Configurar a integração do QRadar com o gerenciamento de registro Umbrella e S3

Contents

Introdução

Este documento descreve como configurar o QRadar para incluir logs de um bucket do AWS S3 para o gerenciamento de logs do Umbrella.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

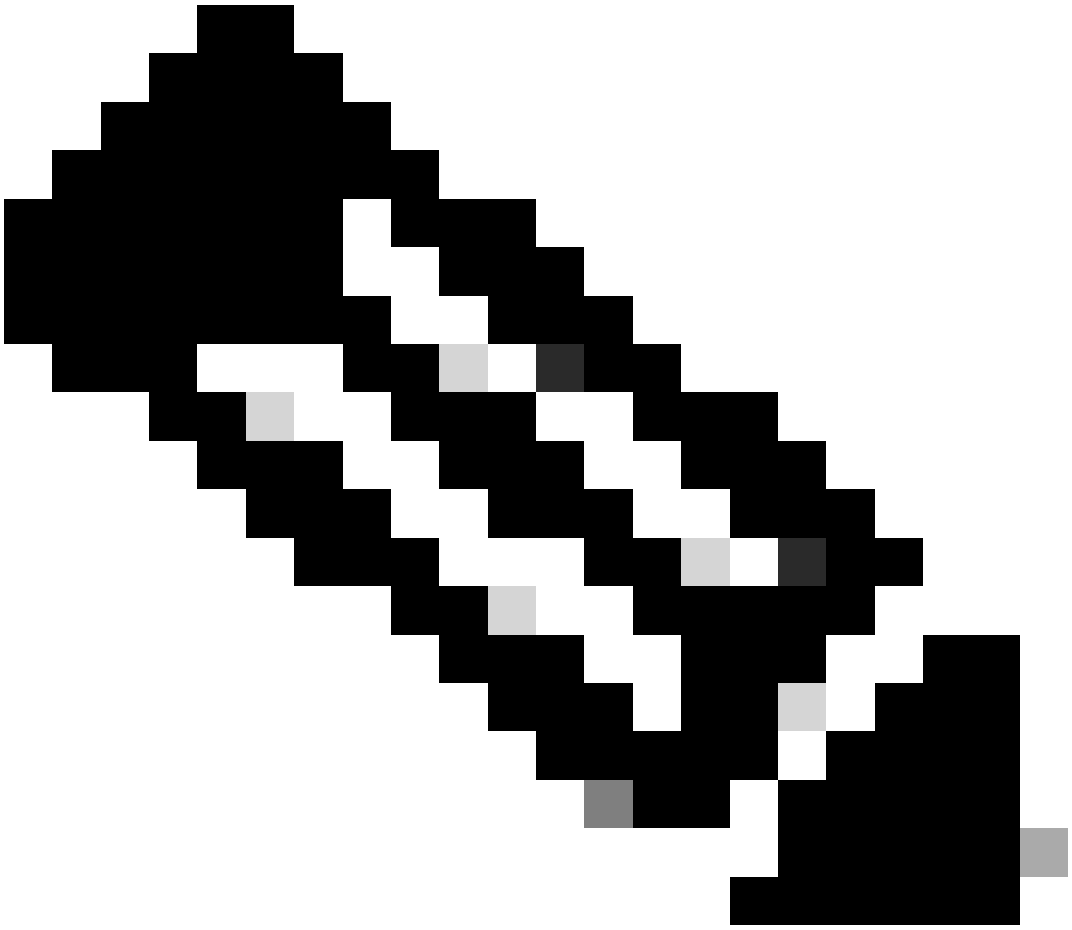
- Este documento pressupõe que o bucket do Amazon AWS S3 foi configurado no Umbrella (Configurações > Gerenciamento de logs) e está mostrando verde com logs recentes que foram carregados. Para obter mais informações sobre como configurar esse recurso, leia este artigo: Download Logs from Umbrella Log Management in AWS S3
- Além dos direitos administrativos para o(s) aparelho(s) QRadar, a configuração do Amazon S3 e o painel Umbrella, essas instruções supõem que o administrador do QRadar esteja familiarizado com a criação de arquivos LSX (extensão de origem de log).

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview



> Note: O melhor método de configuração do QRadar para uso com o Cisco Umbrella é através do aplicativo Cisco Cloud Security. Continue com esse método apenas se o aplicativo não puder ser configurado.

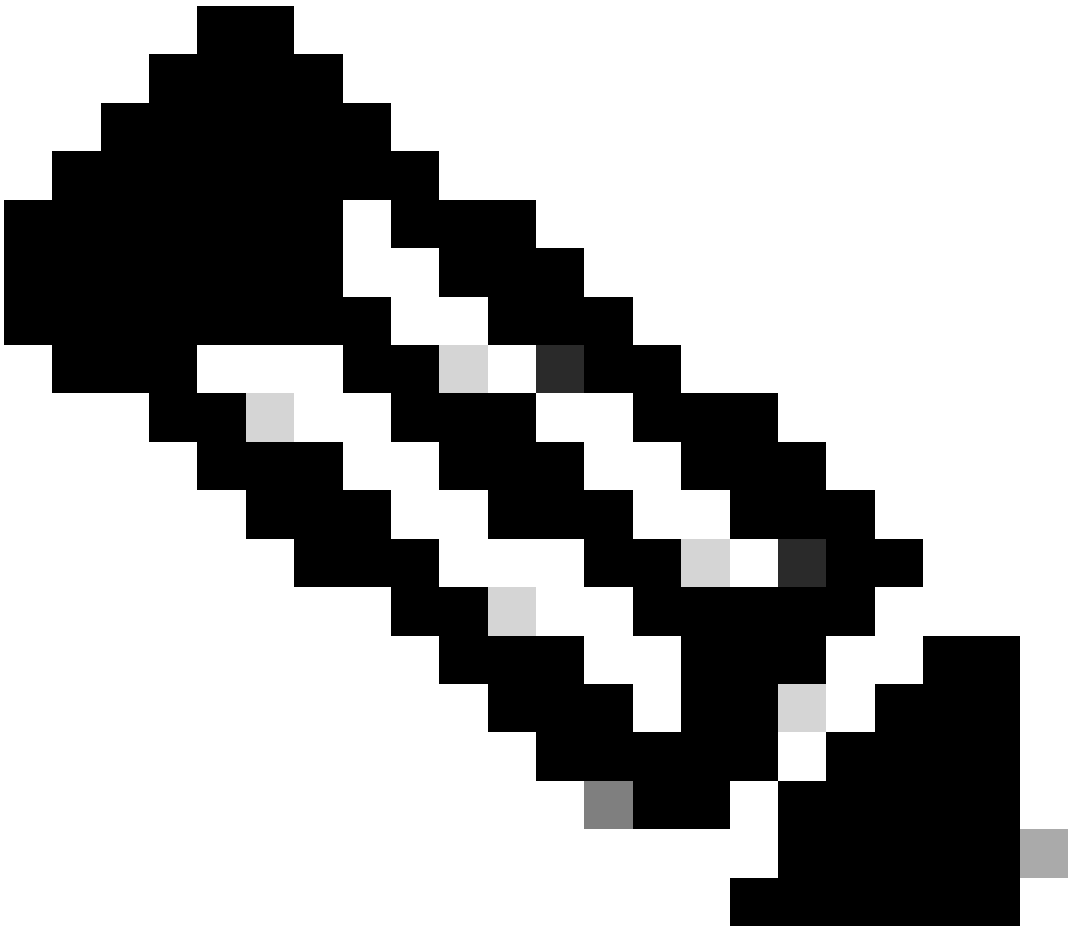
O QRadar da IBM é um SIEM popular para análise de registros. Ele fornece uma interface

eficiente para analisar grandes blocos de dados, como os logs fornecidos pelo Cisco Umbrella para o tráfego DNS da sua organização.

Este artigo descreve como configurar e executar o QRadar para que ele possa extrair os logs do seu bucket S3 e consumi-los. Há dois estágios principais:

- Configure suas Credenciais de Segurança do AWS S3 para permitir acesso do QRadar aos logs.
- Configure o próprio QRadar para apontar para o seu balde.

Se você estiver usando o bucket do S3 gerenciado pela Cisco, use essas instruções no artigo Download Logs from Umbrella Log Management Using the AWS CLI.



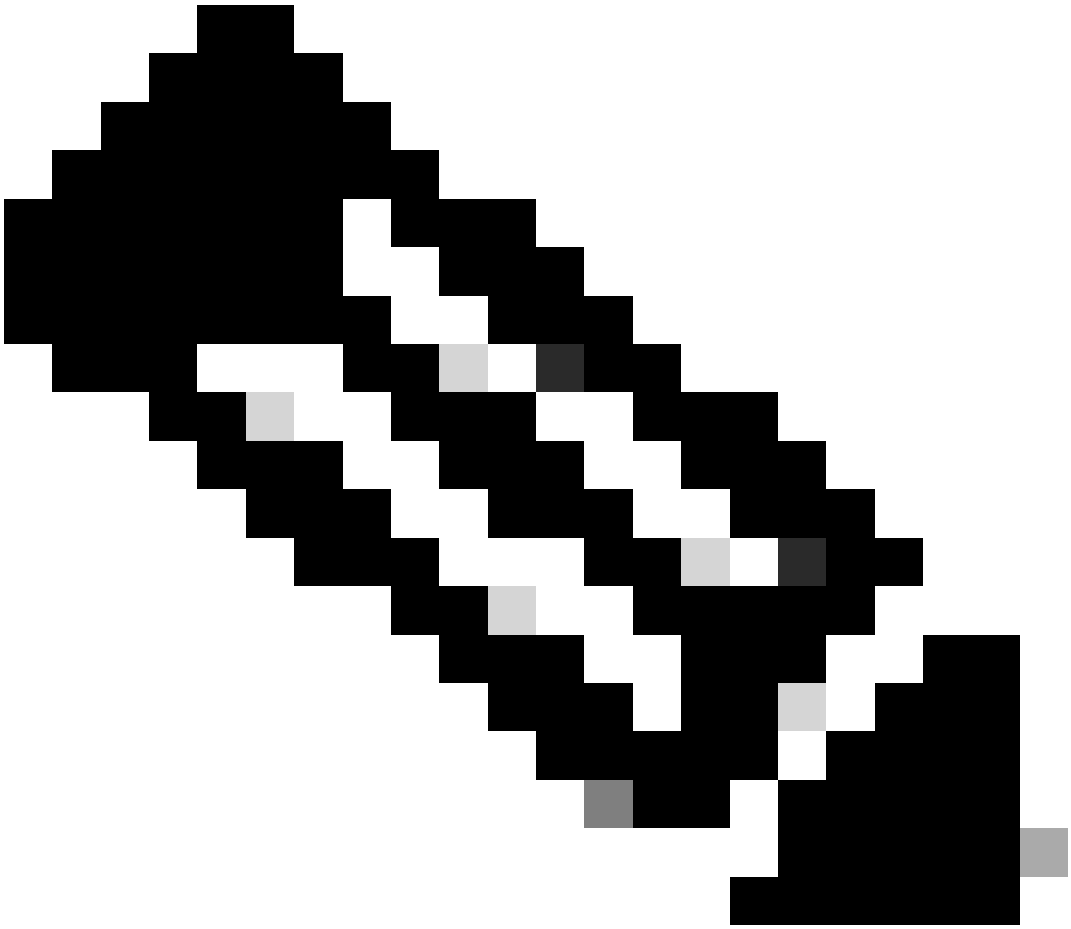
Note: Essa integração foi testada com os buckets S3 gerenciados pelo cliente e os buckets S3 gerenciados pela Cisco. As informações discutidas neste artigo são atuais desde o momento da redação deste documento (outubro de 2019). Elas podem ser alteradas com base na forma como o QRadar e a AWS Services fazem interface. Este documento é um documento ativo. Se você tiver feedback ou encontrar truques ou dicas

---

que possam ajudar outros clientes, entre em contato com o Cisco Umbrella Support.

O suporte para QRadar deve vir da IBM, pois a Cisco não pode oferecer suporte direto a hardware ou software de terceiros. Em caso de problemas de conexão do painel do Umbrella ao balde S3, o Cisco Umbrella pode oferecer suporte. Grande parte das informações encontradas neste artigo também pode ser encontrada no site da IBM.

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 (Download Logs do Gerenciamento de Logs do Umbrella no AWS S3). Se você já tiver executado essas etapas, poderá ir para o estágio 2, embora posteriormente precise das credenciais de segurança do usuário do IAM para autenticar o QRadar no seu bucket.

Passo 1

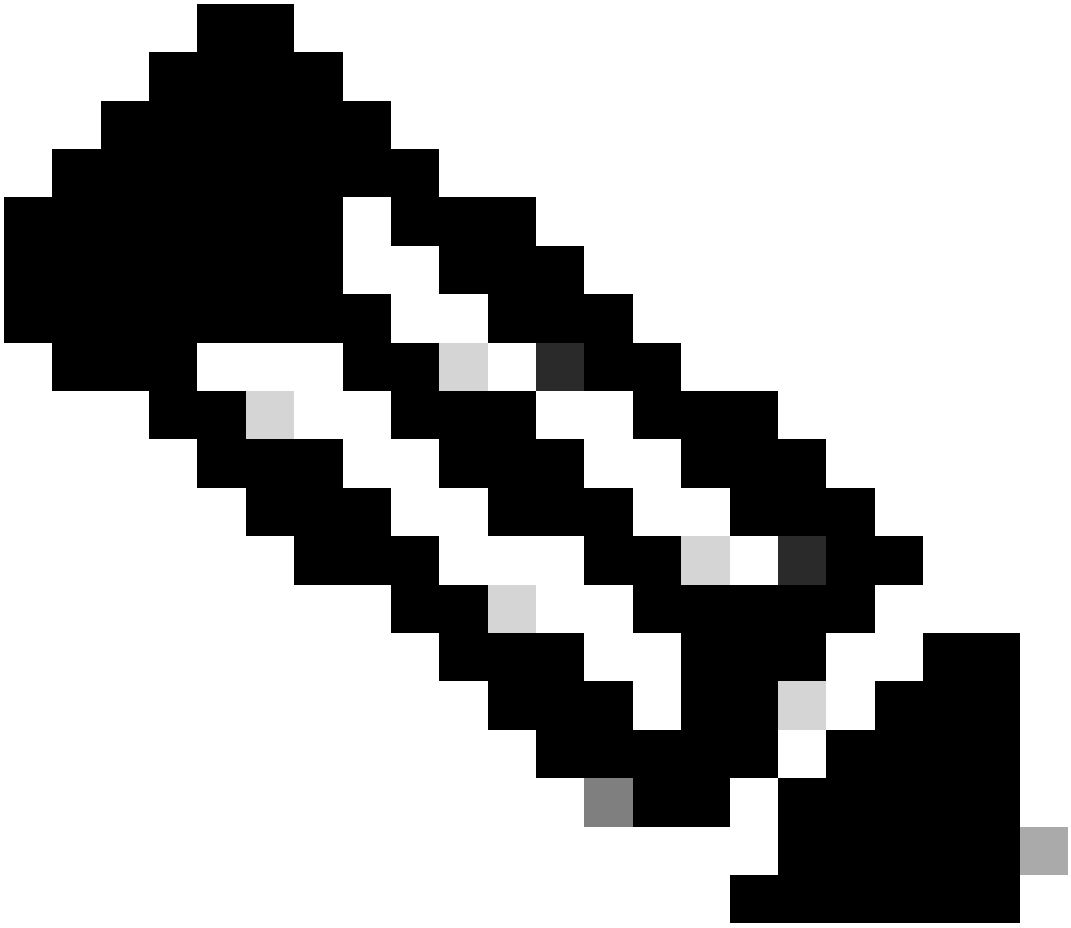
1. Adicione uma chave de acesso à sua conta do Amazon Web Services para permitir o acesso remoto à sua ferramenta local e permitir carregar, baixar e modificar arquivos no S3:

1. Faça login no AWS.
2. Selecione o nome da sua conta no canto superior direito.
3. Na lista suspensa, selecione Credenciais de segurança.

2. Em seguida, você será 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 os usuários do IAM e as práticas recomendadas do AWS, leia a documentação do AWS.

Passo 2

1. Selecione Introdução a usuários do IAM para criar um usuário do IAM para acessar seu bucket do S3. Em seguida, você será direcionado a uma tela onde poderá criar um usuário do IAM.
2. Selecione Novos Usuários e preencha os campos.



Note: A conta de usuário não pode conter espaços.

3. Depois de criar a conta de usuário, você terá apenas uma oportunidade de obter duas informações críticas contendo suas Credenciais de Segurança de Usuário do Amazon. O Umbrella sugere que você faça o download dessas informações usando o botão no canto inferior direito para fazer backup delas. Eles não estarão disponíveis após esta etapa da instalação. Anote a ID da Chave de Acesso e a Chave de Acesso Secreta, pois serão necessários em uma etapa posterior.

Etapa 3

Em seguida, adicione uma política para seu usuário do IAM para que ele tenha acesso ao seu bucket de S3:

1. Selecione o usuário que acabou de criar e role para baixo pelas propriedades dos usuários até ver o botão Attach Policy.

2. Selecione Anexar política e, em seguida, digite "s3" no filtro do tipo de política. Isso mostra dois resultados:

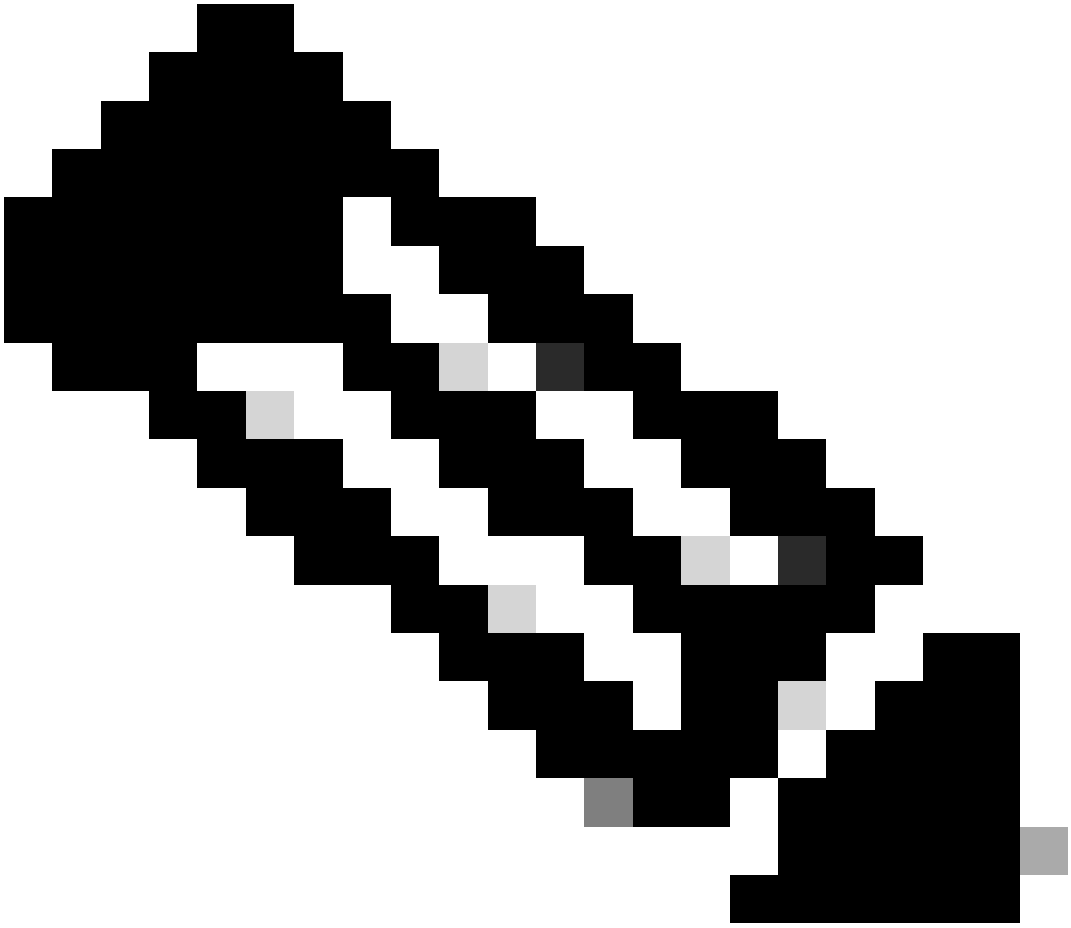
- AmazonS3FullAccess
- AmazonS3AcessoSomenteLeitura

3. Selecione AmazonS3FullAccess e, em seguida, selecione Attach Policy no canto inferior direito.

Estágio 2: Configurando o QRadar para receber dados de log DNS do bucket de S3

O QRadar utiliza o serviço AWS CloudTrail, que é um serviço Web que registra chamadas de API do AWS para sua conta e fornece arquivos de log para você.

Antes do QRadar acessar o Amazon S3, conclua este procedimento da IBM para obter o certificado do servidor do Amazon. Esta parte é difícil, portanto, certifique-se de que você preencheu as instruções exatamente.



Note: No teste, você deve usar o navegador Firefox para que isso funcione como esperado.

Para obter o certificado do servidor do Amazon, você deve mover o certificado no formato DER para o dispositivo QRadar apropriado. O dispositivo QRadar que requer o certificado é o dispositivo atribuído no campo Target Event Collector na fonte de log do Amazon AWS CloudTrail.

Antes de Começar

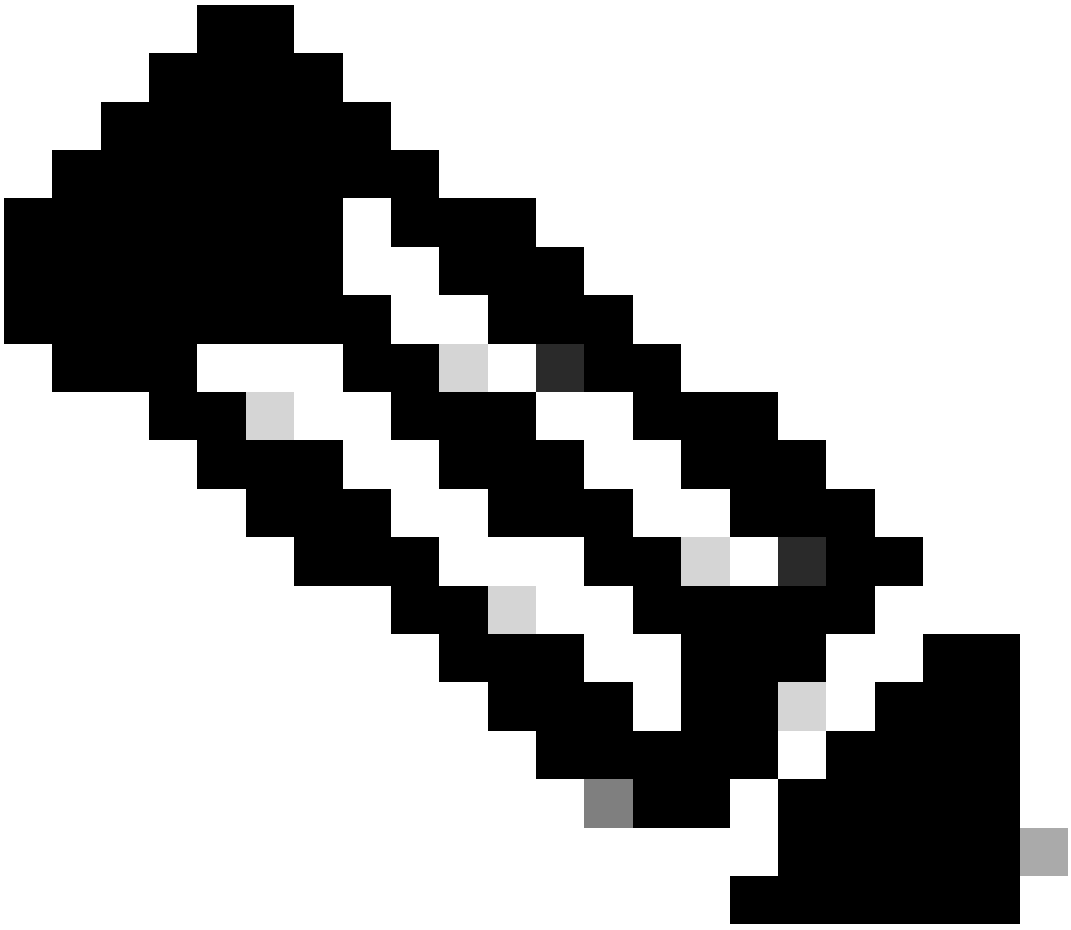
- O certificado deve estar no formato .DER.
- A extensão .DER diferencia maiúsculas de minúsculas e deve ser maiúscula.
- Se o certificado for exportado em minúsculas, a origem do log poderá ter problemas de coleta de eventos.

Etapas iniciais

1. Acesse o bucket do AWS CloudTrail S3: `https://<bucketname>.s3.amazonaws.com`

2. Use o Firefox para exportar o certificado SSL do AWS como um certificado (.DER). O Firefox pode criar o certificado necessário com a extensão .DER:

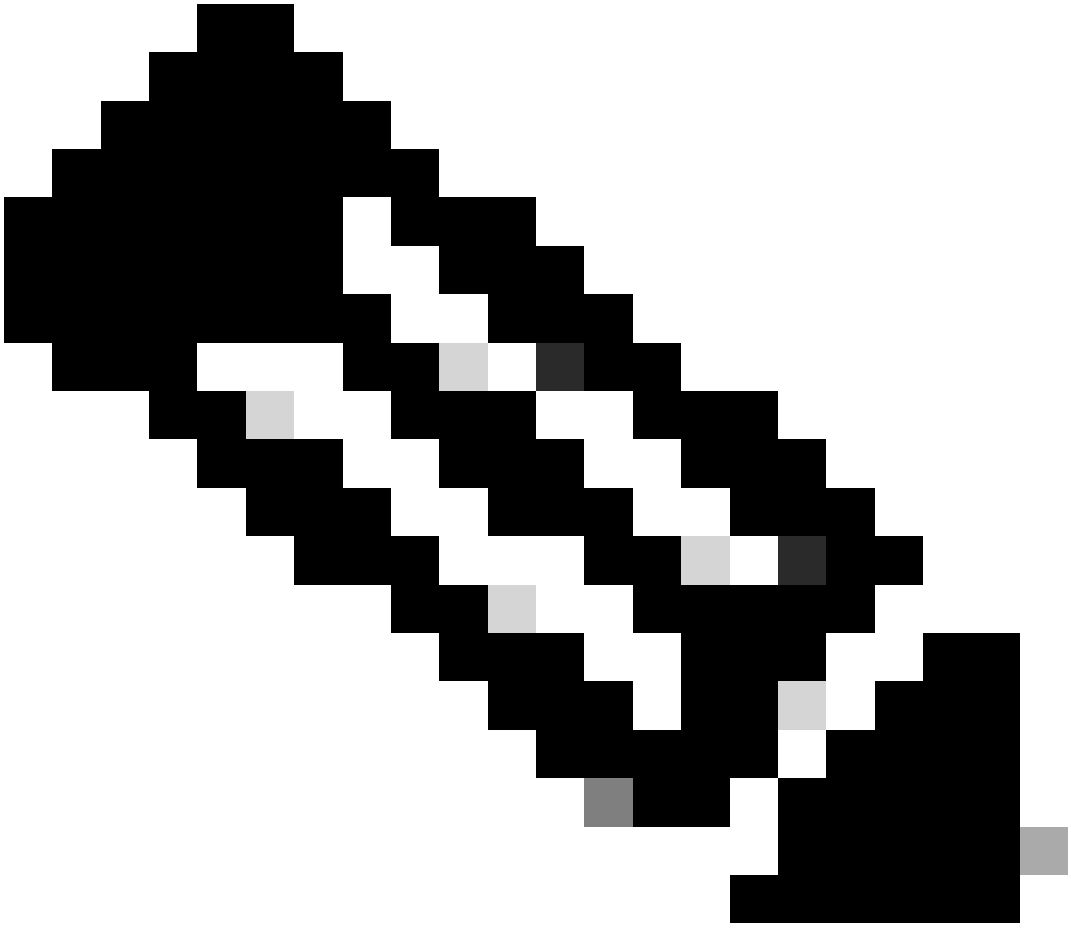
1. Selecione o ícone Identidade do local (o ícone de cadeado na barra de endereços).
2. Selecione More Information > View Certificate e selecione a guia Details.
3. Selecione Exportar para exportar no formato do certificado .DER.



Note: A extensão .DER diferencia maiúsculas de minúsculas e deve ser maiúscula.

---

3. Copie o certificado .DER para o diretório /opt/QRadar/conf/trusted_certificates do dispositivo QRadar que gerencia a fonte de log do Amazon AWS CloudTrail. Você pode usar o WinSCP para copiá-lo.



Note: O dispositivo QRadar que gerencia a fonte de log é identificado pelo campo Target Event Collect na fonte de log do Amazon AWS CloudTrail. O dispositivo QRadar que gerencia a origem de log do Amazon AWS CloudTrail deve ter uma cópia do certificado .DER em /opt/QRadar/conf/trusted_certificates.

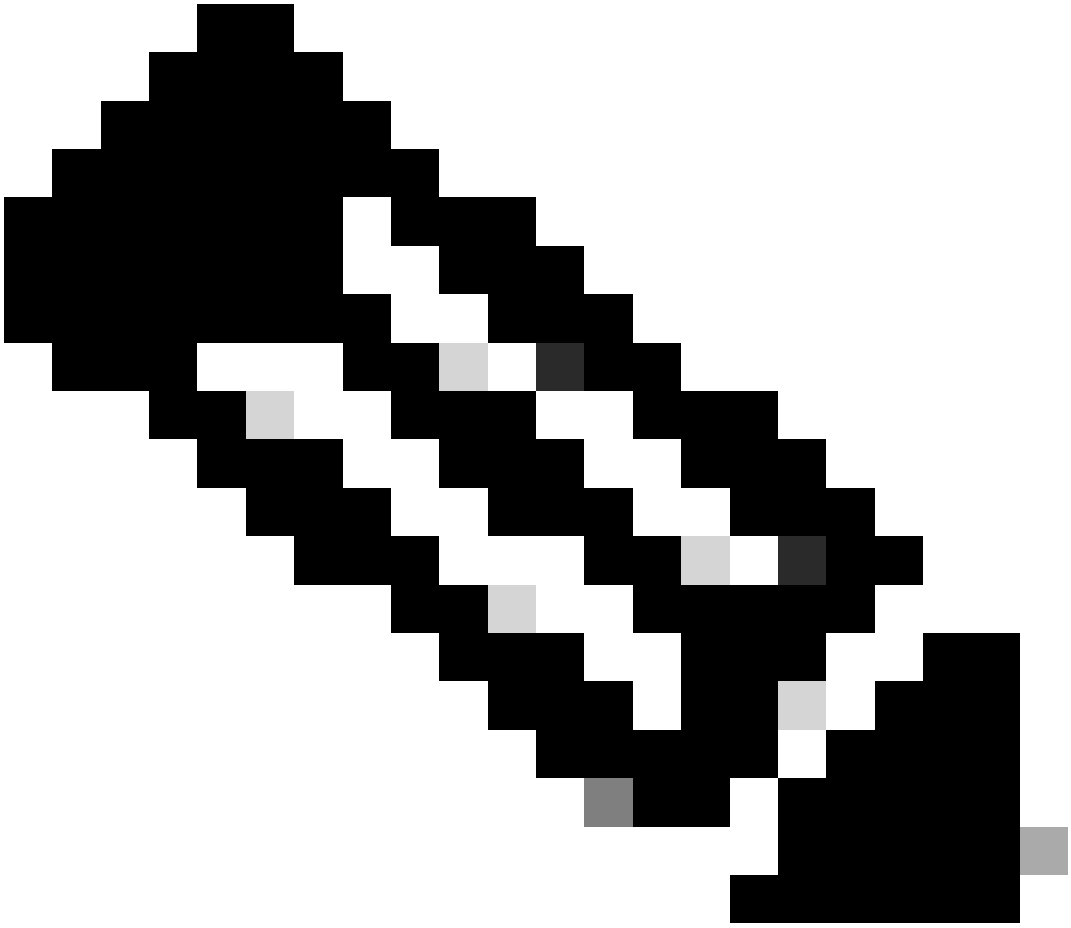
4. Efetue login na interface de usuário do QRadar como um usuário administrativo.

5. Selecione a guia Admin.

6. Selecione o ícone Registrar Origens.

7. Selecione a fonte de log Amazon AWS CloudTrail.

8. No menu de navegação, selecione Enable/Disable para desabilitar e depois habilitar novamente a fonte de log do Amazon AWS CloudTrail.



Note: Quando um administrador força a fonte de log de desabilitada para habilitada, isso permite que o protocolo se conecte ao bucket do Amazon AWS, conforme definido na fonte de log. Em seguida, uma verificação de certificado é realizada como parte da primeira comunicação.

9. Se você continuar a ter problemas, verifique se o campo Log Source Identifier contém o nome correto do bucket do Amazon AWS e se o caminho do Diretório Remoto está correto na configuração da origem do log.

Finalizar a configuração do QRadar

1. No QRadar, certifique-se de que todos os seus protocolos, DSMs e outras informações estejam atualizados. Selecione o LogFileProtocol com essas configurações (sua frequência, Hora de início, Recorrência e outras informações podem ser diferentes).

2. Na guia Origens de Log, informe um Nome da Origem de Log e uma Descrição da Origem de Log. Pode ser o que quiser.

3. Insira o Nome do Recipiente S3, a Chave de Acesso AWS, a Chave Secreta AWS e o Diretório Remoto (provavelmente dnslogs, mas depende da configuração). A adição de um Identificador de origem de log como o ano pode ajudar a filtrar para que somente os logs com "2019" sejam extraídos.

4. Crie um LSX (Log Source Extension) que possa analisar os eventos do Cisco Umbrella. (Isso é o que parece depois da importação para o QRadar.) Mais informações sobre como criar exatamente o LSX podem ser encontradas no site da IBM. Este é apenas um exemplo. Os dados que você deseja extrair dos registros variam de acordo com o caso de uso.

5. Verifique se a Chave de Acesso AWS e a Chave Secreta AWS foram copiadas com êxito e coladas na Configuração de Origem de Log.

6. Selecione o processador GZIP e um Gerador de eventos de Multiline baseado em RegEx. A maneira mais fácil de obter um evento por linha é usando um padrão de início RegEx de:

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}","")
```

Certifique-se de selecionar a Extensão da Origem de Log e a Condição de Uso e, em seguida, salve a origem de log.

7. Execute uma Implantação Completa no QRadar.

A origem do log usa RestAPI para se conectar ao bucket com as credenciais e chaves fornecidas e começar a receber eventos.

Informações adicionais

Habilitar Log de Bucket

Para ativar o registro de bucket, leia a documentação do AWS e conclua os procedimentos descritos. Por padrão, o registro está desativado. Uma vez ativada, uma nova pasta chamada /logs reside na raiz do bucket para mostrar as informações de GETS, PUTS e DELETES.

Gerenciando o Ciclo do Log

Ao usar o S3, você pode gerenciar o ciclo de vida dos dados dentro do bucket para estender a duração do tempo durante o qual deseja manter logs. Dependendo da finalidade para a qual você está usando o gerenciamento de registro externo, a duração pode ser muito curta ou muito longa. Por exemplo, você pode simplesmente baixar os logs do bucket de S3 após 24 horas e armazená-los offline ou manter os logs indefinidamente na nuvem.

Por padrão, a Amazon armazena os dados em um bucket indefinidamente, mas o armazenamento ilimitado aumenta o custo de manutenção do bucket. Para obter mais informações sobre os ciclos de vida de S3, leia a documentação do AWS.

Para configurar o ciclo de vida do seu período:

1. Selecione Propriedades > Ciclo de Vida.

2. Selecione Adicionar uma Regra e, em seguida, Aplicar a Regra ao bucket inteiro (ou a uma subpasta, se você a configurou como tal).

3. Selecione uma Ação em Objetos, como Deletar ou Arquivar, em seguida, selecione o período de tempo e se você deseja usar o armazenamento Glacier para ajudar a reduzir os custos da Amazon. (Glacier é um armazenamento off-line "frio", que, embora mais lento para acessar, é muito mais barato.)

Se você preferir gerenciar logs em outro método (por exemplo, em sua solução de backup interno), poderá simplesmente fazer o download dos logs do S3 e preservá-los de outra forma.

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.