Configurazione di Splunk con un bucket S3 gestito automaticamente

Sommario

Introduzione

Panoramica

Prerequisiti

- Requisiti di sistema di Splunk Enterprise
- Requisiti principali

Fase 1: Configurazione delle credenziali di sicurezza in AWS

- Passaggio 1
- Passaggio 2
- Passaggio 3

Fase 2: Configurazione di Splunk per il prelievo dei dati del registro DNS dal bucket S3

- Passaggio 1: impostazione di Splunk per il prelievo dei dati del registro DNS dal bucket S3 gestito automaticamente

Fase 3: Configurazione degli input di dati per Splunk

- Passaggio 3

Introduzione

In questo documento viene descritto come configurare Splunk con un bucket S3 gestito automaticamente.

Panoramica

Splunk è uno strumento comune per l'analisi dei registri. 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 vengono descritte le nozioni di base per la configurazione e l'esecuzione di Splunk in modo che sia in grado di estrarre i registri dal bucket S3 e utilizzarli. Sono previste due fasi principali: la prima consiste nel configurare le credenziali di sicurezza AWS S3 per consentire l'accesso Splunk ai log, la seconda consiste nel configurare Splunk in modo che punti al bucket.

La documentazione per Splunk Add-on per AWS S3 è qui, alcune delle quali sono state copiate letteralmente in questo documento. Per domande specifiche sulla configurazione di Splunk, visitare il sito Web all'indirizzo http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

Questo articolo è suddiviso nelle seguenti sezioni:

- Prerequisiti
- Fase 1: Configurazione delle credenziali di sicurezza in AWS (solo bucket autogestiti)
- Fase 2: Configurazione di Splunk per il prelievo dei dati del registro DNS dal bucket S3
    - Passaggio 1: Configurazione di Splunk per il prelievo dei dati del registro DNS dal bucket S3 gestito automaticamente
- Fase 3: Configurazione degli input di dati per Splunk

Prerequisiti

Il componente aggiuntivo Splunk per Amazon Web Services supporta queste piattaforme.

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

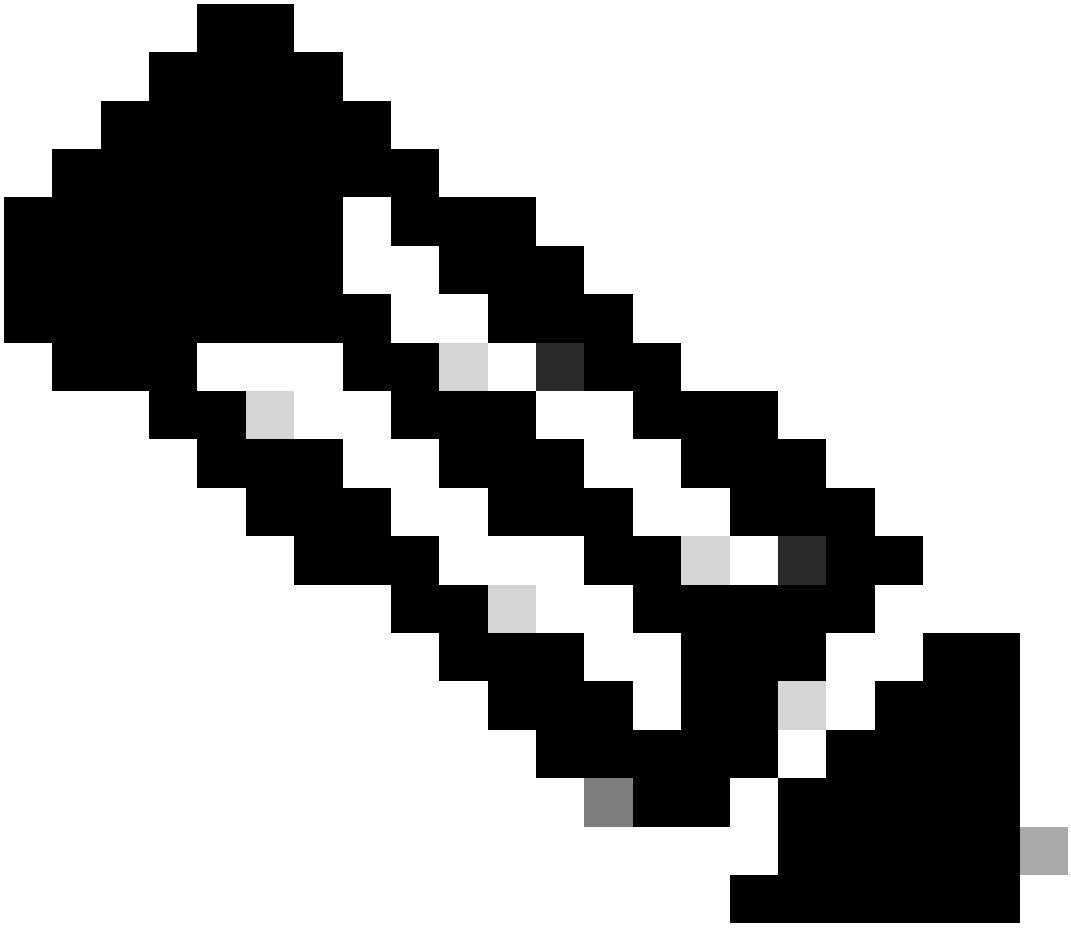
Requisiti di sistema di Splunk Enterprise

Poiché questo componente aggiuntivo viene eseguito su Splunk Enterprise, vengono applicati tutti i requisiti di sistema di Splunk Enterprise. Vedere il "System Requirements" Installation Manual nella documentazione di Splunk Enterprise. Queste istruzioni sono relative a Splunk Enterprise versione 6.2.1.

Requisiti principali

In questo documento si presume che il bucket S3 di Amazon AWS sia stato configurato nel dashboard Umbrella (Admin> Log Management) e sia visualizzato in verde con i log recenti caricati. Per ulteriori informazioni sulla gestione dei registri, vedere Cisco Umbrella Log Management in Amazon S3.

Fase 1: Configurazione delle credenziali di sicurezza in AWS



Nota: Queste operazioni sono le stesse descritte nell'articolo in cui viene descritto come configurare uno strumento per il download dei log dal bucket (Procedura: Download dei log da Cisco Umbrella Log Management in AWS (S3). Se questi passaggi sono già stati eseguiti, è sufficiente passare al passaggio 2, anche se sono necessarie le credenziali di sicurezza dell'utente IAM per autenticare il plug-in Splunk 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 il caricamento, il download e la modifica dei file in S3. Accedere ad AWS e fare clic sul nome dell'account nell'angolo in alto a destra. Nell'elenco a discesa, scegliere Credenziali di sicurezza.
2. Verrà richiesto di utilizzare le procedure consigliate di Amazon e di creare un utente di Gestione identità e accessi AWS (IAM). In sostanza, un utente IAM garantisce che l'account utilizzato da s3cmd per accedere al bucket non sia l'account principale (ad esempio, l'account) 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 AWS, leggere: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Passaggio 2

1. Creare un utente IAM per accedere al bucket S3 facendo clic su Introduzione agli utenti IAM. Viene visualizzata una schermata in cui è possibile creare un utente IAM.
2. Fare clic su Crea nuovi utenti, quindi compilare i campi. Si noti che l'account utente non può contenere spazi.
3. Dopo aver creato l'account utente, hai solo l'opportunità di recuperare due informazioni critiche contenenti le credenziali di protezione utente Amazon. Ti consigliamo vivamente di scaricarle utilizzando il pulsante in basso a destra per eseguirne il backup. Non sono disponibili dopo questa fase dell'installazione. Assicurarsi di annotare sia l'ID della chiave di accesso che la chiave di accesso segreta, in quanto sono necessarie in seguito durante la configurazione di Splunk.

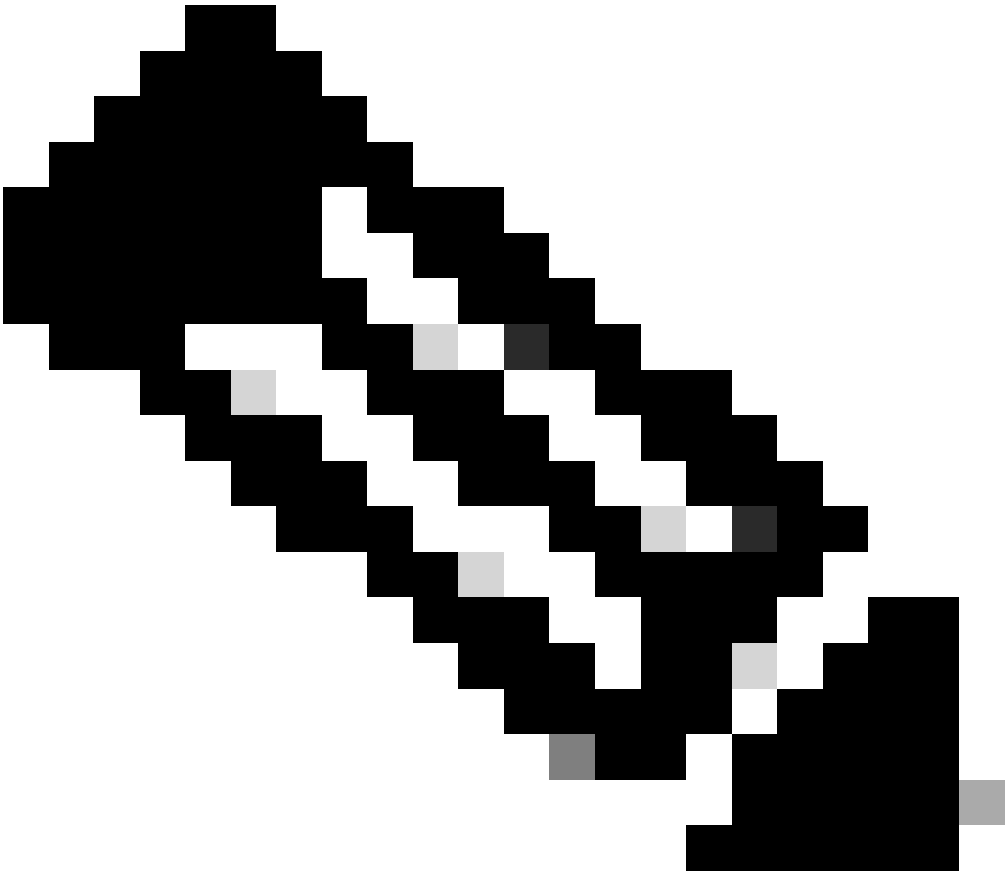
Passaggio 3

1. Aggiungere quindi un criterio per l'utente IAM in modo che possa accedere al bucket S3. Fare clic sull'utente appena creato, quindi scorrere verso il basso le proprietà degli utenti fino a visualizzare il pulsante Allega criterio.
2. Fare clic su Allega criterio, quindi immettere 's3' nel filtro del tipo di criterio. Questo mostra due risultati: "AmazonS3FullAccess" e "AmazonS3ReadOnlyAccess"
3. Selezionare AmazonS3FullAccess, quindi fare clic su Allega criterio.

Fase 2: Configurazione di Splunk per il prelievo dei dati del registro DNS dal bucket S3

Passaggio 1: configurazione di Splunk per il pull dei dati del registro DNS dal bucket S3 gestito automaticamente

1. Installare innanzitutto il componente aggiuntivo Splunk per servizi Web Amazon nell'istanza di Splunk. Aprire il dashboard Splunk e fare clic su App oppure fare clic su Splunk Apps, se visualizzato nel dashboard. Una volta nella sezione Apps, digitare "s3" nella finestra di ricerca per trovare "Splunk Add-on for Amazon Web Services" e installare l'app.



Nota: È probabile che sia necessario riavviare Splunk durante l'installazione. Una volta installata, è possibile vedere Splunk Add-on for AWS con il nome di cartella 'Splunk_TA_aws' ora elencato in Apps.

2. Fare clic su Configura per configurare l'app. A questo punto sono necessarie le credenziali di sicurezza della Fase 1 di questa documentazione.
   L'impostazione richiede l'immissione dei seguenti campi:

   - Un nome descrittivo, ovvero il nome utilizzato per fare riferimento a questa integrazione
   - ID chiave account AWS (dalla fase 1)
   - Password (chiave segreta dell'account AWS, anche dalla fase 1)

È inoltre possibile impostare le informazioni sul proxy locale, se necessarie per consentire a Splunk di raggiungere AWS, nonché regolare la registrazione. La schermata di installazione ha il seguente aspetto:
3. Una volta aggiunte le informazioni pertinenti, fare clic su Save (Salva) per configurare completamente il componente aggiuntivo Splunk per Amazon Web Services.

Fase 3: Configurazione degli input di dati per Splunk

1. Successivamente, si desidera configurare l'input di dati per Amazon Web Services S3. Passare a Impostazioni > Dati > Input di dati e in Input locali è ora visualizzato un elenco di vari input Amazon incluso S3 in fondo all'elenco.
2. Fare clic su AWS S3 per configurare l'input.
3. Fare clic su New.
4. È necessario fornire le seguenti informazioni:

    - Immettere un nome descrittivo per l'integrazione S3.
    - Seleziona il tuo Account AWS dall'elenco a discesa. Questo è il nome descrittivo fornito al passaggio 1.
    - Selezionare il bucket S3 dall'elenco a discesa. Si tratta del nome del bucket specificato nel dashboard Umbrella (Impostazioni > Gestione log).
    - Selezionare il nome del tasto S3 dall'elenco a discesa. Ogni elemento del bucket è elencato. È consigliabile selezionare la directory di livello superiore \dns-logs\, che include tutti i file e le directory in essa contenuti.
    - Ci sono diverse opzioni sotto "Configurazione del sistema di messaggi", si consiglia di lasciarli così come sono: le impostazioni predefinite.
    - Sono disponibili opzioni aggiuntive in "Altre impostazioni". Of note è il "Tipo di origine", che per impostazione predefinita è aws:s3. Si consiglia di lasciare invariato questo stato, ma se lo si modifica, il filtro per i log nella ricerca cambia rispetto a quanto descritto nel Passaggio 3 di queste istruzioni.

Immettere i dettagli e l'input dei dati avrà un aspetto simile al seguente:

4. Fare clic su Avanti per finalizzare i dettagli.
   Viene visualizzata una schermata che indica che l'input è stato creato correttamente

Passaggio 3

Eseguire una ricerca rapida per verificare se i dati vengono importati correttamente. È sufficiente incollare sourcetype="aws:s3" nella finestra di ricerca in alto a destra e quindi selezionare "Open sourcetype="aws:s3" nella ricerca

Verrà visualizzata una schermata simile a quella in cui vengono visualizzati gli eventi dei registri DNS delle organizzazioni. Qui, il servizio mobile Cisco Umbrella sta bloccando i social media su un iPhone. È inoltre possibile utilizzare l'origine del nome file per filtrare in base a un particolare batch di registri.

Dopo questo punto, il job cron in background continua a essere eseguito ed estrae le serie più recenti dalle informazioni di log dal bucket.

Con Splunk è possibile fare molto di più oltre quanto descritto in questo articolo e, se si ha la possibilità di sperimentare l'utilizzo di questi dati nella procedura di risposta di sicurezza, ci

farebbe piacere sentirti dire. Inviare commenti, domande o dubbi a umbrella-support@cisco.com e fare riferimento a questo articolo.

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).