Configurar o Splunk com um Recipiente S3 Autogerenciado

Contents

Introdução

Este documento descreve como configurar o Splunk com um bucket de S3 autogerenciado.

Overview

O Splunk é uma ferramenta comum para a 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 da sua organização.

Este artigo descreve os conceitos básicos de como configurar e executar o Splunk para que ele possa extrair os logs do bucket de S3 e consumi-los. Há dois estágios principais: um é configurar suas Credenciais de Segurança do AWS S3 para permitir o acesso Splunk aos logs e o segundo é configurar o próprio Splunk para apontar para seu bucket.

A documentação para o complemento Splunk para AWS S3 está aqui, alguns dos quais foram copiados literalmente neste documento. Para perguntas específicas sobre a configuração do Splunk, consulte http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

Este artigo tem estas seções:

- Pré-requisitos
- Estágio 1: Configurando suas credenciais de segurança no AWS (apenas bucket autogerenciado)

- Estágio 2: Configurando o Splunk para extrair dados de log DNS do bucket de S3
    - Passo 1: Configurando o Splunk para receber dados de log DNS do bucket de S3 autogerenciado
- Estágio 3: Configurando Entradas de Dados para Splunk

Pré-requisitos

O complemento Splunk para Amazon Web Services oferece suporte a essas plataformas.

- AWS Linux
- RedHat
- Windows 2008R2, 2012R2

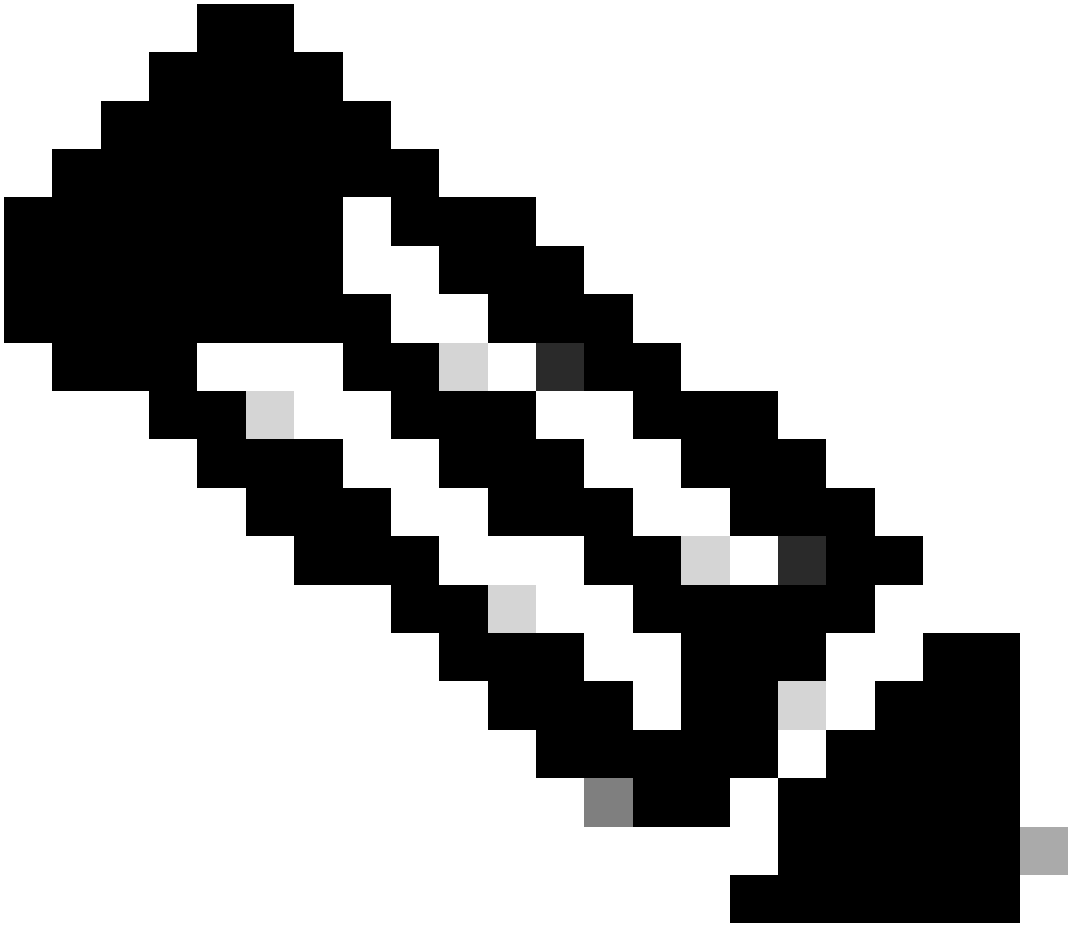
Requisitos do sistema Splunk Enterprise

Como este complemento é executado no Splunk Enterprise, todos os requisitos do sistema do Splunk Enterprise se aplicam. Consulte o Manual de instalação dos "Requisitos do sistema" na documentação do Splunk Enterprise. Estas instruções são para o Splunk Enterprise versão 6.2.1.

Requisitos gerais

Este documento pressupõe que o bucket do Amazon AWS S3 foi configurado no painel do Umbrella (Admin> Gerenciamento de logs) e está verde com os logs recentes carregados. Para obter mais informações sobre o gerenciamento de logs, consulte Gerenciamento de logs do Cisco Umbrella no Amazon S3.

Estágio 1: Configurando suas Credenciais de Segurança no AWS



Note: Essas etapas são as mesmas descritas no artigo que descreve como configurar uma ferramenta para baixar os logs do seu bucket (Como: Download de logs do Cisco Umbrella Log Management no AWS S3). Se você já tiver executado essas etapas, basta passar para a etapa 2, embora precise das credenciais de segurança do usuário do IAM para autenticar o plug-in Splunk no bucket.

Passo 1

1. Adicione uma chave de acesso à sua conta do Amazon Web Services para permitir acesso remoto à sua ferramenta local e permitir o carregamento, o download e a modificação de arquivos no S3. Faça logon no AWS e clique no nome da sua conta no canto superior direito. Na lista suspensa, escolha Credenciais de segurança.
2. Você é solicitado a usar as Melhores formas de aprendizado da Amazon e criar um usuário do AWS Identity and Access Management (IAM). Essencialmente, um usuário do IAM garante que a conta que o s3cmd usa para acessar seu bucket não seja a conta principal (por exemplo, sua conta) para toda a sua configuração do S3. Criando usuários IAM individuais para pessoas que acessam sua conta, você pode fornecer a cada usuário IAM

um conjunto exclusivo de credenciais de segurança. Você também pode conceder permissões diferentes a cada usuário do IAM. Se necessário, você pode alterar ou revogar as permissões de um usuário do IAM a qualquer momento.
Para obter mais informações sobre usuários do IAM e práticas recomendadas do AWS, leia aqui: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Passo 2

1. Crie um usuário do IAM para acessar seu bucket do S3 clicando em Introdução aos usuários do IAM. Você é direcionado para uma tela onde pode criar um usuário do IAM.
2. Clique em Criar novos usuários e preencha os campos. Observe que a conta de usuário não pode conter espaços.
3. Depois de criar a conta de usuário, você tem apenas uma oportunidade de obter duas informações críticas contendo suas Credenciais de Segurança de Usuário do Amazon. É altamente recomendável que você faça o download delas usando o botão no canto inferior direito para fazer o backup. Eles não estarão disponíveis após esta etapa da configuração. Anote a ID da chave de acesso e a chave de acesso secreta, pois precisamos delas mais tarde ao configurar o Splunk.

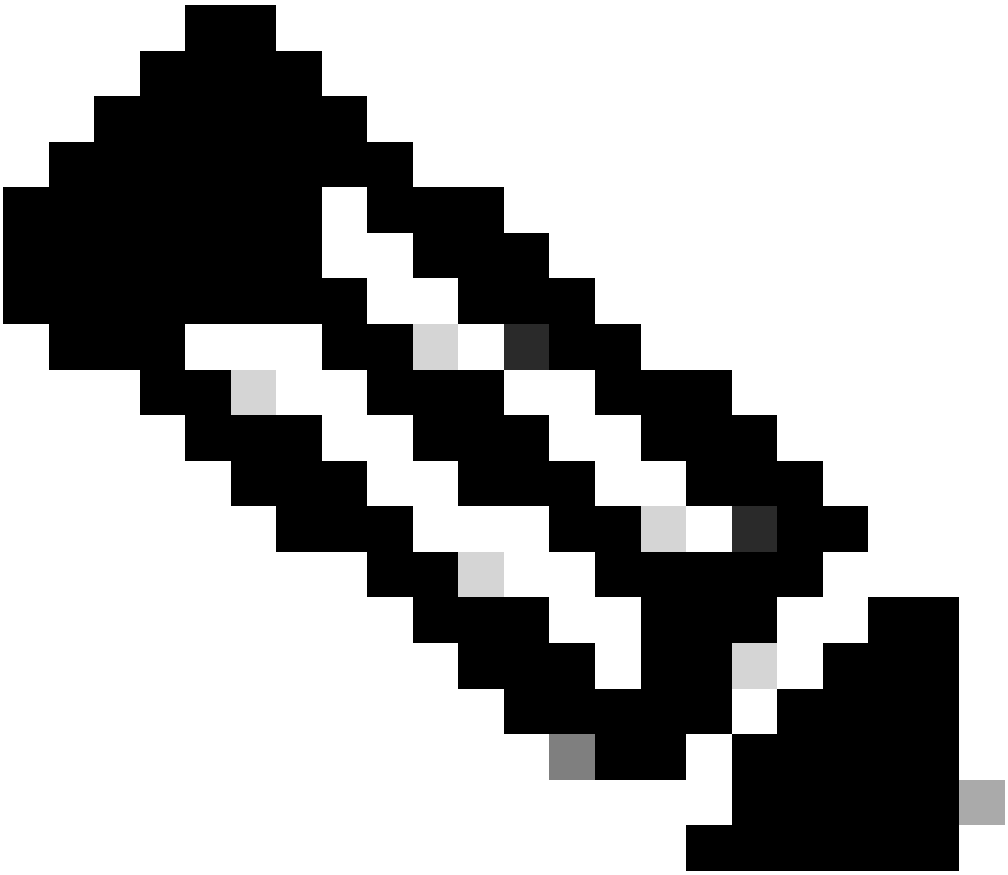
Etapa 3

1. Em seguida, você deseja adicionar uma política para o usuário do IAM para que ele tenha acesso ao bucket de S3. Clique no usuário que acabou de criar e role para baixo pelas propriedades dos usuários até ver o botão Attach Policy (Anexar política).
2. Clique em Attach Policy e digite 's3' no filtro do tipo de política. Isso mostra dois resultados: "AmazonS3FullAccess" e "AmazonS3ReadOnlyAccess".
3. Selecione AmazonS3FullAccess e clique em Attach Policy.

Estágio 2: Configurando o Splunk para extrair dados de log DNS do bucket de S3

Etapa 1: configurar o Splunk para receber dados de log DNS do bucket de S3 autogerenciado

1. Comece instalando o "Complemento Splunk para Amazon Web Services" em sua instância do Splunk. Abra o painel do Splunk e clique em Aplicativos ou clique em Aplicativos do Splunk se ele aparecer no painel. Uma vez na seção Apps, digite "s3" na janela de pesquisa para encontrar "Splunk Add-on para Amazon Web Services", e instalar o aplicativo.



Note: É provável que você precise reiniciar o Splunk durante a instalação.
Uma vez instalado, você verá o Splunk Add-on para AWS com o nome de pasta 'Splunk_TA_aws' agora listado em Aplicativos.

2. Clique em Configurar para configurar o aplicativo. Este é o ponto em que você precisa das Credenciais de segurança do Estágio 1 nesta documentação.
   A configuração exige que estes campos sejam inseridos:

   - Um nome amigável — o nome que você usa para se referir a essa integração
   - Sua ID da chave da conta AWS (do estágio 1)
   - Sua senha (sua chave secreta da conta AWS, também da etapa 1)

Você também pode definir qualquer informação de proxy local se for necessário para que o Splunk acesse o AWS, bem como ajustar o registro. A tela de configuração é semelhante a esta:
3. Depois de adicionar informações relevantes, clique em Salvar e o complemento Splunk para Amazon Web Services estará totalmente configurado.

Estágio 3: Configurando Entradas de Dados para Splunk

1. Em seguida, você deseja configurar a entrada de dados para Amazon Web Services S3. Navegue para Configurações > Dados > Entradas de dados e em Entradas locais, você agora vê uma lista de várias entradas Amazon, incluindo S3 na parte inferior da lista.
2. Clique em AWS S3 para configurar a entrada.
3. Clique em New.
4. Você deve fornecer estas informações:

    - Digite um nome amigável para a integração do S3.
    - Selecione seu Conta AWS do menu suspenso. Esse é o nome amigável que você forneceu na etapa 1.
    - Selecione o período S3 no menu suspenso. Esse é o nome do recipiente conforme especificado no painel Umbrella (Configurações > Gerenciamento de logs).
    - Selecione o nome da chave S3 no menu suspenso. Todos os itens em seu bucket são listados. Recomendamos selecionar o diretório de nível superior \dns-logs\ , que inclui todos os arquivos e diretórios abaixo dele.
    - Há várias opções em "Configuração do sistema de mensagens", recomendamos deixá-las como estão—configurações padrão.
    - Há opções adicionais em "Mais configurações". É importante observar que "Tipo de origem", que é aws:s3 por padrão. Recomendamos deixar isso como está, mas se você alterá-lo, o filtro para seus logs na Pesquisa será alterado a partir do que está descrito na Etapa 3 dessas instruções.

Preencha os detalhes e sua entrada de dados será semelhante a esta:

4. Clique em Próximo para finalizar seus detalhes.
   Você é direcionado para uma tela que mostra que a entrada foi criada com êxito

Etapa 3

Faça uma pesquisa rápida para ver se seus dados estão sendo importados corretamente. Basta colar sourcetype="aws:s3" na janela Pesquisar no canto superior direito e selecionar "Open sourcetype="aws:s3" na pesquisa

Isso o leva a uma tela semelhante àquela em que você vê os eventos dos logs DNS de suas organizações. Aqui, o serviço móvel Cisco Umbrella está bloqueando as mídias sociais em um iPhone. Você também pode usar a origem do nome do arquivo para filtrar em relação a um lote específico de logs.

Depois desse ponto, o trabalho cron em segundo plano continua a ser executado e obtém os conjuntos mais recentes das informações de log do bucket.

Há muito mais que você pode fazer com o Splunk além do que foi delineado neste artigo, e se você teve a chance de experimentar usar esses dados em seu procedimento de resposta de segurança, gostaríamos de saber sua opinião. Envie comentários, perguntas ou preocupações para umbrella-support@cisco.com e consulte este artigo.

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.