Konfiguration der QRadar-Integration mit Umbrella Log Management und S3

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie QRadar so konfiguriert wird, dass Protokolle von einem AWS S3-Bucket für die Umbrella-Protokollverwaltung aufgenommen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

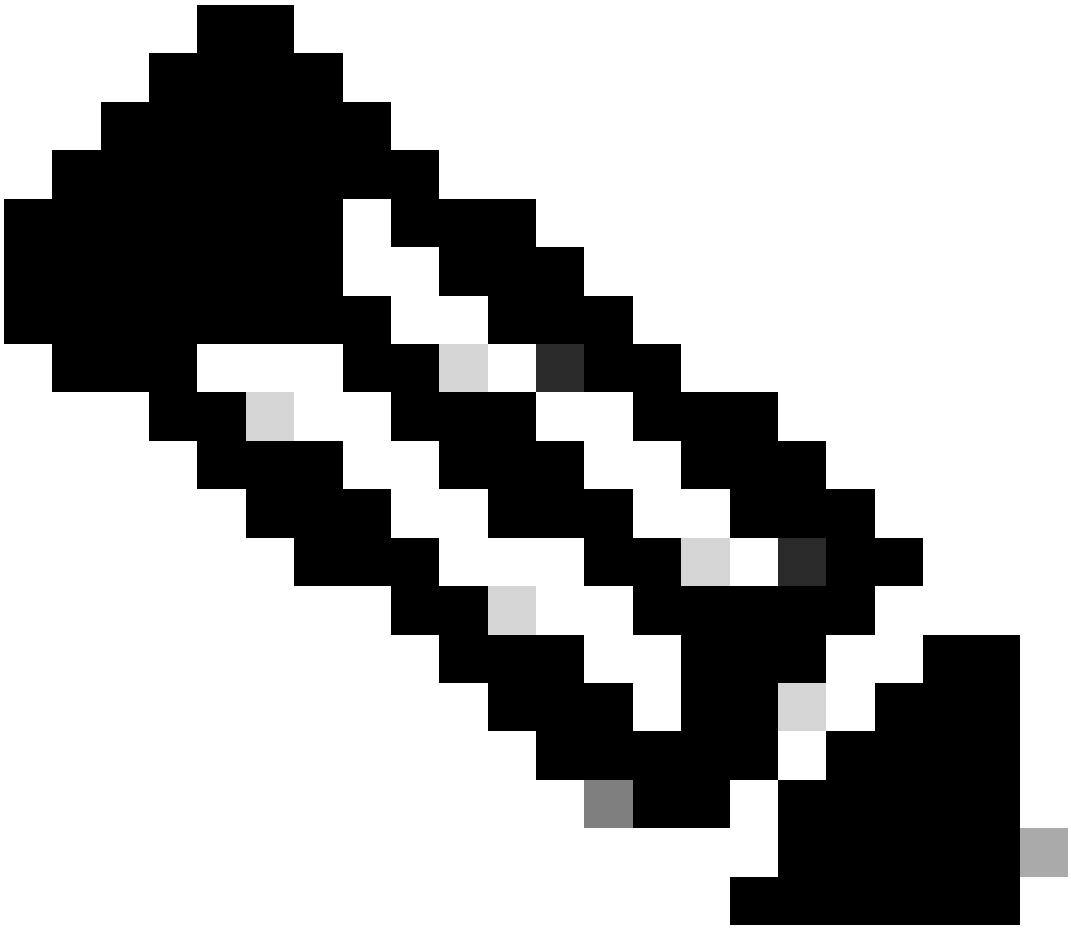
- In diesem Dokument wird davon ausgegangen, dass Ihr Amazon AWS S3-Bucket in Umbrella (Einstellungen > Protokollverwaltung) konfiguriert wurde und grün angezeigt wird, während die letzten Protokolle hochgeladen wurden. Weitere Informationen zur Konfiguration dieser Funktion finden Sie in diesem Artikel: Protokolle von Umbrella Log Management in AWS S3 herunterladen
- Neben Administratorrechten für die QRadar-Appliance(s), die Amazon S3-Konfiguration und das Umbrella Dashboard gehen diese Anweisungen davon aus, dass der QRadar-Administrator mit der Erstellung von LSX-Dateien (Log Source Extension) vertraut ist.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick



> Anmerkung: Die beste Methode, QRadar für Cisco Umbrella zu konfigurieren, ist die Cisco Cloud Security App. Fahren Sie mit dieser Methode nur fort, wenn die App nicht konfiguriert werden kann.

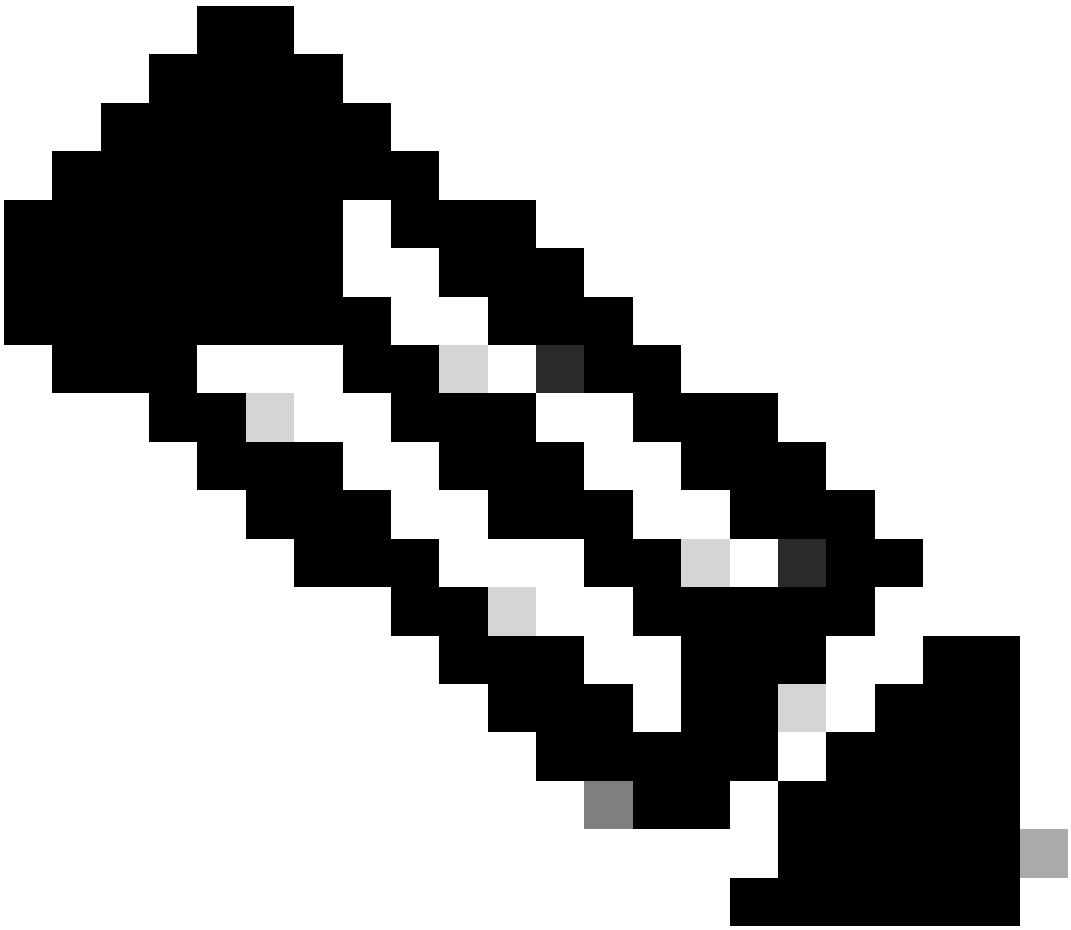
QRadar von IBM ist ein beliebtes SIEM für die Protokollanalyse. Es bietet eine leistungsstarke

Schnittstelle für die Analyse großer Datenmengen, wie z. B. die von Cisco Umbrella bereitgestellten Protokolle für den DNS-Datenverkehr Ihres Unternehmens.

In diesem Artikel wird beschrieben, wie QRadar eingerichtet und ausgeführt wird, damit es die Protokolle aus Ihrem S3-Eimer abrufen und verbrauchen kann. Es gibt zwei Hauptphasen:

- Konfigurieren Sie Ihre AWS S3-Sicherheitsanmeldeinformationen, um QRadar den Zugriff auf die Protokolle zu ermöglichen.
- Konfigurieren Sie QRadar selbst so, dass es auf Ihren Bucket zeigt.

Wenn Sie den von Cisco verwalteten S3-Bucket verwenden, verwenden Sie bitte die folgenden Anweisungen im Artikel Protokolle von Umbrella Log Management mit der AWS CLI herunterladen.



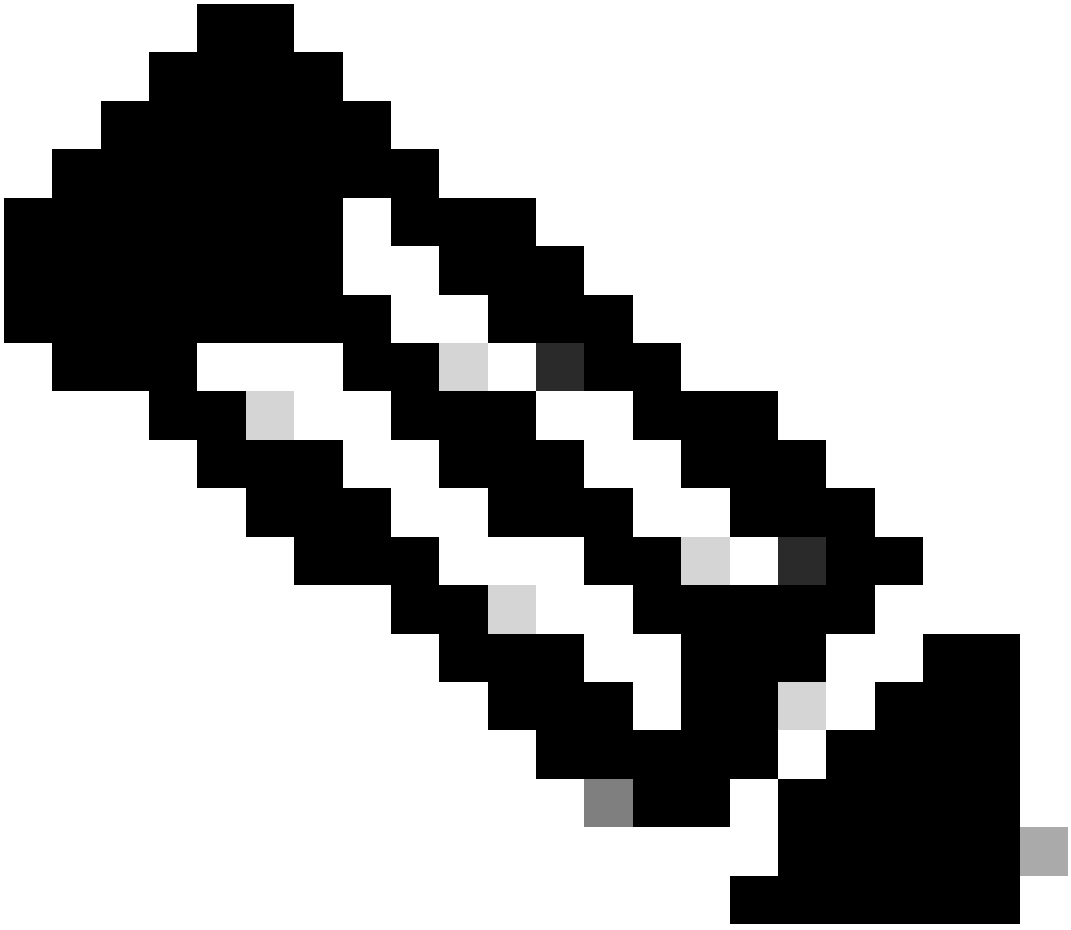
Anmerkung: Diese Integration wurde mit vom Kunden verwalteten S3-Buckets und mit von Cisco verwalteten S3-Buckets getestet. Die in diesem Artikel besprochenen Informationen sind seit diesem Schreiben (Oktober 2019) aktuell. Sie können sich je nach QRadar- und AWS Services-Schnittstelle ändern. Dieses Dokument ist ein lebendiges Dokument. Wenn

---

Sie Feedback gegeben haben oder Tricks oder Hinweise gefunden haben, die anderen Kunden helfen könnten, wenden Sie sich an den Cisco Umbrella Support.

QRadar wird von IBM unterstützt, da Cisco keinen direkten Support für Hardware oder Software von Drittanbietern leistet. Bei Problemen, die das Umbrella Dashboard mit Ihrem S3-Bucket verbinden, kann Cisco Umbrella Sie unterstützen. Viele der in diesem Artikel enthaltenen Informationen finden Sie auch auf der IBM-Website.

Phase 1: Konfigurieren Ihrer Sicherheitsanmeldeinformationen in AWS



Anmerkung: Diese Schritte entsprechen denen, die im Artikel beschrieben werden, in dem beschrieben wird, wie ein Tool zum Herunterladen der Protokolle aus Ihrem Bucket konfiguriert wird (Protokolle aus Umbrella Log Management in AWS S3 herunterladen). Wenn Sie diese Schritte bereits ausgeführt haben, können Sie mit Schritt 2 fortfahren,

obwohl Sie später die Sicherheitsanmeldeinformationen Ihres IAM-Benutzers benötigen, um QRadar für Ihren Bucket zu authentifizieren.

Schritt 1

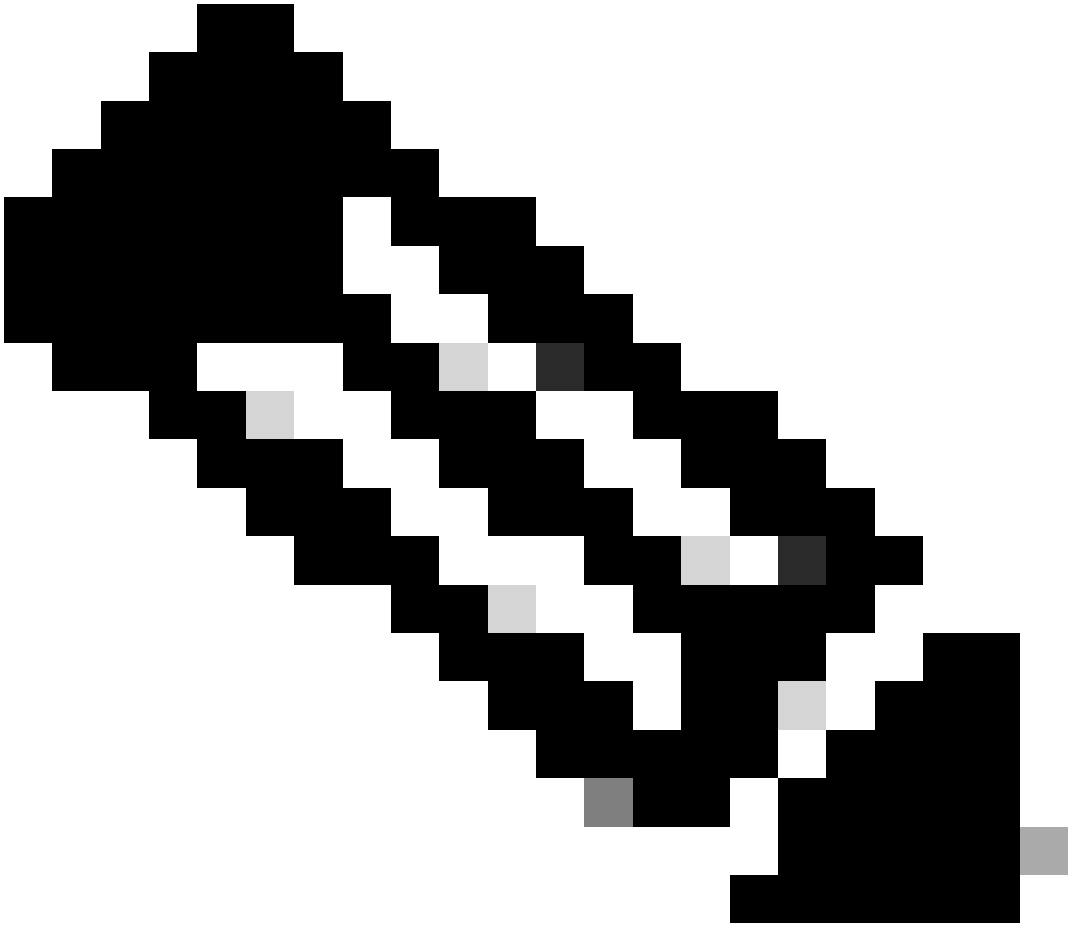
1. Fügen Sie Ihrem Amazon Web Services-Konto einen Zugriffsschlüssel hinzu, um den Remote-Zugriff auf Ihr lokales Tool zu ermöglichen und die Möglichkeit zum Hochladen, Herunterladen und Ändern von Dateien in S3 zu bieten:

1. Bei AWS anmelden
2. Wählen Sie oben rechts Ihren Kontonamen aus.
3. Wählen Sie im Dropdown-Menü die Option Security Credentials (Sicherheitsanmeldeinformationen).

2. Sie werden dann aufgefordert, Amazon Best Practices zu verwenden und einen AWS Identity and Access Management (IAM)-Benutzer zu erstellen. Im Wesentlichen stellt ein IAM-Benutzer sicher, dass das Konto, mit dem s3cmd auf Ihren Bucket zugreift, nicht das Master-Konto (z. B. Ihr Konto) für Ihre gesamte S3-Konfiguration ist. Durch die Erstellung individueller IAM-Benutzer für Personen, die auf Ihr Konto zugreifen, können Sie jedem IAM-Benutzer einen eindeutigen Satz von Sicherheitsanmeldeinformationen zuweisen. Sie können jedem IAM-Benutzer auch unterschiedliche Berechtigungen erteilen. Bei Bedarf können Sie die Berechtigungen eines IAM-Benutzers jederzeit ändern oder widerrufen. Weitere Informationen zu IAM-Benutzern und AWS-Best Practices finden Sie in der AWS-Dokumentation.

Schritt 2

1. Wählen Sie Erste Schritte mit IAM-Benutzern, um einen IAM-Benutzer für den Zugriff auf Ihre S3-Bucket zu erstellen. Sie gelangen dann zu einem Bildschirm, in dem Sie einen IAM-Benutzer erstellen können.
2. Wählen Sie Neue Benutzer aus, und füllen Sie die Felder aus.



Anmerkung: Das Benutzerkonto darf keine Leerzeichen enthalten.

3. Nachdem Sie das Benutzerkonto erstellt haben, erhalten Sie nur noch eine Möglichkeit, zwei wichtige Informationen mit Ihren Amazon User Security-Anmeldeinformationen zu erfassen. Umbrella empfiehlt dringend, diese über die Schaltfläche unten rechts herunterzuladen, um sie zu sichern. Sie sind nach dieser Phase der Einrichtung nicht mehr verfügbar. Notieren Sie sich sowohl die Zugriffsschlüssel-ID als auch den geheimen Zugriffsschlüssel, da diese in einem späteren Schritt erforderlich sind.

Schritt 3

Fügen Sie als Nächstes eine Richtlinie für den IAM-Benutzer hinzu, sodass dieser auf Ihren S3-Bucket zugreifen kann:

1. Wählen Sie den Benutzer aus, der gerade erstellt wurde, und blättern Sie dann nach unten durch die Eigenschaften des Benutzers, bis die Schaltfläche Richtlinie anhängen angezeigt wird.

2. Wählen Sie Attach Policy (Richtlinie anhängen) und geben Sie im Richtlinientypfilter "s3" ein. Dies zeigt zwei Ergebnisse:

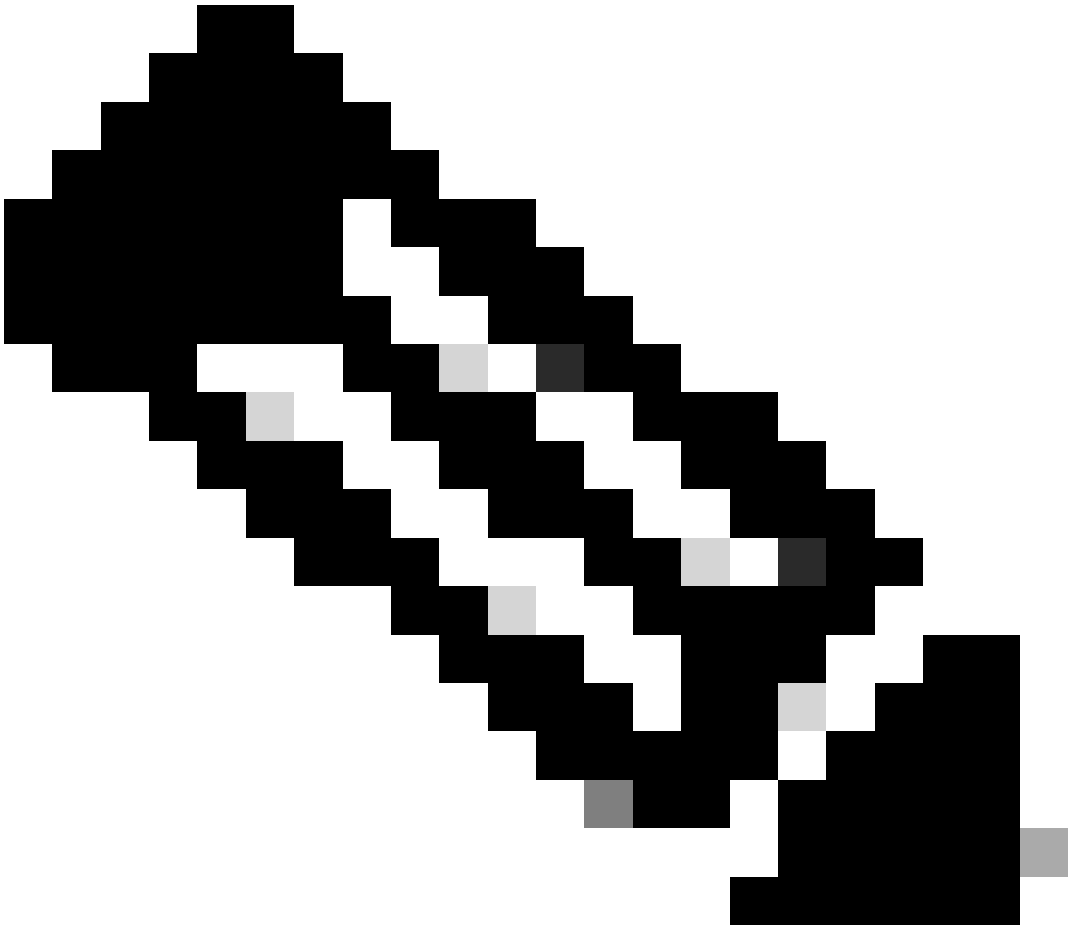
- Amazon S3Vollzugriff
- AmazonS3Schreibgeschützter Zugriff

3. Wählen Sie AmazonS3FullAccess und dann Attach Policy in der rechten unteren Ecke.

Phase 2: Einrichten von QRadar zum Abrufen von DNS-Protokolldaten aus Ihrem S3-Bucket

QRadar nutzt den AWS CloudTrail-Dienst, einen Webdienst, der AWS API-Aufrufe für Ihr Konto aufzeichnet und Protokolldateien an Sie liefert.

Bevor QRadar auf Amazon S3 zugreift, führen Sie dieses Verfahren von IBM aus, um das Amazon-Serverzertifikat zu erhalten. Dieser Teil ist schwierig, also vergewissern Sie sich bitte, dass Sie die Anweisungen genau befolgen.



Anmerkung: In Testing müssen Sie den Firefox-Browser verwenden, damit dies wie erwartet funktioniert.

Um das Amazon-Serverzertifikat zu erhalten, müssen Sie das Zertifikat im DER-Format auf die richtige QRadar-Appliance verschieben. Die QRadar-Appliance, die das Zertifikat benötigt, ist die Appliance, die im Feld Target Event Collector in der Protokollquelle Amazon AWS CloudTrail zugewiesen wird.

Vorbereitungen

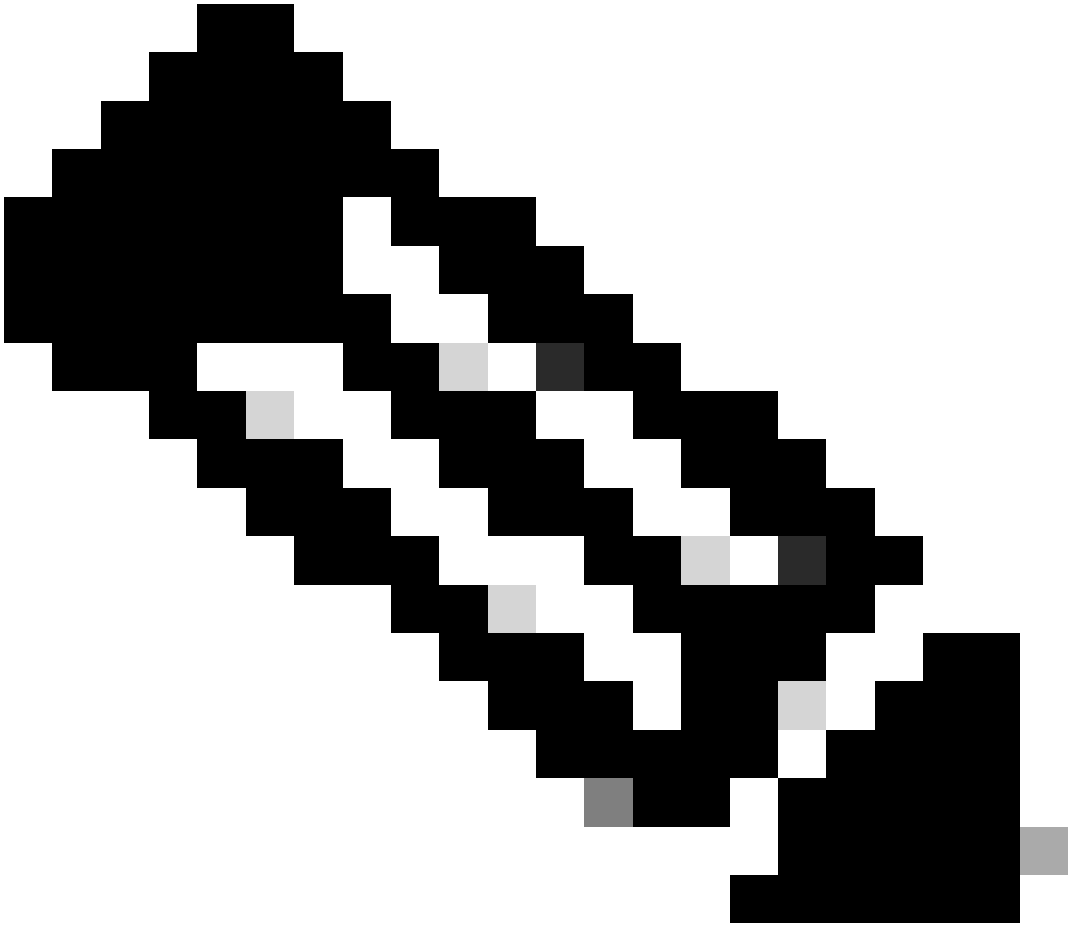
- Das Zertifikat muss das Format .DER haben.
- Die Extension .DER unterscheidet Groß- und Kleinschreibung.
- Wenn das Zertifikat in Kleinbuchstaben exportiert wird, kann es bei der Protokollquelle zu Problemen bei der Ereigniserfassung kommen.

Erste Schritte

1. Zugriff auf Ihren AWS CloudTrail S3 Bucket: `https://<bucketname>.s3.amazonaws.com`

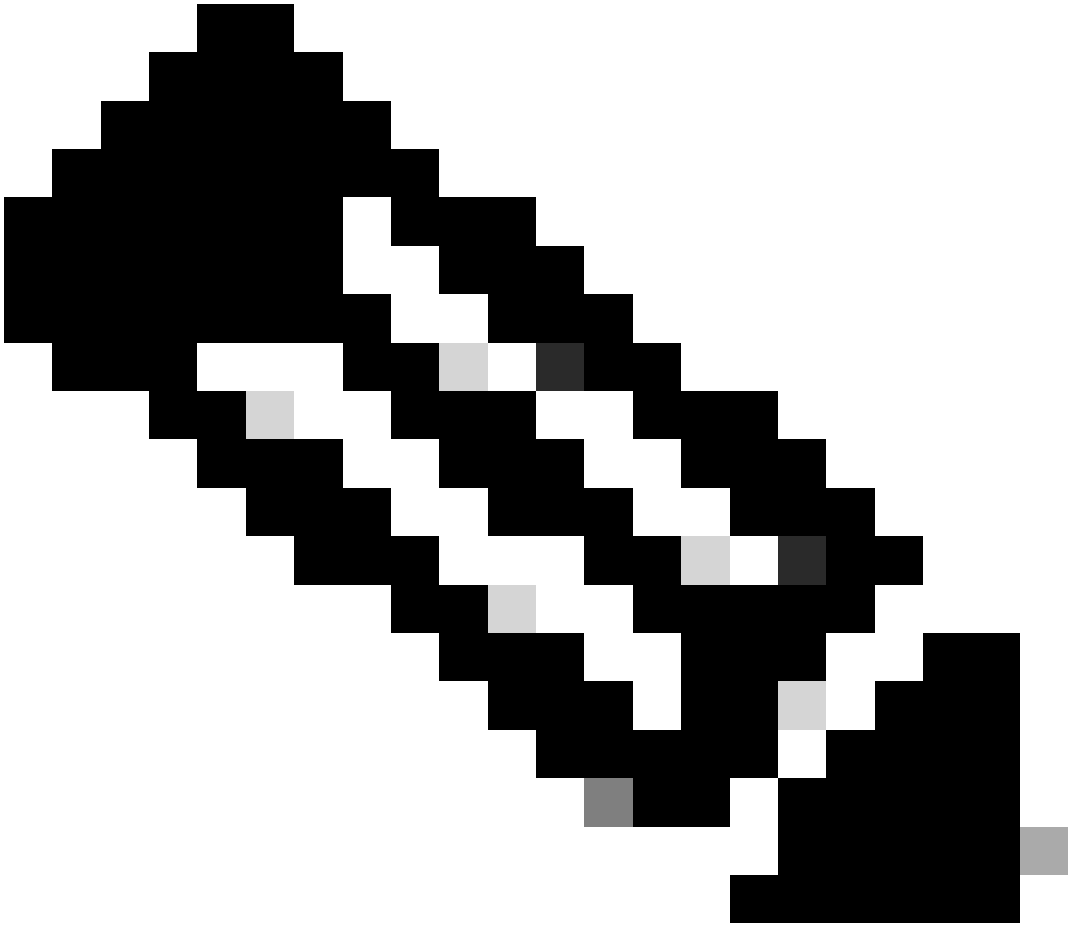
2. Verwenden Sie Firefox, um das SSL-Zertifikat von AWS als (.DER)-Zertifikat zu exportieren. Firefox kann das erforderliche Zertifikat mit der Erweiterung .DER erstellen:

1. Wählen Sie das Symbol Site Identity (Standortidentität) (das Sperrsymbol in der Adressleiste) aus.
2. Wählen Sie Weitere Informationen **>** Zertifikat anzeigen und anschließend die Registerkarte Details aus.
3. Wählen Sie Exportieren, um das Zertifikat im DER-Format zu exportieren.



Anmerkung: Bei der Erweiterung .DER wird Groß- und Kleinschreibung unterschieden.

3. Kopieren Sie das .DER-Zertifikat in das /opt/QRadar/conf/trusted_Certificates-Verzeichnis der QRadar-Appliance, die die Amazon AWS CloudTrail-Protokollquelle verwaltet. Sie können es mit WinSCP kopieren.



Anmerkung: Die QRadar-Appliance, die die Protokollquelle verwaltet, wird durch das Feld Target Event Collect in der Protokollquelle Amazon AWS CloudTrail identifiziert. Die QRadar-Appliance, die die Amazon AWS CloudTrail-Protokollquelle verwaltet, muss über eine Kopie des .DER-Zertifikats in /opt/QRadar/conf/trusted_Certificates verfügen.

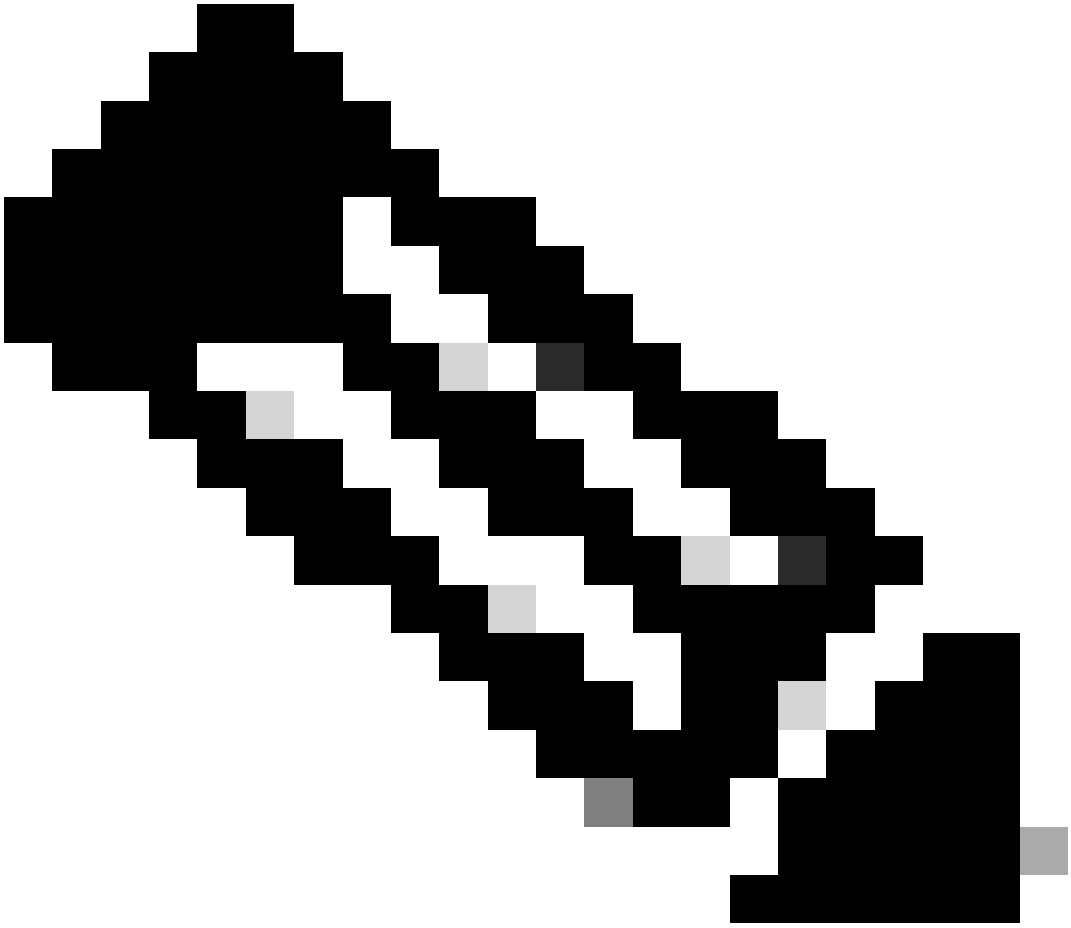
4. Melden Sie sich als Administrator an der QRadar-Benutzeroberfläche an.

5. Wählen Sie die Registerkarte Admin.

6. Wählen Sie das Symbol Protokollquellen.

7. Wählen Sie die Protokollquelle Amazon AWS CloudTrail.

8. Wählen Sie im Navigationsmenü Aktivieren/Deaktivieren, um die Amazon AWS CloudTrail-Protokollquelle zu deaktivieren und dann erneut zu aktivieren.



Anmerkung: Wenn ein Administrator erzwingt, dass die Protokollquelle deaktiviert wird, kann das Protokoll eine Verbindung mit dem Amazon AWS-Bucket herstellen, wie in der Protokollquelle definiert. Im Rahmen der ersten Kommunikation findet dann eine Zertifikatsüberprüfung statt.

9. Wenn weiterhin Probleme auftreten, überprüfen Sie, ob das Feld "Log Source Identifier" den richtigen Amazon AWS-Bucketnamen enthält und ob der Remote Directory-Pfad in der Konfiguration der Protokollquelle korrekt ist.

Abschließen der QRadar-Konfiguration

1. Stellen Sie in QRadar sicher, dass alle Ihre Protokolle, DSMs und andere Informationen auf dem neuesten Stand sind. Wählen Sie das LogFileProtocol mit diesen Konfigurationen aus (Häufigkeit, Startzeit, Wiederholung und andere Informationen können unterschiedlich sein).

2. Geben Sie auf der Registerkarte Protokollquellen einen Protokollquellennamen und eine Protokollquellbeschreibung ein. Die können sein, was du willst.

3. Geben Sie Ihren S3 Bucket-Namen, Ihren AWS-Zugriffsschlüssel, Ihren AWS Secret Key und das Remote Directory ein (wahrscheinlich dnslogs, hängt aber von Ihrer Einrichtung ab). Das Hinzufügen einer Log Source Identifier wie das Jahr kann helfen, zu filtern, sodass nur Protokolle mit "2019" in ihnen gezogen werden.

4. Erstellen Sie eine LSX (Log Source Extension), die die Cisco Umbrella-Ereignisse analysieren kann. (So sieht es nach dem Import in QRadar aus.) Weitere Informationen zur Erstellung von LSX finden Sie auf der IBM Website. Dies ist nur ein Beispiel. Die Daten, die Sie aus den Protokollen abrufen möchten, variieren je nach Anwendungsfall.

5. Überprüfen Sie, ob Ihr AWS-Zugriffsschlüssel und Ihr AWS-Geheimschlüssel erfolgreich kopiert und in die Protokollquellenkonfiguration eingefügt wurden.

6. Wählen Sie den GZIP-Prozessor und einen Ereignisgenerator der RegEx-basierten Mehrzeilenversion. Die einfachste Methode, ein Ereignis pro Zeile zu erhalten, ist die Verwendung eines Startmusters RegEx von:

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

Wählen Sie die Erweiterung der Protokollquelle und die Bedingung verwenden aus, und speichern Sie die Protokollquelle.

7. Durchführen einer vollständigen Bereitstellung in QRadar

Die Protokollquelle verwendet dann die RESTAPI, um sich mit den von Ihnen angegebenen Anmeldeinformationen und Schlüsseln mit Ihrem Bucket zu verbinden und mit dem Abrufen von Ereignissen zu beginnen.

Zusätzliche Informationen

Bucket-Protokollierung aktivieren

Um die Bucket-Protokollierung zu aktivieren, lesen Sie die AWS-Dokumentation, und führen Sie die beschriebenen Verfahren aus. Standardmäßig ist die Protokollierung deaktiviert. Nach der Aktivierung befindet sich ein neuer Ordner namens /logs in Ihrem Bucket-Root, um Ihnen die Informationen zu GETS, PUTS und DELETES anzuzeigen.

Protokollzyklus verwalten

Wenn Sie S3 verwenden, können Sie den Lebenszyklus der Daten innerhalb des Buckets verwalten, um den Zeitraum zu verlängern, für den Sie die Protokolle aufbewahren möchten. Je nachdem, für welchen Zweck Sie die externe Protokollverwaltung verwenden, kann die Dauer sehr kurz oder sehr lang sein. Sie können beispielsweise die Protokolle nach 24 Stunden einfach aus dem S3-Bucket herunterladen und offline speichern oder unbegrenzt in der Cloud speichern.

Standardmäßig speichert Amazon die Daten in einem Bucket unbegrenzt, aber unbegrenzter Speicher erhöht die Kosten für die Wartung des Buckets. Weitere Informationen zu S3-Lebenszyklen finden Sie in der AWS-Dokumentation.

So konfigurieren Sie den Lebenszyklus Ihres Buckets:

1. Wählen Sie Eigenschaften > Lebenszyklus.

2. Wählen Sie Regel hinzufügen, und wenden Sie die Regel auf die gesamte Gruppe (oder einen Unterordner, wenn Sie sie als solche konfiguriert haben) an.

3. Wählen Sie eine Aktion für Objekte, wie Löschen oder Archivieren, dann wählen Sie den Zeitraum und ob Sie Glacier-Speicher verwenden möchten, um Ihre Amazon-Kosten zu reduzieren. (Glacier ist ein "kalter" Offline-Speicher, der zwar langsamer zugänglich ist, aber wesentlich günstiger.)

Wenn Sie Protokolle lieber auf andere Weise verwalten möchten (z. B. in Ihrer internen Backup-Lösung), können Sie die Protokolle einfach von S3 herunterladen und auf andere Weise aufbewahren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.