Configurazione dell'integrazione QRadar con Umbrella Log Management e S3

Sommario

Introduzione

In questo documento viene descritto come configurare QRadar per acquisire i log da un bucket S3 di AWS per la gestione dei log Umbrella.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

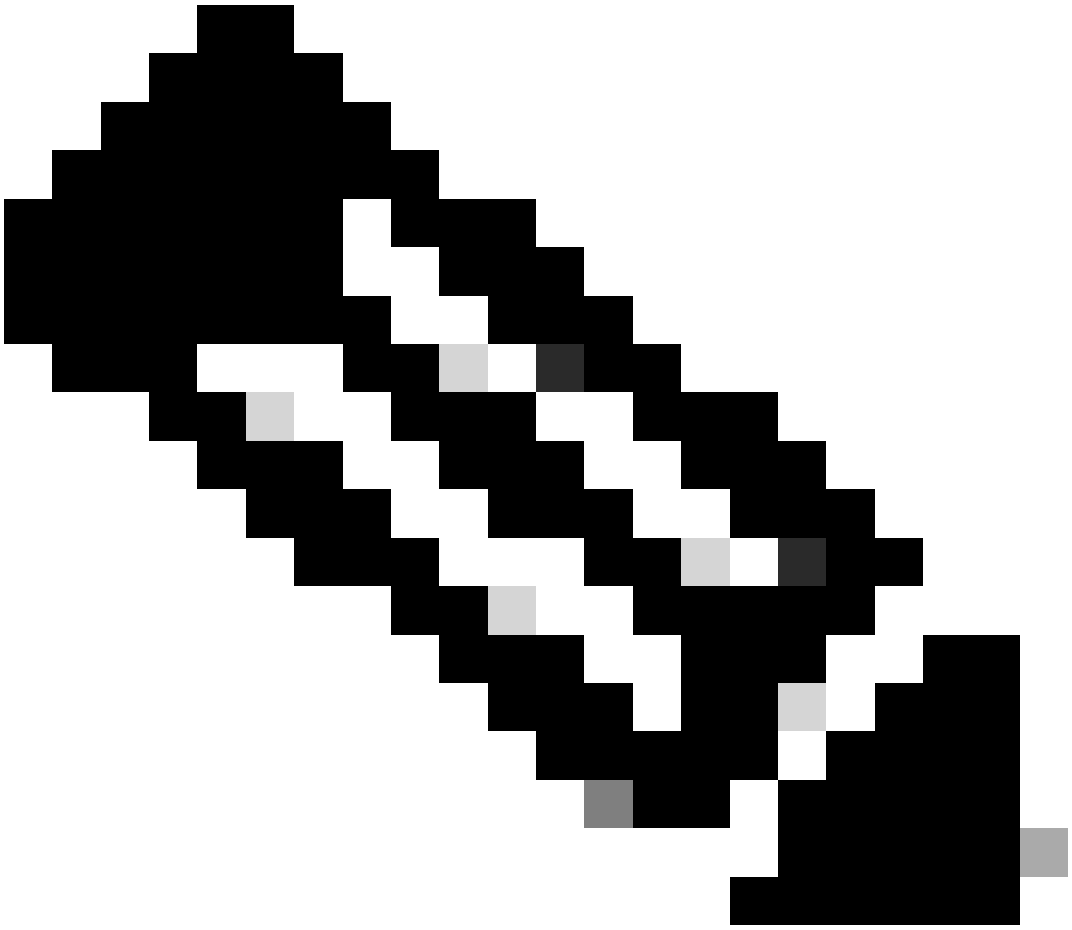
- In questo documento si presume che il bucket S3 di Amazon AWS sia stato configurato in Umbrella (Impostazioni > Gestione log) e sia visualizzato in verde con i log recenti caricati. Per ulteriori informazioni su come configurare questa funzione, leggere questo articolo: Download Logs from Umbrella Log Management in AWS S3
- Oltre ai diritti amministrativi per gli accessori QRadar, la configurazione Amazon S3 e il dashboard Umbrella, queste istruzioni presuppongono che l'amministratore QRadar abbia familiarità con la creazione di file LSX (Log source Extension).

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Umbrella.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica



> Nota: Il metodo migliore per configurare QRadar per l'utilizzo con Cisco Umbrella è tramite Cisco Cloud Security App. Procedere con questo metodo solo se non è possibile configurare l'app.

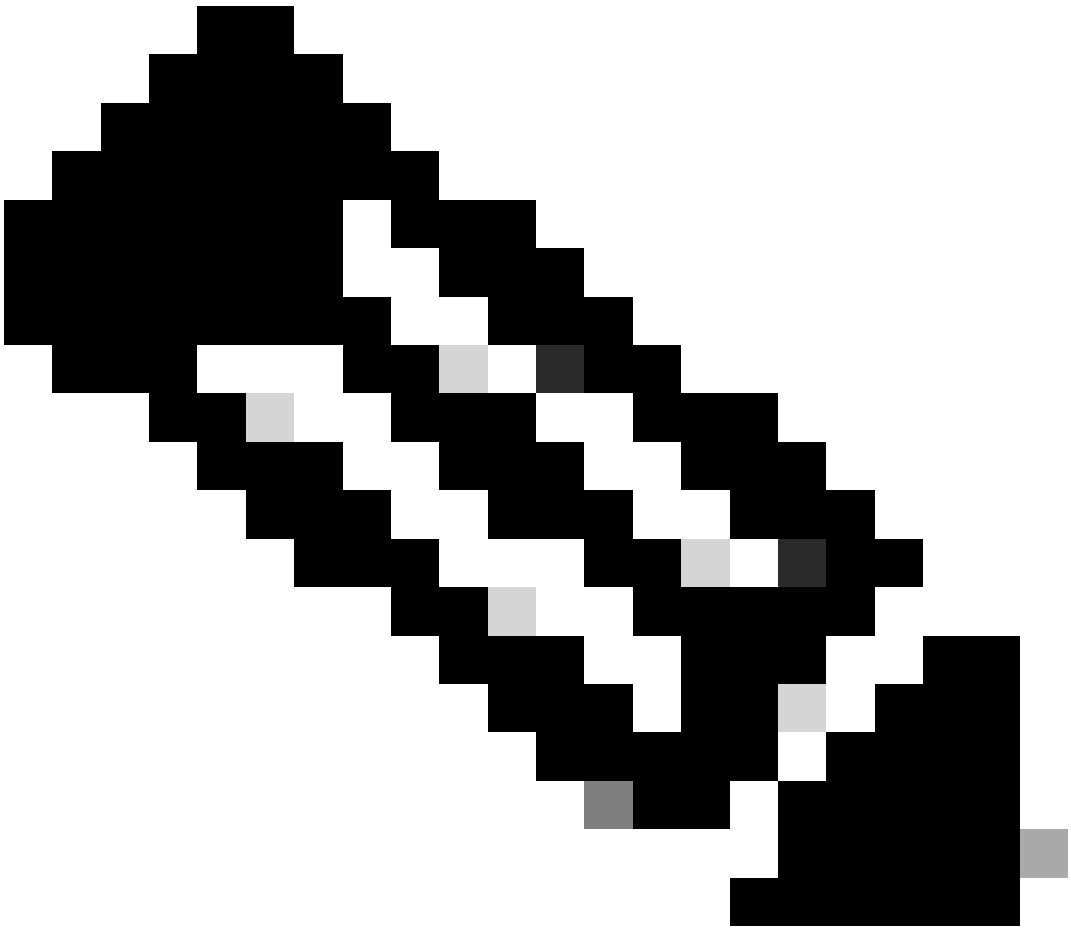
QRadar di IBM è un popolare SIEM per l'analisi dei log. Fornisce una potente interfaccia per

l'analisi di grandi blocchi di dati, ad esempio i registri forniti da Cisco Umbrella per il traffico DNS della tua organizzazione.

In questo articolo viene descritto come configurare e utilizzare QRadar in modo che possa estrarre i registri dal secchio S3 e utilizzarli. Le fasi principali sono due:

- Configurare le credenziali di sicurezza AWS S3 per consentire l'accesso di QRadar ai registri.
- Configurare QRadar in modo che punti al bucket.

Se si sta utilizzando il bucket S3 gestito da Cisco, attenersi alle seguenti istruzioni nell'articolo Download dei log da Umbrella Log Management Using the AWS CLI.



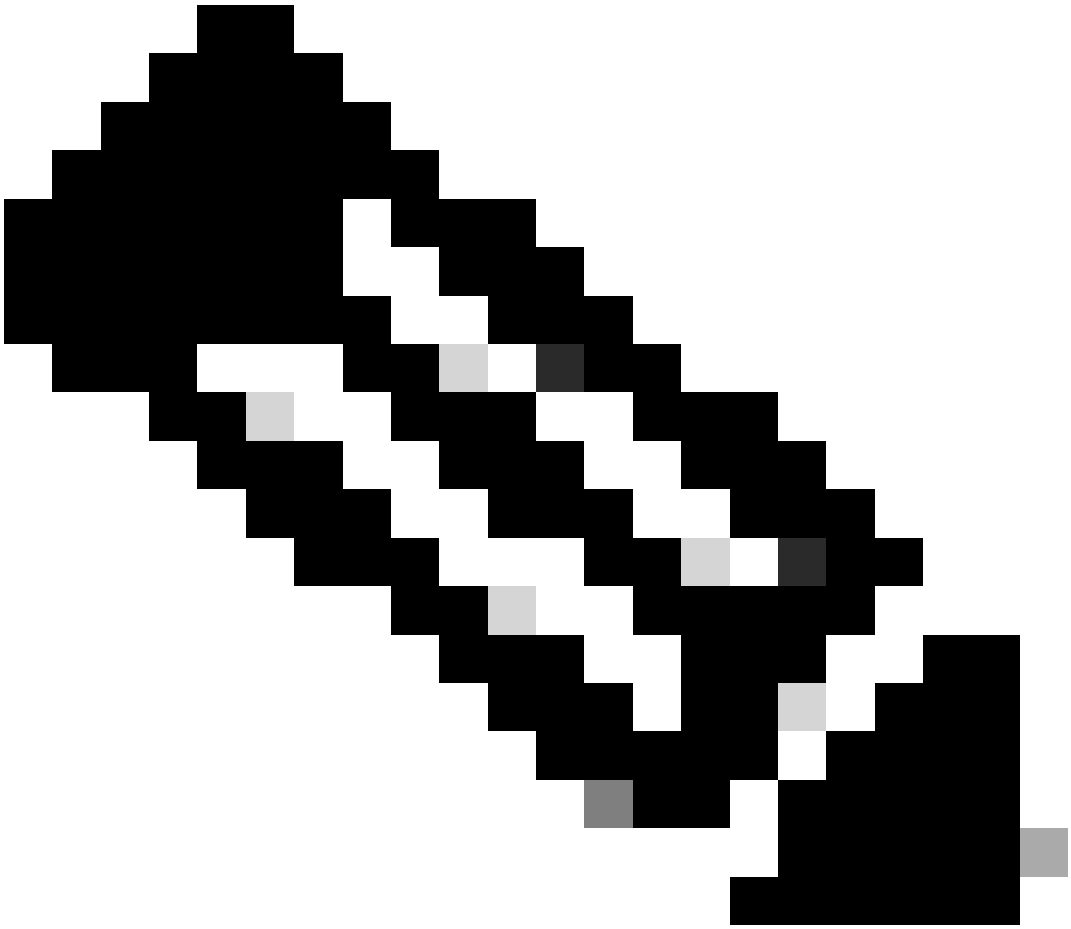
Nota: Questa integrazione è stata testata sia con i bucket S3 gestiti dal cliente che con i bucket S3 gestiti da Cisco. Le informazioni discusse in questo articolo sono aggiornate al presente documento (ottobre 2019). Possono variare in base al modo in cui QRadar e AWS Services si interfacciano. Questo documento è un documento attivo. Se hai dei commenti o hai trovato dei trucchi o dei suggerimenti che potrebbero aiutare altri clienti,

---

contatta il Supporto Cisco Umbrella.

Il supporto per QRadar deve provenire da IBM, in quanto Cisco non è in grado di supportare direttamente hardware o software di terze parti. Per qualsiasi problema relativo al collegamento del dashboard Umbrella al bucket S3, Cisco Umbrella può fornire assistenza. Molte delle informazioni riportate in questo articolo sono reperibili anche sul sito Web di IBM.

Fase 1: Configurazione delle credenziali di sicurezza in AWS



Nota: Questi passaggi sono identici a quelli descritti nell'articolo che descrive come configurare uno strumento per il download dei log dal bucket (Scaricare i log da Umbrella Log Management in AWS S3). Se questi passaggi sono già stati eseguiti, è possibile passare alla fase 2, anche se in seguito sarà necessario disporre delle credenziali di sicurezza dell'utente IAM per autenticare QRadar nel bucket.

Passaggio 1

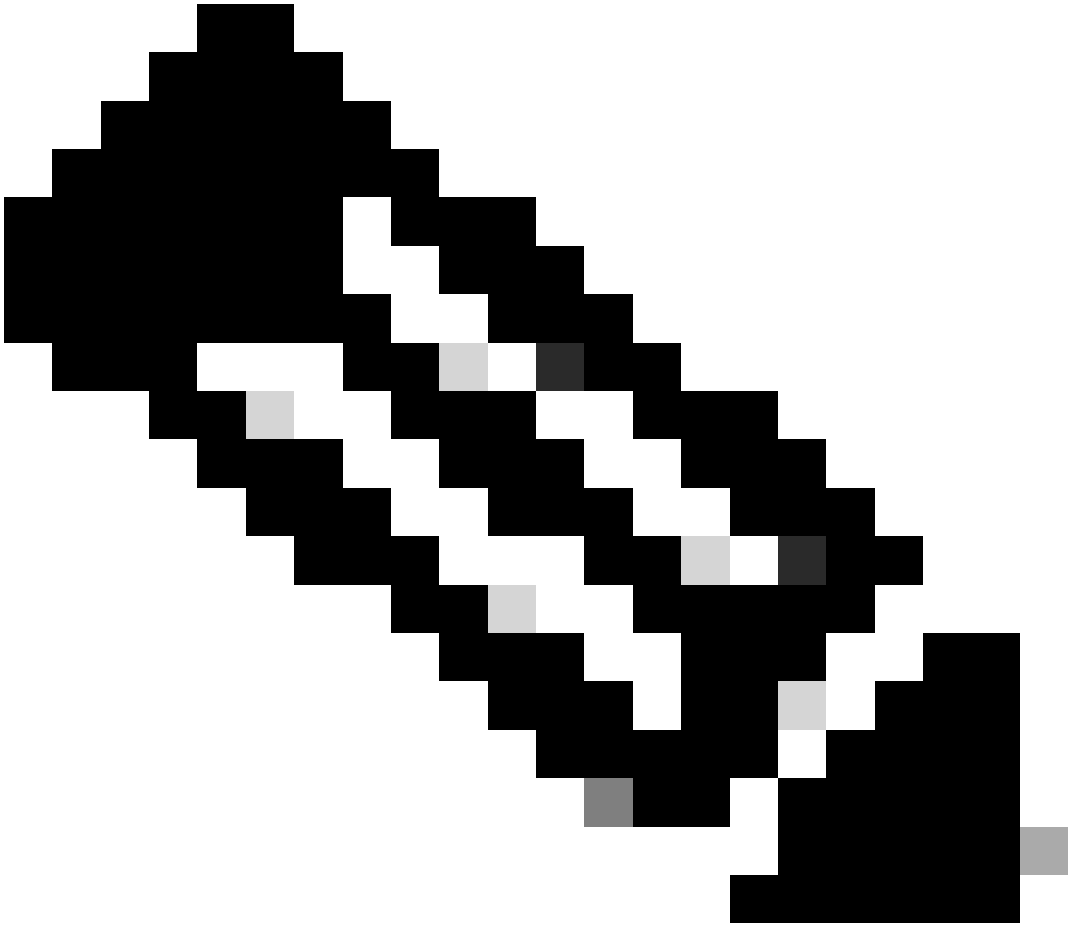
1. Aggiungere una chiave di accesso all'account di Amazon Web Services per consentire l'accesso remoto allo strumento locale e consentire di caricare, scaricare e modificare i file in S3:

1. Accedere a AWS.
2. Selezionare il nome dell'account nell'angolo in alto a destra.
3. Nell'elenco a discesa, selezionare Credenziali di sicurezza.

2. Viene quindi richiesto di utilizzare le procedure consigliate di Amazon e di creare un utente AWS Identity and Access Management (IAM). In sostanza, un utente IAM garantisce che l'account utilizzato da s3cmd per accedere al bucket non sia l'account master (ad esempio, l'account in uso) per l'intera configurazione S3. Creando singoli utenti IAM per gli utenti che accedono all'account, è possibile assegnare a ogni utente IAM un set univoco di credenziali di sicurezza. È inoltre possibile concedere autorizzazioni diverse a ogni utente IAM. Se necessario, è possibile modificare o revocare le autorizzazioni di un utente IAM in qualsiasi momento. Per ulteriori informazioni sugli utenti IAM e sulle procedure consigliate di AWS, consultare la documentazione di AWS.

Passaggio 2

1. Selezionare Introduzione agli utenti IAM per creare un utente IAM per accedere al bucket S3. Viene visualizzata una schermata in cui è possibile creare un utente IAM.
2. Selezionare Nuovi utenti, quindi completare i campi.



Nota: L'account utente non può contenere spazi.

3. Dopo aver creato l'account utente, ti viene data solo un'opportunità di prendere due pezzi critici di informazioni che contengono le credenziali di protezione dell'utente Amazon. Umbrella consiglia vivamente di scaricare questi usando il pulsante in basso a destra per eseguirne il backup. Non sono disponibili dopo questa fase dell'installazione. Assicurarsi di annotare sia l'ID chiave di accesso che la chiave di accesso segreta poiché sono necessarie in un passaggio successivo.

Passaggio 3

Aggiungere quindi un criterio per l'utente IAM in modo che possa accedere al bucket S3:

1. Selezionare l'utente appena creato, quindi scorrere verso il basso le proprietà degli utenti fino a visualizzare il pulsante Allega criterio.

2. Selezionare Allega criterio, quindi immettere "s3" nel filtro del tipo di criterio. Questo mostra due

risultati:

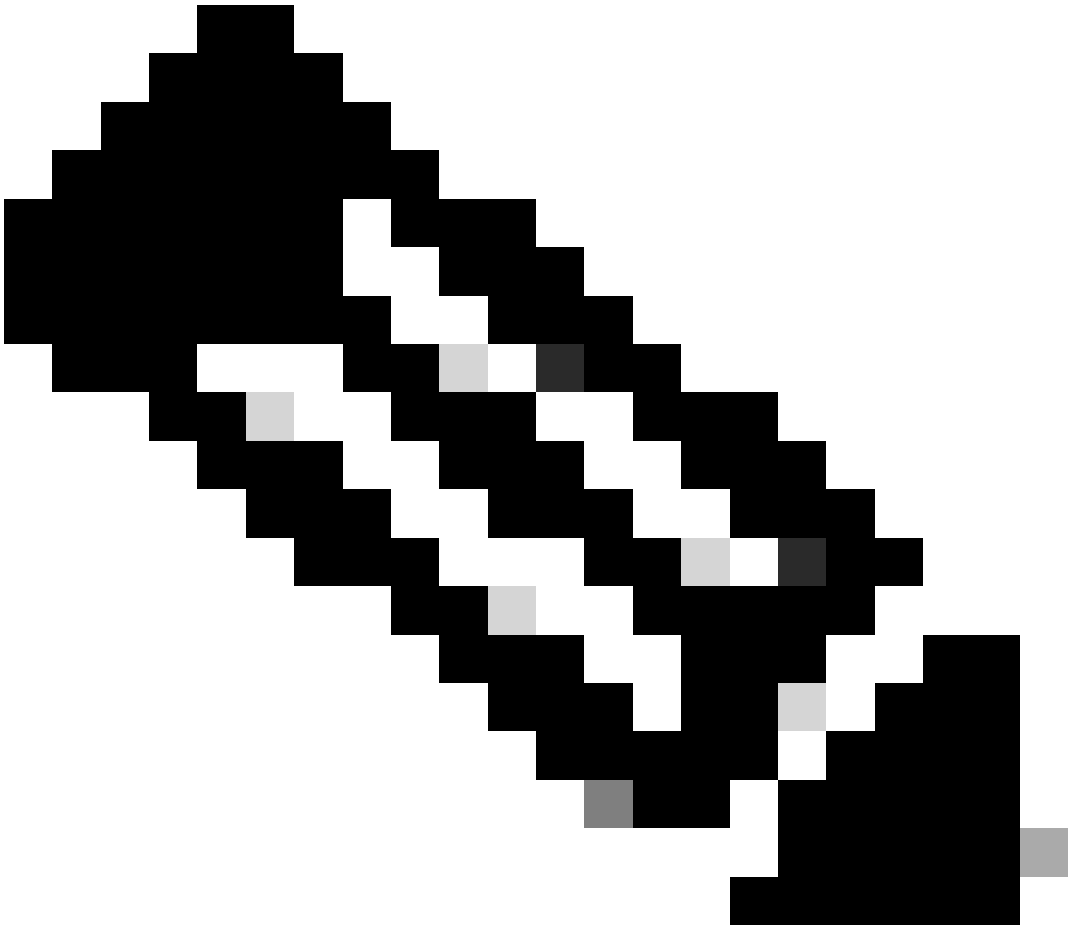
- AmazonS3FullAccess
- AmazonS3AccessoSolaLettura

3. Selezionare AmazonS3FullAccess, quindi selezionare Allega criterio nell'angolo in basso a destra.

Fase 2: Impostazione di QRadar per il pull dei dati di registro DNS dal bucket S3

QRadar utilizza il servizio AWS CloudTrail, un servizio Web che registra le chiamate API AWS per l'account e fornisce i file di registro.

Prima di QRadar per accedere ad Amazon S3, completare questa procedura da IBM per ottenere il certificato server Amazon. Questa parte è difficile, quindi assicurati di completare le istruzioni esattamente.



Nota: Durante il test, è necessario utilizzare il browser Firefox per fare in modo che funzioni come previsto.

Per ottenere il certificato del server Amazon, è necessario spostare il certificato in formato DER nell'accessorio QRadar appropriato. L'accessorio QRadar che richiede il certificato è l'accessorio assegnato nel campo Target Event Collector nell'origine del registro Amazon AWS CloudTrail.

Operazioni preliminari

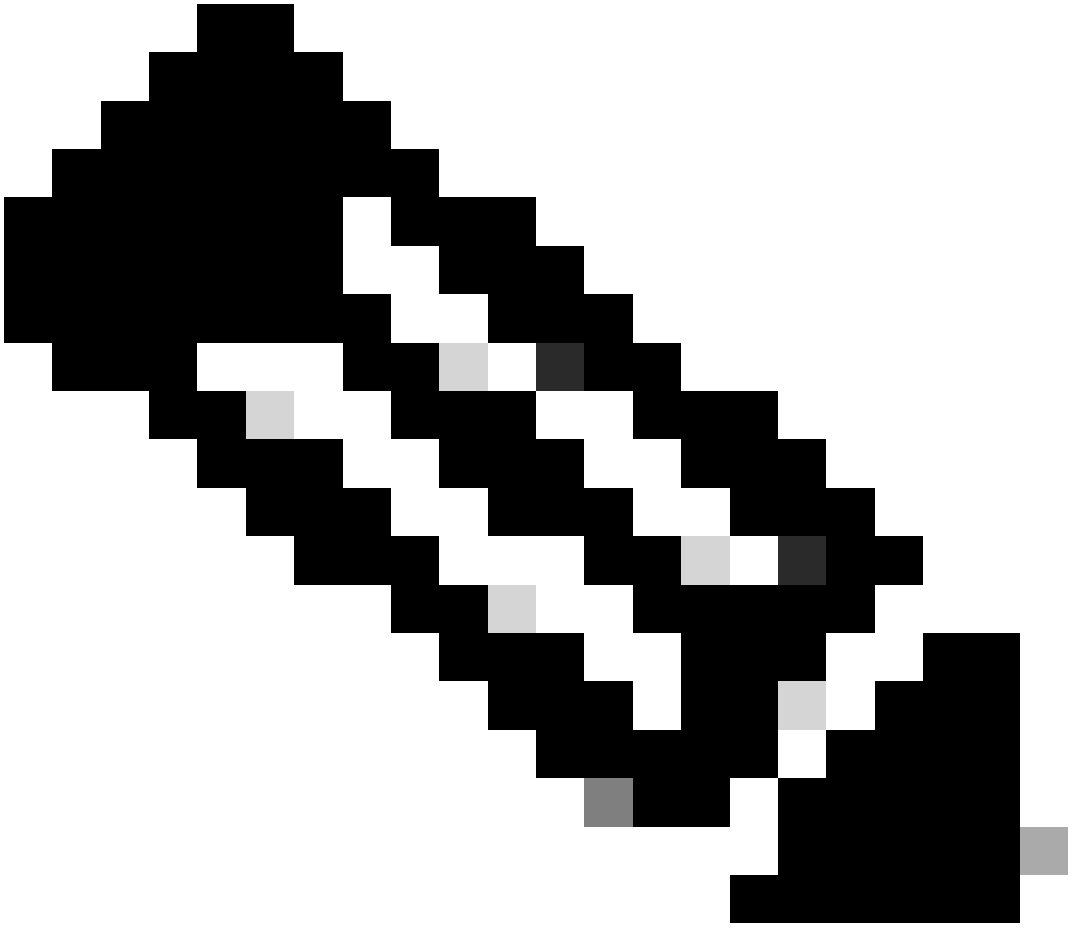
- Il certificato deve essere in formato DER.
- L'estensione .DER fa distinzione tra maiuscole e minuscole e deve essere maiuscola.
- Se il certificato viene esportato in lettere minuscole, nell'origine del registro possono verificarsi problemi di raccolta di eventi.

Fasi iniziali

1. Accedere al bucket di AWS CloudTrail S3: `https://<bucketname>.s3.amazonaws.com`

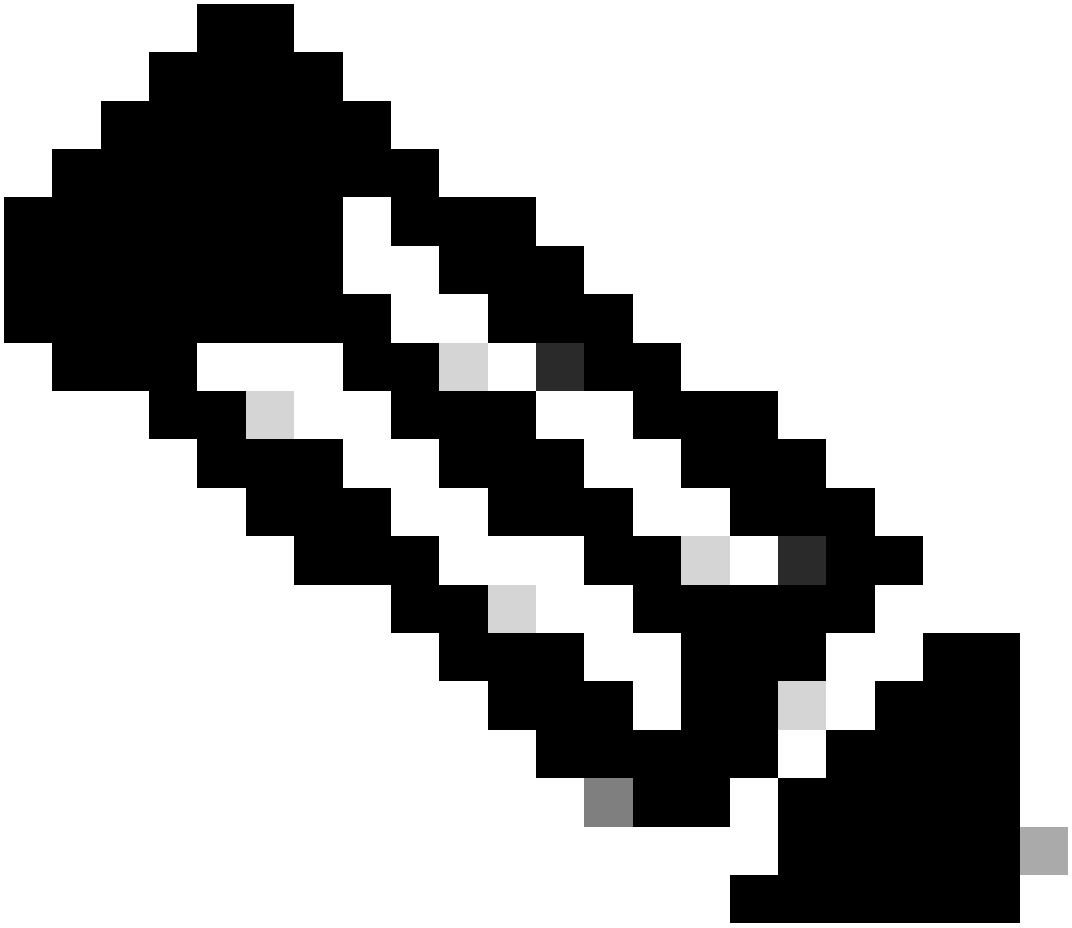
2. Utilizzare Firefox per esportare il certificato SSL da AWS come certificato (.DER). Firefox può creare il certificato richiesto con l'estensione .DER:

1. Selezionare l'icona Identità sito (l'icona a forma di lucchetto nella barra degli indirizzi).
2. Selezionare Ulteriori informazioni > Visualizza certificato e selezionare la scheda Dettagli.
3. Selezionare Esporta per esportare nel formato certificato .DER.



Nota: L'estensione .DER fa distinzione tra maiuscole e minuscole e deve essere maiuscola.

3. Copiare il certificato .DER nella directory /opt/QRadar/conf/trusted_certificates dell'appliance QRadar che gestisce l'origine del registro Amazon AWS CloudTrail. È possibile utilizzare WinSCP per copiarlo.



Nota: L'appliance QRadar che gestisce l'origine del registro è identificata dal campo Target Event Collect nell'origine del registro Amazon AWS CloudTrail. L'appliance QRadar che gestisce l'origine del registro Amazon AWS CloudTrail deve disporre di una copia del certificato .DER in /opt/QRadar/conf/trusted_certificates.

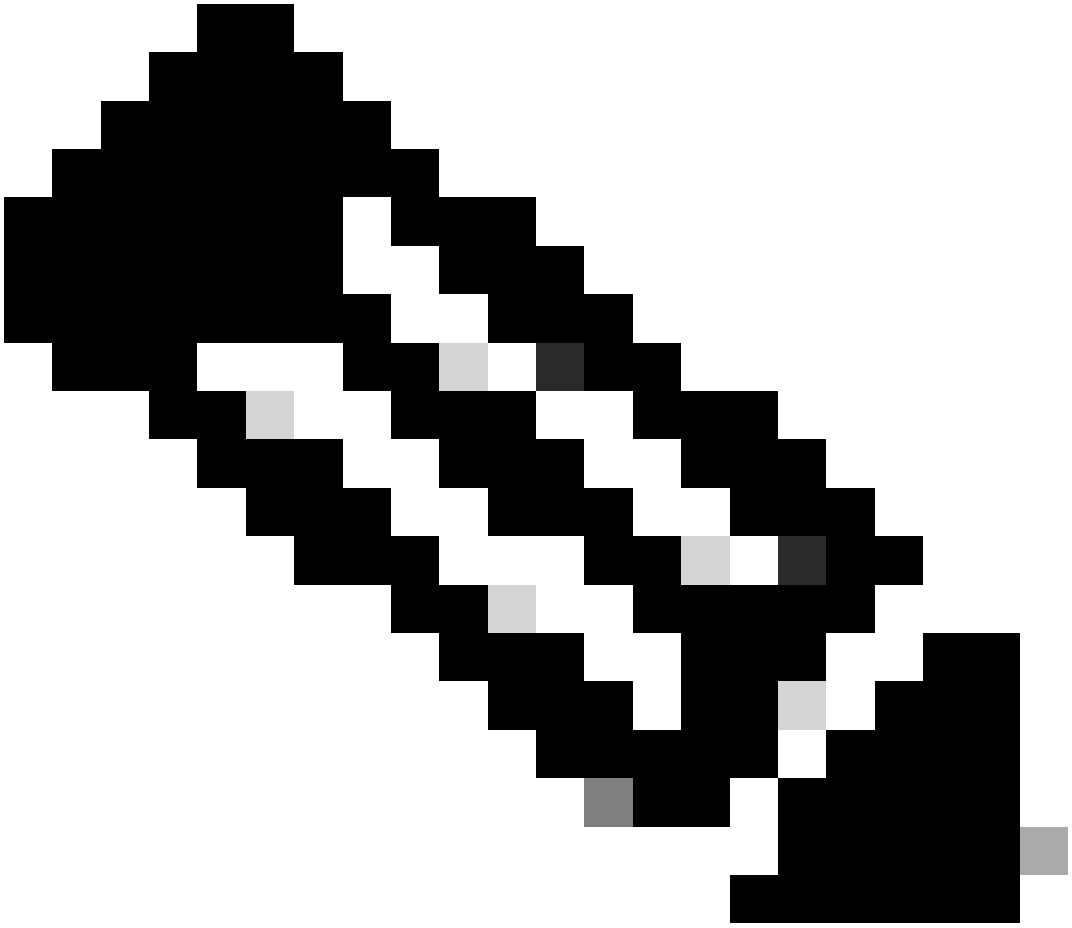
4. Accedere all'interfaccia utente QRadar come utente amministrativo.

5. Selezionare la scheda Admin.

6. Selezionare l'icona Origini log.

7. Selezionare l'origine del log Amazon AWS CloudTrail.

8. Dal menu di navigazione, selezionare Enable/Disable (Abilita/Disabilita) per disabilitare e quindi riabilitare l'origine del log Amazon AWS CloudTrail.



Nota: Quando un amministratore forza la disabilitazione dell'origine del log, il protocollo si connette al bucket AWS Amazon come definito nell'origine del log. Nella prima comunicazione viene quindi eseguita una verifica del certificato.

9. Se i problemi persistono, verificare che il campo Identificatore origine log contenga il nome del bucket Amazon AWS corretto e che il percorso della directory remota sia corretto nella configurazione dell'origine del log.

Completamento della configurazione di QRadar

1. In QRadar assicurarsi che tutti i protocolli, DSM e altre informazioni siano aggiornati. Selezionare il LogFileProtocol con queste configurazioni (la frequenza, l'ora di inizio, la ricorrenza e altre informazioni possono essere diverse).

2. Nella scheda Origini log, immettere un nome origine log e una descrizione origine log. Questi possono essere quello che vuoi.

3. Inserire il nome del bucket S3, la chiave di accesso AWS, la chiave segreta AWS e la directory remota (probabilmente dnslogs, ma dipende dalla configurazione). L'aggiunta di un identificatore dell'origine del log come l'anno può aiutare a filtrare in modo che vengano estratti solo i log contenenti "2019".

4. Creare un LSX (Log Source Extension) in grado di analizzare gli eventi Cisco Umbrella. (Questo è quello che appare dopo l'importazione in QRadar.) Ulteriori informazioni su come esattamente creare LSX sono disponibili sul sito Web IBM. Questo è solo un esempio. I dati che si desidera estrarre dai registri variano a seconda dello Use Case.

5. Verificare che la chiave di accesso AWS e la chiave privata AWS siano state copiate e incollate correttamente nella configurazione dell'origine del log.

6. Selezionare il processore GZIP e un generatore di eventi per la multiriga basata su RegEx. Il modo più semplice per ottenere un evento per riga consiste nell'utilizzare uno schema di inizio RegEx di:

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

Accertarsi di selezionare l'estensione dell'origine del registro e Usa condizione, quindi salvare l'origine del registro.

7. Eseguire una distribuzione completa in QRadar.

L'origine del registro utilizzerà quindi RestAPI per connettersi al bucket con le credenziali e le chiavi specificate e inizierà il pull degli eventi.

Ulteriori informazioni

Abilita registrazione bucket

Per abilitare la registrazione dei bucket, leggere la documentazione di AWS e completare le procedure descritte. Per impostazione predefinita, la registrazione è disattivata. Una volta abilitata, una nuova cartella denominata /logs risiede nella radice del bucket per mostrare le informazioni di GET, PUT e DELETES.

Gestione del ciclo di log

Quando si utilizza S3, è possibile gestire il ciclo di vita dei dati all'interno del bucket per estendere la durata del tempo per cui si desidera conservare i log. A seconda dello scopo per cui si utilizza la gestione dei registri esterni, la durata può essere molto breve o molto lunga. Ad esempio, è possibile semplicemente scaricare i log dal bucket S3 dopo 24 ore e archiviarli offline, oppure conservarli indefinitamente nel cloud.

Per impostazione predefinita, Amazon archivia i dati in un bucket per un periodo di tempo indefinito, ma lo storage illimitato aumenta il costo di manutenzione del bucket. Per ulteriori informazioni sui cicli di vita S3, consultare la documentazione di AWS.

Per configurare il ciclo di vita del bucket:

1. Selezionare Proprietà > Ciclo di vita.

2. Selezionare Aggiungi regola, quindi Applica la regola all'intero periodo fisso (o a una sottocartella se configurata come tale).

3. Selezionare un'azione sugli oggetti, ad esempio Elimina o Archivia, quindi selezionare il periodo di tempo e se si desidera utilizzare la memoria Ghiacciaio per ridurre i costi Amazzoni. (Glacier è un sistema di storage offline "freddo", che, sebbene lento nell'accesso, è molto meno costoso).

Se si preferisce gestire i log in un altro metodo, ad esempio nella soluzione di backup interno, è sufficiente scaricare i log da S3 e conservarli in un altro modo.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).