思科安全邮件网关的手动日志删除

目录

简介

本文档介绍新操作deletelogfiles，包括对Cisco安全邮件网关(SEG)执行操作的步骤。

作者：Chris Arellano Cisco TAC工程师。

先决条件

AsyncOS 15.0.0及更高版本适用于云邮件安全和内部安全邮件设备。

使用的组件

思科SEG

CLI访问方法

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

以下说明提供了新的日志功能，用于删除每个SEG设备中的单个日志文件。

为什么？某些情况可能证实需要从SEG中清除敏感内容。

每个日志订阅都由一组独立文件组成，这些文件包含名称中每个文件的日期戳，结束于下一个日志的开始，该日志包含名称中的连续日期。

该操作可以在独立SEG上执行，也可以在集群内的机器级别执行。

步骤1: 通过CLI登录并键入以下命令logconfig > deletelogfile > 选择表示日志订阅的编号 > 选择表示日志的编号> Y以确认。

注：删除操作是即时、永久的，不需要用户提交更改。

```
> logconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode (Machine es

What would you like to do?
```

```
1. Switch modes to edit at mode "Cluster Hosted_Cluster".
2. Start a new, empty configuration at the current mode (Machine esa1.hcXXXX-XX.iphmx.com).
3. Copy settings from another cluster mode to the current mode (Machine esa1.hcXXXX-XX.iphmx.com).
[1]>

Currently configured logs:
    Log Name            Log Type                            Retrieval           Interval
 -------------------------------------------------------------------------------------
 1. amp                 AMP Engine Logs                     Manual Download     None
 2. amparchive          AMP Archive                         Manual Download     None
 3. antispam            Anti-Spam Logs                      Manual Download     None
 4. antivirus           Anti-Virus Logs                     Manual Download     None
 5. asarchive           Anti-Spam Archive                   Manual Download     None
 6. audit_logs          Audit Logs                          Manual Download     None
 7. authentication      Authentication Logs                 Manual Download     None
 8. avarchive           Anti-Virus Archive                  Manual Download     None
 9. bounces             Bounce Logs                         Manual Download     None
10. cli_logs            CLI Audit Logs                      Manual Download     None
11. cloud_connector     Cloud Connector Logs                Manual Download     None
12. config_history      Configuration History Logs          Manual Download     None
13. content_scanner     Content Scanner Logs                Manual Download     None
14. csa                 Cisco Security Awareness Logs       Manual Download     None
15. csn_logs            CSN Logs                            Manual Download     None
16. ctr_logs            CTR Logs                            Manual Download     None
17. dlp                 DLP Logs                            Manual Download     None
18. eaas                Advanced Phishing Protection Logs   Manual Download     None
19. ecs_logs            ESA Cloud Scanner Logs              Manual Download     None
20. encryption          Encryption Logs                     Manual Download     None
21. error_logs          IronPort Text Mail Logs             Manual Download     None
22. euq_logs            Spam Quarantine Logs                Manual Download     None
23. euqgui_logs         Spam Quarantine GUI Logs            Manual Download     None
24. ftpd_logs           FTP Server Logs                     Manual Download     None
25. gmarchive           Graymail Archive                    Manual Download     None
26. graymail            Graymail Engine Logs                Manual Download     None
27. gui_logs            HTTP Logs                           Manual Download     None
28. ipr_client          IP Reputation Logs                  Manual Download     None
29. mail_logs           IronPort Text Mail Logs             Manual Download     None
30. remediation         Remediation Logs                    Manual Download     None
31. reportd_logs        Reporting Logs                      Manual Download     None
32. reportqueryd_logs   Reporting Query Logs                Manual Download     None
33. s3_client           S3 Client Logs                      Manual Download     None
34. scanning            Scanning Logs                       Manual Download     None
35. sdr_client          Sender Domain Reputation Logs       Manual Download     None
36. service_logs        Service Logs                        Manual Download     None
37. slbld_logs          Safe/Block Lists Logs               Manual Download     None
38. smartlicense        Smartlicense Logs                   Manual Download     None
39. snmp_logs           SNMP Logs                           Manual Download     None
40. sntpd_logs          NTP logs                            Manual Download     None
41. status              Status Logs                         Manual Download     None
42. system_logs         System Logs                         Manual Download     None
43. threatfeeds         Threat Feeds Logs                   Manual Download     None
44. trackerd_logs       Tracking Logs                       Manual Download     None
45. updater_logs        Updater Logs                        Manual Download     None
46. upgrade_logs        Upgrade Logs                        Manual Download     None
47. url_rep_client      URL Reputation Logs                 Manual Download     None

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- DELETELOGFILE - Delete log files
- SETUP - General settings.
```

```
- LOGHEADERS - Configure headers to log.
- CEFLOGHEADERS - Configure list of headers to add in CEF log files.
- HOSTKEYCONFIG - Configure SSH host keys.
- CLUSTERSET - Set how logs are configured in a cluster.
- CLUSTERSHOW - Display how logs are configured in a cluster.
[]> deletelogfile

Currently configured logs:
    Log Name            No of Log Files
 ------------------------------------------------------------------------------
 1. amparchive          3
 2. antispam            1
 3. asarchive           3
 4. audit_logs          9
 5. authentication      9
 6. avarchive           3
 7. bounces             3
 8. cli_logs            9
 9. config_history      49
10. error_logs          3
11. euq_logs            3
12. euqgui_logs         3
13. ftpd_logs           3
14. gmarchive           3
15. graymail            1
16. gui_logs            9
17. ipr_client          6
18. mail_logs           4
-Note: 19-47 removed from sample view -
Enter the number of the log file you want to delete.
[]> 18

   Log File Name                    File Size File Created At
 ------------------------------------------------------------------------------
1. mail.@20230517T021023.s          99941403  Wed May 17 02:10:23 2023
2. mail.@20230706T063330.s          35603294  Thu Jul  6 06:33:30 2023
3. mail.@20230712T073148.s          93764     Wed Jul 12 07:31:48 2023
4. mail.@20230712T095042.s          6756      Wed Jul 12 09:50:42 2023

Enter the number of the log file you want to delete.

Notes:
- To specify multiple log files, enter the required numbers separated by commas (for example: 2,3,9)
- To specify a range of log files, enter the required range numbers with a dash (for example: 2-5).
- To specify a combination of single and range, enter the required numbers with comma and dash (for exa
[]> 1

Warning:
The following log files - ['mail.@20230517T021023.s'] will be removed from the email gateway immediatel
Do you want to continue? [N]> y

Log file /data/pub/mail_logs/mail.@20230517T021023.s has been deleted successfully
```

验证

要验证是否只需再次执行deletelogfile，请选择相同的订用以查看

```
Note: Edited output to illustrate the change in log count from 4 to 3 post deletion.
Enter the number of the log file you want to delete.
[]> 18

Log File Name File Size File Created At
--------------------------------------------------------------------------------
1. mail.@20230706T063330.s 35603294 Thu Jul 6 06:33:30 2023
2. mail.@20230712T073148.s 93764 Wed Jul 12 07:31:48 2023
3. mail.@20230712T095042.s 6756 Wed Jul 12 09:50:42 2023
```

相关信息

- 邮件安全设置指南
- 支持指南的思科安全邮件网关发布页面

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。