In che modo è possibile automatizzare i trasferimenti di log?

Sommario

[Domanda](#)
[Ambiente](#)
[GUI](#)
[CLI (Command Line Interface)](#)
[FTP](#)
[SCP](#)

Domanda

In che modo è possibile automatizzare i trasferimenti di log?

Ambiente

Cisco Email Security Appliance (ESA), Web Security Appliance (WSA), Security Management Appliance (SMA) e tutte le versioni di AsyncOS.

In Security Appliance vengono creati molti tipi diversi di registri. È possibile che si desideri trasferire automaticamente alcuni registri su un altro server.

Questa configurazione può essere effettuata dalla GUI o dalla CLI usando il protocollo FTP o SCP. Leggi le specifiche seguenti:

GUI

1. Andare a **Amministrazione del sistema -> Registra sottoscrizioni**.
2. Fare clic sul nome del registro che si desidera modificare nel campo 'Nome registro'.
3. In 'Metodo di recupero' è possibile selezionare 'FTP su server remoto' o 'SCP su server remoto'.
4. Immettere i valori corretti nello scenario appropriato scelto. Se non si conoscono i valori corretti, contattare l'amministratore di sistema o di rete in quanto possono aiutare a determinare quali server sono disponibili nella rete.

CLI (Command Line Interface)

Vedere la seguente sequenza 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
```

Scegliere il metodo che si desidera impostare. Da questo punto, la CLI guida l'utente attraverso le stesse impostazioni di connessione disponibili nella GUI.

Si tratta di:

FTP

- Intervallo di tempo massimo tra due trasferimenti: 3600 secondi
- Host FTP: Nome host/indirizzo IP del server FTP
- Directory: Directory remota sul server FTP (relativa all'accesso FTP. In genere '/')
- Username: Nome utente FTP
- Password: Password FTP

SCP

- Intervallo di tempo massimo tra due trasferimenti: 3600 secondi
- Protocollo: SSH1 o SSH2
- Host SCP: Nome host / indirizzo IP del server SCP
- Directory: Directory remota sul server SCP (relativa all'accesso SCP). In genere '/')
- Username: Nome utente SCP
- Abilita controllo chiave host
- Scansione automatica
- Immetti manualmente

NOTA: FTP è un protocollo di testo normale, il che significa che i dati sensibili possono essere leggibili da chiunque sniffi il traffico di rete. SCP è un protocollo crittografato, pertanto lo sniffing non è efficace per lo snooping dei dati. Se i dati sono riservati e la sicurezza è un problema, si consiglia di utilizzare SCP anziché FTP.