Descargar registros de Umbrella Log Management en AWS S3

Contenido

Introducción

Este documento describe cómo descargar registros de Umbrella Log Management en AWS S3.

Overview

Una vez que haya configurado y probado que Log Management en Amazon S3 funciona correctamente, es posible que desee comenzar a descargar y almacenar automáticamente los registros dentro de su infraestructura de red, ya sea para su retención o consumo (o ambos).

Para ello, hemos esbozado un enfoque que utiliza s3tools de http://s3tools.org. s3tools utiliza la utilidad de línea de comandos s3cmd para Linux o OS/X. Existen otras herramientas que pueden lograr una función similar para los usuarios de Windows:

- Para una herramienta de línea de comandos, puede descargar un pequeño ejecutable de línea de comandos aquí.
- Si prefiere una interfaz gráfica, consulte S3 Browser (https://s3browser.com/), aunque no se trata de cómo utilizarlo porque la interfaz gráfica no es programable para automatizar el proceso. En este artículo se proporcionan los pasos necesarios para configurar ambas herramientas de línea de comandos. Puede utilizar la información de la etapa 1 para configurar la aplicación s3browser si lo prefiere.

Comience descargando la herramienta para el sistema operativo que desea utilizar. Por ahora, solo estamos cubriendo s3cmd para OS/X y Linux, aunque los pasos para acceder a su cubeta y descargar los datos son efectivamente los mismos para Windows.

Agarre el instalador de s3tools aquí.

El instalador no requiere que instale el programa para ejecutar la línea de comandos, así que simplemente extraiga el paquete que ha descargado.

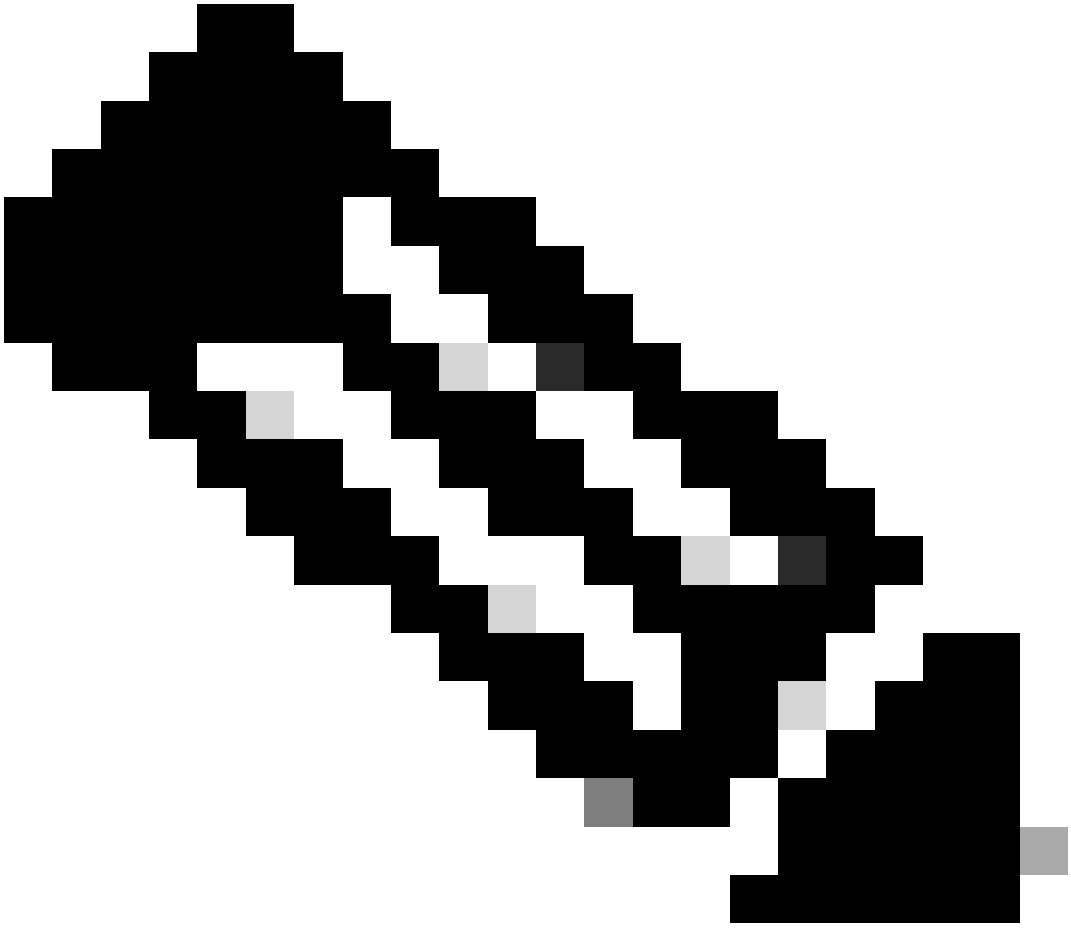
Etapa 1: Configuración de sus credenciales de seguridad en AWS

Paso 1

1. Agregue una clave de acceso a su cuenta de Amazon Web Services para permitir el acceso remoto a su herramienta local y la capacidad de cargar, descargar y modificar archivos en S3. Inicie sesión en AWS y haga clic en el nombre de su cuenta en la esquina superior derecha. En el menú desplegable, seleccione Security Credentials.
2. Un mensaje le indica que utilice las mejores prácticas de Amazon y que cree un usuario de Administración de acceso e identidad (IAM) de AWS. Básicamente, un usuario de IAM se asegura de que la cuenta que s3cmd utiliza para acceder a su cubeta no sea la cuenta principal (por ejemplo, su cuenta) para toda su configuración de S3. Al crear usuarios IAM individuales para las personas que acceden a su cuenta, puede proporcionar a cada usuario IAM un conjunto único de credenciales de seguridad. También puede conceder diferentes permisos a cada usuario de IAM. Si es necesario, puede cambiar o revocar los permisos de un usuario de IAM en cualquier momento.
   Para obtener más información sobre los usuarios de IAM y las prácticas recomendadas de AWS, lea aquí.

Paso 2

1. Haga clic en Get Started with IAM Users para crear un usuario IAM con acceso a su cubeta S3. Vaya a una pantalla en la que puede crear un usuario de IAM.
2. Haga clic en Create New Users y rellene los campos.
3. Después de crear la cuenta de usuario, solo tiene una oportunidad de obtener dos piezas críticas de información que contienen sus credenciales de seguridad de usuario de Amazon. Le recomendamos que descargue estos archivos con el botón de la parte inferior derecha para realizar una copia de seguridad. No están disponibles después de esta fase de la configuración. Asegúrese de anotar su ID de clave de acceso y la clave de acceso secreta, ya que las necesitamos en un paso posterior.



Nota: La cuenta de usuario no puede contener espacios.

Paso 3

1. A continuación, desea agregar una política para el usuario de IAM de modo que tenga acceso a la cubeta de S3. Haga clic en el usuario que acaba de crear y, a continuación, desplácese hacia abajo por las propiedades de los usuarios hasta que aparezca el botón Adjuntar directiva.
2. Haga clic en Adjuntar política, luego ingrese 's3' en el filtro de tipo de política. Esto debería mostrar dos resultados "AmazonS3FullAccess" y "AmazonS3ReadOnlyAccess".
3. Seleccione AmazonS3FullAccess y, a continuación, haga clic en Adjuntar directiva.

Etapa 2: Configuración de una Herramienta para Descargar Registros DNS desde el Bucket

s3cmd para MacOS y Linux

1. Vaya a la ruta que ha extraído del s3cmd en la etapa anterior y desde Terminal, escriba:

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

   Esto debería llevarle a un mensaje solicitándole que proporcione sus credenciales de seguridad:

Introduzca nuevos valores o acepte los valores por defecto entre paréntesis con Enter (Introducir).

Consulte el manual del usuario para obtener una descripción detallada de todas las opciones.

La clave de acceso y la clave secreta son sus identificadores para Amazon S3. Déjelos vacíos para utilizar las variables env.

Clave de acceso [YOUR ACCESS KEY]:

Clave secreta [SU CLAVE SECRETA]:

2. A continuación, se le hará una serie de preguntas sobre cómo le gustaría configurar el acceso a su cubeta. En este caso, no estamos configurando una contraseña de cifrado (GPG) y no estamos utilizando HTTPS o un servidor proxy. Si la red o las preferencias son distintas, rellene los campos obligatorios:

Región predeterminada [US]:

La contraseña de cifrado se utiliza para evitar que personas no autorizadas lean los archivos durante la transferencia a S3

Contraseña de cifrado:

Ruta al programa GPG [None]:

Cuando se utiliza el protocolo HTTPS seguro, toda la comunicación con los servidores Amazon S3 está protegida contra la intercepción de terceros. Este método es

más lento que el HTTP normal y solo se puede habilitar para proxy con Python 2.7 o posterior

Usar protocolo HTTPS [No]:

En algunas redes, todo el acceso a Internet debe pasar por un proxy HTTP.

Intente configurarlo aquí si no puede conectarse directamente a S3

Nombre del servidor proxy HTTP:

Después de introducir cualquier configuración específica de la red o cualquier cifrado, tiene la oportunidad de revisar:

Nuevos parámetros:

Clave de acceso: SU CLAVE

Clave secreta: SU CLAVE SECRETA

Región predeterminada: US

Contraseña de cifrado:

Ruta al programa GPG: Ninguno

Usar protocolo HTTPS: Falso

Nombre del servidor proxy HTTP:

Puerto del servidor proxy HTTP: 0

Por último, se le pedirá que pruebe y, si es correcto, guarde los parámetros:

¿Desea probar el acceso con las credenciales proporcionadas? [S/n] y

Espere; intentando enumerar todos los depósitos...

Éxito. La clave de acceso y la clave secreta funcionaban correctamente ��

Comprobando que el cifrado funciona...

No configurado. No importa.

¿Guardar parámetros? [s/N]

Ejecutable de línea de comandos de Windows (s3.exe)

Después de descargar la herramienta (https://s3.codeplex.com/releases/view/47595), copie el archivo .exe en la carpeta de trabajo que desee y, desde el símbolo del sistema, escriba esto, sustituyendo la clave de acceso y el secreto:

<#root>

```
s3 auth [
```

```
]
```

Para obtener más información sobre la sintaxis de autenticación, lea aquí.

Etapa 3: Prueba de la descarga de archivos desde el depósito

Paso 1: Pruebe la descarga

s3cmd para OS/X y Linux

Desde el terminal, ejecute este comando donde "my-organization-name-log-bucket" es el nombre de su depósito ya configurado en la parte Log Management del panel de Umbrella. En este ejemplo, se ejecuta desde la carpeta que contiene el ejecutable s3cmd y los archivos se envían a la misma ruta, pero se pueden cambiar:

<#root>

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

Si hay una diferencia entre los archivos de la cubeta y los archivos de la ruta de destino del disco, la sincronización debe descargar los archivos que faltan o los que se han actualizado. El primer archivo recuperado debe ser el archivo README que se carga normalmente:

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

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

1800 de 1800 100% en 0 s 15,00 kB/s realizado

Listo. 1800 bytes descargados en 1,0 segundos, 1800,00 B/s

También se descargan todos los archivos de registro presentes. Depende de usted si desea configurar un trabajo cron para programar esta función de forma regular, pero ahora debería poder descargar automáticamente cualquier archivo de registro nuevo o modificado en su cubeta a una ruta local para la retención a largo plazo.

Ejecutable de línea de comandos de Windows (s3.exe)

Desde el símbolo del sistema, ejecute este comando donde 'my-organization-name-log-bucket' es el nombre de su depósito ya configurado en la parte de Gestión de registros del

panel de Umbrella. En este ejemplo, todos los archivos de la cubeta (definida con el comodín asterisco) se descargan en la carpeta \dnslogbackups\.

<#root>

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

Para obtener más información sobre la sintaxis de este comando, lea aquí.

Paso 2: Automatizar la descarga

Una vez que la sintaxis ha sido probada y funciona según lo esperado, copie las instrucciones en una configuración de script, un trabajo cron (OS X / Linux) o una tarea programada (Windows) o utilice cualquier otra herramienta de automatización de tareas que pueda tener a su disposición. También es posible utilizar las herramientas para eliminar archivos de su cubeta después de que los haya descargado para liberar espacio en su instancia S3. Le animamos a que consulte la documentación de la herramienta que está utilizando para ver qué puede funcionar mejor para su política de retención de datos.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).