Integración de Splunk con Umbrella Log Management mediante S3 y Local Sync

Contenido

Introducción

Este documento describe cómo configurar Splunk para analizar los registros de tráfico DNS desde una cubeta S3 administrada por Cisco.

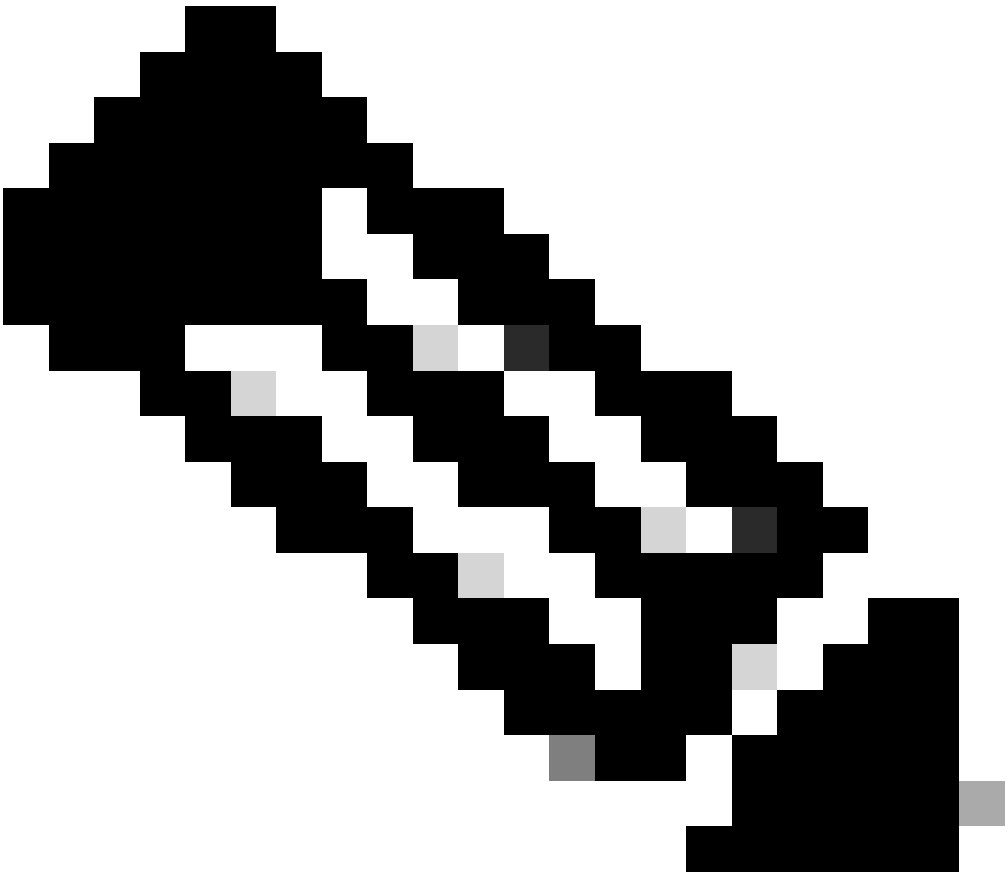
Overview

Splunk es una herramienta para el análisis de registros. Proporciona una interfaz potente para analizar grandes fragmentos de datos, como los registros proporcionados por Cisco Umbrella para el tráfico DNS. En este artículo se describe cómo:

- Configure la cubeta S3 gestionada por Cisco en el panel.
- Asegúrese de que se cumplen los requisitos previos de AWS Command Line Interface (AWS CLI).
- Cree un trabajo cron para recuperar archivos de la cubeta y almacenarlos localmente en su servidor.
- Configure Splunk para leer desde un directorio local.

Prerequisites

- Descargue e instale la interfaz de línea de comandos de AWS (AWS CLI).
- Cree su cubeta S3 gestionada por Cisco.



Nota: Los clientes existentes de Umbrella Insights y Umbrella Platform pueden acceder a Log Management con Amazon S3 a través del panel. La administración de registros no está disponible en todos los paquetes. Póngase en contacto con su gerente de cuentas si está interesado en esta función.

Creación de un trabajo cron en el servidor Splunk

1. Cree una secuencia de comandos shell denominada **pull-umbrella-logs.sh** con el contenido proporcionado, que se ejecuta en un trabajo cron programado:

```
#!/bin/sh
cd <local data dir>
AWS_ACCESS_KEY_ID=<accesskey> AWS_SECRET_ACCESS_KEY=<secretkey> aws s3 sync <data path> .
```

Reemplace los marcadores de posición por sus valores reales:

-

: Directorio en disco para almacenar los archivos de registro descargados.

- : Clave de acceso desde el panel de Umbrella.
- : Clave secreta del panel de Umbrella.
- : Ruta de datos de la interfaz de usuario de administración de registros (por ejemplo, s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/
).

2. Guarde el script de shell y establezca el permiso de ejecución. El script debe ser propiedad de root.

```
$ chmod u+x pull-umbrella-logs.sh
```

3. Ejecute el **pull-umbrella-logs.sh** script manualmente para confirmar que el proceso de sincronización funciona correctamente. No es necesario completarlo completamente; este paso confirma que las credenciales y la lógica del script son correctas.

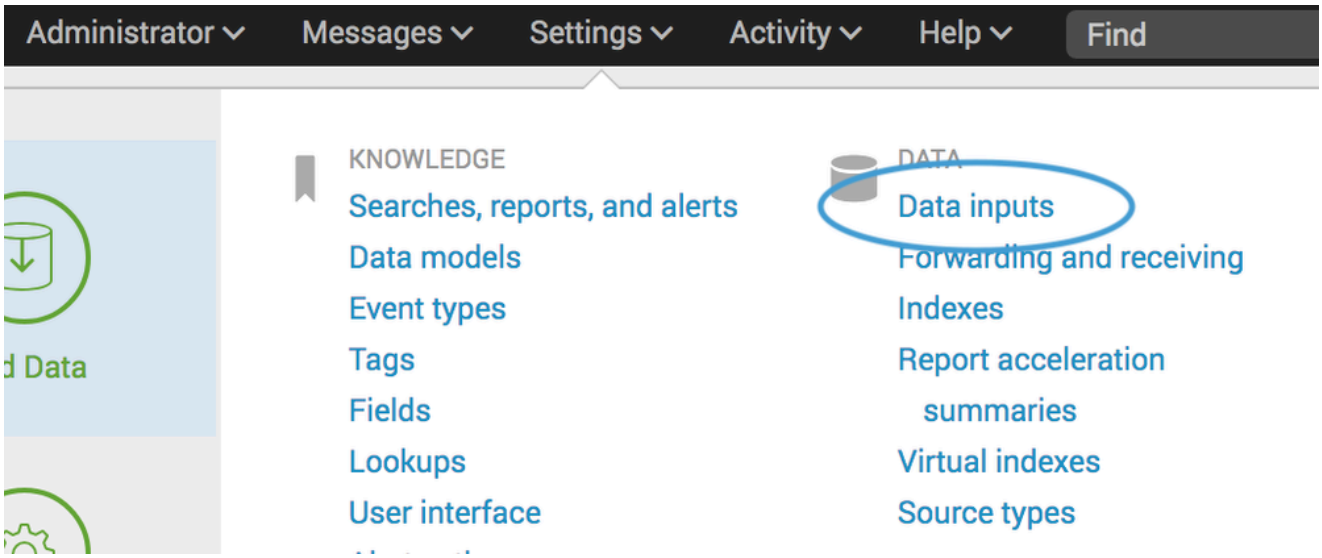
4. Agregue esta línea a su crontab de servidor Splunk:

```
*/5 * * * * root root /path/to/pull-umbrella-logs.sh &2>1 >/var/log/pull-umbrella-logs.txt
```

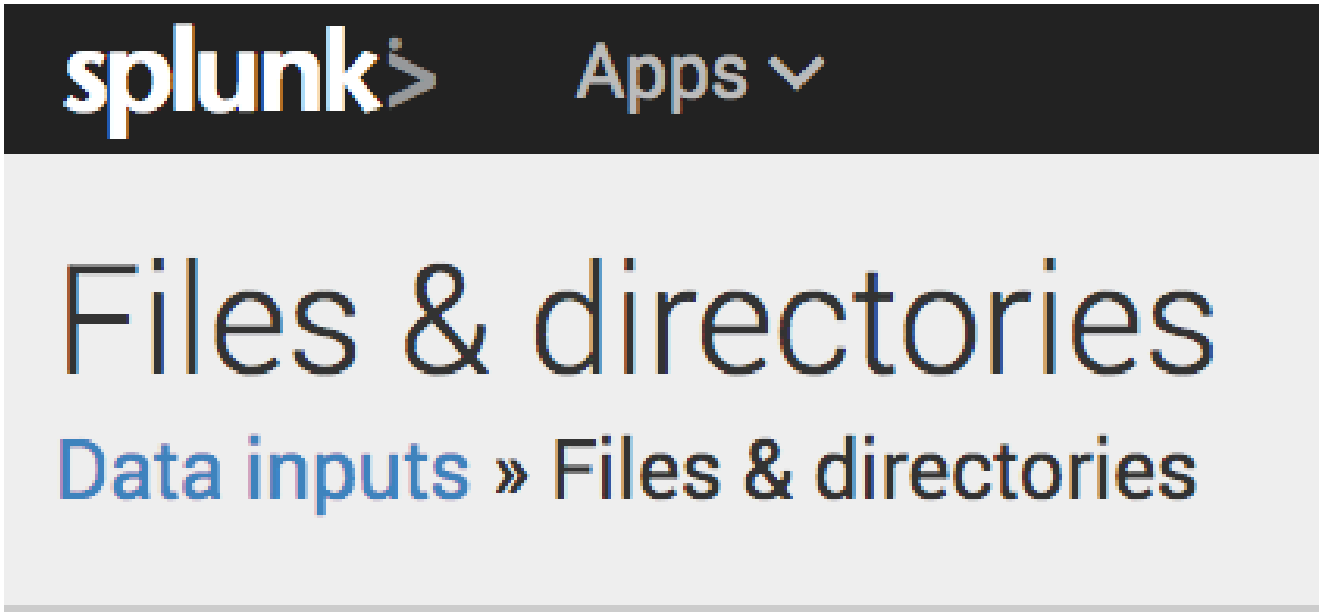
Asegúrese de editar la línea para utilizar la ruta correcta al script. Esto ejecuta una sincronización cada cinco minutos. El directorio de almacenamiento S3 se actualiza cada 10 minutos y los datos permanecen en el almacenamiento S3 durante 30 días. Esto mantiene a los dos en sincronía.

Configurar Splunk para leer desde un directorio local

1. En Splunk, navegue hasta Configuraciones **>** Entradas de datos **>** Archivos y directorios y seleccione Nuevo.

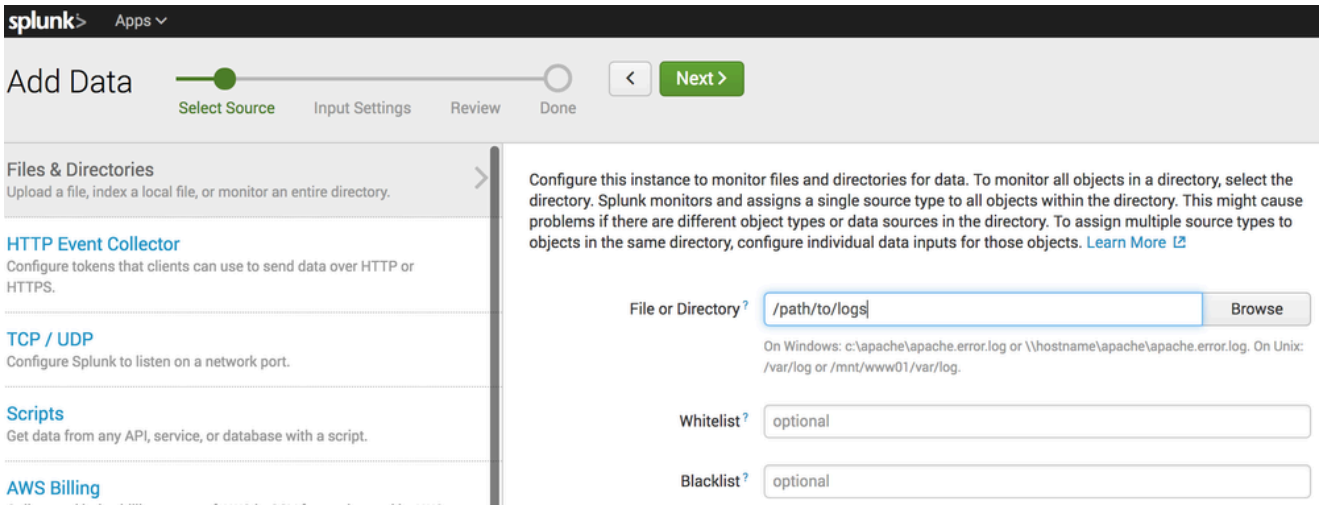


360002731126



360002731146

2. En el campo Archivo o Directorio, especifique el directorio local donde la sincronización S3 coloca los archivos.



360002731106

3. Haga clic en Next y complete el asistente con la configuración predeterminada.

Una vez que haya datos en el directorio local y se haya configurado Splunk, los datos pueden estar disponibles para consultar e informar sobre ellos en Splunk.

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).