Integre o Splunk com o gerenciamento de logs de guarda-chuva usando S3 e a sincronização local

Contents

Introdução

Este documento descreve como configurar o Splunk para analisar logs de tráfego DNS de um bucket de S3 gerenciado pela Cisco.

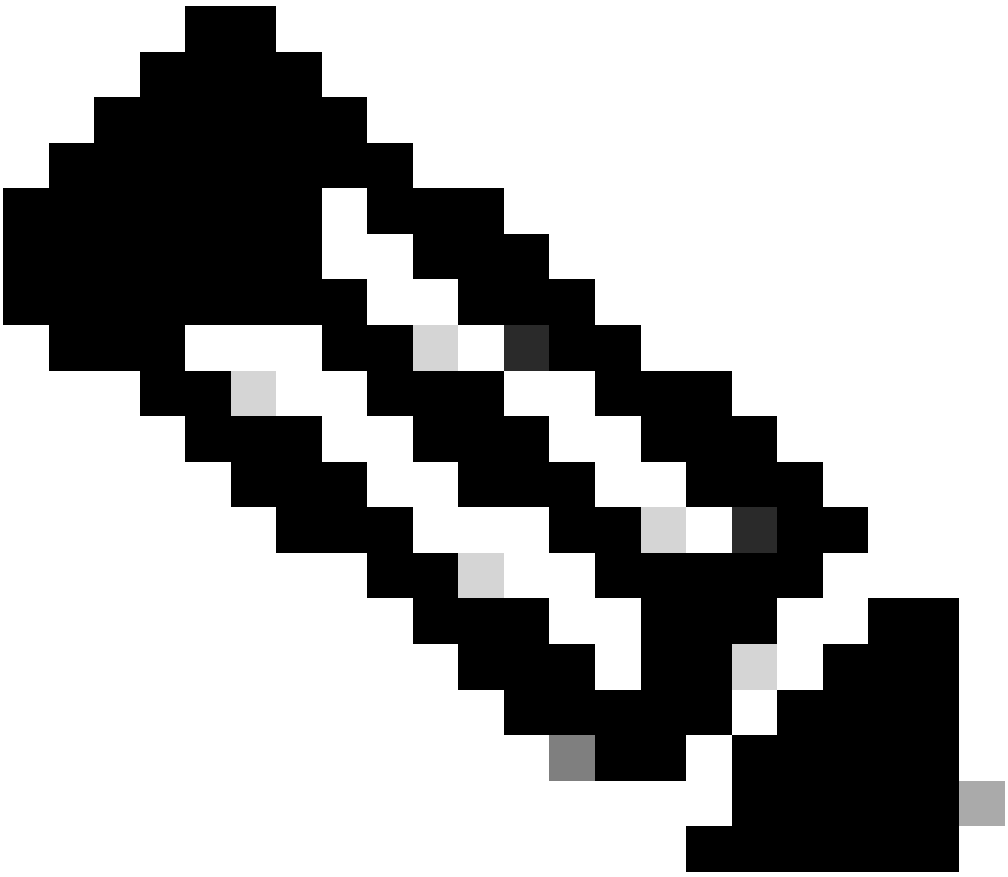
Overview

O Splunk é uma ferramenta para análise de log. Ele fornece uma interface eficiente para analisar grandes blocos de dados, como os logs fornecidos pelo Cisco Umbrella para o tráfego DNS. Este artigo descreve como:

- Configure o balde S3 gerenciado pela Cisco em seu painel.
- Verifique se os pré-requisitos da AWS Command Line Interface (AWS CLI) foram atendidos.
- Crie um trabalho cron para recuperar arquivos do bucket e armazená-los localmente no servidor.
- Configurar o Splunk para ler a partir de um diretório local.

Pré-requisitos

- Baixe e instale a AWS Command Line Interface (AWS CLI).
- Crie seu depósito S3 gerenciado pela Cisco.



Note: Os clientes atuais da Umbrella Insights e da Umbrella Platform podem acessar o Gerenciamento de logs com o Amazon S3 por meio do painel. O Gerenciamento de logs não está disponível em todos os pacotes. Entre em contato com seu gerente de contas se estiver interessado nesse recurso.

Crie um trabalho Cron no servidor Splunk

1. Crie um script de shell chamado **pull-umbrella-logs.sh** com o conteúdo fornecido, que seja executado em um trabalho cron agendado:

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

Substitua os espaços reservados pelos valores reais:

-

: Diretório no disco para armazenar os arquivos de log baixados.

- : Acesse a chave no painel do Umbrella.
- : Chave secreta do painel do Umbrella.
- : Caminho de dados da interface do usuário de gerenciamento de logs (por exemplo, s3://cisco-managed-

/1_2xxxxxxxxxxxxxxxxxa120c73a7c51fa6c61a4b6/dnslogs/
).

2. Salve o script de shell e defina a permissão de execução. O script deve pertencer à raiz.

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

3. Execute o **pull-umbrella-logs.sh** script manualmente para confirmar se o processo de sincronização está funcionando. O preenchimento completo não é necessário; esta etapa confirma que as credenciais e a lógica do script estão corretas.

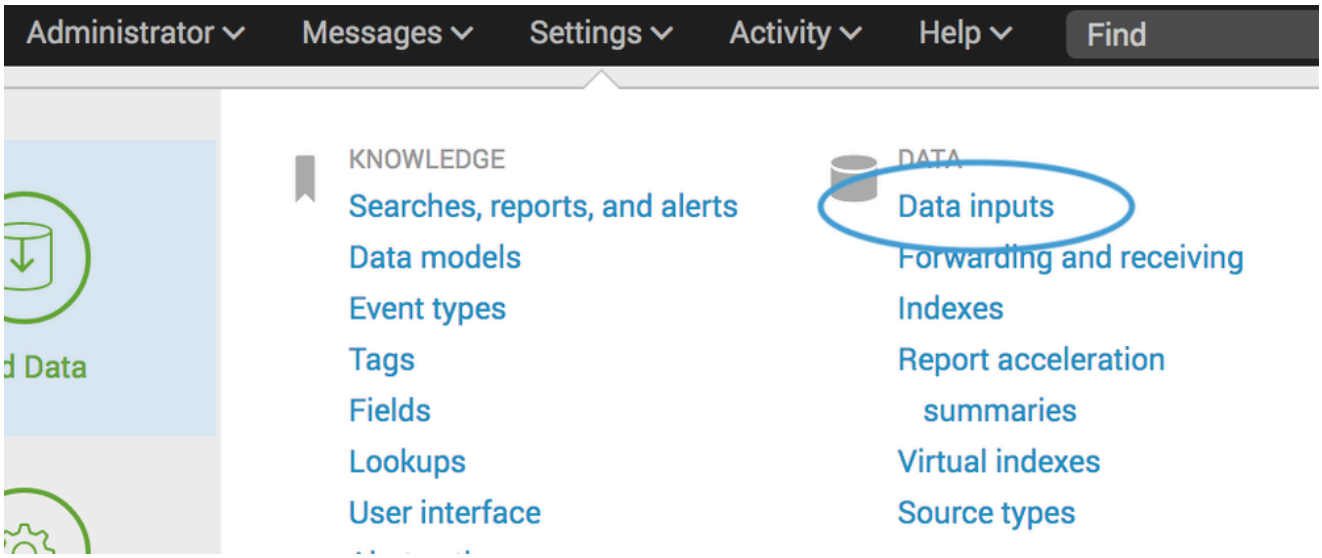
4. Adicione esta linha ao crontab do servidor Splunk:

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

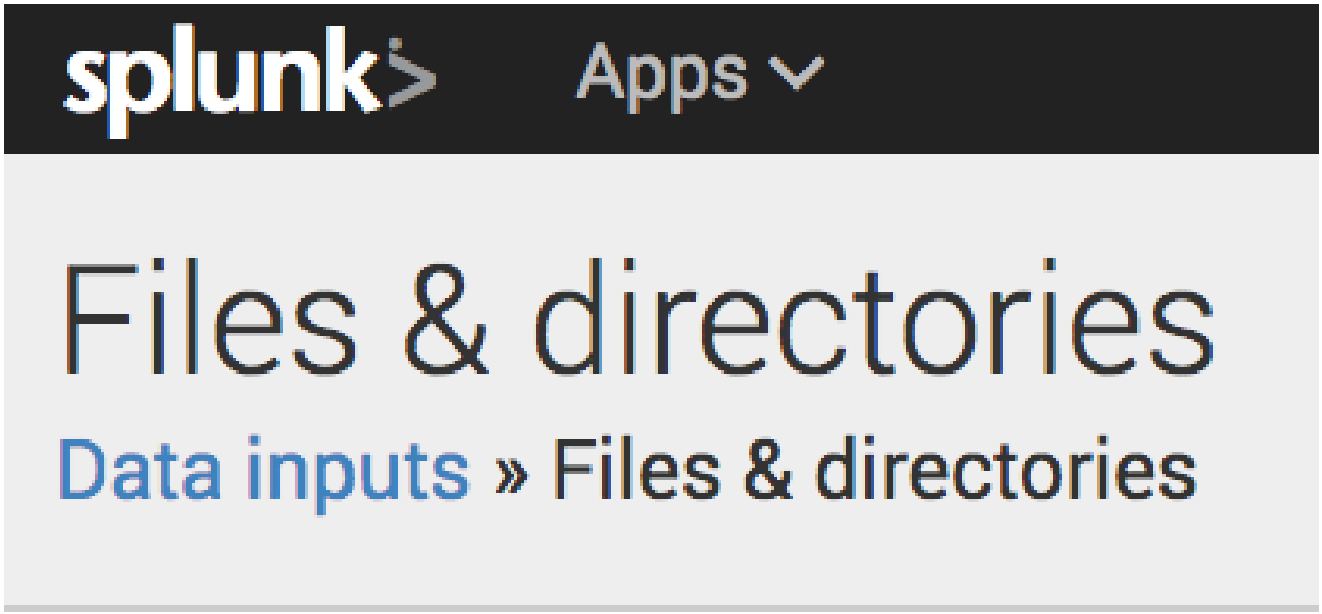
Não se esqueça de editar a linha para usar o caminho correto para o script. Isso executa uma sincronização a cada cinco minutos. O diretório de armazenamento S3 é atualizado a cada 10 minutos e os dados permanecem no armazenamento S3 por 30 dias. Isso mantém os dois em sincronia.

Configurar o 'Splunk' para ler a partir de um diretório local

1. Em Splunk, navegue para Settings > Data Inputs > Files & Directories e selecione New.

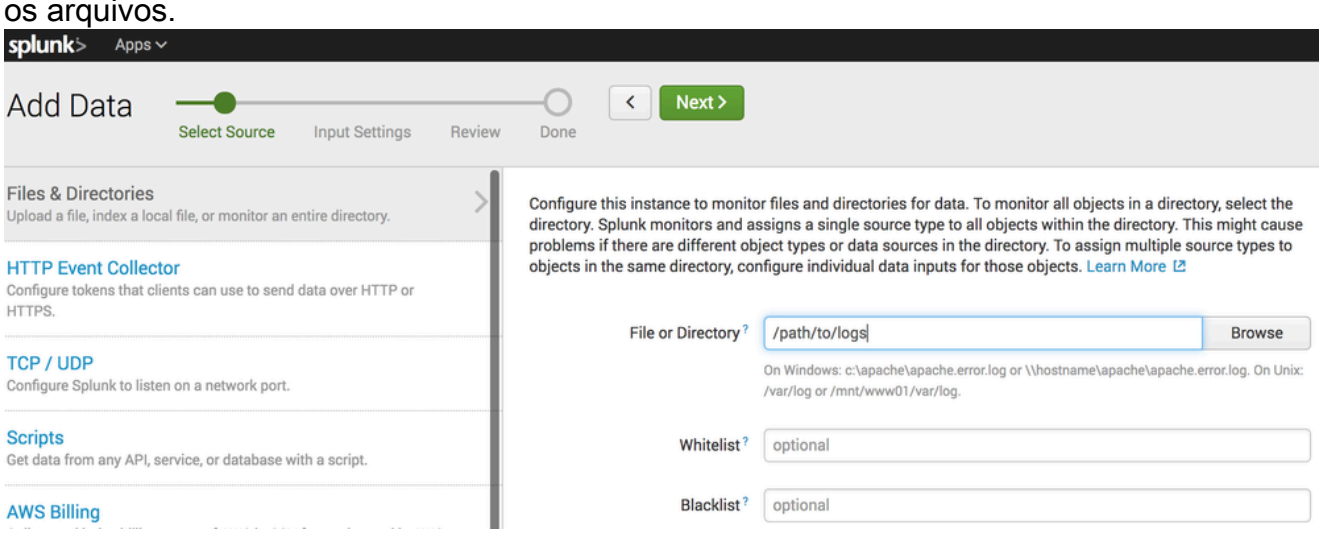


360002731126



360002731146

2. No campo File or Diretory, especifique o diretório local onde a sincronização do S3 coloca os arquivos.



360002731106

3. Clique em Avançar e conclua o assistente usando as configurações padrão.

Quando houver dados no diretório local e o Splunk estiver configurado, os dados poderão ser consultados e relatados no Splunk.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.