Cisco Secure Email Gateway의 수동 로그 삭제

목차

소개

이 문서에서는 Cisco SEG(Secure Email Gateway)에 대한 작업을 수행하는 단계를 포함하여 새로운 작업 deletelogfiles에 대해 설명합니다.

기고자: Chris Arellano Cisco TAC 엔지니어

사전 요구 사항

Cloud Email Security 및 온프레미스 Secure Email Appliance용 AsyncOS 15.0.0 이상

사용되는 구성 요소

Cisco SEG

CLI 액세스 방법

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

다음 지침은 각 SEG 디바이스 내의 개별 로그 파일을 삭제하는 새로운 로그 기능을 제공합니다.

왜 그럴까요? 일부 상황에서는 SEG에서 민감한 콘텐츠를 삭제할 필요성을 보증할 수 있습니다.

각 로그 서브스크립션은 이름 내의 각 파일에 대한 날짜 스탬프가 포함된 개별 파일의 컬렉션으로 구성되며, 이름 내의 순차적인 날짜를 포함하는 다음 로그의 시작으로 끝납니다.

이 작업은 독립형 SEG뿐만 아니라 클러스터 내의 시스템 레벨에서도 수행할 수 있습니다.

1단계. CLI를 통해 로그인하고 다음 명령 logconfig > deletelogfile > 로그 서브스크립션을 나타내는 번호를 > 로그를 나타내는 번호를 > Y를 입력하여 확인합니다.

참고: 삭제 작업은 즉각적이고 영구적이며 사용자가 변경 사항을 커밋할 필요가 없습니다.

```
> 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
```

다음을 확인합니다.

동일한 서브스크립션을 선택하여 deletelogfile을 한 번 더 실행하여

```
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
```

관련 정보

- 이메일 보안 설정 가이드
- Cisco Secure Email Gateway 시작 페이지 - 지원 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.