

ESA域調試日誌配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹如何在思科電子郵件安全裝置(ESA)上設定網域偵錯日誌。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ESA
- AsyncOS

採用元件

本文檔中的資訊基於AsyncOS的所有版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

域調試日誌是一個系統日誌，旨在記錄特定域與ESA之間有限會話數量之內的所有簡單郵件傳輸協定(SMTP)流量。

此日誌型別有助於嘗試排除與特定收件人域或主機相關的問題。記錄每個會話，直到達到定義的會話數，然後資料收集停止。要在記錄所有會話之前結束域調試日誌資料收集，您可以刪除或編輯日誌訂閱。

設定

若要建立和配置域調試日誌，請在ESA CLI中輸入logconfig命令。

附註：如果要使用ESA GUI配置域調試日誌，請參閱高級使用手冊的日誌訂閱部分。

以下是使用ESA CLI建立域調試日誌訂閱的示例：

```
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
```

驗證

以下是ESA向收件人域example.com傳送消息時的域調試日誌示例：

```
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'
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [AsyncOS 電子郵件使用手冊](#)

- [技術支援與文件 - Cisco Systems](#)