Scaricare i log da Umbrella Log Management in AWS S3

Sommario

Introduzione

Questo documento descrive come scaricare i log da Umbrella Log Management in AWS S3.

Panoramica

Una volta configurato e verificato il corretto funzionamento di Log Management in Amazon S3, è possibile iniziare a scaricare e archiviare automaticamente i log all'interno dell'infrastruttura di rete, per la conservazione o l'utilizzo (o entrambi).

A tal fine, abbiamo delineato un approccio utilizzando s3tools di http://s3tools.org. s3tools utilizza l'utilità della riga di comando s3cmd per Linux o OS/X. Esistono altri strumenti che possono eseguire una funzione simile per gli utenti di Windows:

- Per uno strumento da riga di comando, è possibile scaricare qui un eseguibile da riga di comando di piccole dimensioni.
- Se si preferisce un'interfaccia grafica, controllare S3 Browser (https://s3browser.com/), anche se non stiamo trattando come usarla perché l'interfaccia grafica non è scriptable per automatizzare il processo. In questo documento viene descritto come configurare entrambi gli strumenti della riga di comando. Se lo si desidera, è possibile utilizzare le informazioni della fase 1 per configurare l'applicazione s3browser.

Iniziare scaricando lo strumento per il sistema operativo che si intende utilizzare. Per il momento,

stiamo solo coprendo s3cmd per OS/X e Linux, anche se i passaggi per accedere al bucket e scaricare i dati sono effettivamente gli stessi per Windows.

Prendere il programma di installazione da s3tools qui.

Poiché non è necessario installare il programma per eseguire la riga di comando, è sufficiente estrarre il pacchetto scaricato.

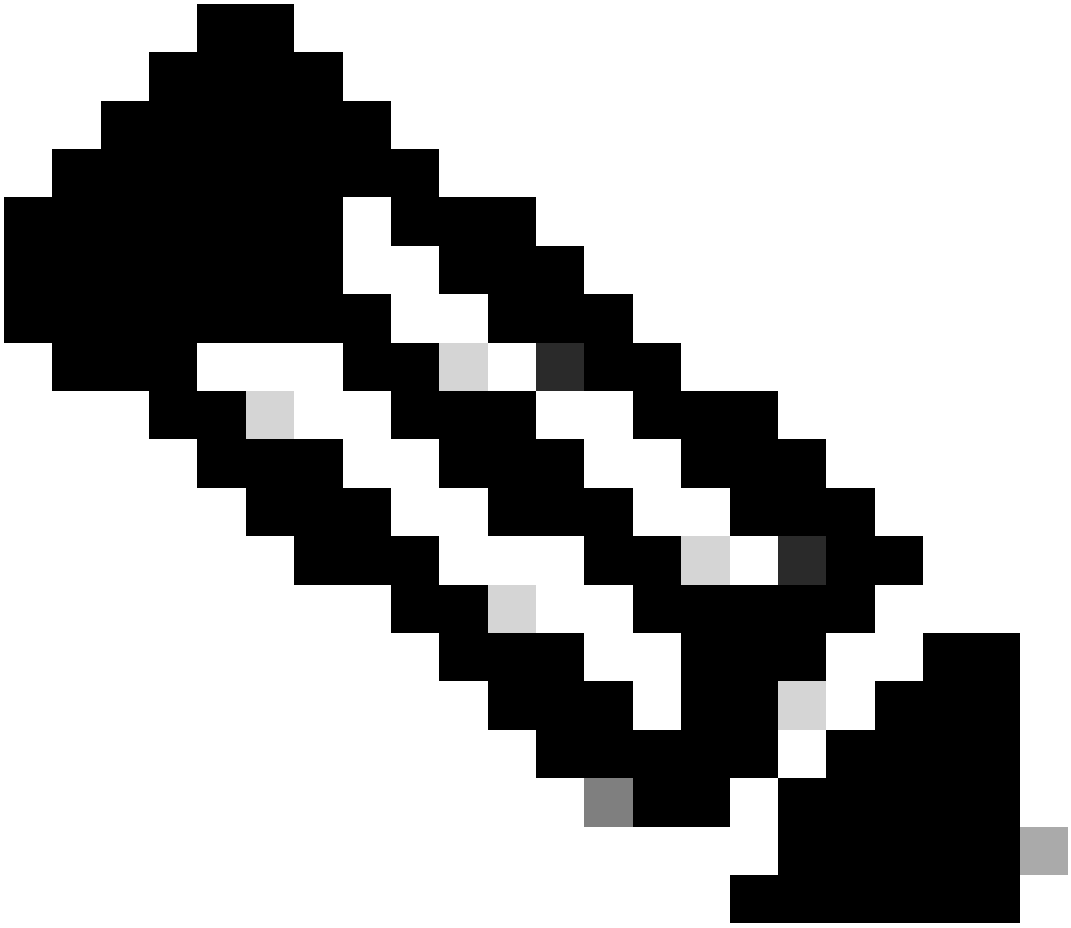
Fase 1: Configurazione delle credenziali di sicurezza in AWS

Passaggio 1

1. Aggiungere una chiave di accesso all'account di Amazon Web Services per consentire l'accesso remoto allo strumento locale e la possibilità di caricare, scaricare e modificare 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. Un prompt indica di utilizzare le procedure ottimali di Amazon e di creare un utente di Gestione identità e accesso 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 qui.

Passaggio 2

1. Fare clic su Introduzione agli utenti IAM per creare un utente IAM con accesso al bucket S3. Passare a una schermata in cui è possibile creare un utente IAM.
2. Fare clic su Crea nuovi utenti e compilare i campi.
3. Dopo aver creato l'account utente, hai solo la possibilità di recuperare due informazioni critiche contenenti le credenziali di protezione utente Amazon. Ti consigliamo di scaricarli 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 della chiave di accesso che la chiave di accesso segreta, come sarà necessario in un passaggio successivo.



Nota: L'account utente non può contenere spazi.

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. Dovrebbero essere visualizzati due risultati: "AmazonS3FullAccess" e "AmazonS3ReadOnlyAccess".
3. Selezionare AmazonS3FullAccess, quindi fare clic su Allega criterio.

Fase 2: Configurazione di uno strumento per il download dei registri DNS dal bucket

s3cmd per MacOS e Linux

1. Andare al percorso estratto dal s3cmd nella fase precedente e da Terminale, digitare:

```
./s3cmd --configure
```

Verrà visualizzata una richiesta di immissione delle credenziali di sicurezza:

Immettete nuovi valori o accettate i valori di default tra parentesi con Invio.

Per una descrizione dettagliata di tutte le opzioni, consultare il manuale dell'utente.

La chiave di accesso e la chiave segreta sono gli identificatori per Amazon S3. Lasciarli vuoti per l'utilizzo delle variabili env.

Access Key [CODICE DI ACCESSO]:

Secret Key [CHIAVE SEGRETA]:

2. Successivamente, verrà visualizzata una serie di domande relative alla configurazione dell'accesso al bucket. In questo caso, non viene impostata una password di crittografia (GPG) e non viene utilizzato HTTPS o un server proxy. Se la rete o le preferenze sono diverse, compilare i campi obbligatori:

Default Region [US]:

La password di crittografia viene utilizzata per proteggere i file dalla lettura da parte di persone non autorizzate durante il trasferimento a S3

Password di crittografia:

Path to GPG program [None]:

Quando si utilizza il protocollo HTTPS sicuro, tutte le comunicazioni con i server Amazon S3 sono protette dalle intercettazioni di terze parti. Questo metodo è

più lento del semplice HTTP e può essere trasmesso solo con Python 2.7 o versioni successive

Use HTTPS protocol [No]:

In alcune reti l'accesso a Internet deve passare attraverso un proxy HTTP.

Se non è possibile collegarsi direttamente a S3, provare a impostarlo qui

Nome server proxy HTTP:

Dopo aver immesso le impostazioni specifiche della rete o qualsiasi crittografia, è possibile esaminare:

Nuove impostazioni

Chiave di accesso: CHIAVE

Chiave segreta: CHIAVE SEGRETA

Area predefinita: STATI UNITI

Password di crittografia:

Percorso del programma GPG: Nessuna

Usa protocollo HTTPS: Falso

Nome server proxy HTTP:

Porta server proxy HTTP: 0

Infine, viene richiesto di eseguire il test e, se l'operazione ha esito positivo, salvare le impostazioni:

Verificare l'accesso con le credenziali fornite? [S/n] s

Attendere. Tentativo di elencare tutti i bucket...

Successo. La tua chiave di accesso e la chiave segreta hanno funzionato bene ·

Verifica del funzionamento della crittografia in corso...

Non configurato. Non importa.

Salvare le impostazioni? [S/N]

Eseguibile della riga di comando di Windows (s3.exe)

Dopo aver scaricato lo strumento (https://s3.codeplex.com/releases/view/47595), copiare il file exe nella cartella di lavoro preferita e dal prompt dei comandi digitare questo comando, sostituendo la chiave di accesso e il segreto:

<#root>

s3 auth [

```
]
```

Per ulteriori informazioni sulla sintassi di autenticazione, leggere qui.

Fase 3: Verifica del download dei file dal bucket

Passaggio 1: Verifica il download

s3cmd per OS/X e Linux

Dal terminale, eseguire questo comando dove "my-organization-name-log-bucket" è il nome del bucket già configurato nella sezione Gestione dei log del dashboard Umbrella. In questo esempio, viene eseguito dalla cartella che contiene l'eseguibile s3cmd e i file vengono recapitati nello stesso percorso, ma è possibile modificare questi valori:

<#root>

```
./s3cmd sync s3://my-organization-name-log-bucket ./
```

Se esiste una differenza tra i file nel bucket e i file nel percorso di destinazione su disco, la sincronizzazione dovrebbe scaricare i file mancanti o aggiornati. Il primo file recuperato deve essere il file README che viene in genere caricato:

./s3cmd sync s3://nome-organizzazione-registro-bucket ./

s3://my-organization-name-log-bucket/README_FROM_UMBRELLA.txt -> <fdopen> [1 di 1]

1800 di 1800 100% in 0s 15,00 kB/s completato

Done. Scaricati 1800 byte in 1,0 secondi, 1800,00 MB/s

Verranno scaricati anche tutti i file di log presenti. Spetta all'utente impostare un processo cron per pianificare questa funzione su base regolare, ma ora dovrebbe essere possibile scaricare automaticamente tutti i file di log nuovi o modificati nel bucket in un percorso locale per la conservazione a lungo termine.

Eseguibile della riga di comando di Windows (s3.exe)

Dal prompt dei comandi, eseguire questo comando dove 'nome-organizzazione-registro-

bucket' è il nome del bucket già configurato nella sezione Gestione log del dashboard Umbrella. In questo esempio, tutti i file nel bucket (definiti con il carattere jolly asterisco) vengono scaricati nella cartella \dnslogbackups\.

<#root>

```
s3 get my-organization-name-log-bucket/* c:\dnslogbackups\
```

Per ulteriori informazioni sulla sintassi di questo comando, vedere qui.

Passaggio 2: Automatizza il download

Una volta verificata la sintassi e verificato il funzionamento previsto, copiare le istruzioni in uno script di impostazione di un lavoro cron (OS X / Linux) o di un'operazione pianificata (Windows) oppure utilizzare qualsiasi altro strumento di automazione delle operazioni disponibile. È inoltre possibile utilizzare gli strumenti per rimuovere i file dal bucket dopo averli scaricati per liberare spazio nell'istanza S3. È consigliabile consultare la documentazione relativa allo strumento utilizzato per individuare le soluzioni più adatte alle regole di conservazione dei dati.

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).