如何在思科郵件安全裝置(ESA)上建立並配置日誌？

目錄

問題

如何在思科郵件安全裝置(ESA)上建立並配置日誌？

答案

思科電子郵件安全裝置(ESA)的一個重要功能是其日誌功能。ESA上的AsyncOS可以生成多種型別的日誌，記錄各種型別的資訊。日誌檔案包含系統各個元件的常規操作和異常的記錄。此資訊在監控Cisco ESA時以及在故障排除或檢查效能時很有用。

可以使用「logconfig」命令通過CLI或通過**「系統管理」>「日誌訂閱」>「新增日誌訂閱」**下的GUI配置並建立日誌。

以下是使用CLI建立LDAP調試日誌訂閱的示例：。

```
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
```
以下是編輯現有日誌的示例。

```
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
```