Faça o download de registros do Gerenciamento de registros de guarda-chuva no AWS S3

Contents

- Introdução
- Overview
- Estágio 1: Configurando suas credenciais de segurança no AWS
  - Passo 1
  - Passo 2
  - Etapa 3
- Estágio 2: Configurando uma ferramenta para fazer download de logs de DNS do bucket
  - s3cmd para MacOS e Linux
  - Executável da Linha de Comando do Windows (s3.exe)
- Estágio 3: Testando o download de arquivos do seu balde
  - Passo 1: Testar o download
    - s3cmd para OS/X e Linux
    - Executável da Linha de Comando do Windows (s3.exe)
  - Passo 2: Automatizar o download

Introdução

Este documento descreve como fazer download de logs do Umbrella Log Management no AWS S3.

Overview

Depois de configurar e testar se o gerenciamento de logs no Amazon S3 está funcionando corretamente, talvez você queira começar a fazer o download e armazenar automaticamente os logs em sua infraestrutura de rede, para retenção ou consumo (ou ambos).

Para fazer isso, descrevemos uma abordagem usando s3tools de http://s3tools.org. O s3tools usa o utilitário de linha de comando s3cmd para Linux ou OS/X. Há outras ferramentas que podem realizar uma função semelhante para usuários do Windows:

- Para uma ferramenta de linha de comando, você pode baixar um pequeno executável de linha de comando aqui.
- Se você preferir uma interface gráfica, verifique o S3 Browser (https://s3browser.com/), embora não estejamos abordando como usá-la, porque a interface gráfica não é passível de script para automatizar o processo. Este artigo fornece as etapas para configurar as duas ferramentas de linha de comando. Você pode usar as informações na etapa 1 para configurar o aplicativo s3browser, se preferir.

Comece fazendo o download da ferramenta para o sistema operacional que você pretende usar. Por enquanto, estamos apenas cobrindo s3cmd para OS/X e Linux, embora as etapas para acessar seu bucket e baixar os dados são efetivamente as mesmas para o Windows.

Pegue o instalador do s3tools aqui.

O instalador não requer que você instale o programa para executar a linha de comando, portanto, simplesmente extraia o pacote que você baixou.

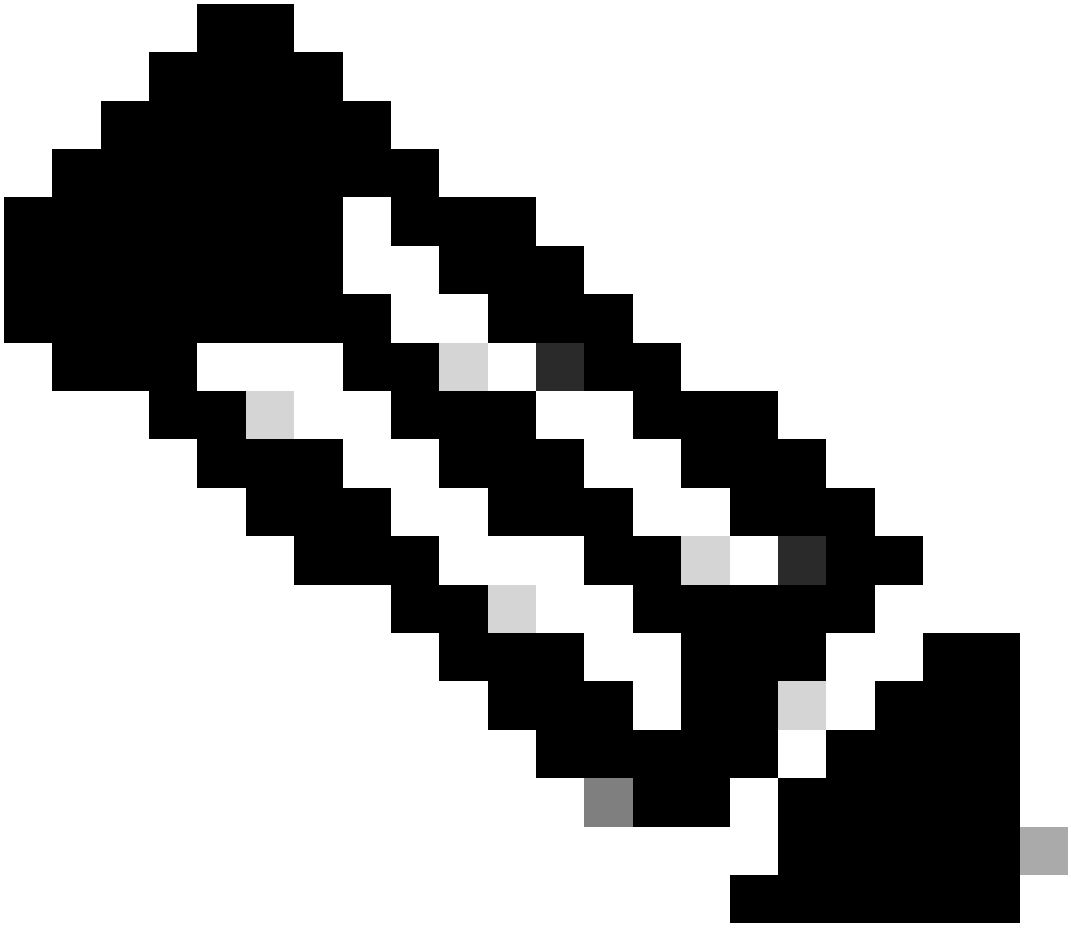
Estágio 1: Configurando suas credenciais de segurança no AWS

Passo 1

1. Adicione uma chave de acesso à sua conta do Amazon Web Services para habilitar o acesso remoto à sua ferramenta local e a capacidade de carregar, baixar e modificar arquivos no S3. Faça login no AWS e clique no nome da sua conta no canto superior direito. Na lista suspensa, escolha Credenciais de segurança.
2. Um prompt o instrui 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 os usuários do IAM e as práticas recomendadas do AWS, leia aqui.

Passo 2

1. Clique em Introdução aos usuários do IAM para criar um usuário do IAM com acesso ao bucket do S3. Navegue até uma tela onde você pode criar um usuário do IAM.
2. Clique em Criar novos usuários e preencha os campos.
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 desses itens usando o botão no canto inferior direito para fazer o backup. Eles não estarão disponíveis após esta etapa da instalação. Anote a ID da chave de acesso e a chave de acesso secreta, pois precisaremos deles em uma etapa posterior.



Note: A conta de usuário não pode conter espaços.

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 deve mostrar dois resultados "AmazonS3FullAccess" e "AmazonS3ReadOnlyAccess".
3. Selecione AmazonS3FullAccess e clique em Attach Policy.

Estágio 2: Configurando uma ferramenta para fazer download de logs de DNS do bucket

s3cmd para MacOS e Linux

1. Vá para o caminho em que você extraiu o s3cmd no estágio anterior e, em Terminal, digite:

```
./s3cmd --configure
```

Isso o levará a um prompt solicitando que você forneça suas credenciais de segurança:

Informe novos valores ou aceite padrões entre colchetes com Enter.

Consulte o manual do usuário para obter uma descrição detalhada de todas as opções.

A chave de acesso e a chave secreta são seus identificadores do Amazon S3. Deixe-os em branco para usar as variáveis env.

Chave de acesso [SUA CHAVE DE ACESSO]:

Chave secreta [SUA CHAVE SECRETA]:

2. Em seguida, você receberá uma série de perguntas sobre como gostaria de configurar o acesso ao seu bucket. Nesse caso, não estamos configurando uma senha de criptografia (GPG) e não estamos usando HTTPS ou um servidor proxy. Se sua rede ou suas preferências forem diferentes, preencha os campos obrigatórios:

Região padrão [EUA]:

A senha de criptografia é usada para proteger seus arquivos contra a leitura por pessoas não autorizadas durante a transferência para o S3

Senha de criptografia:

Caminho para o programa GPG [Nenhum]:

Ao usar o protocolo HTTPS seguro, toda a comunicação com servidores Amazon S3 é protegida contra espionagem de terceiros. Este método é

mais lento que o HTTP simples e só pode receber proxy com Python 2.7 ou mais recente

Usar protocolo HTTPS [Não]:

Em algumas redes, todo o acesso à Internet deve passar por um proxy HTTP.

Tente defini-lo aqui se não conseguir se conectar diretamente ao S3

Nome do servidor proxy HTTP:

Depois de inserir qualquer configuração específica da rede ou qualquer criptografia, você terá a oportunidade de revisar:

Novas configurações:

Chave de acesso: SUA CHAVE

Chave Secreta: SUA CHAVE SECRETA

Região padrão: US

Senha de criptografia:

Localização do programa GPG: Nenhum

Usar protocolo HTTPS: Falso

Nome do servidor proxy HTTP:

Porta do servidor proxy HTTP: 0

Por fim, você será solicitado a testar e, se obtiver êxito, salvar as configurações:

Testar o acesso com as credenciais fornecidas? [S/n] y

Aguarde, tentando listar todos os buckets...

Sucesso. A chave de acesso e a chave secreta funcionaram bem ��

Verificando se a criptografia funciona...

Não configurado. Não importa.

Salvar configurações? [s/N]

Executável da Linha de Comando do Windows (s3.exe)

Após fazer o download da ferramenta (https://s3.codeplex.com/releases/view/47595), copie o .exe para a pasta de trabalho de sua preferência e, no prompt de comando, digite-o, substituindo sua chave de acesso e segredo:

<#root>

s3 auth [

]

Para obter mais informações sobre a sintaxe de autenticação, leia aqui.

Estágio 3: Testando o download de arquivos do seu balde

Passo 1: Testar o download

s3cmd para OS/X e Linux

No terminal, execute este comando onde "my-organization-name-log-bucket" é o nome do seu bucket já configurado na parte de Gerenciamento de logs do painel do Umbrella. Neste exemplo, ele é executado a partir da pasta que contém o executável s3cmd e os arquivos são entregues no mesmo caminho, mas eles podem ser alterados:

<#root>

```
./s3cmd sync s3://my-organization-name-log-bucket ./
```

Se houver uma diferença entre os arquivos em seu bucket e os arquivos no caminho de destino no disco, a sincronização deverá baixar os arquivos ausentes ou atualizados. O primeiro arquivo recuperado deve ser o arquivo LEIAME que geralmente é carregado:

./s3cmd sync s3://my-organization-name-log-bucket ./

s3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [1 de 1]

1800 de 1800 100% em 0s 15,00 kB/s concluído

Concluído. Baixados 1.800 bytes em 1 segundo, 1.800.00 B/s

Todos os arquivos de log presentes também são baixados. Cabe a você definir um trabalho cron para agendar essa função regularmente, mas agora você pode fazer o download automático de qualquer arquivo de log novo ou alterado no bucket para um caminho local para retenção a longo prazo.

Executável da Linha de Comando do Windows (s3.exe)

No prompt de comando, execute esse comando onde 'my-organization-name-log-bucket' é o nome do seu bucket já configurado na parte de Gerenciamento de logs do painel do

Umbrella. Neste exemplo, todos os arquivos no bucket (definido com o curinga asterisco) são transferidos por download para a pasta \dnslogbackups\.

<#root>

```
s3 get my-organization-name-log-bucket/* c:\dnslogbackups\
```

Para obter mais informações sobre a sintaxe desse comando, leia aqui.

Passo 2: Automatizar o download

Depois que a sintaxe tiver sido testada e funcionar como esperado, copie as instruções em um script de configuração de um trabalho cron (OS X / Linux) ou uma tarefa agendada (Windows) ou use qualquer outra ferramenta de automação de tarefas que você possa ter à sua disposição. Também é possível usar as ferramentas para remover arquivos de seu bucket depois de baixá-los para liberar espaço em sua instância do S3. Recomendamos que você consulte a documentação da ferramenta que está usando para ver o que pode funcionar melhor para sua política de retenção de dados.

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.