

ESA 도메인 디버그 로그 컨피그레이션 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 도메인 디버그 로그를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ESA
- AsyncOS

사용되는 구성 요소

이 문서의 정보는 모든 버전의 AsyncOS를 기반으로 합니다.

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

배경 정보

도메인 디버그 로그는 특정 도메인과 ESA 간의 모든 SMTP(Simple Mail Transfer Protocol) 트래픽

을 한정된 세션 수로 기록하도록 설계된 시스템 로그입니다.

이 로그 유형은 특정 수신자 도메인 또는 호스트와 관련된 문제를 해결하는 데 도움이 될 수 있습니다. 각 세션은 정의된 세션 수에 도달하고 데이터 수집이 중지될 때까지 기록됩니다. 모든 세션이 기록되기 전에 도메인 디버그 로그 데이터 수집을 종료하려면 로그 서브스크립션을 삭제하거나 편집할 수 있습니다.

구성

Domain Debug Logs(도메인 디버그 로그)를 생성하고 구성하려면 ESA CLI에 logconfig 명령을 입력합니다.

참고:ESA GUI를 사용하여 도메인 디버그 로그를 구성하려면 고급 사용자 가이드의 로그 서브스크립션 섹션을 참조하십시오.

다음은 ESA CLI를 사용하여 도메인 디버그 로그 서브스크립션 생성에 대한 예입니다.

```
example.com> logconfig
```

```
Currently configured logs:
```

1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
5. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
6. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
7. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
8. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
9. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
10. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
11. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
12. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
13. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
14. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
15. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
16. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
17. "status" Type: "Status Logs" Retrieval: FTP Poll
18. "system_logs" Type: "System Logs" Retrieval: FTP Poll
19. "updater_logs" Type: "Updater 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:
```

1. IronPort Text Mail Logs
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. LDAP Debug Logs
 14. Anti-Virus Logs
 15. Anti-Virus Archive
 16. Scanning Logs
 17. IronPort Spam Quarantine Logs
 18. IronPort Spam Quarantine GUI Logs
 19. Reporting Logs
 20. Reporting Query Logs
 21. Updater Logs
- [1]> 6

Please enter the name for the log:

[> **debug_example**

Enter the name of the domain for which you want to record debug information.

[> **example.com**

Please enter the number of SMTP sessions you want to record for this domain.

[1]> 8

Choose the method to retrieve the logs.

1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push

[1]>

Filename to use for log files:

[example.com.text]> example.com.text

Please enter the maximum file size:

[10485760]>

Please enter the maximum number of files:

[10]>

Currently configured logs:

1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
5. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
6. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
7. "debug_example" Type: "Domain Debug Logs" Retrieval: FTP Poll
8. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
9. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
10. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
11. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
12. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
13. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
14. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
15. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
16. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
17. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
18. "status" Type: "Status Logs" Retrieval: FTP Poll
19. "system_logs" Type: "System Logs" Retrieval: FTP Poll
20. "updater_logs" Type: "Updater 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.

[]>

example.com> **commit**

다음을 확인합니다.

다음은 ESA가 수신자 도메인 **example.com**에 메시지를 전달하는 도메인 디버그 로그의 예입니다.

```
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '220 ESmtpt mail.example.com
ESMTP service ready'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'EHLO example.com'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250-mail.example.com'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250-8BITMIME'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250-SIZE 31981568'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 PIPELINING'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'MAIL FROM:<user@example.com>'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 sender <user@example.com> ok'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'RCPT TO:<test@example.com>'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 recipient <test@example.com> ok'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'DATA'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '354 go ahead'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'Received: from unknown (HELO)
(10.250.7.164)rn by example.com with SMTP; 22 Mar 2005 16:52:08 -0800rn'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'Message-ID:
<000d01c52f43$48dacba0$fa0a@example.com>rnFrom: "User" <user@example.com>
rnTo:<test@example.com>rn Subject:TestrnDate:Tue,22Mar200516:57:28-0800rnMIME-
Version:1.0rn
Content-Type:multipart/alternative;rntboundary="-----
_NextPart_000_000A_01C52F00.3AA3B580"rnX-Priority: 3rnX-MSMail-Priority:
Normalrn X-Mailer: Microsoft Outlook Express 6.00.2900.2180rnX-MimeOLE:
Produced ByMicrosoft MimeOLEV6.00.2900.2180rnrnThis is a multi-part
messageinMIMEformat.rnrn-----_NextPart_000_000A_01C52F00.3AA3B580rn
Content-Type:text/plain;rntcharset= "iso-8859-1"rnContent-Transfer-Encoding:
quoted-printablernrnThis isthebodyofthemail.rnThisisadisclaimer.rnrn-----
_NextPart_000_000A_01C52F00.3AA3B580rnContent-Type:text/html;rntcharset=
"iso-8859-1"rnContent-Transfer-Encoding:quoted-printablernrn<!DOCTYPEHTMLPUBLIC
"-//W3C//DTDHTML4.0Transitional//EN">rn<HTML><HEAD>rn<METAhttp-equiv=
3DContent-Typecontent= 3D"text/html;charset= 3Diso-8859-1">rn<METAcontent=
3D"MSHTML6.00.2900.2523"name= 3DGENERATOR>rn<STYLE></STYLE>rn</HEAD>rn
<BODYbgColor= 3D#ffffff>rn<DIV><FONTface= 3DArialsize= 3D2>This is the body
of thernmail.</FONT></DIV><pre> This is a disclaimer.rn </pre></BODY></HTML>
rnrn-----_NextPart_000_000A_01C52F00.3AA3B580--rn'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: '.rn'
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '250 ok dirdel'
Tue Mar 22 16:52:12 2005 Info: 411 Sent: 'QUIT'
Tue Mar 22 16:52:12 2005 Info: 411 Rcvd: '221 mail.example.com'
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [AsyncOS 이메일 사용 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)