

# Wie werden Protokolle auf einer Cisco E-Mail Security Appliance (ESA) erstellt und konfiguriert?

## Inhalt

[Frage](#)

[Antwort](#)

## Frage

Wie werden Protokolle auf der Cisco E-Mail Security Appliance (ESA) erstellt und konfiguriert?

## Antwort

Eine wichtige Funktion der Cisco E-Mail Security Appliance (ESA) sind die Protokollierungsfunktionen. AsyncOS auf der ESA kann viele Arten von Protokollen generieren und verschiedene Arten von Informationen aufzeichnen. Protokolldateien enthalten die Datensätze regulärer Vorgänge und Ausnahmen von verschiedenen Systemkomponenten. Diese Informationen können bei der Überwachung der Cisco ESA sowie bei der Fehlerbehebung oder Leistungsüberprüfung hilfreich sein.

Protokolle können mithilfe des Befehls "logconfig" oder über die GUI unter '**Systemverwaltung**' > '**Protokollabonnements**' > '**Protokollabonnement hinzufügen ...**' über die CLI konfiguriert und erstellt werden.

Im Folgenden sehen Sie ein Beispiel für das Erstellen eines LDAP-Debug-Protokoll-Abonnements mithilfe der 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**

Im Folgenden finden Sie ein Beispiel zum Bearbeiten eines vorhandenen Protokolls.

—

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**