WSA日志转移到一个远程SCP服务器

Contents

Introduction

本文描述如何从Cisco Web安全工具(WSA)调用日志到一个远程思科安全复制(SCP)服务器。您能配置WSA日志，例如访问和认证日志，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。

本文的信息描述如何配置对于一次成功的转移是必需的到SCP服务器的日志循环规则以及安全壳SSH键。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Configure

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. 日志到WSA Web GUI里。

2. 连接对**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字，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**。

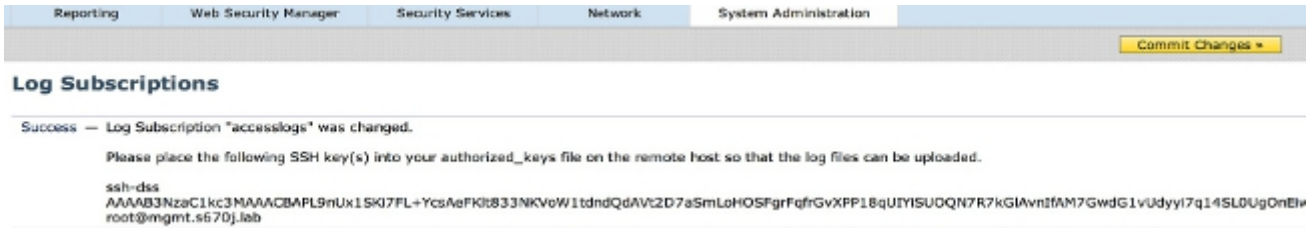
5. 输入SCP主机名或SCP服务器的IP地址。

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

8. 输入SCP服务器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，然后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键应该在**编辑日志订阅**页的顶层附近当前出现。这是一successfulmessage的示例从WSA的：



11. 点击**进行更改**。

12. 如果SCP切断是Linux或UNIX服务器或者Macintosh机器，则粘贴从WSA的SSH键到位于SSH目录的**authorized_keys**文件：

    连接对**用户> <username> > .ssh**目录。

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

Verify

完成这些步骤为了验证日志顺利地调用到SCP服务器：

1. 连接对WSA**日志订阅**页。

2. 在**反转**列，请选择您为SCP检索配置的日志。

3. **当前**找出并且点击**反转**。

4. 连接到您为日志检索配置的SCP服务器文件夹并且验证日志调用到该位置。

完成这些步骤为了监控日志转移到SCP服务器从WSA ：

1. 日志到WSA CLI里通过SSH。
2. 输入**grep命令**。
3. 进入您要监控的日志的适当数量。例如，从**system_logs的**grep列表请输入**31**。
4. 进入**scp**在*进入常规表示对grep*提示为了过滤日志，以便您能监控仅SCP处理。
5. 输入**Y**在*您希望此搜索是不区分的案件？*提示。
6. 输入**Y**在*您要盯梢日志？*提示。
7. 输入**N**在*您要上页数输出？*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
```

Troubleshoot

目前没有针对此配置的故障排除信息。