Hoe maak en vorm ik logs op een Cisco e-mail security applicatie (ESA)?

Inhoud

vraag

Hoe maak en vorm ik logs op Cisco Email Security Appliance (ESA)?

Antwoord

Een belangrijke functie binnen Cisco Email Security Appliance (ESA) is de opslagfuncties. AsyncOS op ESA kan veel typen logbestanden genereren, verschillende soorten informatie opnemen. Logbestanden bevatten de records van reguliere bewerkingen en uitzonderingen op verschillende onderdelen van het systeem. Deze informatie kan waardevol zijn tijdens het controleren van Cisco ESA zowel als tijdens het oplossen van een probleem of het controleren van prestaties.

Logs kunnen worden geconfigureerd en vanaf de CLI worden gemaakt met behulp van de opdracht **"logbestand"** of met behulp van de GUI onder **'systeembeheer' > 'Log abonnementen' >'Add Log abonnement ...'**

Hieronder zie je een voorbeeld van het maken van een logabonnement met LDAP debug met behulp van de 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
```

Hieronder staat een voorbeeld voor het bewerken van een bestaand logbestand.

—

```
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
```