How do I create and configure logs on a Cisco Email Security Appliance (ESA)?

Document ID: 118456

Contributed by John Yu and Siddharth Rajpathak, Cisco TAC Engineers.

Oct 13, 2014

Contents

Question

How do I create and configure logs on the Cisco Email Security Appliance (ESA)?

Answer

An important feature within the Cisco Email Security appliance (ESA) is its logging capabilities. AsyncOS on ESA can generate many types of logs, recording varying types of information. Log files contain the records of regular operations and exceptions from various components of the system. This information can be valuable while monitoring Cisco ESA as well as during troubleshooting of an issue or checking performance.

Logs can be configured and created from the CLI using "***logconfig***" command or via the GUI under '***System Administration***' > '***Log Subscriptions***' > '***Add Log Subscription ...***'

Below is an example of creating a LDAP debug log subscription using the 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]> <Press Enter>

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

Please enter the maximum file size:
[10485760]> <Press Enter>

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

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
```

Below is an example for editing an existing log.

```
_____________________________________________________________________________

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]>  <Press Enter>

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
```