如何自动化日志转移？

目录

问题

如何自动化日志转移？

环境

思科电子邮件安全工具(ESA)， Web安全工具(WSA)，安全管理设备(SMA)和AsyncOS所有版本。

许多不同种类的日志在安全工具创建。您可以自动地希望安排设备转接某些日志到另一个服务器。

使用FTP或SCP协议，此设置可以通过GUI或CLI完成。请读下面特定：

GUI

1. 去**系统管理- >日志订阅**。
2. 点击您希望修改在‘日志名称’字段下日志的日志名称。
3. 在‘检索方法下’，您可以选择‘在远程服务器的在远程服务器的FTP’或‘SCP’。
4. 输入在您选择的适当的方案的正确值。如果不熟悉正确值，请与您的系统/network管理员联系，他们可帮助您确定哪些服务器是可用的在您的网络。

CLI (命令行界面)

请参阅以下CLI顺序：

```
S-Series> logconfig
[]> edit
[]> <appropriate number correlating to the log you wish to modify>

Please enter the name for the log:
[Log_name]> <enter for default>
```

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace

[3]> <enter for the default>

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
```

选择您希望设置的方法。从此点， CLI通过是可用的在GUI的同样连接设置将走您。

这些如下：

FTP

- 在转接之间的最大时间时间间隔：3600秒
- FTP主机： FTP服务器的主机名/IP地址
- 目录： 在FTP服务器的远程目录(相对FTP登录。典型地‘/’)
- 用户名： FTP用户名
- 密码： FTP密码

SCP

- 在转接之间的最大时间时间间隔：3600秒
- 协议： SSH1或SSH2
- SCP主机： SCP服务器的主机名/IP地址
- 目录： 在SCP服务器的远程目录(相对SCP登录。典型地‘/’)
- 用户名： SCP用户名
- Enable (event)主机密钥检查
- 自动扫描
- 手工回车

注意：FTP是纯文本协议，含义敏感数据可能是可读的由探测网络流量的人。SCP是一份已加密协议，因而进行的探测无效在监听的数据。如果数据是敏感的，并且安全是注意事项，推荐SCP使用而不是FTP。