Ritardo di indicizzazione rilevato tra l'ora del registro eventi Winevent e l'ora dell'indice Splunk

Applicabilità

Splunk Enterprise

Descrizione

Come identificarlo

Prima di tutto, confermare il delta tra l'ora dell'evento (_time) e l'ora di indicizzazione (_indextime) di Splunk, modificare quanto segue in base all'indice e al tipo di origine interessati. In questo esempio viene eseguita una query sulla registrazione degli eventi del canale di protezione:

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

Indagine

Elementi importanti da verificare:

- Quando è stato visualizzato per la prima volta il ritardo di indicizzazione?
- Quali eventuali modifiche sono state apportate all'installazione nel momento in cui è apparso il ritardo?
- La latenza aumenta nel tempo (lineare) o fluttua?

Confermare l'evento massimo e medio al secondo (eps):

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

Se la latenza varia nel tempo, un valore EPS elevato può indicare colli di bottiglia nella trasmissione dei dati.

Risoluzione

Correzione rapida

Questa opzione è valida solo se si desidera ottenere gli eventi correnti e non si è interessati ai dati cronologici mancanti. Per ogni server di inoltro problemi è necessario eseguire una alla volta le operazioni seguenti:

1. Impostare `current_only = 1` in `$SPLUNK_HOME\etc\system\local\inputs.conf`:

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

2. Arresta il server d'inoltro
3. Rinominare il file di checkpoint non aggiornato:

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

4. Avvia il server di inoltro
5. Verificare che sia stato generato un nuovo file del checkpoint di protezione
6. Confermare che i registri di checkpoint e di sicurezza siano in poche centinaia di eventi l'uno con l'altro
7. Rinominare il file `$SPLUNK_HOME\etc\system\local\inputs.conf` per ripristinare l'impostazione `current_only=1` predefinita.
8. Riavvia Splunk
9. Ricerca per confermare l'acquisizione dei dati

Perché eseguire riavvii UF regolari probabilmente non sarà di aiuto

Il riavvio dell'UF forza semplicemente la lettura dei checkpoint e lo svuotamento dei buffer di memoria. Poiché la frequenza di generazione degli eventi supera il limite di elaborazione/throughput, il server d'inoltro inizierà di nuovo ad accumulare ritardo entro pochi minuti dal riavvio.

Soluzioni a lungo termine

La correzione rapida richiede l'intervento manuale su ogni UF interessata, cosa che in genere non è fattibile in un'installazione di grandi dimensioni (e alcuni amministratori non dispongono dell'accesso da riga di comando alle UF). Inoltre, è molto probabile che le UF restino indietro. L'opzione migliore potrebbe essere quella di fornire una soluzione a lungo termine. Poiché ogni ambiente è diverso, non esiste un'impostazione semplice che possa essere applicata a ogni scenario. Tuttavia, i suggerimenti in questa KB dovrebbero funzionare per molti casi di utilizzo. Tutti i suggerimenti di configurazione in questo articolo richiedono il riavvio di Splunk sull'interfaccia utente per avere effetto. Verificare quindi che l'app personalizzata sul server di distribuzione sia selezionata per il riavvio di Splunk.

Provare prima questo (limits.conf)

Apri maxKBps

Prima di modificare le opzioni riportate di seguito, verificate il file `limits.conf/[thruput]maxKBps`. L'impostazione predefinita di un UF è 256KB/s, che limita il server di inoltro a circa 22 GB/giorno di trasmissione di rete totale. Un server occupato che genera registri di protezione produce con facilità più di 256 KB/s, rendendo fisicamente impossibile la gestione da parte del server d'inoltro.

Quindi, prima cosa: Impostare questo valore su 0 (illimitato) nel file `limits.conf` per sbloccare la larghezza di banda della rete:

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

Poiché la maggior parte dei server d'inoltro universali sta telefonando a casa di un server di distribuzione, è consigliabile impostare questa configurazione tramite un'app di distribuzione in modo che tutti i server d'inoltro la ricevano contemporaneamente (prima in un ambiente di test se possibile, quindi in produzione). Un'altra opzione, se l'ambiente di test non è disponibile, consiste nell'eseguire la distribuzione su una classe server di "test" di un piccolo gruppo di UF e di monitor

prima di applicarla ovunque. Lo stesso vale per tutti i suggerimenti offerti in questo articolo della Knowledge Base.

Opzioni aggiuntive

Se l'apertura del throughput dei server d'inoltro non risolve completamente il problema, tenere presente quanto segue:

Specifico di `inputs.conf/[WinEventLog://Security]`

Opzione 1: modificare le dimensioni del batch

Per impostazione predefinita, Splunk raccoglie gli eventi in piccoli batch (10 eventi) e aggiorna frequentemente il file del checkpoint sul disco. Negli host occupati, l'I/O su disco nel file del checkpoint diventa un punto di interruzione principale. L'impostazione di `batch_size = 500`, il ritardo della sincronizzazione del disco a 600 (`checkpointInterval = 600`) e l'impostazione di `suppress_checkpoint = true` aumentano drasticamente la velocità di trasmissione EPS (eventi al secondo) di `splunk-winevtlog.exe`.

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

Opzione 2 - Utilizzare renderXML per ridurre il numero di chiamate API

Per impostazione predefinita, Splunk invia una chiamata API per ogni campo all'interno dell'evento. L'abilitazione di renderXml genera invece una chiamata API per evento, migliorando potenzialmente le prestazioni: Visualizza eventi del registro eventi di Windows in XML

```
renderXml = true
```

Opzione 3: filtrare i campi soppressi per ridurre il payload dei dati

Questa opzione è valida per la velocità raw, ma assicurarsi che soddisfi i requisiti di verifica (se

applicabili).

Queste impostazioni eliminano i campi dell'intestazione dall'evento raw prima dell'invio per ridurre le dimensioni dei byte e le chiamate di rendering API. Se i relativi dashboard SIEM, CIM o di conformità si basano su `parole chiave` (ad esempio, Controllo riuscito/non riuscito), `TaskCategory` o `Opcode`, l'eliminazione di questi campi interromperà tali rilevamenti.

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

Option#4 - Abilita l'API **`FormatMessage()`** nella stanza di input

`evtFormatMessage()` è l'API predefinita nella maggior parte delle distribuzioni di Windows, che presenta un sovraccarico di elaborazione maggiore rispetto alla precedente API FormatMessage(). Il ripristino dell'API precedente può ridurre il ritardo di indicizzazione.

Non impostare questo valore se dove **`renderXml = true`**. L'API `FormatMessage()` legacy è più veloce solo quando si analizzano i registri multilinea di testo normale classici (`renderXml = false`), perché ignora la ricerca di stringhe della DLL `evtFormatMessage()` complessa. Quando si utilizza `renderXml = true`, Splunk legge già direttamente dall'API EVTX moderna (`EvtRender`) in formato strutturato senza chiamare le DLL di formattazione dei messaggi.

```
use_old_eventlog_api = true
```

Aumentare le pipeline di ingestione UF (server.conf)

Per impostazione predefinita, un server d'inoltro esegue una singola pipeline di analisi e acquisizione. Per le macchine multi-core che acquisiscono un volume di eventi pesante, il set di pipeline può essere aumentato per consentire l'elaborazione parallela. Controlla il numero di thread interni utilizzati dal server di inoltro per leggere i dati dalle API Windows locali, inserirli in un pacchetto e inserirli nella rete.

Su un UF, l'ingombro di risorse dovuto all'aumento delle pipeline di acquisizione da `1` a `2` è molto ridotto rispetto a un Indexer o Heavy Forwarder, in quanto il UF esegue solo letture, batch e output

di rete leggeri (nessuna trasformazione regex, estrazione campo o indicizzazione su disco).

Se il server Windows dispone di almeno 4 core CPU e 8 GB di RAM, l'impostazione di `parallelIngestionPipelines = 2` è in genere sicura e consente di eliminare in modo significativo un backlog di eventi pesante e di evitare ritardi futuri. L'utilizzo della CPU può aumentare mentre l'UF rimane inattivo, ma si ridurrà una volta che l'acquisizione ritorna ai livelli normali.

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

Dimensione coda Outputs.conf

Se si regola il batch di input su 500, verificare che la coda di output TCP disponga di un buffer di memoria sufficiente in modo che il livello di rete non blocchi il processo di lavoro di input:

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

Verifica le esclusioni di Windows Defender/Antivirus

Gli agenti degli endpoint di sicurezza (ad esempio, Defender, CrowdStrike, Carbon Black) possono ispezionare in modo aggressivo `splunk-winevtlog.exe` e bloccare la directory `$SPLUNK_HOME\var\lib\splunk\modinput\WinEventLog\`. Assicurarsi che l'intera directory `$SPLUNK_HOME` e `splunk-winevtlog.exe` siano esclusi dall'ispezione del file system in tempo reale.

Affinità controller di dominio/Routing di rete:

Se gli UF con il problema sono in esecuzione sui controller di dominio o gestiscono un traffico Active Directory elevato, assicurarsi che non vi sia alcun firewall locale o limitazione della velocità di rete che limiti la porta TCP Splunk (predefinita: `9997`) al livello ricevente (HF o indicizzatori).

Collegamenti correlati

- Documentazione Splunk:
  - Monitoraggio dei dati del registro eventi di Windows con Splunk Enterprise
  - Configurazioni avanzate per il server di inoltro universale
  - File di specifiche: server.conf, input.conf, output.conf
- Articoli della Knowledge Base di Splunk
  - Risoluzione dei problemi relativi a registri ritardati da UF o HF
  - UF: impossibile inviare i registri di protezione a Splunk
- Articolo su Splunk Lantern: Ottimizzazione delle prestazioni del livello di inoltro

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).