Transferencia del registro WSA a un servidor remoto de SCP

Contenido

Introducción

Este documento describe cómo transferir los registros del dispositivo de seguridad de la red de Cisco (WSA) a un servidor remoto del Secure Copy (SCP). Usted puede configurar los registros WSA, tales como registros del acceso y de la autenticación, para remitirlos a un servidor externo con el protocolo de SCP cuando los registros derriban o envuelven.

La información en este documento describe cómo configurar las reglas de la rotación del registro así como las claves del Secure Shell (SSH) que se requieren para una transferencia acertada a un servidor de SCP.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

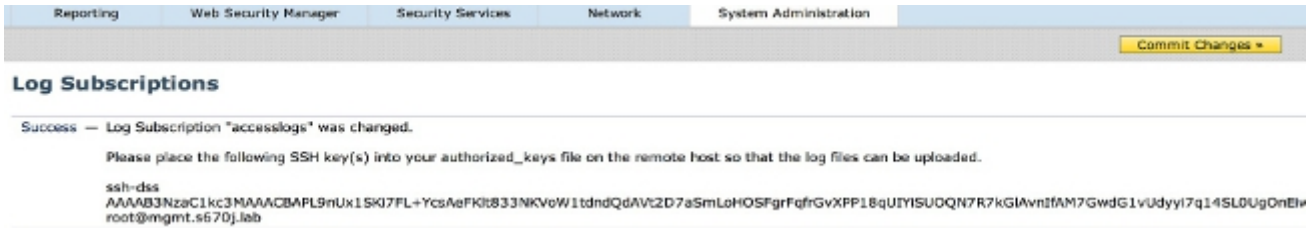
Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Complete estos pasos para configurar los registros WSA para poderlos retreived con SCP en un servidor remoto:

1. Registro en la red GUI WSA.
2. Navegue a las **suscripciones de la administración del sistema** > del **registro**.
3. Seleccione el nombre de los registros para los cuales usted desea de configurar este método de la extracción, tal como **registros del acceso**.
4. En el campo del método de la extracción, elija **SCP en el servidor remoto**.
5. Ingrese el nombre del host del SCP o el IP Address del servidor del SCP.
6. Ingrese el número del puerto del SCP.
   Note: La configuración predeterminada es el **puerto 22**.
7. Ingrese el nombre de ruta completa del directorio objetivo del servidor del SCP al cual el registros serán transferidos.
8. Ingrese el nombre de usuario para el usuario autenticado del servidor del SCP.
9. Si usted quiere explorar automáticamente la clave de host o ingresar manualmente la clave de host, después habilite **marcar de la clave de host**.
10. Haga clic en Submit (Enviar). La clave de SSH que usted pondrá en los **authorized_keys del** servidor de SCP el archivo debe ahora aparecer cerca del top de la página de la **suscripción del registro del editar**. Aquí está un ejemplo de un successfulmessage del WSA:



11. **Cambios del cometer del** tecleo.
12. Si SCP separa es Linux o servidor Unix o una máquina de Macintosh, después pega las claves de SSH del WSA en los **authorized_keys** clasifía localizado en el directorio de SSH:

    Navegue a los **usuarios > al <username> > al** directorio **.ssh**.

    Pegue la clave WSA SSH en los **authorized_keys** clasifían y salvan los cambios.
    Note: Usted debe crear manualmente los **authorized_keys** clasifía si uno no existe en el directorio de SSH.

Verificación

Complete estos pasos para verificar que los registros están transferidos con éxito al servidor de SCP:

1. Navegue a la página de las **suscripciones del registro** WSA.
2. En la columna de la **renovación**, elija el registro que usted configuró para la extracción de SCP.
3. **Ahora** localice y haga clic la **renovación**.
4. Navegue a la carpeta del servidor de SCP que usted configuró para la extracción del registro y verifique que los registros están transferidos a esa ubicación.

Complete estos pasos para monitorear la transferencia del registro al servidor de SCP del WSA:

1. Registro en el WSA CLI vía SSH.
2. Ingrese el **comando grep**.
3. Ingrese el número apropiado para el registro que usted quiere monitorear. Por ejemplo, ingrese **31 de la** lista del grep para los **system_logs**.
4. Ingrese el **scp** en el *ingresar la expresión normal al* prompt del *grep* para filtrar los registros de modo que usted pueda monitorear solamente las transacciones del SCP.
5. ¿Ingrese **Y** en *usted quisieran que esta búsqueda fuera sin diferenciación entre mayúsculas y minúsculas?* mensaje
6. ¿Ingrese **Y** en *usted quieren atar los registros?* mensaje
7. ¿Ingrese **N** en *usted quieren paginar la salida?* mensaje El WSA entonces enumera las transacciones de SCP en el tiempo real. Aquí está un ejemplo de las transacciones acertadas de SCP de los system_logs WSA:

```
Wed Jun 11 15:06:14 2014 Info: Push success for subscription <the name of the log>:
Log aclog@20140611T145613.s pushed to remote host <IP address of the SCP Server>:22
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.