원격 SCP 서버로 WSA 로그 전송

목차

소개

이 문서에서는 Cisco WSA(Web Security Appliance)에서 원격 SCP(Secure Copy) 서버로 로그를 전송하는 방법에 대해 설명합니다.WSA 로그(예: 액세스 및 인증 로그)를 구성하여 로그가 롤오버 또는 래핑될 때 SCP 프로토콜을 사용하여 외부 서버로 전달되도록 할 수 있습니다.

이 문서의 정보는 SCP 서버로 성공적으로 전송하는 데 필요한 SSH(Secure Shell) 키와 로그 순환 규칙을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

원격 서버에서 SCP를 사용하여 수신할 수 있도록 WSA 로그를 구성하려면 다음 단계를 완료합니다.

1. WSA 웹 GUI에 로그인합니다.

2. System **Administration(시스템 관리)** > Log Subscriptions(**로그 서브스크립션)로 이동합니다**.

3. 이 검색 방법을 구성하려는 로그(예: **액세스 로그)**의 이름을 **선택합니다**.

4. Retrieval Method(검색 방법) 필드에서 **Remote Server(원격 서버)에서 SCP를** 선택합니다.

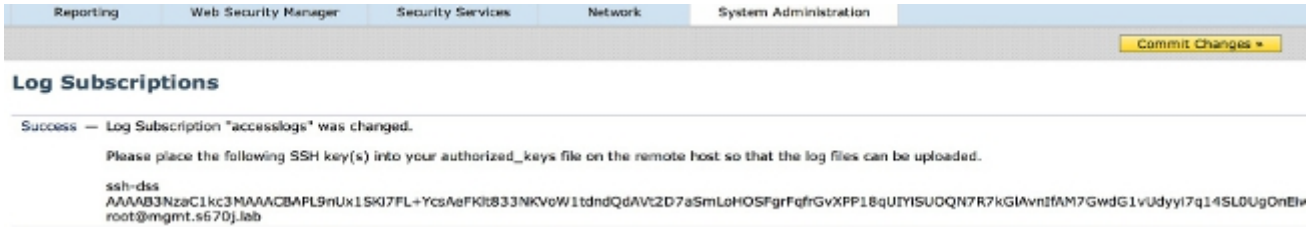
5. SCP 서버의 SCP 호스트 이름 또는 IP 주소를 입력합니다.

6. SCP 포트 번호를 입력합니다.
   참고:기본 설정은 **포트 22입니다**.
7. 로그를 전송할 SCP 서버 대상 디렉토리의 전체 경로 이름을 입력합니다.

8. SCP 서버 인증 사용자의 사용자 이름을 입력합니다.

9. 호스트 키를 자동으로 스캔하거나 수동으로 호스트 키를 입력하려면 Host **Key Checking을 활성화합니다**.

10. Submit(제출)**을 클릭합니다**.이제 SCP 서버 authorized_**keys** 파일에 넣을 SSH 키가 **Edit Log Subscription** 페이지 상단 근처에 나타나야 합니다.다음은 WSA에서 성공한 메시지의 예입니다.



11. Commit **Changes를 클릭합니다**.

12. SCP 서버가 Linux, Unix 서버 또는 Macintosh 시스템인 경우 WSA의 SSH 키를 SSH 디렉토리에 있는 **authorized_keys** 파일에 붙여넣습니다.

    Users(**사용자) > <username> > .ssh** 디렉토리**로** 이동합니다.

    WSA SSH 키를 authorized_**keys** 파일에 붙여넣고 변경 사항을 저장합니다.
    참고:SSH 디렉토리에 **authorized_keys** 파일이 없는 경우 수동으로 생성해야 합니다.

다음을 확인합니다.

로그가 SCP 서버로 성공적으로 전송되었는지 확인하려면 다음 단계를 완료하십시오.

1. WSA **Log Subscriptions** 페이지**로** 이동합니다.

2. Rollover(롤오버) 열에서 SCP 검색을 위해 구성한 로그를 선택합니다.

3. Rollover Now(지금 롤오버)**를 찾아 클릭합니다**.

4. 로그 검색을 위해 구성한 SCP 서버 폴더로 이동하고 로그가 해당 위치로 전송되었는지 확인합니다.

WSA에서 SCP 서버에 대한 로그 전송을 모니터링하려면 다음 단계를 완료합니다.

1. SSH를 통해 WSA CLI에 로그인합니다.

2. grep 명령을 **입력합니다**.

3. 모니터링할 로그의 적절한 번호를 입력합니다.예를 들어, **system_logs**의 grep 목록에서 **31**을 입력합니다.

4. SCP **트랜잭션**만 *모니터링할* 수 있도록 로그를 필터링하려면 grep*에* 정규식을 입력합니다.

5. *이 검색을 대/소문자를 구분하지 않도록 하시겠습니까?*프롬프트에서 중단될 수 있습니다.

6. Do you want to tail the logs(*로그를 미닫으시겠습니까?)에 Y를 입력합니다.*프롬프트에서 중단될 수 있습니다.

7. *출력을 페이징하시겠습니까?에 N을 입력합니다.*프롬프트에서 중단될 수 있습니다.그런 다음 WSA는 SCP 트랜잭션을 실시간으로 나열합니다.다음은 WSA system_logs에서 성공한 SCP 트랜잭션의 예입니다.

```
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
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.