic des problèmes : Les logs permettent aux développeurs et aux administrateurs système de retracer les actions précédentes en cas de dysfonctionnement ou de problème. Cela facilite l'identification et la correction des erreurs.
2. Sécurité : Les logs jouent un rôle crucial dans la détection des activités suspectes ou des tentatives d'intrusion. Ils fournissent une piste de vérification pour examiner les comportements anormaux et identifier les menaces potentielles à la sécurité du système.
3. Conformité réglementaire : Dans de nombreux secteurs, il est obligatoire de conserver des logs pour se conformer aux réglementations en matière de sécurité et de confidentialité des données. Les logs peuvent être utilisés pour démontrer que des mesures de sécurité adéquates ont été mises en place et que les données sensibles sont protégées conformément aux normes réglementaires.
4. Audit et traçabilité : Les logs fournissent une traçabilité des actions effectuées dans un système, ce qui est crucial pour les audits internes et externes. Ils permettent de vérifier qui a accédé à quelles données et quand, ce qui est essentiel pour assurer la responsabilité et la transparence.
5. Optimisation des performances : En analysant les logs, les administrateurs peuvent identifier les goulots d'étranglement et les inefficacités dans le système, ce qui leur permet d'apporter des modifications.

**Les failles les plus courantes :**

* Les connexions, échecs de connexion ou de transactions sensibles ne sont pas journalisées
  + - Impact : Rend difficile la détection des comportements anormaux, des attaques potentielles ou des violations de sécurité.
    - Impact : Les attaquants peuvent exploiter cette lacune pour accéder illicitement au système ou effectuer des activités malveillantes sans être détectés.
* Les alertes ou les erreurs ne font l’objet que de journalisations insuffisantes ou peu claires, s’ils en font l’objet tout court.
  + - Impact : Les journalisations insuffisantes ou peu claires rendent difficile l'identification et la compréhension des causes des alertes ou des erreurs.
    - Impact : Les erreurs ou les alertes non journalisées ou mal journalisées peuvent entraîner la perte de données importantes ou de transactions critiques.
* Manque de journalisation liées à la santé d’un système et performance d’un système.
  + - Impact : Peut entraîner une augmentation des temps de réponse, des ralentissements et une dégradation des performances globales.
    - Impact : Difficile d'identifier les goulots d'étranglement et les problèmes de performance du système
* Les protocoles d’API et d’application ne sont pas contrôlés pour déceler des activités suspectes
* Logs non centralisés.
  + - Impact : Rend difficile leur gestion et leur analyse. Les administrateurs doivent naviguer à travers plusieurs sources pour accéder aux informations nécessaires, ce qui peut entraîner une perte de temps et une inefficacité opérationnelle.
* Mauvaise conservation des données liées au logs.
  + - Impact : devient difficile voire impossible de retracer l'historique des événements pour comprendre comment un incident s'est produit et quelles mesures doivent être prises pour éviter qu'il ne se reproduise.
    - Impact : Difficulté à identifier des problèmes récurrents.
    - Impact : De nombreuses réglementations et normes de conformité exigent la conservation des données de journalisation pendant une certaine période. Ceci peut entrainer des amendes et d'autres sanctions.
* Information sensible mal traité dans Les logs de journalisation.
  + - Impact : Fuite de données sensibles potentiel.
* Structure de logs non optimal.
  + - Impact : Une inefficacité opérationnelle.
    - Impact : Complique l'analyse des logs pour diagnostiquer les problèmes.
    - Impact : Entraîne une perte d'informations importantes pour la sécurité.
* Il n’y a pas de seuil ou un seuil inefficace d’alerte ni de remontée d’information pour y répondre
* Il n’est pas possible d’identifier une attaque en temps réel

**Comment y remédier :**

* Mettez en œuvre un processus de contrôle et journalisez tout ce qui concerne la connexion ou l’accès d’un utilisateur.
* Déterminez quels événements liés à la connexion et à l'accès des utilisateurs doivent être journalisés.
* Être capable de retracer la vie d’un utilisateur dans un système.
* Logger les tentatives de connexion de l’utilisateur.
* Logger les changements de mots de passe.
* Logger les changements d’accès.
* Logger les ressources accédées par l’utilisateur.
* Logger les actions effectuées.
* Etc..
* Mettre en place un processus de journalisation d’erreur.
* Configurez vos systèmes pour qu'ils captent les événements d'erreur système pertinents.
* Assurez-vous que les logs d'erreur incluent des informations détaillées telles que l'heure de l'incident, la nature de l'erreur, les codes d'erreur, les processus associés.
* Utilisez des alertes pour être informé immédiatement des erreurs critiques afin de pouvoir réagir rapidement.
* Enregistrement des informations pertinentes : Dans vos points de journalisation, enregistrez des informations utiles telles que le nom de la fonction appelée, les paramètres passés à la fonction, les valeurs de retour, les exceptions levées, etc.
* Retracer rapidement la source d’une erreur afin de pouvoir debugger et corriger.
* Analyse des performances de l’application à travers les logs.
* Dans le code ajouter des marqueurs de temps ou compteurs d’événements.
* Inclure des métriques telles que le temps de réponse, le débit, l'utilisation du CPU, la mémoire, le réseau, etc.
* Permet d’identifier les goulots d'étranglement.
* Permet de trouver les inefficacités et les opportunités d'optimisation des performances du système.
* Conservez les données de journalisation suffisamment longtemps.
* La conservation à long terme des logs peut être utile pour l'analyse des tendances et la détection des menaces à long terme.
* Assurez-vous de disposer de processus robustes pour la suppression sécurisée des logs une fois qu'ils ont dépassé leur durée de conservation.
* Stockez les journaux de manière sécurisée pour éviter toute altération ou suppression non autorisée.
* Faciliter l’accès aux logs en centralisant les journaux afin d’obtenir une vision complète et globale des performances de l’application.
* Comme Windows event viewer envoyer tous les logs d’un système à un endroit spécifique.
* Et catégoriser les logs d’une manière approprié.
* Permet Avoir une vue d'ensemble d'éléments cruciaux à la bonne gestion.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Ou dans le cas d’une application utilisé un système come Splunk .

Journalisation Centralisée : Splunk est conçu pour collecter, indexer et analyser les données de journal provenant de différentes sources en un seul endroit centralisé. Il vous permet d'agréger les journaux de différents systèmes, applications et appareils, fournissant une seule source de vérité pour les données de journal.

API pour l'Intégration : Splunk fournit une API REST robuste qui vous permet d'interagir avec les fonctionnalités de Splunk de manière programmable. Cette API vous permet d'effectuer une large gamme d'opérations, notamment :

Envoyer des données de journal à Splunk depuis des sources externes.

Rechercher et récupérer des données de journal stockées dans les index Splunk.

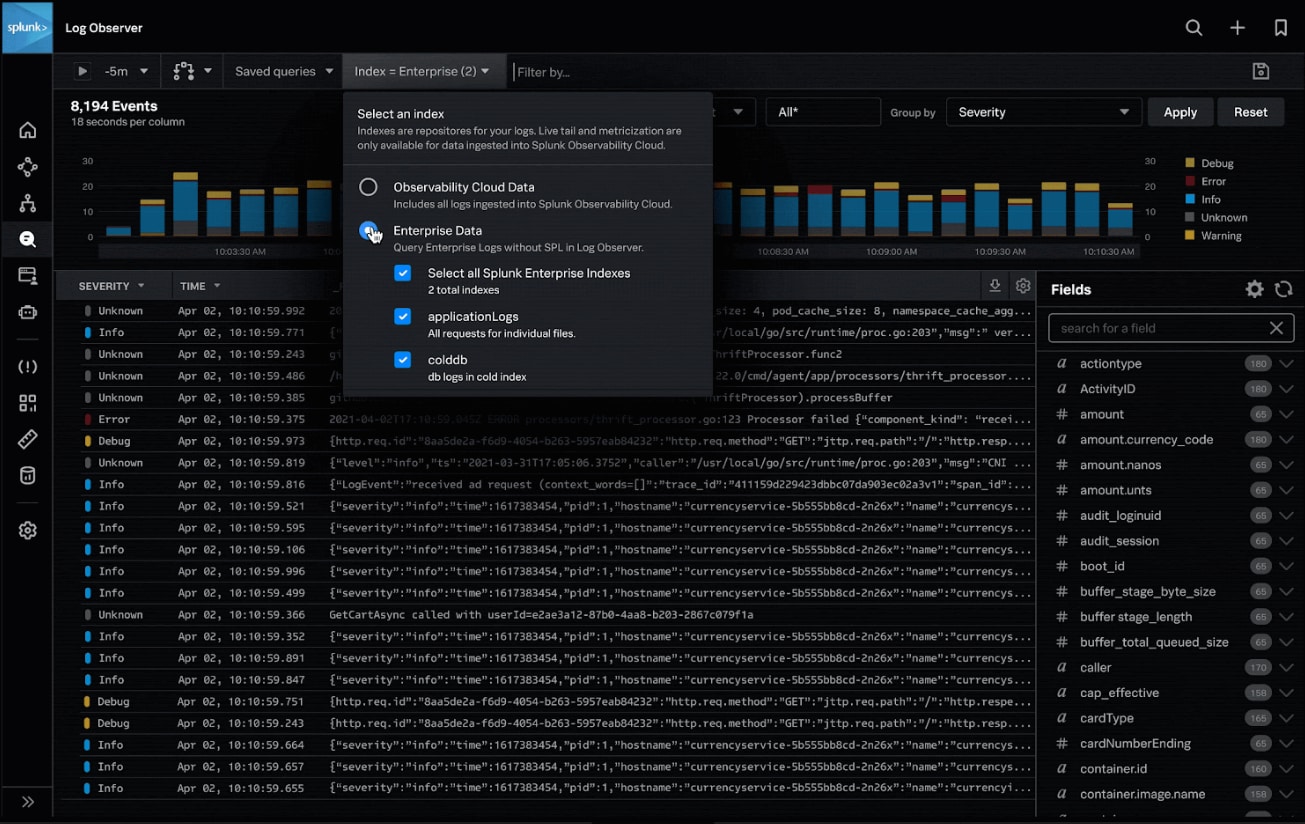
Créer et gérer des recherches enregistrées, des alertes et des tableaux de bord.

Configurer les entrées, sorties et index de données.

Gérer les utilisateurs, les rôles et les autorisations.

Automatiser les tâches administratives et les workflows.

Exemple : Splunk vous permet de centraliser la journalisation des microservices. Au lieu de gérer les journaux séparément pour chaque microservice, vous pouvez regrouper tous les journaux dans Splunk, fournissant un emplacement centralisé pour la surveillance et l'analyse.



* Utiliser un format de log structuré optimal
* Exemple mettre le niveau de journalisation. (info, error, warning, debug )
* Aussi mettre la date et heure du log.
* Ajouter la source de l’évènement.
* Utiliser des messages de journalisation descriptifs.
* Traiter les informations sensibles de manière appropriée
* Ne jamais retourner les logs d’un système comportant des informations sensibles à un utilisateur.
* Éviter de mettre des informations sensibles dans les logs système.

## Références :

[Placer ici l’ensemble des références que vous avez utilisé selon les normes APA. Voir : <https://mondiapason.ca/fichiers/OutilBibliographique/index_APA.php>].

Un grand merci à Chat gpt.

[OWASP Top 10 : les plus grosses failles de sécurité des applications web - Digicomp Blog](https://www.digicomp.ch/blognews/2022/11/29/owasp-top-10-failles-securitaires-applications-web#9)

[Bonnes pratiques de journalisation - CrowdStrike](https://www.crowdstrike.fr/cybersecurity-101/observability/logging-best-practices/)