Délai d'indexation signalé entre l'heure d'événement du journal Winevent et l'heure d'index Splunk

Applicabilité

Splunk Enterprise

Description

Comment l'identifier

Tout d'abord, confirmez l'écart entre l'heure de l'événement (_time) et l'heure d'indexation du splunk (_indextime), puis modifiez ce qui suit en fonction de l'index et du type de source affectés. Cet exemple demande la journalisation des événements du canal de sécurité :

```
index=<splunk_index> sourcetype="WinEventLog:Security" host=<splunk_forwarder>
| fields _time, _indextime, host
| eval delay=(_indextime - _time)/60
| timechart avg(delay) by host
```

Enquête

Éléments importants à vérifier :

- Quand le délai d'indexation est-il apparu pour la première fois ?
- Quelles modifications, le cas échéant, ont été apportées au déploiement au moment où le délai est apparu pour la première fois ?
- La latence augmente-t-elle avec le temps (linéairement) ou fluctue-t-elle ?

Confirmez le nombre maximal et la moyenne d'événements par seconde (eps) :

```
index=_internal source=*metrics.log* security per_source_thruput host=<splunk_forwarder>
| timechart max(eps) max(max_age)
```

Si la latence varie dans le temps, une valeur EPS élevée peut indiquer des goulots d'étranglement dans le débit des données.

Résolution

Solution rapide

Cette option s'applique uniquement si vous souhaitez obtenir les événements actuels et ne vous souciez pas des données historiques manquantes. Les opérations suivantes doivent être effectuées une par une sur chaque redirecteur de problème :

1. Définissez `current_only = 1` dans `$SPLUNK_HOME\etc\system\local\inputs.conf` :

   ```
   [WinEventLog://Security]
   current_only = 1
   ```

2. Arrêter le redirecteur
3. Renommez le fichier de point de contrôle obsolète :

   ```
   ren "C:\Program Files\SplunkUniversalForwarder\var\lib\splunk\modinput\WinEventLog\Securit
   ```

4. Démarrez le redirecteur
5. Assurez-vous qu'un nouveau fichier de point de contrôle de sécurité est généré
6. Confirmer que les journaux de contrôle et de sécurité contiennent quelques centaines d'événements les uns des autres
7. Renommez le fichier `$SPLUNK_HOME\etc\system\local\inputs.conf` pour rétablir le paramètre par défaut `current_only=1`.
8. Redémarrer le Splunk
9. Rechercher pour confirmer que les données sont en cours d'acquisition

Pourquoi effectuer des redémarrages UF réguliers n'aidera probablement pas

Le redémarrage de l'UF le force simplement à relire les points de contrôle et à vider brièvement les mémoires tampons. Étant donné que le taux de génération d'événements dépasse la limite de traitement/débit, le redirecteur recommencera immédiatement à accumuler du retard dans les minutes qui suivent le redémarrage.

Solutions à long terme

La solution rapide nécessite une intervention manuelle sur chaque UF affecté, ce qui n'est généralement pas possible dans un déploiement de grande envergure (et certains administrateurs n'ont pas d'accès en ligne de commande aux UF) appliqué. En plus de cela, il est très probable que les UFs tomberont à nouveau derrière. Votre meilleure option peut être de fournir une solution à long terme. Chaque environnement étant différent, il n'existe pas de paramètre simple pouvant être appliqué à chaque scénario. Cependant, les suggestions de cette base de connaissances devraient fonctionner pour de nombreux cas d'utilisation. Toutes les suggestions de configuration de cet article nécessitent le redémarrage du Splunk sur le UF pour prendre effet. Assurez-vous donc que l'option Splunk redémarre l'application personnalisée sur le serveur de déploiement.

Essayez d'abord (limits.conf)

Ouvrir maxKBps

Avant de modifier les options ci-dessous, consultez le fichier `limits.conf/[débit]maxKBps`. Le paramètre par défaut d'un UF est de 256 Ko/s, ce qui limite le redirecteur à ~22 Go/jour de transmission réseau totale. Un serveur occupé générant des journaux de sécurité produit facilement plus de 256 Ko/s, ce qui rend physiquement impossible le suivi par le redirecteur.

Donc, la première chose : Définissez cette valeur sur 0 (illimité) dans `limits.conf` pour libérer la bande passante du réseau :

```
[thruput]
maxKBps = 0
```

Comme la plupart des redirecteurs universels appellent un serveur de déploiement à leur domicile, il est recommandé de définir cette configuration via une application de déploiement afin que tous

les redirecteurs la reçoivent en même temps (d'abord dans un environnement de test si possible, puis en production). Une autre option, si un environnement de test n'est pas disponible, consiste à déployer sur une classe de serveur « test » d'un petit groupe de UF et de surveillance avant de l'appliquer partout. Il en va de même pour toutes les suggestions proposées dans cet article de la base de connaissances.

Options supplémentaires

Si l'ouverture du débit des redirecteurs ne résout pas entièrement le problème, tenez compte des points suivants :

Spécifique à **`input.conf/[WinEventLog://Security]`**

Option n° 1 - Modifier la taille du lot

Par défaut, Splunk récupère les événements par petits lots (10 événements) et met fréquemment à jour le fichier de point de contrôle sur le disque. Sur les hôtes occupés, les E/S disque du fichier de point de contrôle deviennent un point d'étranglement majeur. Le paramètre `batch_size = 500`, le report de la synchronisation du disque à 600 (`checkpointInterval = 600`) et le paramètre `suppress_checkpoint = true` augmentent considérablement le débit EPS (événements par seconde) de `splunk-winevtlog.exe`.

```
batch_size = 500
suppress_checkpoint = true
checkpointInterval = 600
```

Option#2 - Utilisez renderXML pour réduire le nombre d'appels API

Par défaut, Splunk émet un appel d'API pour chaque champ de l'événement. L'activation de renderXml émettra à la place un appel API par événement, ce qui peut améliorer les performances : [Afficher les événements du journal des événements Windows au format XML]

```
renderXml = true
```

Option 3 : filtrer les champs supprimés pour réduire la charge utile des données

Cette option est efficace pour la vitesse brute, mais assurez-vous qu'elle répond aux exigences d'audit (le cas échéant).

Ces paramètres éliminent les champs d'en-tête de l'événement brut avant l'envoi pour réduire la taille des octets et les appels de rendu API. Si leurs modèles SIEM, CIM ou leurs tableaux de bord de conformité reposent sur des `mots clés` (par exemple, réussite/échec d'audit), `TaskCategory`, ou `Opcode`, la suppression de ces champs interrompra ces détections.

```
suppress_sourcename = true
suppress_keywords = true
suppress_type = true
suppress_task = true
suppress_opcode = true
```

Option#4 - Activer l'API **`FormatMessage()`** dans la strophe d'entrée

`evtFormatMessage()` est l'API par défaut dans la plupart des déploiements Windows, qui a une surcharge de traitement accrue par rapport à l'API FormatMessage() précédente. Le retour à l'ancienne API peut réduire le délai d'indexation.

Ne définissez pas ceci si où **`renderXml = true`**. L'API `FormatMessage()` héritée est seulement plus rapide lors de l'analyse des journaux à plusieurs lignes en texte clair classiques (`renderXml = false`), parce qu'elle contourne la recherche de chaîne DLL `evtFormatMessage()` lourde. Lorsque vous utilisez `renderXml = true`, Splunk lit déjà directement à partir de l'API EVTX moderne (`EvtRender`) au format structuré sans appeler de DLL de mise en forme de message.

```
use_old_eventlog_api = true
```

Augmenter les pipelines d'ingestion UF (server.conf)

Par défaut, un redirecteur exécute un seul pipeline d'analyse et de réception. Pour les machines multicoeurs ingérant un volume d'événements important, l'ensemble de pipelines peut être augmenté pour permettre un traitement parallèle. Cela contrôle le nombre de threads internes que le redirecteur utilise pour lire des données à partir d'API Windows locales, les empaqueter et les

envoyer sur le réseau.

Sur un UF, l'encombrement en ressources des pipelines d'ingestion croissants de `1` à `2` est très léger par rapport à un indexeur ou un redirecteur lourd, car le UF ne fait que des lectures, des traitements par lots et des sorties réseau légers (pas de transformation regex, d'extraction de champ ou d'indexation sur disque).

Si le serveur Windows a au moins 4 coeurs de CPU et 8 Go de RAM, le réglage de `parallelIngestionPipelines = 2` est généralement sûr et aidera considérablement à effacer un lourd arriéré d'événements et à empêcher de futurs retards. L'utilisation du processeur peut augmenter pendant que l'UF est rattrapé, mais diminuera à nouveau une fois que l'ingestion revient à des niveaux normaux.

```
[general]
parallelIngestionPipelines = 2
```

Taille de file d'attente Outputs.conf

Si vous réglez le traitement par lots d’entrée sur 500, assurez-vous que la file d’attente de sortie TCP dispose d’une mémoire tampon suffisante pour que la couche réseau ne bloque pas le travailleur d’entrée :

```
[tcpout:myindexers]
maxQueueSize = 50MB
```

Vérifier les exclusions de Windows Defender / Antivirus

Les agents des points d'extrémité de sécurité (par exemple, Defender, CrowdStrike, Carbon Black) peuvent inspecter de manière agressive `splunk-winevtlog.exe` et verrouiller le répertoire `$SPLUNK_HOME\var\lib\splunk\modinput\WinEventLog\`. Assurez-vous que l'intégralité du répertoire `$SPLUNK_HOME` et le répertoire `splunk-winevtlog.exe` sont exclus de l'inspection du système de fichiers en temps réel.

Affinité du contrôleur de domaine / Routage réseau :

Si le problème provient de l'exécution d'UF sur des contrôleurs de domaine ou de la gestion d'un

trafic Active Directory élevé, assurez-vous qu'aucun pare-feu local ou limitation de débit réseau ne limite le port TCP Splunk (`9997` par défaut) à la couche de réception (HF ou indexeurs).

Liens connexes

- Documentation sur le Splunk :
  - Surveillance des données du journal des événements Windows avec Splunk Enterprise
  - Configurations avancées pour Universal Forwarder
  - Fichiers de spécifications : server.conf, input.conf, output.conf
- Articles de la base de connaissances Splunk
  - Dépannage des journaux différés à partir de UF ou HF
  - UF n'envoie pas de journaux de sécurité au Splunk
- Article de lanterne de javelot : Réglage des performances du niveau de transfert

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.