Configuración de Splunk con un Bucket S3 autoadministrado

Contenido

Introducción

Este documento describe cómo configurar Splunk con una cubeta S3 autogestionada.

Overview

Splunk es una herramienta común para el análisis de registros. Proporciona una interfaz potente para analizar grandes fragmentos de datos, como los registros proporcionados por Cisco Umbrella para el tráfico DNS de su organización.

Este artículo describe los aspectos básicos de la configuración y ejecución de Splunk para que pueda extraer los registros de su cubeta S3 y consumirlos. Hay dos etapas principales, una es configurar las credenciales de seguridad de AWS S3 para permitir el acceso de Splunk a los registros, y la segunda es configurar Splunk para que apunte a su cubeta.

La documentación para el Splunk Add-on para AWS S3 está aquí, parte de la cual ha sido copiada textualmente en este documento. Para preguntas específicas relacionadas con la configuración de Splunk, consulte http://docs.splunk.com/Documentation/AddOns/latest/AWS/Description

Este artículo tiene estas secciones:

Prerequisites

El complemento Splunk para Amazon Web Services es compatible con estas plataformas.

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

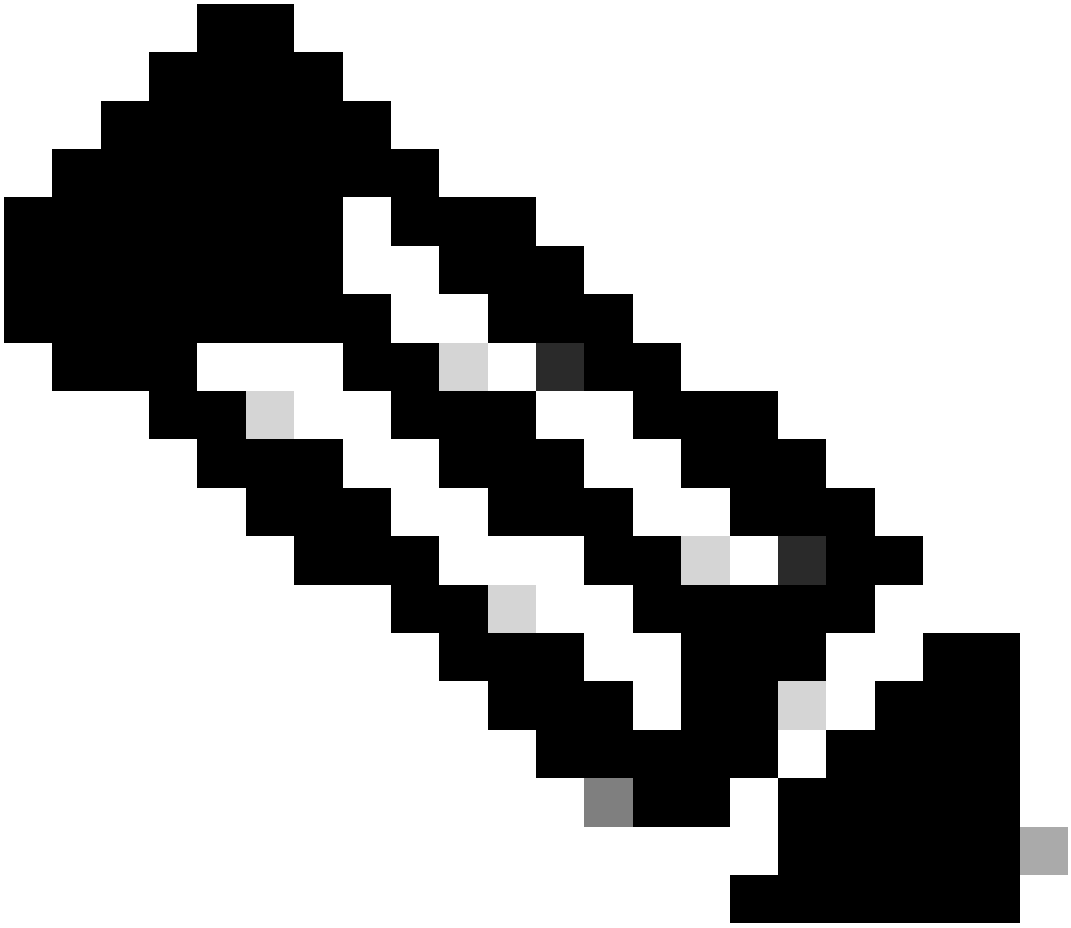
Requisitos del sistema Splunk Enterprise

Dado que este complemento se ejecuta en Splunk Enterprise, se aplican todos los requisitos del sistema de Splunk Enterprise. Consulte el manual de instalación de "Requisitos del sistema" en la documentación de Splunk Enterprise. Estas instrucciones son para la versión 6.2.1 de Splunk Enterprise.

Requisitos generales

Este documento asume que su cubeta Amazon AWS S3 se ha configurado en el panel de Umbrella (Admin> Log Management) y se muestra en verde con los registros recientes que se han cargado. Para obtener más información sobre la administración de registros, consulte Administración de registros de Cisco Umbrella en Amazon S3.

Etapa 1: Configuración de sus credenciales de seguridad en AWS



Nota: Estos pasos son los mismos que los descritos en el artículo que describe cómo configurar una herramienta para descargar los registros de su cubeta (Cómo: Descarga de registros de Cisco Umbrella Log Management en AWS S3). Si ya ha realizado esos pasos, puede simplemente saltar al paso 2, aunque necesita las credenciales de seguridad de su usuario de IAM para autenticar el plugin Splunk en su cubeta.

Paso 1

1. Añada una clave de acceso a su cuenta de Amazon Web Services para permitir el acceso remoto a su herramienta local y permitir 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 Credenciales de seguridad.
2. Se le solicita que utilice las mejores prácticas de Amazon y 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: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Paso 2

1. Cree un usuario IAM para acceder a su cubeta S3 haciendo clic en Get Started with IAM Users. Accederá a una pantalla en la que podrá crear un usuario de IAM.
2. Haga clic en Create New Users, a continuación, rellene los campos. Tenga en cuenta que la cuenta de usuario no puede contener espacios.
3. Después de crear la cuenta de usuario, solo se le da una oportunidad de obtener dos piezas críticas de información que contienen sus credenciales de seguridad de usuario de Amazon. Recomendamos encarecidamente que descargue estas con el botón de la parte inferior derecha para realizar una copia de seguridad. No estarán disponibles después de esta fase de la configuración. Asegúrese de anotar tanto su ID de clave de acceso como su Clave de acceso secreta, ya que los necesitamos más adelante al configurar Splunk.

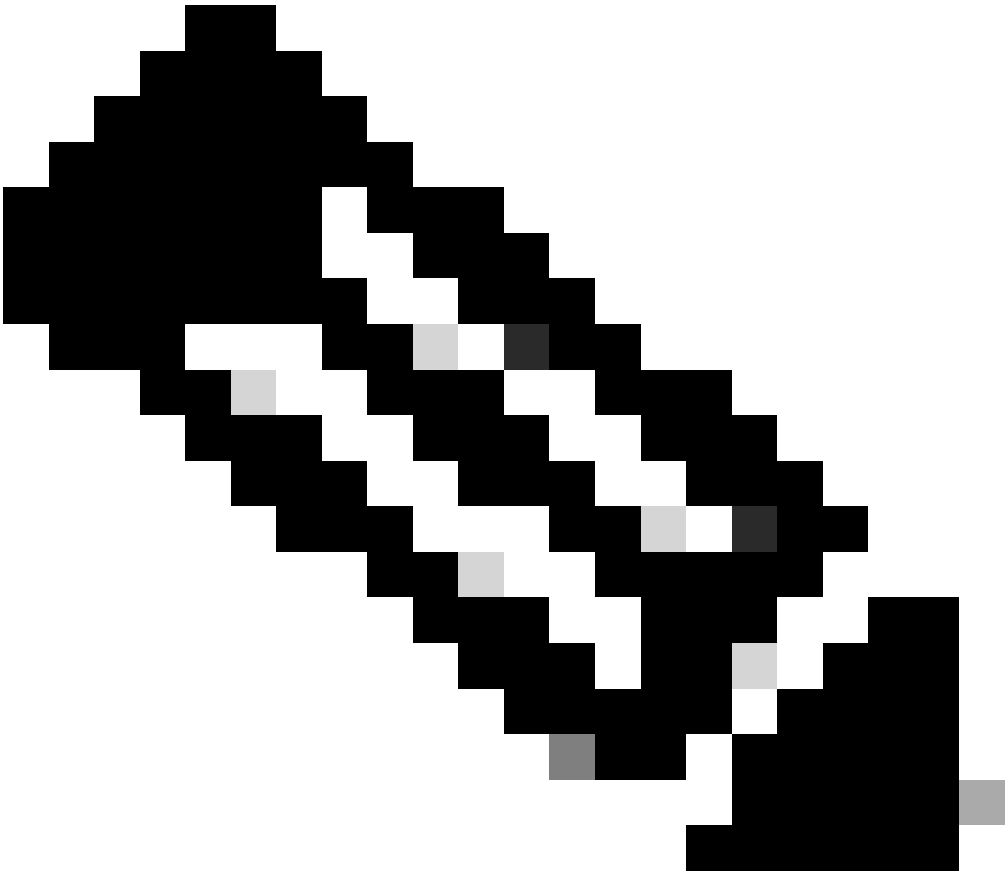
Paso 3

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 muestra dos resultados: "AmazonS3FullAccess" y "AmazonS3ReadOnlyAccess".
3. Seleccione AmazonS3FullAccess y, a continuación, haga clic en Adjuntar directiva.

Etapa 2: Configuración de Splunk para extraer datos de registro DNS de la cubeta S3

Paso 1: Configuración de Splunk para extraer datos de registro DNS desde la cubeta S3 autogestionada

1. Comience instalando el "complemento Splunk para Amazon Web Services" en su instancia de Splunk. Abra el panel de Splunk y haga clic en Aplicaciones, o haga clic en Aplicaciones de Splunk si aparece en el panel. Una vez en la sección Aplicaciones, escriba "s3" en la ventana de búsqueda para encontrar "Splunk Add-on for Amazon Web Services" e instale la aplicación.



Nota: Es probable que tenga que reiniciar Splunk durante la instalación. Una vez instalado, verá Splunk Add-on for AWS con el nombre de carpeta 'Splunk_TA_aws' ahora listado en Aplicaciones.

2. Haga clic en Configurar para configurar la aplicación. Este es el punto en el que necesita las credenciales de seguridad de la etapa 1 de esta documentación.
   La configuración requiere que se introduzcan estos campos:

   - Un nombre descriptivo: el nombre que utiliza para hacer referencia a esta integración
   - Su ID de clave de cuenta de AWS (desde la etapa 1)
   - Su contraseña (la clave secreta de su cuenta de AWS, también de la etapa 1)

   También puede configurar cualquier información de proxy local si se requiere para que Splunk llegue a AWS, así como ajustar el registro. La pantalla de configuración tiene el siguiente aspecto:
   3. Una vez que haya agregado la información relevante, haga clic en Guardar y el complemento Splunk para Amazon Web Services esté completamente configurado.

Etapa 3: Configuración de entradas de datos para Splunk

1. A continuación, desea configurar la entrada de datos para Amazon Web Services S3. Navegue hasta Configuraciones > Datos > Entradas de datos y bajo Entradas locales, ahora verá una lista de varias entradas de Amazon, incluida S3, al final de la lista.
2. Haga clic en AWS S3 para configurar la entrada.
3. Haga clic en New.
4. Se le solicita que proporcione la siguiente información:

    - Introduzca un nombre descriptivo para la integración de S3.
    - Seleccione su Cuenta AWS del menú desplegable. Este es el nombre descriptivo que ha proporcionado en el paso 1.
    - Seleccione la cubeta S3 en el menú desplegable. Se trata del nombre del depósito tal y como se especifica en el panel de Umbrella (Configuración > Gestión de registros).
    - Seleccione el nombre de la clave S3 en el menú desplegable. Se enumeran todos los elementos de la cubeta. Recomendamos seleccionar el directorio de nivel superior \dns-logs\ , que incluye todos los archivos y directorios que contiene.
    - Hay varias opciones bajo "Configuración del sistema de mensajes", recomendamos dejarlas tal cual: configuración predeterminada.
    - Hay opciones adicionales en "Más configuraciones". Cabe destacar el "Tipo de origen", que es aws:s3 de forma predeterminada. Recomendamos dejar esto tal cual, pero si lo cambia, el filtro para sus registros en la Búsqueda cambia de lo que se describe en el Paso 3 de estas instrucciones.

Rellene los detalles y los datos introducidos serán similares a los siguientes:

4. Haga clic en Siguiente para finalizar sus detalles.
   Accederá a una pantalla que indica que la entrada se ha creado correctamente

Paso 3

Realice una búsqueda rápida para ver si los datos se están importando correctamente. Solo pega sourcetype="aws:s3" en la ventana de búsqueda en la parte superior derecha y luego selecciona "Open sourcetype="aws:s3" en la búsqueda

Esto le lleva a una pantalla similar a la que muestra los eventos de los registros DNS de su organización. En este caso, el servicio móvil Cisco Umbrella está bloqueando las redes sociales en un iPhone. También puede utilizar el origen del nombre de archivo para filtrar un lote concreto de registros.

Después de este punto, el trabajo cron en segundo plano continúa ejecutándose y extrae los conjuntos más recientes de la información de registro de su cubeta.

Hay mucho más que puede hacer con Splunk más allá de lo que se ha descrito en este artículo, y si ha tenido la oportunidad de experimentar con el uso de estos datos en su procedimiento de respuesta de seguridad, nos encantaría saber de usted. Envíe cualquier comentario, pregunta o inquietud a umbrella-support@cisco.com y haga referencia a este artículo.

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).