Журнал WSA передает удаленному серверу SCP

Содержание

Введение

Этот документ описывает, как передать журналы от Cisco Web Security Appliance (WSA) к удаленному серверу Протокола SCP. Можно настроить журналы WSA, такие как доступ и опознавательные журналы, так, чтобы они были переданы внешнему серверу с протоколом SCP когда одновременное нажатие клавиш журналов или обертка.

Сведения в этом документе описывают, как настроить регистрационные правила вращения, а также ключи Secure Shell (SSH), которые требуются для успешной передачи в сервер SCP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Выполните эти шаги для настройки журналов WSA так, чтобы они могли быть получены с SCP на удаленном сервере:

1. Войдите в веб-GUI WSA.

2. Перейдите к **Администрированию системы> Регистрационные Подписки**.

3. Выберите название журнала (журналов), для которого вы желаете настроить этот метод поиска, такой **как журналы доступа**.

4. В поле Retrieval Method выберите **SCP on Remote Server**.

5. Введите имя хоста SCP или IP-адрес сервера SCP.

6. Введите номер порта SCP.
   Примечание: Настройка по умолчанию является **портом 22**.
7. Введите имя полного пути целевого каталога сервера SCP, которому будут переданы журналы.

8. Введите имя пользователя для проверенного пользователя сервера SCP.

9. Если вы хотите автоматически просмотреть ключ хоста или вручную ввести ключ хоста, то включите **Проверку Ключа хоста**.

10. **Нажмите кнопку Submit (Отправить).** SSH-ключ, что вы разместите в сервер SCP **authorized_keys** файл, должен теперь появиться около вершины страницы **Edit Log Subscription**. Вот пример successfulmessage от WSA:

11. Нажмите **Commit Changes**.

12. Если SCP разъединяет, сервер Linux или Unix или машина Macintosh, то вставьте SSH-ключи от WSA в **authorized_keys** файл, расположенный в каталоге SSH:

    Перейдите **Пользователям> <username>> .ssh** каталог.

    Вставьте SSH-ключ WSA в **authorized_keys** файл и сохраните изменения.
    Примечание: Необходимо вручную создать **authorized_keys** файл, если вы не существуете в каталоге SSH.

Проверка

Выполните эти шаги, чтобы проверить, что журналы успешно переданы серверу SCP:

1. Перейдите к странице **WSA Log Subscriptions**.

2. В **столбце Rollover** выберите журнал, который вы настроили для извлечения SCP.

3. Найдите и нажмите **Rollover Now**.

4. Перейдите к папке server SCP, которую вы настроили для регистрационного извлечения, и проверьте, что журналы переданы тому местоположению.

Выполните эти шаги для мониторинга регистрационной передачи в сервер SCP от WSA:

1. Войдите в CLI WSA через SSH.

2. Введите **команду grep**.

3. Введите соответствующий номер для журнала, который вы хотите контролировать. Например, войдите **31** из списка grep для **system_logs**.

4. Введите **scp** во *Введение регулярного выражения к* приглашению *grep* для фильтрации журналов так, чтобы можно было контролировать только транзакции SCP.

5. Введите **Y** в*, вы хотите, чтобы этот поиск был нечувствителен к регистру?* (приглашение)# .

6. Введите **Y** в*, вы хотите выследить журналы?* (приглашение)# .

7. Введите **N** в*, вы хотите разбить на страницы выходные данные?* (приглашение)# . WSA тогда перечисляет транзакции SCP в режиме реального времени. Вот пример успешных транзакций SCP от WSA system_logs:

```
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
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.