Come creare e configurare i log su Cisco Email Security Appliance (ESA)?

Sommario

Domanda

Come creare e configurare i log su Cisco Email Security Appliance (ESA)?

Risposta

Una funzionalità importante di Cisco Email Security Appliance (ESA) è la capacità di registrazione. AsyncOS su ESA può generare molti tipi di log, registrando diversi tipi di informazioni. I file registro contengono i record delle operazioni regolari e le eccezioni di vari componenti del sistema. Queste informazioni possono essere utili durante il monitoraggio di Cisco ESA, nonché durante la risoluzione di un problema o la verifica delle prestazioni.

I log possono essere configurati e creati dalla CLI usando il comando "**logconfig**" o tramite la GUI in **'Amministrazione del sistema' > 'Sottoscrizioni log' > 'Aggiungi sottoscrizione log ...'**

Di seguito è riportato un esempio di creazione di una sottoscrizione del log di debug LDAP tramite la CLI:.

—

```
CLI> logconfig

Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
4. "brightmail" Type: "Symantec Brightmail Anti-Spam Logs" Retrieval: FTP Poll
5. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]>  NEW
```

```
Choose the log file type for this subscription:
...
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. System Logs
9. CLI Audit Logs
10. FTP Server Logs
11. HTTP Logs
12. NTP logs
13. Mailflow Report Logs
14. Symantec Brightmail Anti-Spam Logs
15. Symantec Brightmail Anti-Spam Archive
16. Anti-Virus Logs
17. Anti-Virus Archive
18. LDAP Debug Logs
[1]>  18

Please enter the name for the log:
[]>  ldap_debug

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
[1]>




Filename to use for log files:
[ldap.log]>




Please enter the maximum file size:
[10485760]>




Please enter the maximum number of files:
[10]>




Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll

....

7. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
8. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
```

```
9. "ldap_debug" Type: "LDAP Debug Logs" Retrieval: FTP Poll

.....

CLI> commit
```

Di seguito è riportato un esempio di modifica di un registro esistente.

—

```
CLI> logconfig


Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
4. "brightmail" Type: "Symantec Brightmail Anti-Spam Logs" Retrieval: FTP Poll
5. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
.....


Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> EDIT

Enter the number of the log you wish to edit.

[]> 9

Please enter the name for the log:
[ldap_debug]>

Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
[1]>

Please enter the filename for the log:
[ldap.log]>




Please enter the maximum file size:


[10485760]> 52422880

Please enter the maximum number of files:
[10]> 100

Currently configured logs:
1. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
2. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
3. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
```

```
4. "brightmail" Type: "Symantec Brightmail Anti-Spam Logs" Retrieval: FTP Poll
5. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
....

CLI > commit
```