Transferência do log WSA a um server remoto SCP

Índice

Introdução

Este documento descreve como transferir logs da ferramenta de segurança da Web de Cisco (WSA) a um server remoto do Secure Copy (SCP). Você pode configurar os logs WSA, tais como logs do acesso e da autenticação, de modo que estejam enviados a um servidor interno com protocolo SCP quando os logs se viram ou se envolvem.

A informação neste documento descreve como configurar as regras da rotação do log assim como as chaves do Shell Seguro (ssh) que são exigidas para transferência bem sucedida a um server SCP.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Termine estas etapas a fim configurar os logs WSA de modo que possam ser retreived com SCP em um servidor remoto:

1. Log na Web GUI WSA.
2. Navegue às **assinaturas da administração do sistema >** do **log**.
3. Selecione o nome dos logs para que você deseja configurar este método da recuperação, tal como **logs do acesso**.
4. No campo do método da recuperação, escolha o **SCP no servidor remoto**.
5. Incorpore o nome de host SCP ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do server SCP.
6. Entre no número de porta SCP.
   Nota: A configuração padrão é a **porta 22**.
7. Dê entrada com o nome do caminho cheio do diretório de destino do server SCP a que o os logs serão transferidos.
8. Incorpore o username para o usuário autenticado do server SCP.
9. Se você quer fazer a varredura automaticamente da chave Host ou incorporar manualmente a chave Host, a seguir permita a **verificação da chave Host**.
10. Clique em Submit. A chave SSH que você colocará em **authorized_keys do** server SCP o arquivo deve agora aparecer perto da parte superior da página da **assinatura do log da edição**. Está aqui um exemplo de um successfulmessage do WSA:
11. O clique **compromete mudanças**.
12. Se o SCP separa é Linux ou um servidor Unix ou uma máquina de Macintosh, a seguir cola as chaves SSH do WSA nos **authorized_keys** arquiva localizado no diretório SSH:

    Navegue aos **usuários > ao <username> > ao** diretório **.ssh**.

    Cole a chave WSA SSH nos **authorized_keys** arquivam e salvar as mudanças.
    Nota: Você deve manualmente criar **authorized_keys** arquiva se um não existe no diretório SSH.

Verificar

Termine estas etapas a fim verificar que os logs estão transferidos com sucesso ao server SCP:

1. Navegue à página das **assinaturas do log** WSA.

2. Na coluna do **derrubamento**, escolha o log que você configurou para a recuperação SCP.

3. Encontre e clique o **derrubamento agora**.

4. Navegue ao dobrador do server SCP que você configurou para a recuperação do log e verifique que os logs estão transferidos a esse lugar.

Termine estas etapas a fim monitorar transferência do log ao server SCP do WSA:

1. Log no WSA CLI através do SSH.

2. Inscreva o **comando grep**.

3. Incorpore o número apropriado para o log que você quer monitorar. Por exemplo, incorpore **31 da** lista do grep para os **system_logs**.

4. Incorpore o **scp na** *entrada a expressão regular à* alerta do *grep* a fim filtrar os logs de modo que você possa monitorar somente as transações SCP.

5. Incorpore **Y no** *você querem esta busca ser não diferenciando maiúsculas e minúsculas?* prompt.

6. Incorpore **Y no** *você querem atar os logs?* prompt.

7. Incorpore **N no** *você querem paginar a saída?* prompt. O WSA alista então as transações SCP no tempo real. Está aqui um exemplo de transações bem sucedidas SCP dos 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.