Gestion des logs et des traces dans la solution Nuabee

Architecture sécurité · https://preview.nuabee.fr/documents/gestion-logs-traces-solution-nuabee/

Introduction

La gestion des logs et des traces est une composante essentielle pour la supervision et la sécurité des environnements Cloud, en particulier durant un Plan de Reprise d'Activité (PRA).

Les logs et les traces permettent de suivre l'activité des systèmes, de diagnostiquer les problèmes, et de garantir la conformité avec les politiques de sécurité. Ce document se concentre sur les solutions de gestion des logs disponibles dans le Cloud T Cloud Public (anciennement Open Telekom Cloud) et leur périmètre d'application dans les espaces de PRA.

Importance de la gestion des logs et des traces

La gestion des logs et des traces offre plusieurs avantages cruciaux, notamment :

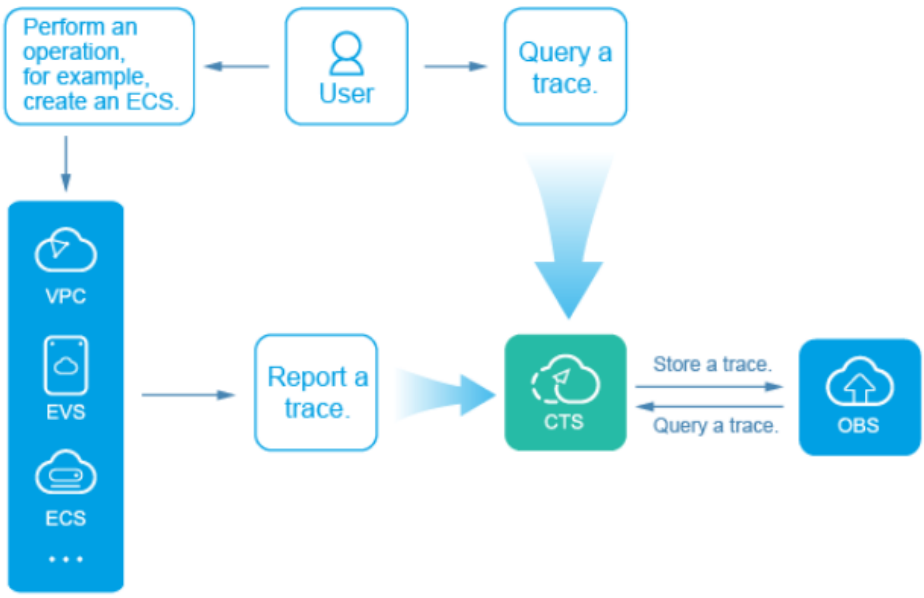
1. **Supervision et Surveillance** : Les logs permettent de surveiller en temps réel l'état des ressources Cloud, facilitant ainsi la détection rapide des anomalies et des défaillances.
2. **Diagnostic et Dépannage** : En cas d'incident, les traces détaillées des activités système permettent d'identifier et de résoudre rapidement les problèmes.
3. **Sécurité et Conformité** : Les logs fournissent des enregistrements essentiels pour les audits de sécurité et la conformité réglementaire, aidant à prouver que les systèmes sont utilisés conformément aux politiques de sécurité établies.
4. **Analyse des Performances** : L'analyse des logs peut révéler des opportunités d'optimisation des performances des systèmes et des applications.

Solutions de gestion des logs

Le Cloud T Cloud Public propose plusieurs solutions pour la gestion des logs et des traces, adaptées aux besoins spécifiques des espaces de PRA.

Le module Cloud Cloud Trace Service (CTS)

Cloud Trace Service (CTS) est une solution avancée de journalisation et de surveillance des activités dans les environnements Cloud. Elle permet de tracer en détail les actions effectuées sur les ressources Cloud, offrant une vue complète et chronologique des opérations. Cette visibilité est cruciale pour la sécurité, le diagnostic des incidents, et la conformité réglementaire.



Collecte des Journaux d’Activité

CTS collecte des journaux d’activité détaillés pour chaque opération effectuée dans l’environnement Cloud. Ces journaux incluent des informations telles que :

- **Type d’opération** : Opérations comme la création, la modification, ou la suppression de ressources.
- **Horodatage** : Date et heure précises de chaque événement.
- **Identifiants d’utilisateur** : ID de l’utilisateur ou du service ayant initié l’opération.
- **Adresses IP** : IP source et de destination pour tracer l’origine des requêtes.
- **Statut de l’opération** : Indications sur le succès ou l’échec des opérations, incluant des codes d’erreur et des messages descriptifs.

Stockage des Journaux

Les journaux collectés sont stockés de manière sécurisée dans un bucket S3 ou un équivalent, avec des mesures de chiffrement pour protéger les données sensibles. CTS supporte des

politiques de rétention configurables, permettant de conserver les journaux pour des durées spécifiques afin de répondre aux exigences de conformité. Ces journaux peuvent être exportés pour une analyse approfondie ou pour les besoins d'audit.

Alertes et Notifications

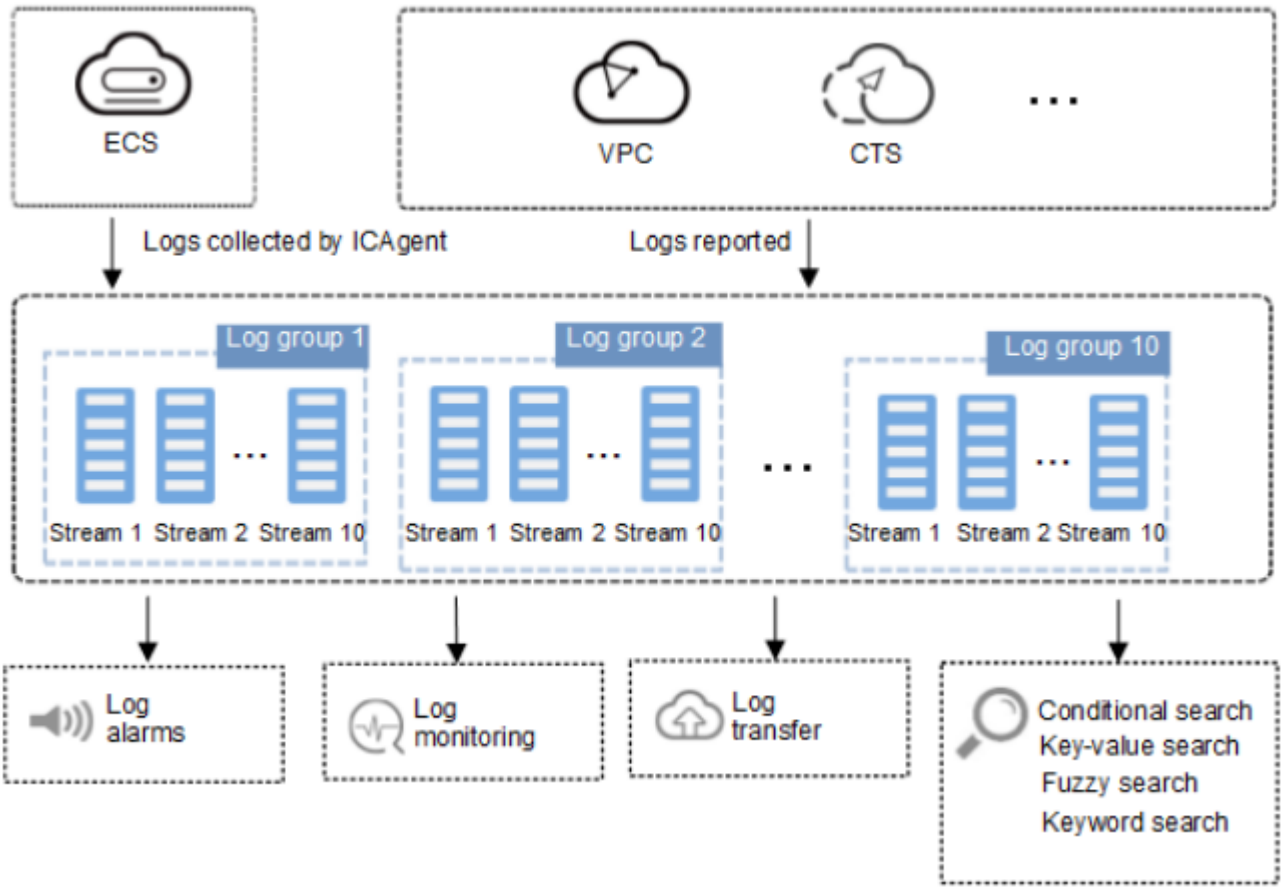
CTS offre des fonctionnalités d'alertes en temps réel basées sur des critères prédéfinis. Par exemple, les administrateurs peuvent configurer des notifications pour des activités suspectes, telles que des tentatives de connexion échouées répétées ou des modifications non autorisées de configurations critiques. Ces alertes peuvent être envoyées via divers canaux, y compris les e-mails et les services de messagerie instantanée.

Intégration avec une solution SIEM

CTS peut être intégré avec des solutions SIEM (Security Information and Event Management) comme Splunk ou Graylog, facilitant une analyse centralisée et la corrélation des événements de sécurité. Cette intégration permet de créer des rapports et des tableaux de bord personnalisés pour une meilleure visibilité des menaces potentielles.

Module Cloud Log Tank Service (LTS)

Cloud Log Tank Service (LTS) est une solution de gestion des logs robuste, conçue pour la collecte, le stockage, l'analyse et la gestion des logs générés au sein des infrastructures Cloud. LTS joue un rôle crucial dans la surveillance continue des systèmes, le diagnostic des problèmes et l'amélioration de la sécurité globale.



Collecte des Logs

LTS supporte une collecte exhaustive des logs provenant de diverses sources, y compris :

- **Logs système** : Journaux du système d'exploitation et des services de base.
- **Logs d'application** : Logs générés par les applications déployées, incluant les messages d'erreur, les traces de pile, et les informations de débogage.
- **Logs réseau** : Journaux relatifs au trafic réseau, capturant les connexions entrantes et sortantes, les pare-feux, et les routes de trafic.
- **Logs de sécurité** : Inclut les événements liés à la sécurité comme les tentatives d'accès non autorisé, les alertes IDS/IPS, et les audits de sécurité.

Stockage Centralisé

Les logs sont stockés de manière centralisée dans un système de stockage élastique, souvent basé sur des technologies telles que le stockage objet S3. LTS permet de définir des politiques de rétention pour conserver les logs selon les besoins spécifiques des entreprises, allant de quelques semaines à plusieurs années.

Analyse et Visualisation

LTS inclut des outils pour l'analyse et la visualisation des données de logs. Les administrateurs peuvent utiliser des tableaux de bord interactifs, des filtres avancés, et des requêtes de recherche pour explorer les données.

Des fonctionnalités de machine learning et de détection d'anomalies peuvent également être intégrées pour identifier des comportements inhabituels ou des incidents de sécurité.

Gestion des Accès et Sécurité

LTS intègre des mécanismes de gestion des accès stricts, assurant que seules les personnes autorisées peuvent accéder et analyser les logs. Les contrôles d'accès basés sur les rôles (RBAC), l'authentification multifactorielle (MFA), et le chiffrement des données en transit et au repos sont des mesures couramment mises en place pour protéger les données sensibles.

Alertes et Surveillance

Comme CTS, LTS permet de configurer des règles d'alerte pour surveiller les logs en temps réel. Les alertes peuvent être déclenchées par des événements spécifiques, des seuils définis, ou des patterns d'anomalies détectés dans les logs. Ces alertes sont cruciales pour une réponse proactive aux incidents de sécurité ou aux problèmes opérationnels.

Intégration avec d'autres Services

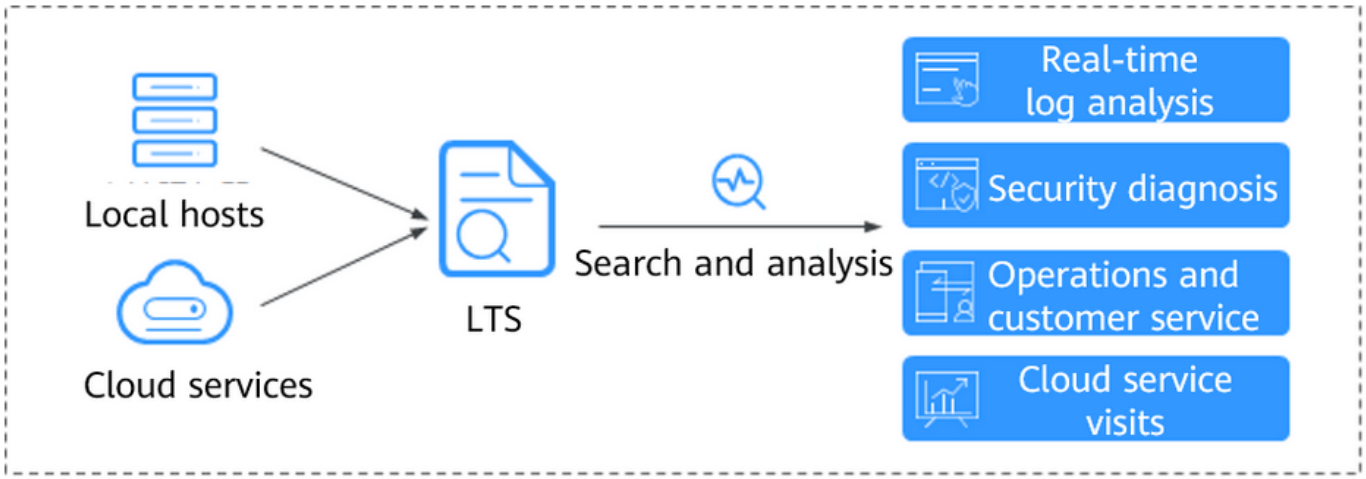
LTS est conçu pour une intégration fluide avec d'autres services Cloud et des outils de monitoring tiers. Par exemple, il peut se connecter avec des systèmes SIEM pour une analyse consolidée, ou avec des outils de DevOps pour intégrer les logs dans les pipelines CI/CD.

Cette intégration renforce la capacité à surveiller et gérer les logs à travers divers environnements et technologies.

Intégration CTS avec LTS

L'intégration du Cloud Trace Service (CTS) avec le Cloud Log Tank Service (LTS) offre une solution robuste pour la gestion complète des logs et des traces. CTS enregistre les activités des utilisateurs et les opérations effectuées sur les ressources Cloud, générant des journaux détaillés d'événements. Ces journaux peuvent ensuite être centralisés et stockés dans LTS, où ils sont accessibles pour une analyse approfondie. Cette intégration permet de corréler facilement les

événements de sécurité et les activités système, facilitant ainsi le suivi des incidents et l'audit de conformité. De plus, en combinant les capacités de collecte et de surveillance de CTS avec les fonctionnalités d'analyse et de gestion des logs de LTS, nous obtenons une vue d'ensemble complète et cohérente de l'espace de PRA, optimisant ainsi la sécurité et la performance des systèmes.



Conclusion

Les services **Cloud Trace Service (CTS)** et **Cloud Log Tank Service (LTS)** du Cloud T Cloud Public offrent une couverture complète pour la gestion des logs et des traces dans l'espace de PRA.

CTS se concentre sur les journaux d'activité et la traçabilité des opérations menées dans le Cloud, tandis que LTS fournit une solution globale pour la collecte, le stockage, et l'analyse des logs provenant de diverses sources.

Ensemble, ces services constituent une fondation solide pour la sécurité, la conformité, et la gestion opérationnelle des ressources cloud.

Pour aller plus loin : documentation sur la gestion des logs