Integrazione di Splunk con la gestione dei registri Umbrella utilizzando S3 e la sincronizzazione locale

Sommario

Introduzione

In questo documento viene descritto come configurare Splunk per analizzare i log del traffico DNS da un bucket S3 gestito da Cisco.

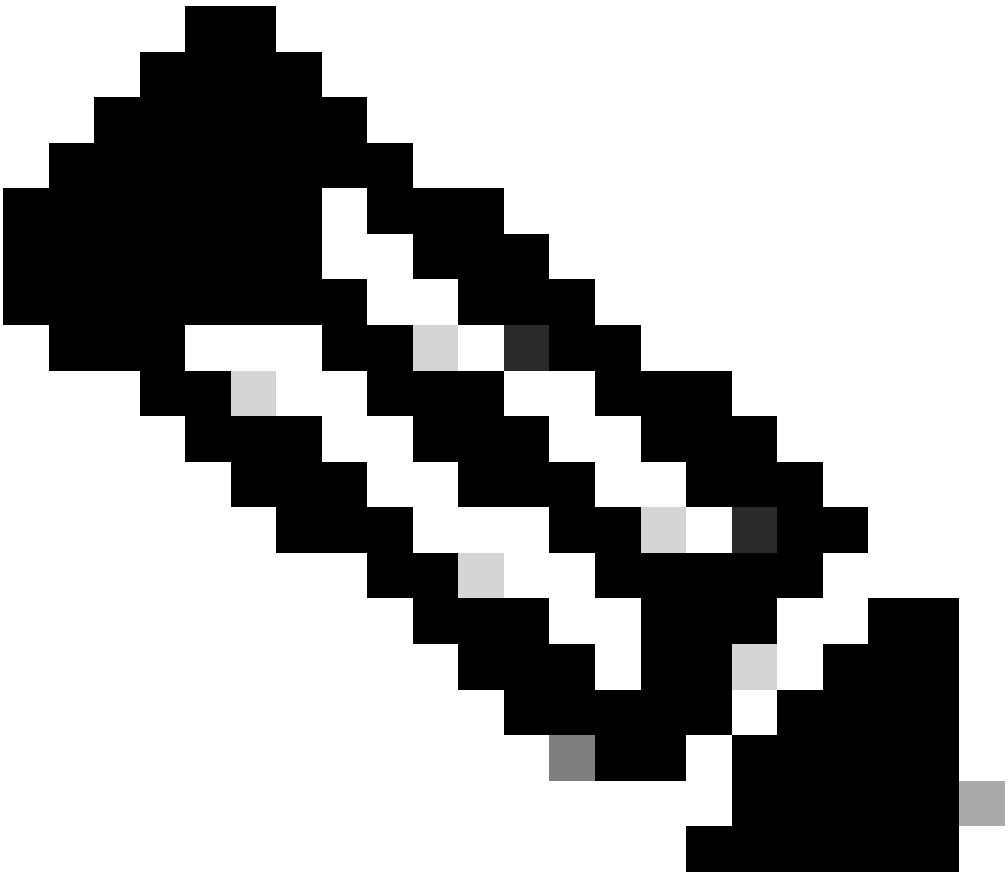
Panoramica

Splunk è uno strumento per l'analisi dei registri. Offre una potente interfaccia per l'analisi di grandi blocchi di dati, ad esempio i registri forniti da Cisco Umbrella per il traffico DNS. In questo articolo viene descritto come:

- Configurare il bucket S3 gestito da Cisco nel dashboard.
- Verificare che i prerequisiti di AWS Command Line Interface (AWS CLI) siano soddisfatti.
- Creare un processo cron per recuperare i file dal bucket e archiviarli localmente sul server.
- Configurare Splunk per la lettura da una directory locale.

Prerequisiti

- Scaricare e installare AWS Command Line Interface (AWS CLI).
- Creare il bucket S3 gestito da Cisco.



Nota: I clienti esistenti di Umbrella Insights e Umbrella Platform possono accedere alla gestione dei registri con Amazon S3 tramite il dashboard. Gestione registro non è disponibile in tutti i pacchetti. Se sei interessato a questa funzione, contatta il tuo account manager.

Creare un processo Cron sul server Splunk

1. Creare uno script shell denominato **pull-umbrella-logs.sh** con il contenuto fornito, che viene eseguito su un processo cron pianificato:

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

Sostituire i segnaposto con i valori effettivi:

-

: Directory su disco in cui archiviare i file di registro scaricati.

- : Chiave di accesso dal dashboard Umbrella.
- : Chiave segreta dal dashboard Umbrella.
- : Percorso dati dall'interfaccia utente di gestione dei registri (ad esempio, s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/

).

2. Salvare lo script della shell e impostare l'autorizzazione di esecuzione. Lo script deve essere di proprietà della radice.

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

3. **pull-umbrella-logs.sh** Eseguire lo script manualmente per verificare che il processo di sincronizzazione funzioni correttamente. Il completamento completo non è richiesto; in questo passaggio viene confermata la correttezza delle credenziali e della logica dello script.

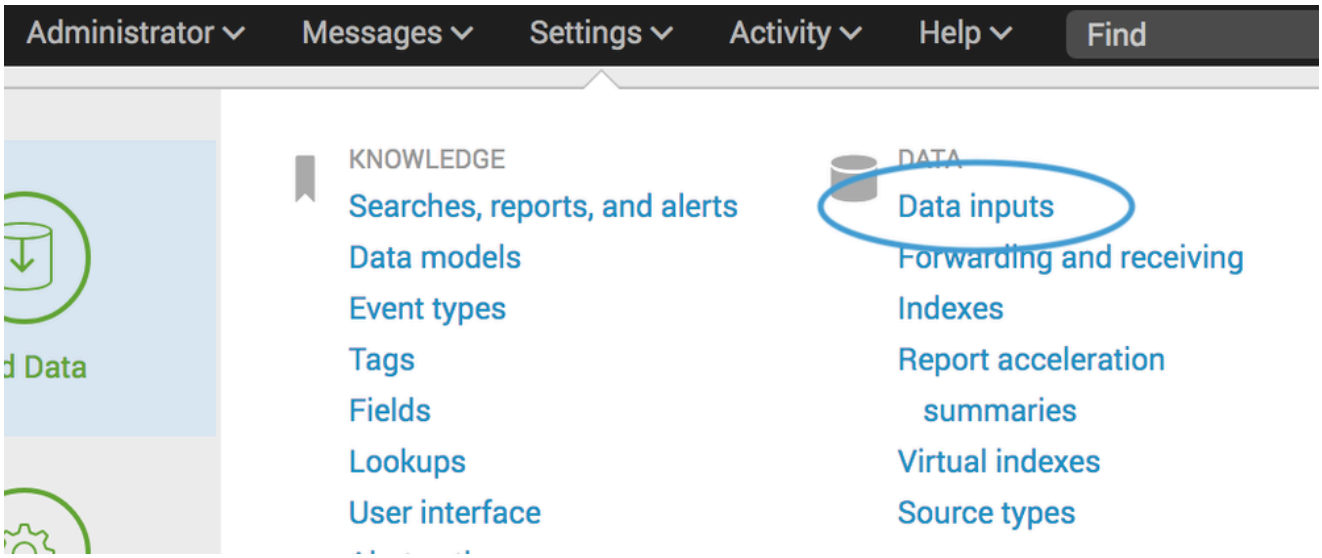
4. Aggiungere questa riga alla scheda del nodo del server Splunk:

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

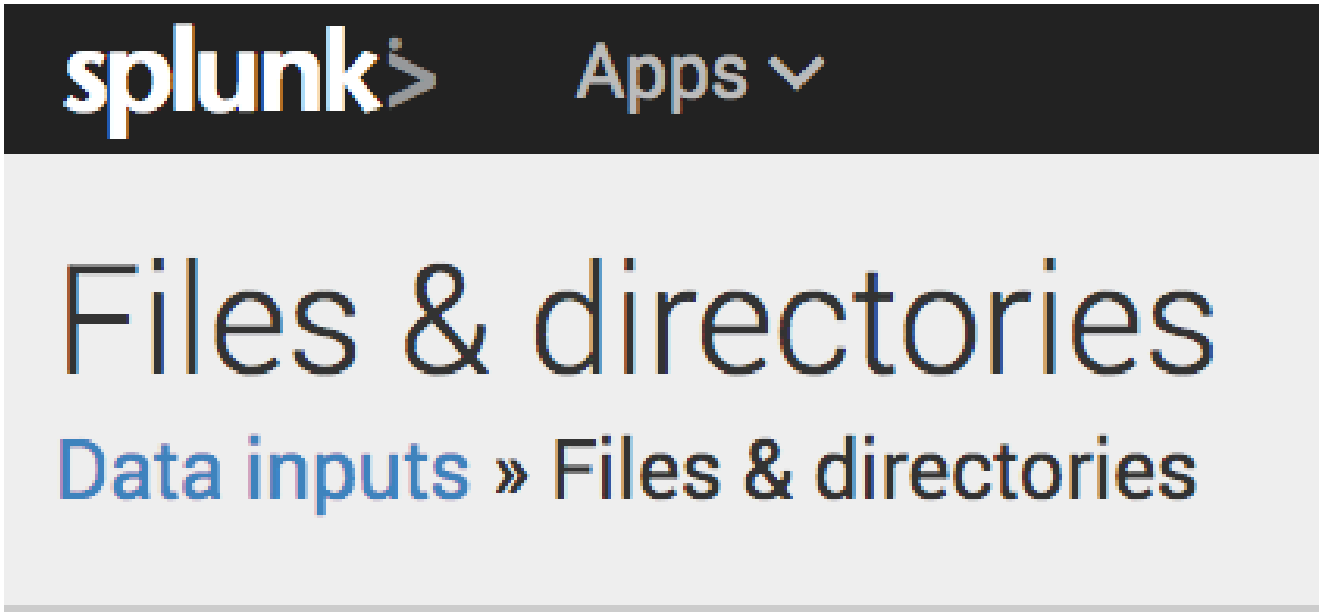
Assicurarsi di modificare la riga per utilizzare il percorso corretto dello script. Viene eseguita una sincronizzazione ogni cinque minuti. La directory di storage S3 viene aggiornata ogni 10 minuti e i dati rimangono sullo storage S3 per 30 giorni. In questo modo i due elementi rimangono sincronizzati.

Configurare Splunk per la lettura da una directory locale

1. In Splunk, selezionare Settings > Data Inputs > Files & Directories (Impostazioni > Input dati > File e directory) e selezionare New (Nuovo).

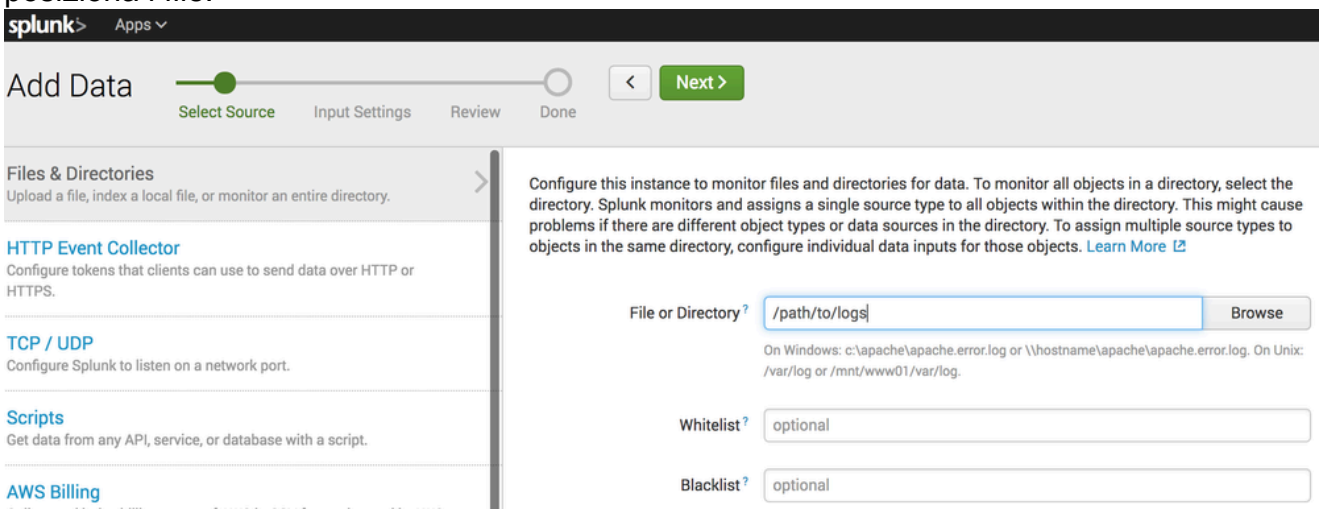


360002731126



360002731146

2. Nel campo File o Directory, specificare la directory locale in cui la sincronizzazione S3 posiziona i file.



360002731106

3. Fare clic su Avanti e completare la procedura guidata utilizzando le impostazioni predefinite.

Una volta che sono presenti dati nella directory locale ed è stato configurato Splunk, i dati possono essere disponibili per eseguire query e creare report in Splunk.

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).