Konfigurieren von Splunk mit einem selbst verwalteten S3-Bucket

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Splunk mit einem selbst verwalteten S3-Bucket konfiguriert wird.

Überblick

Splunk ist ein gängiges Tool 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.

Dieser Artikel beschreibt die Grundlagen von Splunk einrichten und ausführen, sodass es in der Lage ist, die Protokolle aus Ihrem S3 Eimer zu ziehen und verbrauchen. Es gibt zwei Hauptphasen: eine besteht darin, Ihre AWS S3-Sicherheitsanmeldeinformationen so zu konfigurieren, dass Splunk Zugriff auf die Protokolle erhält, und die zweite darin, Splunk selbst so zu konfigurieren, dass es auf Ihren Bucket zeigt.

Die Dokumentation für das Splunk Add-on für AWS S3 ist hier, von denen einige wörtlich in dieses Dokument kopiert wurden. Spezifische Fragen zur Splunk-Einrichtung finden Sie unter http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

Dieser Artikel ist in folgende Abschnitte gegliedert:

Voraussetzungen

Das Splunk Add-on für Amazon Web Services unterstützt diese Plattformen.

- AWS Linux
- RedHat
- Windows 2008R2, 2012R2

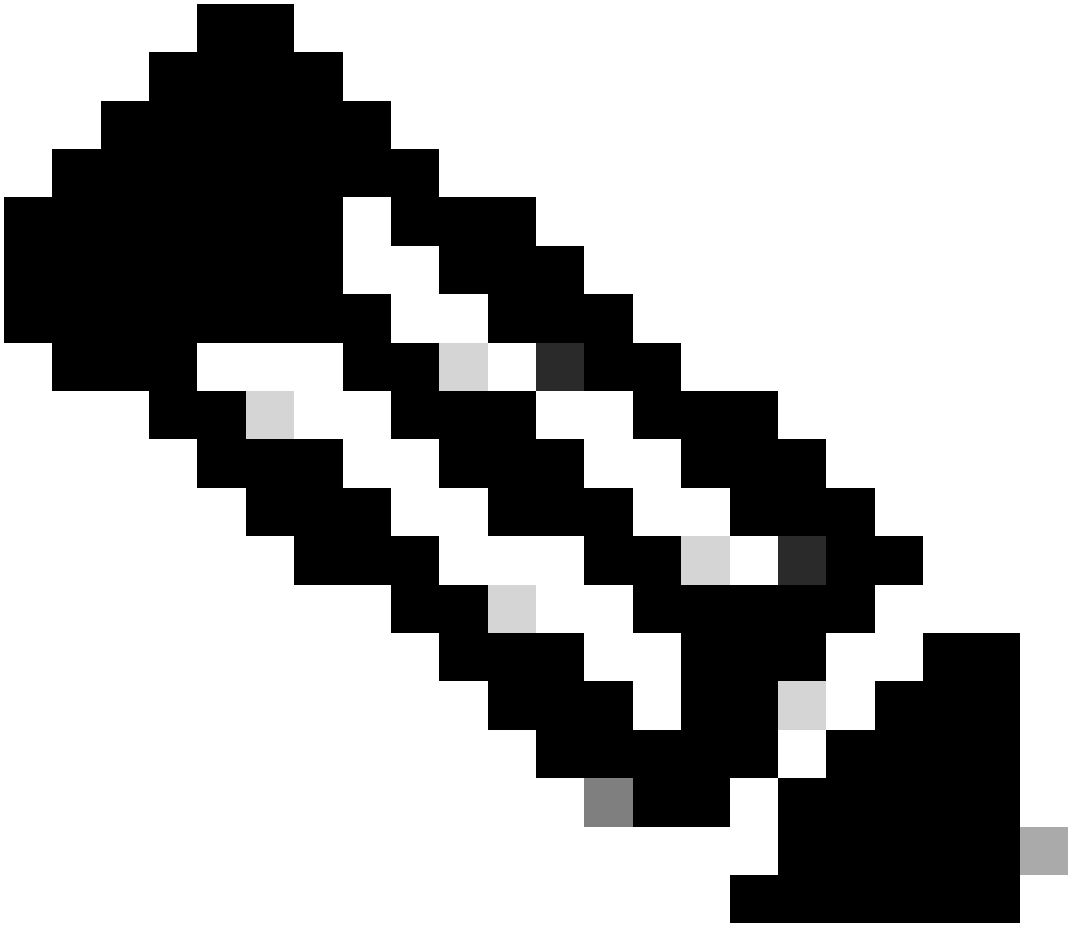
Splunk Enterprise-Systemanforderungen

Da dieses Add-on auf Splunk Enterprise ausgeführt wird, gelten alle Systemanforderungen von Splunk Enterprise. Siehe "Systemanforderungen" Installationshandbuch in der Splunk Enterprise-Dokumentation. Diese Anweisungen gelten für Splunk Enterprise Version 6.2.1.

Allgemeine Anforderungen

In diesem Dokument wird davon ausgegangen, dass Ihr Amazon AWS S3-Bucket im Umbrella Dashboard (Admin > Log Management) konfiguriert wurde. Es wird grün angezeigt, und die letzten Protokolle wurden hochgeladen. Weitere Informationen zur Protokollverwaltung finden Sie unter Cisco Umbrella Log Management in Amazon S3.

Phase 1: Konfigurieren Ihrer Sicherheitsanmeldeinformationen in AWS



Anmerkung: Diese Schritte sind die gleichen wie die, die im Artikel beschrieben werden, wie man ein Tool zum Herunterladen der Protokolle aus Ihrem Bucket (Gewusst wie: Herunterladen von Protokollen von Cisco Umbrella Log Management in AWS S3). Wenn Sie diese Schritte bereits ausgeführt haben, können Sie einfach mit Schritt 2 fortfahren. Sie benötigen jedoch die Sicherheitsdaten Ihres IAM-Benutzers, um das Splunk-Plugin für Ihren Bucket zu authentifizieren.

Schritt 1

1. Fügen Sie Ihrem Amazon Web Services-Konto einen Zugriffsschlüssel hinzu, um Remote-Zugriff auf Ihr lokales Tool zu ermöglichen und die Möglichkeit zum Hochladen, Herunterladen und Ändern von Dateien in S3 zu bieten. Melden Sie sich bei AWS an, und klicken Sie in der oberen rechten Ecke auf Ihren Kontonamen. Wählen Sie im Dropdown-Menü die Option Security Credentials (Sicherheitsanmeldeinformationen).
2. Sie werden 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 primäre 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 hier:
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Schritt 2

1. Erstellen Sie einen IAM-Benutzer, um auf Ihre S3-Bucket zuzugreifen, indem Sie auf Erste Schritte mit IAM-Benutzern klicken. Sie gelangen zu einem Bildschirm, auf dem Sie einen IAM-Benutzer erstellen können.
2. Klicken Sie auf Neue Benutzer erstellen, und füllen Sie dann die Felder aus. Beachten Sie, dass das Benutzerkonto keine Leerzeichen enthalten darf.
3. Nach der Erstellung des Benutzerkontos haben Sie nur eine Möglichkeit, zwei wichtige Informationen mit Ihren Amazon User Security-Anmeldeinformationen zu erfassen. Wir empfehlen Ihnen dringend, diese über die Schaltfläche unten rechts herunterzuladen, um sie zu sichern. Sie sind nach dieser Phase der Konfiguration nicht mehr verfügbar. Notieren Sie sich später bei der Einrichtung von Splunk sowohl Ihre Zugriffsschlüssel-ID als auch Ihren geheimen Zugriffsschlüssel.

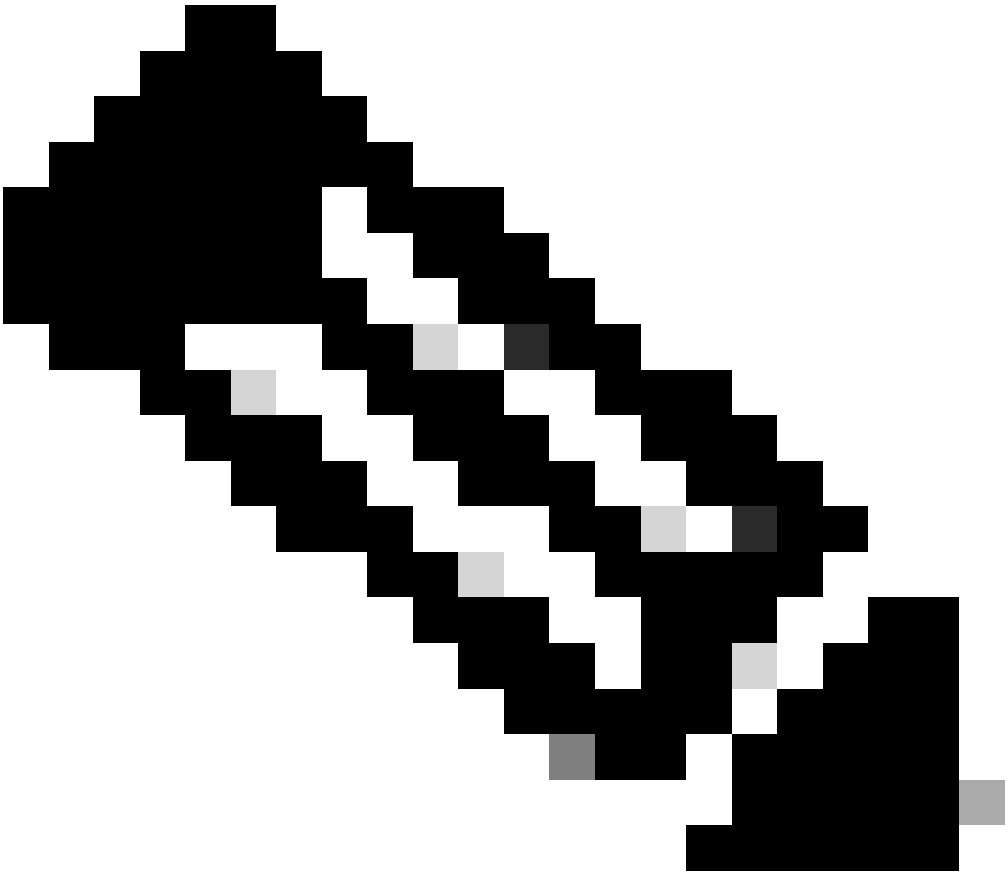
Schritt 3

1. Als Nächstes fügen Sie eine Richtlinie für den IAM-Benutzer hinzu, damit dieser auf Ihren S3-Bucket zugreifen kann. Klicken Sie auf den soeben erstellten Benutzer, und scrollen Sie dann nach unten durch die Eigenschaften des Benutzers, bis die Schaltfläche Richtlinie anhängen angezeigt wird.
2. Klicken Sie auf Richtlinie anhängen, und geben Sie im Richtlinientyp-Filter 's3' ein. Dies zeigt zwei Ergebnisse: "AmazonS3FullAccess" und "AmazonS3ReadOnlyAccess".
3. Wählen Sie AmazonS3FullAccess aus, und klicken Sie dann auf Richtlinie anhängen.

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

Schritt 1: Einrichten von Splunk zum Abrufen von DNS-Protokolldaten aus dem selbst verwalteten S3-Bucket

1. Beginnen Sie mit der Installation des "Splunk Add-ons für Amazon Web Services" auf Ihrer Splunk-Instanz. Öffnen Sie Ihr Splunk-Dashboard, und klicken Sie auf Apps, oder klicken Sie auf Splunk Apps, wenn es auf Ihrem Dashboard angezeigt wird. Geben Sie im Abschnitt "Apps" im Suchfenster "s3" ein, um "Splunk Add-on für Amazon Web Services" zu finden, und installieren Sie die App.



Anmerkung: Wahrscheinlich müssen Sie Splunk während der Installation neu starten.
Sobald es installiert ist, sehen Sie Splunk Add-on für AWS mit dem Ordnernamen 'Splunk_TA_aws' jetzt unter Apps aufgelistet.

2. Klicken Sie auf Einrichten, um die App zu konfigurieren. An diesem Punkt benötigen Sie die Anmeldeinformationen für Stufe 1 in dieser Dokumentation.
   Für die Einrichtung müssen folgende Felder eingegeben werden:

   - Ein Anzeigename - der Name, den Sie für diese Integration verwenden
   - Ihre AWS-Kontoschlüssel-ID (aus Phase 1)
   - Ihr Passwort (Ihr AWS-Konto Secret Key, ebenfalls aus Schritt 1)

Sie können auch lokale Proxy-Informationen festlegen, wenn es erforderlich ist, dass Splunk AWS erreicht, sowie die Protokollierung anpassen. Der Setup-Bildschirm sieht wie folgt aus:
3. Sobald Sie relevante Informationen hinzugefügt haben, klicken Sie auf Speichern und das Splunk-Add-on für Amazon Web Services ist vollständig konfiguriert.

Phase 3: Konfigurieren von Dateneingaben für Splunk

1. Als Nächstes möchten Sie die Dateneingabe für Amazon Web Services S3 konfigurieren. Navigieren Sie zu Einstellungen > Daten > Dateneingaben, und unter Lokale Eingaben sehen Sie jetzt eine Liste verschiedener Amazon-Eingaben, einschließlich S3, am Ende der Liste.
2. Klicken Sie auf AWS S3, um die Eingabe zu konfigurieren.
3. Klicken Sie auf Neu.
4. Sie müssen die folgenden Informationen angeben:

    - Geben Sie einen Anzeigenamen für Ihre S3-Integration ein.
    - Wählen Sie AWS-Konto aus der Dropdown-Liste. Dies ist der Anzeigename, den Sie in Schritt 1 angegeben haben.
    - Wählen Sie aus dem Dropdown-Menü Ihren S3-Bucket aus. Dies ist der Bucketname, der in Ihrem Umbrella Dashboard angegeben ist (Einstellungen > Protokollverwaltung).
    - Wählen Sie aus dem Dropdown-Menü den Namen des Schlüssels S3 aus. Jedes Element in Ihrem Bucket wird aufgelistet, wir empfehlen die Auswahl des übergeordneten Verzeichnisses \dns-logs\ , das alle Dateien und Verzeichnisse darunter enthält.
    - Es gibt mehrere Optionen unter "Message system configuration". Wir empfehlen, diese unverändert zu belassen - Standardeinstellungen.
    - Unter "Weitere Einstellungen" gibt es weitere Optionen. Zu beachten ist der "Quelltyp", der standardmäßig aws:s3 lautet. Wir empfehlen, dies so zu belassen, wie es ist, aber wenn Sie es ändern, ändert sich der Filter für Ihre Logs in der Suche von dem, was in Schritt 3 dieser Anleitung beschrieben wird.

    Füllen Sie die Details aus, und Ihre Dateneingabe sieht ähnlich aus:

4. Klicken Sie auf Weiter, um Ihre Angaben abzuschließen.
   Sie gelangen zu einem Bildschirm, der anzeigt, dass die Eingabe erfolgreich erstellt wurde.

Schritt 3

Führen Sie eine Schnellsuche durch, um festzustellen, ob Ihre Daten ordnungsgemäß importiert werden. Fügen Sie einfach sourcetype="aws:s3" in das Suchfenster oben rechts ein und wählen Sie dann "Open sourcetype="aws:s3" in der Suche

Dadurch gelangen Sie zu einem Bildschirm, ähnlich dem, auf dem Sie die Ereignisse aus den DNS-Protokollen Ihrer Organisation sehen. Hier blockiert der mobile Cisco Umbrella-Service soziale Medien auf einem iPhone. Sie können auch die Quelle des Dateinamens verwenden, um nach einem bestimmten Stapel von Protokollen zu filtern.

Danach wird der Cron-Job im Hintergrund weiter ausgeführt, und die neuesten Sätze werden aus den Protokollinformationen Ihres Buckets abgerufen.

Es gibt viel mehr, was Sie mit Splunk tun können, als in diesem Artikel beschrieben wurde, und wenn Sie die Chance hatten, mit der Verwendung dieser Daten in Ihrem Sicherheitsverfahren zu experimentieren, würden wir uns freuen, von Ihnen zu hören. Senden Sie Feedback, Fragen oder

Bedenken an umbrella-support@cisco.com, und verweisen Sie auf diesen Artikel.

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.