Configurar registros de eventos consolidados para envio AWS S3

Contents

Introduction

Este documento descreve como configurar registros de eventos consolidados a serem enviados para um bucket S3 em um Email Security Appliance (ESA) ou Cloud Email Security (CES).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ESA executando Async OS 13.0 ou superior
- Acesso administrativo ao dispositivo
- Conta e acesso do Amazon Web Services (AWS) para criar e gerenciar o bucket S3

Componentes Utilizados

As informações neste documento são baseadas em todos os modelos de hardware ESA suportados e dispositivos virtuais que executam o Async OS 13.0 ou posterior. Para verificar as informações da versão do dispositivo na CLI, insira o comando version. Na GUI, selecione **Monitor > System Status**.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer configuração.

Informações de Apoio

A partir do sistema operacional assíncrono 13.0 e superior, o ESA permite a configuração de

registro baseado no Unified Common Event Format (CEF) conhecido como Consolidated Event Logs (Logs de eventos consolidados), amplamente usado por fornecedores de SIEM. Consulte as notas de versão do SEC 13.0 aqui.

Os registros CEF também podem ser configurados para serem enviados para um bucket AWS S3 além do download manual, SCP e envio de syslog.

> **Note**: As etapas fornecidas para a configuração do AWS baseiam-se nas informações disponíveis no momento em que este artigo é escrito.

Configurar

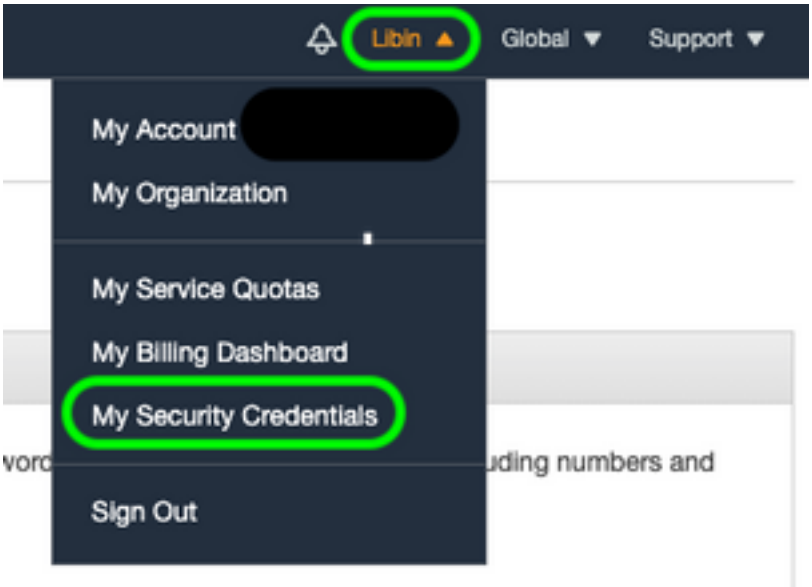
1. Navegue até o console AWS Cloud para coletar o nome do bucket S3, a chave de acesso S3 e a chave de segredo S3.

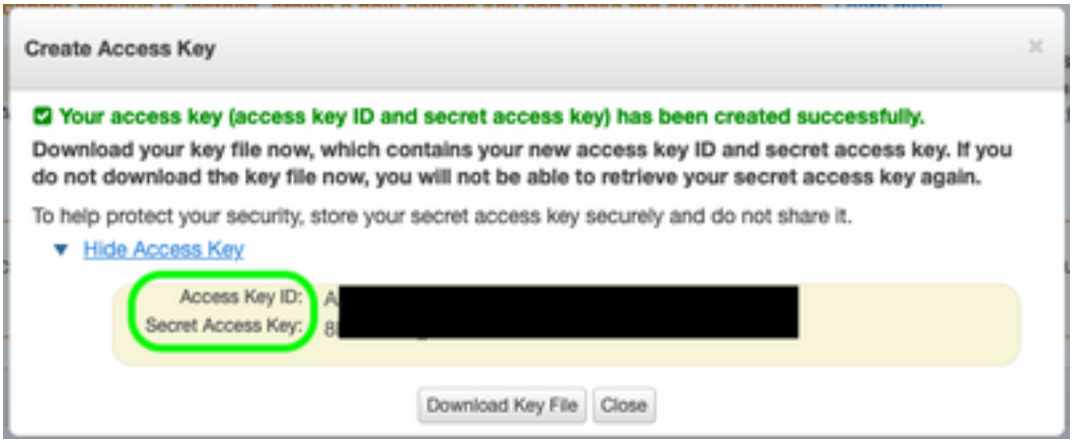
Para Nome do Balde S3:

Depois de fazer login no AWS Cloud, use o menu suspenso Services para selecionar S3 ou use a barra de pesquisa na parte superior para localizar S3. Crie um bucket com opções padrão ou nome de captura para um dos buckets existentes a serem usados.

Para chave de acesso S3 e chave secreta S3:

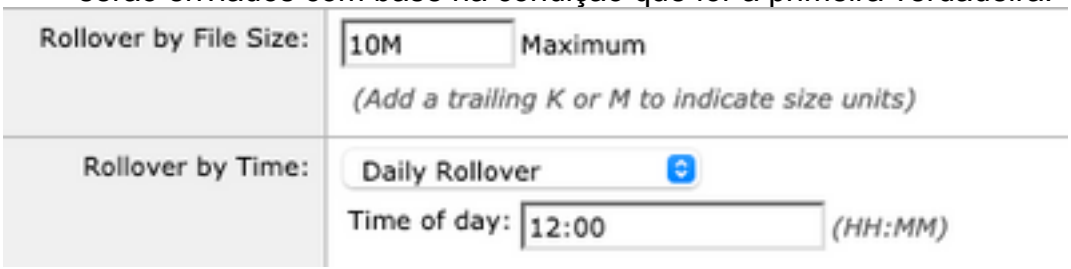
Clique no nome da sua conta na parte superior direita e, na lista suspensa, selecione "Minhas credenciais de segurança". Na página aberta, clique em "Access keys (access key ID and secret access key). Crie uma nova chave de acesso, exiba ou faça o download dos detalhes da chave.



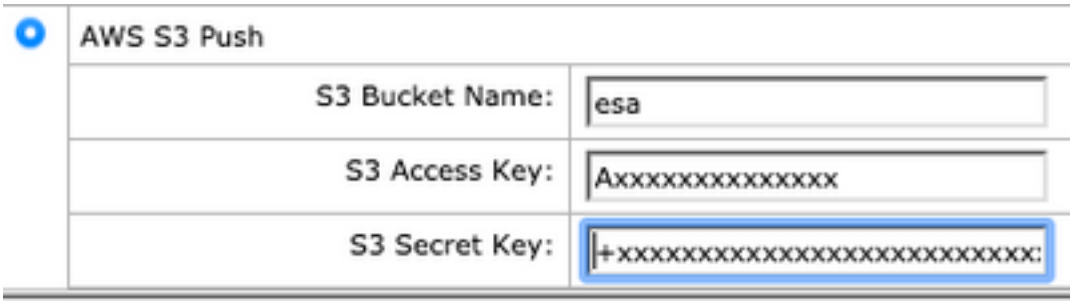


Caution: NÃO compartilhe chaves de acesso em fóruns públicos. Verifique se essas informações estão armazenadas com segurança.

2. Navegue até ESA com registros CEF configurados em **Administração do sistema > Inscrições de log** e clique no nome do **log**.
3. Selecione **Rollover de** log **por tamanho de arquivo** ou **Rollover por hora** ou ambos e os logs serão enviados com base na condição que for a primeira verdadeira.



4. Selecione AWS S3 Push, insira as informações coletadas na Etapa 1.



5. Enviar e confirmar alterações.

Se os registros CEF já estiverem presentes no dispositivo, os arquivos de log existentes serão enviados imediatamente e devem aparecer no bucket S3 configurado. A próxima programação de envio de log ocorrerá com base no tamanho e no tempo de transferência configurados.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Utilize os registros s3_client disponíveis no dispositivo para rastrear os registros sendo enviados ou quaisquer erros que se conectem a ele.

Successful log push

```
Fri Feb 19 11:21:38 2021 Info: S3_CLIENT: Uploaded 3 file(s) to the S3 Bucket esa for the
subscription: cef

Fri Feb 19 12:03:16 2021 Info: S3_CLIENT: Uploading files to S3 Bucket esa for the subscription:
cef
Fri Feb 19 12:03:22 2021 Info: S3_CLIENT: Uploaded 1 file(s) to the S3 Bucket esa for the
subscription: cef
```

Unsuccessful log push

```
Fri Feb 19 12:34:10 2021 Info: S3_CLIENT: Uploading files to S3 Bucket esa for the subscription:
cef
Fri Feb 19 12:34:11 2021 Warning: S3_CLIENT: ERROR: Upload Failed to S3 bucket esa. Reason:
Failed to upload /data/pub/cef/sll.@20210219T120000.s to esa/sll.@20210219T120000.s: An error
occurred (InvalidAccessKeyId) when calling the PutObject operation: The AWS Access Key Id you
provided does not exist in our records.
Fri Feb 19 12:34:11 2021 Warning: S3_CLIENT: Uploading files to S3 Bucket esa encountered one or
more failures for the subscription: cef.
Upload failed for the following:
[u'sll.@20210219T120000.s']

Re-check your configuration.
```

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guias do usuário final do Cisco Email Security Appliance
- Notas de versão e informações gerais do Cisco Email Security Appliance
- Linha de registro único CES (SLL)
- AWS Criando o bucket S3
- **Suporte Técnico e Documentação - Cisco Systems**