

Como você automatiza transferências do log?

Índice

[Pergunta](#)

[Ambiente](#)

[GUI](#)

[CLI \(interface da linha de comando\)](#)

[FTP](#)

[SCP](#)

Pergunta

Como você automatiza transferências do log?

Ambiente

Cisco envia por correio eletrônico a ferramenta de segurança (ESA), a ferramenta de segurança da Web (WSA), o dispositivo do Gerenciamento de segurança (S A), e todas as versões de AsyncOS.

Muitos tipos diferentes de logs são criados na ferramenta de segurança. Você pode desejar mandar o dispositivo automaticamente transferir determinados logs a um outro server.

Esta instalação pode ser feita através do GUI ou do CLI usando os protocolos FTP ou SCP. Leia por favor específicos abaixo:

GUI

1. Vão à **administração do sistema - > as assinaturas do log**.
2. Clique o nome do log do log que você deseja alterar sob do “o campo do nome log”.
3. Sob da “o método recuperação”, você pode selecionar o “FTP no servidor remoto” ou o “SCP no servidor remoto”.
4. Incorpore os valores corretos à encenação que apropriada você escolhe. Se você não é familiar com os valores corretos, contacte por favor seus sistemas/administrador de rede como podem o ajudar a determinar que server estão disponíveis em sua rede.

CLI (interface da linha de comando)

Veja a seguinte sequência CLI:

```
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

Escolha o método que você deseja estabelecer. Deste ponto, o CLI andar^á voc^ê atrav^{és} das mesmas configurações de conexão que est^{ão} dispon^{íveis} no GUI.

Estes s^{ão} como segue:

FTP

- Intervalo de tempo m^áximo entre a transfer^ência: 3600 segundos
- Host FTP: Nome de host/endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor FTP
- Diret^ório: Diret^ório remoto no servidor FTP (relativo ao fazer logon FTP. Tipicamente "/")
- Nome de usu^ário: Nome de usu^ário de FTP
- Senha: Senha de FTP

SCP

- Intervalo de tempo m^áximo entre a transfer^ência: 3600 segundos
- Protocolo: SSH1 ou SSH2
- Host SCP: Nome de host/endereço IP de Um ou Mais Servidores Cisco ICM NT do server SCP
- Diret^ório: Diret^ório remoto no server SCP (relativo ao fazer logon SCP. Tipicamente "/")
- Nome de usu^ário: Username SCP
- Permita a verificaç^{ão} da chave Host
- Automaticamente varredura
- Entre manualmente

NOTA: O FTP ^é um protocolo do texto simples, significando que os dados sens^{íveis} podem ser leg^{íveis} por algu^{ém} que est^á aspirando o tráfego de rede. O SCP ^é um protocolo cifrado, assim fazendo aspirar ineficaz em dados da esp^{ião}. Se os dados s^{ão} sens^{íveis} e a Segurança ^é um interesse, recomenda-se que o SCP esteja usado em vez do FTP.