WSA日志转移到远程SCP服务器

目录

简介

本文描述如何转接从思科Web安全工具(WSA)的日志到一个远程思科安全复制(SCP)服务器。您能配置WSA日志，例如访问和验证日志，因此他们转发到有SCP协议的一个外部服务器，当日志反转或换行时。

本文档中的信息描述如何配置为一次成功的转移要求到SCP服务器的日志循环规则以及安全壳SSH密钥。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

完成这些步骤为了配置WSA日志，以便他们可以retreived与在远程服务器的SCP ：

1. 登录WSA Web GUI。

2. 导航对**系统管理>日志订阅**。

3. 选择您希望配置此检索方法日志的名称，例如**访问日志**。

4. 在检索方法字段，请选择**在远程服务器的SCP**。

5. 输入SCP主机名或SCP服务器的IP地址。

6. 输入SCP端口号。
   注意：默认设置是**端口22**。
7. 输入日志将转接SCP服务器目标目录的完整路径名。

8. 输入SCP服务器已认证的用户的用户名。

9. 如果要自动地扫描主机密钥或手工输入主机密钥，则enable (event)**主机密钥检查**。

10. 单击 **submit**。您将放置到SCP服务器**authorized_keys**文件的SSH密钥应该在**编辑日志订阅**页的顶部附近当前出现。这是一successfulmessage的示例从WSA的：

11. 点击**进行更改**。

12. 如果SCP服务器是Linux或UNIX服务器或者麦金塔计算机，则请粘贴从WSA的SSH密钥到在SSH目录查找的**authorized_keys**文件：

    导航对**用户> <username> > .ssh**目录。

    粘贴WSA SSH密钥到**authorized_keys**文件并且保存更改。
    注意：如果一个在SSH目录，不存在您必须手工创建**authorized_keys**文件。

验证

完成这些步骤为了验证日志顺利地转接到SCP服务器：

1. 导航对WSA**日志订阅**页。

2. 在**反转**列，请选择该的日志您为SCP检索配置。

3. **当前**找出并且单击**反转**。

4. 导航到您为日志检索配置的SCP服务器文件夹并且验证日志转接到该位置。

完成这些步骤为了监控日志转移到SCP服务器从WSA ：

1. 通过SSH登录WSA CLI。

2. 输入**grep命令**。

3. 进入您要监控的日志的适当数量。例如，从grep列表的输入**31 system_logs的**。

4. 在*回车的*回车**scp***对grep*提示符的*常规表示*为了过滤日志，以便您能监控仅SCP处理。

5. 在的回车**Y是否***希望此搜索是不区分的案件？*提示。

6. 在的回车**Y是否***要盯梢日志？*提示。

7. 在的回车**N是否***要上页数输出？*提示。WSA在实时然后列出SCP处理。这是成功的SCP处理示例从WSA system_logs的：

```
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
```

故障排除

目前没有针对此配置的故障排除信息。