Retraso de indización notificado entre la hora del evento del registro de eventos Winevent y la hora del índice de Splunk

Aplicabilidad

Splunk Enterprise

Descripción

Cómo identificarlo.

En primer lugar, confirme el delta entre el tiempo del evento (_time) y el tiempo del índice de Splunk (_indextime) y modifique lo siguiente en función del índice y el tipo de origen que se vean afectados. Este ejemplo está consultando el registro de eventos del canal de seguridad:

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

Investigación

Aspectos importantes que se deben verificar:

- ¿Cuándo apareció por primera vez el retraso de indexación?
- ¿Qué cambios, si los hubiera, se hicieron en la implementación aproximadamente en el momento en que apareció el retraso?
- ¿Aumenta la latencia con el tiempo (lineal) o fluctúa?

Confirme el máximo y el promedio de eventos por segundo (eps):

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

Si la latencia varía con el tiempo, un valor EPS alto puede indicar cuellos de botella en el rendimiento de los datos.

Resolución

Reparación rápida

Esta opción sólo se aplica si desea obtener eventos actuales y no le preocupan los datos históricos que faltan. Se debe realizar lo siguiente de uno en uno en cada reenviador de problemas:

1. Establezca `current_only = 1` en `$SPLUNK_HOME\etc\system\local\inputs.conf`:

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

2. Detener el reenviador
3. Cambie el nombre del archivo de punto de control obsoleto:

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

4. Iniciar el reenviador
5. Asegúrese de que se genera un nuevo archivo de punto de control de seguridad
6. Confirme que el punto de control y los registros de seguridad están entre sí en unos cientos de eventos
7. Cambie el nombre del archivo `$SPLUNK_HOME\etc\system\local\inputs.conf` para volver a establecer el valor `current_only=1` como predeterminado.
8. Reiniciar Splunk
9. Buscar para confirmar que se están ingiriendo datos

¿Por qué realizar reinicios de UF regulares probablemente no ayudará?

El reinicio de la UF simplemente la obliga a volver a leer los puntos de control y a vaciar brevemente las memorias intermedias. Debido a que la velocidad de generación de eventos excede el límite de procesamiento/rendimiento, el reenviador comenzará inmediatamente a acumular retardo nuevamente a los pocos minutos del reinicio.

Soluciones a largo plazo

La solución rápida requiere la intervención manual en cada UF afectada, lo que generalmente no es factible en una implementación grande (y algunos administradores no tienen acceso a la línea de comandos para UF) aplicada. Además de esto, es muy probable que los UF se queden atrás otra vez. Su mejor opción puede ser proporcionar una solución a largo plazo. Dado que cada entorno es diferente, no existe una configuración sencilla que se pueda aplicar a cada escenario. Sin embargo, las sugerencias de este KB deberían funcionar para muchos casos prácticos. Todas las sugerencias de configuración de este artículo requieren que se reinicie Splunk en UF para que surta efecto, por lo que debe asegurarse de que la aplicación personalizada en Deployment Server haya reiniciado Splunk activada.

Pruebe primero (limits.conf)

Abrir máx. KBps

Antes de ajustar las siguientes opciones, mire `limits.conf/[thruput]maxKBps`. La configuración predeterminada en una UF es 256 KB/s, lo que limita el reenviador a ~22 GB/día de transmisión de red total. Un servidor ocupado que genera registros de seguridad fácilmente produce más de 256 KB/s, lo que hace físicamente imposible que el reenviador esté a la altura.

Así que, lo primero: Establezca este valor en 0 (ilimitado) en `limits.conf` para liberar el ancho de banda de la red:

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

Dado que la mayoría de los reenviadores universales llaman al inicio de un servidor de implementación, se recomienda establecer esta configuración mediante una aplicación de

implementación para que todos los reenviadores la reciban a la vez (primero en un entorno de prueba si es posible y después en producción). Otra opción, si no hay un entorno de prueba disponible, es implementar en una clase de servidor de "prueba" de una pequeña agrupación de UF y supervisar antes de aplicar en todas partes. Lo mismo se aplica a todas las sugerencias que se ofrecen en este artículo de KB.

Opciones adicionales

Si la apertura del rendimiento de los reenviadores no resuelve el problema por completo, tenga en cuenta lo siguiente:

Específico de `input.conf/[WinEventLog://Security]`

Opción n.º 1: Cambiar el tamaño del lote

De forma predeterminada, Splunk captura eventos en pequeños lotes (10 eventos) y actualiza el archivo de punto de control en el disco con frecuencia. En hosts ocupados, la E/S de disco en el archivo de punto de control se convierte en un punto de bloqueo importante. La configuración de `batch_size = 500`, el retraso de la sincronización del disco a 600s (`checkpointInterval = 600`) y la configuración de `suppress_checkpoint = true` aumenta drásticamente el rendimiento de EPS (eventos por segundo) de `splunk-winevtlog.exe`.

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

Opción n.º 2: Utilice renderXML para reducir el número de llamadas de API

De forma predeterminada, Splunk emite una llamada API para cada campo del evento. Al habilitar renderXml, se emitirá una llamada API por evento, lo que podría mejorar el rendimiento: Mostrar eventos del registro de eventos de Windows en XML

```
renderXml = true
```

Opción n.º 3: filtrar qué campos se suprimen para reducir la carga útil de datos

Esta opción es eficaz para la velocidad sin formato, pero asegúrese de que cumple los requisitos de auditoría (si procede).

Esta configuración elimina los campos de encabezado del evento sin procesar antes de enviarlo para reducir el tamaño de bytes y las llamadas de representación de API. Si sus modelos de SIEM, CIM o paneles de cumplimiento se basan en `Palabras clave` (p. ej., Auditoría de aciertos/errores), `TaskCategory` u `Opcode`, la eliminación de estos campos interrumpirá esas detecciones.

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

Option#4 - Habilite la API **`FormatMessage()`** en la estrofa de entrada

`evtFormatMessage()` es la API predeterminada en la mayoría de las implementaciones de Windows, que tiene una sobrecarga de procesamiento mayor en comparación con la API FormatMessage() anterior. Volver a la API anterior puede aliviar el retraso de la indización.

No establezca esta opción si where **`renderXml = true`**. La API `FormatMessage()` heredada es sólo más rápida al analizar registros clásicos de varias líneas de texto sin formato (`renderXml = false`), ya que omite la búsqueda de cadenas de `DLL` pesada de `evtFormatMessage()`. Cuando se utiliza `renderXml = true`, Splunk ya lee directamente desde la moderna API de EVTX (`EvtRender`) en formato estructurado sin llamar a los archivos DLL de formato de mensajes.

```
use_old_eventlog_api = true
```

Aumento de las canalizaciones de ingestión de UF (server.conf)

De forma predeterminada, un reenviador ejecuta una única canalización de análisis e ingestión. En el caso de máquinas multinúcleo que ingieren grandes volúmenes de eventos, el conjunto de tuberías se puede aumentar para permitir el procesamiento paralelo. Esto controla cuántos

subprocesos internos utiliza el reenviador para leer datos de las API locales de Windows, empaquetarlos e insertarlos en la red.

En una UF, la huella de recursos de aumentar las canalizaciones de ingestión de `1` a `2` es muy ligera en comparación con un indizador o un reenviador pesado, porque la UF solo realiza una lectura ligera, procesamiento por lotes y salida de red (sin transformaciones de expresiones regulares, extracción de campo o indización en disco).

Si el servidor de Windows tiene al menos 4 núcleos de CPU y 8 GB de RAM, la configuración de `allelIngestionPipelines = 2` es generalmente segura y ayudará significativamente a borrar un gran retraso de eventos y evitar retrasos futuros. El uso de la CPU puede aumentar mientras la UF se pone al día, pero volverá a descender una vez que la ingestión vuelva a los niveles normales.

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

Tamaño de cola de Outputs.conf

Si ajusta el procesamiento por lotes de entrada a 500, considere la posibilidad de asegurarse de que la cola de salida TCP tenga suficiente memoria intermedia para que la capa de red no bloquee al trabajador de entrada:

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

Comprobar exclusiones de Windows Defender y antivirus

Los agentes de extremos de seguridad (p. ej., Defender, CrowdStrike, Carbon Black) pueden inspeccionar de forma agresiva `splunk-winevtlog.exe` y bloquear el directorio `$SPLUNK_HOME\var\lib\splunk\modinput\WinEventLog\`. Asegúrese de que todo el directorio `$SPLUNK_HOME` y `splunk-winevtlog.exe` se excluyen de la inspección del sistema de archivos en tiempo real.

Afinidad del controlador de dominio / Ruteo de red:

Si el UF del problema se está ejecutando en los controladores de dominio o está manejando un

tráfico alto de Active Directory, asegúrese de que ningún firewall local o límite de velocidad de red está limitando el puerto TCP de Splunk (predeterminado `9997`) a la capa de recepción (HF o indizadores).

Enlaces relacionados

- Documentación de Splunk:
  - Supervisión de datos de Windows Eventlog con Splunk Enterprise
  - Configuraciones avanzadas para Universal Forwarder
  - Ficheros de especificaciones: server.conf, input.conf, output.conf
- Artículos de Splunk KB
  - Solución de problemas de registros retrasados de UF o HF
  - UF no envía registros de seguridad a Splunk
- Artículo de Splunk Lantern: Ajuste del rendimiento del nivel de reenvío

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).