SSH Tectia 4.0 服务器如何设置 SCP 日志推送用户密钥？

文档编号：117992

作者：Josh Wolfer 和 Siddharth Rajpathak，Cisco TAC 工程师。

2014 年 7 月 17 日

目录

问题

SSH Tectia 4.0 服务器如何设置 SCP 日志推送用户密钥？

环境

思科网络安全设备 (WSA)，所有 AsyncOS 版本。

解决方案

注意：本知识库文章中提及到不由思科维护或支持的软件。 本文在此提供相关信息，以便您参考。 要获得进一步帮助，请与软件供应商联系。

有关下面介绍的 SSH Tectia 服务器的信息，请参见 http://www.ssh.com/support/documentation/all/server/4.0/（第 51-52 页）。

1. 复制将 SCP 设置为日志推送机制时提供的用户密钥。
    a. 在 GUI 中，选择***系统管理 (System Administration)*** *选项卡* > ***日志订阅 (Log Subscriptions)*** > ***访问日志 (Accesslogs)***。
    b. 在 CLI 中，输入 ***logconfig***。
2. 点击 ***提交 (submit)***（或完成 ***logconfig*** CLI 命令）后，屏幕上将显示用户公共密钥。
3. 记录下此密钥文本，并保存到 Tectia SSH 服务器的文件中。
    a. 请注意，应将该文本保存在一行中。 如果密钥中有回车，请在保存前予以删除。
    b. 将文件保存到以下位置：***~/.ssh2/<public_key_filename>***。
    c. 此路径必须位于您要使用此密钥进行身份验证的用户的主目录中。
4. 创建以下文件：***~/.ssh2/authorization***。
    a. 文件中应包括以下信息：
    Key <public_key_filename>

b. 此命令可通知 SSH Tectia 服务器使用以下密钥对相应的用户进行身份验证。

注意： 在标准 Linux/Unix 服务器上，需要将 SSH 密钥复制并粘贴到名为 ***~/.ssh/authorized_keys*** 的文件中。 此文件位于您想要对其进行身份验证的用户的主目录中。

更新日期：2014 年 7 月 17 日　　文档编号：117992
