Indizierungsverzögerung gemeldet zwischen Winevent-Protokollereigniszeit und Splunk-Indexzeit

Geltungsbereich

Splunk Enterprise

Beschreibung

Identifizierung

Bestätigen Sie zunächst das Delta zwischen Ereigniszeit (_time) und Splunk-Indexzeit (_indextime). Ändern Sie die folgenden Angaben, je nachdem, welcher Index und welcher Quelltyp betroffen ist. In diesem Beispiel wird die Ereignisprotokollierung des Sicherheitskanals abgefragt:

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

Untersuchung

Wichtige Punkte zu überprüfen:

- Wann trat die Indexierungsverzögerung zum ersten Mal auf?
- Welche Änderungen wurden ggf. an der Bereitstellung vorgenommen, etwa zu dem Zeitpunkt, als die Verzögerung erstmals auftrat?
- Erhöht sich die Latenz im Laufe der Zeit (linear) oder schwankt sie?

Bestätigen Sie die maximale und durchschnittliche Anzahl von Ereignissen pro Sekunde (eps):

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

Wenn sich die Latenz im Laufe der Zeit ändert, kann ein hoher EPS-Wert auf Engpässe im Datendurchsatz hinweisen.

Auflösung

Schnellreparatur

Diese Option gilt nur, wenn Sie aktuelle Ereignisse abrufen möchten und sich nicht um fehlende historische Daten kümmern. Folgende Schritte müssen nacheinander für jeden Problemweiterleitungs-Manager ausgeführt werden:

1. Legen Sie `current_only = 1` in $`SPLUNK_HOME\etc\system\local\inputs.conf fest`:

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

2. Forwarder anhalten
3. Umbenennen der veralteten Prüfpunktdatei:

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

4. Forwarder starten
5. Stellen Sie sicher, dass eine neue Sicherheits-Prüfpunktdatei generiert wird.
6. Bestätigung, dass die Prüfpunkt- und Sicherheitsprotokolle einige hundert Ereignisse voneinander enthalten
7. Benennen Sie die Datei `$SPLUNK_HOME\etc\system\local\inputs.conf` um, um die Einstellung `current_only=1` wieder auf den Standardwert zurückzusetzen.
8. Splunk neu starten
9. Suche zur Bestätigung, dass die Daten empfangen werden

Warum die Durchführung regelmäßiger UF-Neustarts wahrscheinlich nicht helfen

Nach dem Neustart wird die UF lediglich dazu gezwungen, Prüfpunkte erneut zu lesen und Speicherpuffer kurzzeitig zu leeren. Da die Ereignisgenerierungsrate den Verarbeitungs-/Durchsatzgrenzwert überschreitet, beginnt der Forwarder innerhalb von Minuten nach dem Neustart sofort wieder mit der akkumulierten Verzögerung.

Langfristige Lösungen

Die schnelle Behebung erfordert manuelle Eingriffe in jede betroffene UF, was in einer umfangreichen Bereitstellung (und einigen Administratoren fehlt der Zugriff auf die UFs über die Kommandozeile) nicht möglich ist. Obendrein ist es sehr wahrscheinlich, dass die UFs wieder zurückfallen. Am besten stellen Sie eine langfristige Lösung dar. Da jede Umgebung anders ist, gibt es keine einfache Einstellung, die auf jedes Szenario angewendet werden kann. Die Vorschläge in dieser KB sollten jedoch für viele Anwendungsfälle funktionieren. Alle Konfigurationsvorschläge in diesem Artikel erfordern, dass Splunk auf der UF neu gestartet wird, um wirksam zu werden. Stellen Sie daher sicher, dass für die benutzerdefinierte App auf dem Bereitstellungsserver "Splunkd neu starten" aktiviert ist.

Versuchen Sie es zuerst (limits.conf)

Max. KBps öffnen

Bevor Sie die Optionen unten anpassen, lesen Sie die Datei `limits.conf/[durchsatz]maxKBps`. Die Standardeinstellung für eine UF ist 256 KB/s. Dadurch ist die Netzwerkübertragung für den Forwarder auf ~22 GB/Tag beschränkt. Ein ausgelasteter Server, der Sicherheitsprotokolle generiert, erzeugt problemlos mehr als 256 KB/s, sodass der Forwarder nicht mithalten kann.

Zunächst also: Legen Sie diesen Wert in `limits.conf` auf 0 (unbegrenzt) `fest`, um die Netzwerkbandbreite zu entkappen:

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

Da die meisten Universal Forwarder mit einem Bereitstellungsserver telefonieren, empfiehlt es sich, diese Konfiguration über eine Bereitstellungs-App festzulegen, sodass alle Forwarder sie

gleichzeitig erhalten (zunächst in einer Testumgebung, wenn möglich, dann in der Produktion). Eine weitere Option, falls eine Testumgebung nicht verfügbar ist, besteht darin, sie auf einer "Test"-Serverklasse einer kleinen Gruppierung von UFs und Monitor bereitzustellen, bevor sie überall angewendet werden. Gleiches gilt für alle Vorschläge, die in diesem KB-Artikel angeboten werden.

Zusätzliche Optionen

Wenn das Problem durch das Öffnen des Durchsatzes des Spediteurs nicht vollständig gelöst wird, berücksichtigen Sie Folgendes:

Spezifisch für `input.conf/[WinEventLog://Security]`

Option 1: Ändern der Stapelgröße

Standardmäßig erfasst Splunk Ereignisse in kleinen Batches (10 Ereignisse) und aktualisiert die Prüfpunktdatei auf der Festplatte regelmäßig. Bei ausgelasteten Hosts wird der Datenträger-E/A in der Prüfpunktdatei zu einem Engpass. Durch Festlegen von `batch_size = 500`, Verzögern der Datenträgersynchronisierung auf 600 s (`checkpointInterval = 600`) und Festlegen von `suppress_checkpoint = true` wird der EPS-Durchsatz (Ereignisse pro Sekunde) von `splunk-winevtlog.exe` drastisch erhöht.

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

Option 2: Reduzieren der Anzahl von API-Aufrufen mithilfe von renderXML

Standardmäßig gibt Splunk einen API-Aufruf für jedes Feld innerhalb des Ereignisses aus. Bei Aktivierung von renderXml wird stattdessen ein API-Aufruf pro Ereignis ausgegeben, wodurch die Leistung potenziell verbessert wird: [Windows-Ereignisprotokollereignisse in XML anzeigen]

```
renderXml = true
```

Option 3: Unterdrückung von Feldern filtern, um die Datennutzlast zu reduzieren

Diese Option ist für die Raw-Geschwindigkeit wirksam, aber stellen Sie sicher, dass sie die Audit-Anforderungen erfüllt (falls zutreffend).

Diese Einstellungen entfernen Headerfelder aus dem Raw-Ereignis, bevor sie gesendet werden, um die Bytegröße und API-Rendering-Aufrufe zu reduzieren. Wenn SIEM-, CIM-Modelle oder Compliance-Dashboards auf `Schlüsselwörtern (`z. B. Erfolgreiche/fehlgeschlagene Prüfung), `TaskCategory` oder `Opcode` basieren, werden diese Erkennungen durch das Löschen dieser Felder aufgehoben.

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

Option 4: Aktivieren der **`FormatMessage()`**-API im Eingabestoff

`evtFormatMessage()` ist die Standard-API in den meisten Windows-Bereitstellungen, die im Vergleich zur vorherigen FormatMessage()-API einen erhöhten Verarbeitungsaufwand aufweist. Das Zurücksetzen auf die ältere API kann die Indexierungsverzögerung verringern.

Legen Sie dies nicht fest, wenn **`renderXml = true ist`**. Die ältere `FormatMessage()`-API ist nur schneller, wenn klassische mehrzeilige Nur-Text-Protokolle analysiert werden (`renderXml = false`), da sie die umfangreiche `evtFormatMessage()` DLL-Suche umgeht. Bei der Verwendung von `renderXml = true` liest Splunk bereits direkt aus der modernen EVTX-API (`EvtRender`) im strukturierten Format, ohne Nachrichtenformatierungs-DLLs aufzurufen.

```
use_old_eventlog_api = true
```

Erhöhung der UF-Übernahmerohre (server.conf)

Standardmäßig führt ein Forwarder eine einzelne Parsing- und Eingangspipeline aus. Bei Multicore-Systemen, die ein hohes Ereignisvolumen aufnehmen, kann der Pipeline-Satz erweitert werden, um eine parallele Verarbeitung zu ermöglichen. Diese Einstellung steuert, wie viele

interne Threads der Forwarder verwendet, um Daten von lokalen Windows-APIs zu lesen, in Pakete zu packen und in das Netzwerk zu übertragen.

Auf einer UF ist der Ressourcenbedarf der zunehmenden Aufnahme-Pipelines von `1` bis `2` sehr gering im Vergleich zu einem Indexer oder Heavy Forwarder, da die UF nur leichte Lese-, Batch- und Netzwerkausgaben ausführt (keine Regex-Transformationen, Feldextraktion oder Indizierung auf Festplatte).

Wenn der Windows-Server über mindestens 4 CPU-Kerne und 8 GB RAM verfügt, ist das Einstellen von `parallelIngestionPipelines = 2` in der Regel sicher und hilft erheblich, einen schweren Ereignisrückstand zu beheben und künftige Verzögerungen zu vermeiden. Die CPU-Auslastung kann steigen, während die UF eingeholt wird, fällt aber wieder ab, sobald die Aufnahme wieder normal ist.

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

Größe der Ausgabewarteschlange.conf

Wenn Sie die Eingabe-Batchverarbeitung auf 500 einstellen, sollten Sie sicherstellen, dass die TCP-Ausgabewarteschlange über einen ausreichenden Speicherpuffer verfügt, damit die Netzwerkschicht den Eingabe-Worker nicht blockiert:

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

Windows Defender-/Antivirus-Ausschlüsse überprüfen

Sicherheitsendpunkt-Agents (z. B. Defender, CrowdStrike, Carbon Black) können `splunk-winevtlog.exe` aggressiv inspizieren und das Verzeichnis `$SPLUNK_HOME\var\lib\splunk\modinput\WinEventLog\` sperren. Stellen Sie sicher, dass das gesamte `$SPLUNK_HOME`-Verzeichnis und `splunk-winevtlog.exe` von der Echtzeitdateisystemüberprüfung ausgeschlossen sind.

Domänencontroller-Affinität/Netzwerkrouting:

Wenn das Problem auf Domänencontrollern ausgeführt wird oder hohen Active Directory-Datenverkehr verarbeitet, stellen Sie sicher, dass keine lokale Firewall oder Netzwerk-Ratenbegrenzung den Splunk-TCP-Port (Standard: `9997`) auf die empfangende Schicht (HFs oder Indexer) begrenzt.

Verwandte Links

- Splunk-Dokumentation:
  - Überwachen von Windows-Ereignisprotokolldaten mit Splunk Enterprise
  - Erweiterte Konfigurationen für den Universal Forwarder
  - Spezifikationsdateien: server.conf, input.conf, output.conf
- Splunk-KB-Artikel
  - Fehlerbehebung bei verzögerten Protokollen von UF oder HF
  - UF sendet keine Sicherheitsprotokolle an Splunk
- Splunk Lantern Artikel: Performance-Optimierung der Weiterleitungsebene

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.