

Eliminación manual de registros para Cisco Secure Email Gateway

Contenido

Introducción

Este documento describe la nueva acción **deletelogfiles**, incluidos los pasos para realizar la acción para Cisco Secure Email Gateway (SEG).

Colaboración de Chris Arellano, ingeniero del TAC de Cisco.

Prerequisitos

AsyncOS 15.0.0 y posterior para Cloud Email Security y el dispositivo de correo electrónico seguro en las instalaciones.

Componentes Utilizados

Cisco SEG

método de acceso CLI

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Las siguientes instrucciones presentan la nueva funcionalidad de registro para eliminar archivos de registro individuales dentro de cada dispositivo SEG.

¿Por qué? Algunas situaciones pueden justificar la necesidad de purgar el contenido confidencial del SEG.

Cada suscripción a registro se compone de una colección de archivos individuales que contienen una marca de fecha para cada archivo dentro del nombre, que termina con el inicio del siguiente registro que contiene una fecha secuencial dentro del nombre.

La acción se puede realizar en un SEG independiente, así como en el nivel de máquina dentro de un clúster.

Paso 1. Inicie sesión a través de CLI y escriba los siguientes comandos `logconfig > deletelogfile >` Seleccione el número que representa la suscripción al registro > Seleccione el número que representa el registro >Y para confirmar.

Nota: La acción de eliminación es inmediata, permanente y no requiere que el usuario realice cambios.

> logconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode (Machine esa1.hcXXXX-XX.iphmx.com).

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.
 - DELETEDLOGFILE - 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 example: 2,3-5)
- [> 1

Warning:

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

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

Verificación

Para verificar simplemente ejecute el archivo deletelogfile una vez más seleccionando la misma suscripción para ver el

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
```

Información Relacionada

- [Guía de configuración de Email Security](#)
- [Página de inicio de Cisco Secure Email Gateway para las guías de asistencia](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).