

En Splunk se observa un registro duplicado de Kubernetes mediante ingestión de HEC

Aplicabilidad

Splunk Enterprise Kubernetes

Descripción

Los datos de HEC no se indexan como se esperaba y crean duplicados en varios servidores para un índice específico que tiene una fuente específica de Kubernetes

Investigación

1. Primero verifique el estado del token de HEC usando el siguiente comando en la GUI de Splunk SH.

```
|rest /services/data/inputs/http/http  
| table name, token , disabled
```

2. Los duplicados pueden surgir si el origen está etiquetando incorrectamente varios tipos de origen. Por lo tanto, verifique si el origen o los tipos de origen están mal configurados.

```
index=<index_name> | stats count by source ,sourcetype
```

3. Confirm si los eventos duplicados vienen más de una vez.

```
index=<index_name> | stats count by _time, source, host | where count > 1
```

4. Inspeccione la configuración de entradas de HEC en Splunk navegando hasta Configuraciones > Entradas de datos > Recopilador de eventos HTTP en la GUI de Splunk. Asegúrese de que no se ha definido ninguna entrada HEC dos veces para el mismo origen o aplicación.

5. Compruebe los registros internos de Splunk para ver si hay errores o advertencias relacionados con la ingestión de HEC que puedan indicar errores de configuración o problemas.

```
index=_internal spource*splunkd.log* component-HttpEventCollector*
```

Resolución

- Para la fuente de Kubernetes, el comando "stats count by _raw ...el campo N donde count > 1" método de detección de duplicados no es confiable porque esto se debe a los eventos que no tienen ningún campo único como ID de evento, etc. por lo que parece que todos los eventos son duplicados cuando se verifica en la GUI de Splunk. A menos que un campo relativamente único como kubernetes.docker_id o kubernetes.pod_id se incluya en los datos sin procesar y verifique los duplicados desde el extremo de origen.
- Los duplicados tuvieron lugar ya que había varios balanceadores de carga presentes. Asegúrese de que el equilibrio de carga esté configurado correctamente para dirigir los datos a los indizadores correctos, ya que una configuración incorrecta puede hacer que los

mismos datos se configuren en varios indizadores y provocará duplicados.

Enlaces relacionados

[¿Cómo puedo encontrar eventos duplicados?](#)

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).