

# 从ESA的Trace出站邮件SMTP塞申斯

## 目录

### [简介](#)

### [Trace出站邮件SMTP塞申斯每个接收域](#)

### [相关信息](#)

## 简介

本文描述如何跟踪和查看从您的思科电子邮件安全工具(ESA)的一次整个电子邮件会话。

## Trace出站邮件SMTP塞申斯每个接收域

域调试日志允许您跟踪一次整个简单邮件传输协议(SMTP)会话在您的ESA和目的地域/host之间。在域调试日志的每条线路概述发送的数据(发送)并且接收(Rcvd)在SMTP会话时。

输入logconfig命令到ESA CLI为了配置记录日志，以便ESA记录接收域的一本域调试日志利益：

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. gmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. URL Filtering Logs
17. Graymail Engine Logs
18. Anti-Spam Archive
19. Anti-Virus Logs

20. Anti-Virus Archive  
21. Scanning Logs  
22. Spam Quarantine Logs  
23. Spam Quarantine GUI Logs  
24. Reporting Logs  
25. Reporting Query Logs  
26. Updater Logs  
27. SNMP Logs  
28. Tracking Logs  
29. Safe/Block Lists Logs  
30. Authentication Logs  
31. FIPS Logs  
32. Upgrade Logs  
33. Configuration History Logs  
34. Reputation Engine Logs  
35. AMP Engine Logs  
36. AMP Archive  
37. API Logs  
38. Graymail Archive  
[1]> 6

Please enter the name for the log:  
[> example.com.domain.debug

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]> 10000

Choose the method to retrieve the logs.  
1. Download Manually: FTP/HTTP(S)/SCP  
2. FTP Push  
3. SCP Push  
4. Syslog Push  
[1]>

Filename to use for log files:  
[example.com.text]>

Would you like to append system based unique identifiers  
like \$hostname, \$serialnumber to the log filename? [N]>

Please enter the maximum file size. You can specify suffixes:  
"m" for megabytes, "k" for kilobytes. Suffixes are  
case-insensitive:  
[10485760]>

Please enter the maximum number of files:  
[10]>

Should an alert be sent when files are removed due to the  
maximum number of files allowed? [N]>

Do you want to configure time-based log files rollover? [N]>

**Note:**保证您确认任意更改，在域调试日志配置后。

日志为您为域配置会话的数量是活跃的。为了查看实际电子邮件会话的trace，输入尾标  
**example.com.domain.debug**命令到ESA CLI。

这是生成的示例域调试日志，当ESA提供消息对接收域example.com时：

```
Tue Mar 22 16:52:07 2005 Info: 411 Rcvd: '220 ESmtpl 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)
\r\n by example.com with SMTP; 22 Mar 2005 16:52:08 -0800\r\n'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: 'Message-ID:
<000d01c52f43$48dacba0$a407fa0a@example.com>\r\nFrom: "User"
<user@example.com>\r\nTo:<test@example.com>\r\n Subject:Test\r\nDate:
Tue,22Mar200516:57:28-0800\r\nMIME-Version:1.0\r\n
Content-Type:multipart/alternative;\r\n\tboundary="-----_Next
Part_000_000A_01C52F00.3AA3B580"\r\nX-Priority: 3\r\nX-MSMail-Priority: Normal\r\n
X-Mailer: Microsoft Outlook Express 6.00.2900.2180\r\nX-MimeOLE: Produced ByMicrosoft
MimeOLEV6.00.2900.2180\r\n\r\nThis is a multi-part messageinMIMEformat.\r\n\r\
n-----_NextPart_000_000A_01C52F00.3AA3B580\r\nContent-Type:text/plain;\r\n\
tcharset= "iso-8859-1"\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\nThis
is the body of the mail.\r\nThis isadisclaimer.\r\n\r\n-----=
_NextPart_000_000A_01C52F00.3AA3B580\r\nContent-Type:text/html;\r\n\tcharset=
"iso-8859-1"\r\nContent-Transfer-Encoding: quoted-printable\r\n\r\n<!DOCTYPE HTML
PUBLIC"-//W3C//DTDHTML4.0Transitional//EN">\r\n<HTML><HEAD>\r\n<METAhttp-equiv=
3DContent-Typecontent= 3D"text/html;charset= 3Diso-8859-1">\r\n<METAcontent=3D"
MSHTML6.00.2900.2523"name= 3DGENERATOR>\r\n<STYLE></STYLE>\r\n</HEAD>\r\n
<BODYbgColor= 3D#ffffff>\r\n<DIV><FONTface= 3DArialsize= 3D2>This is the body of
the\r\nmail.</FONT></DIV><pre> This is a disclaimer.\r\n </pre></BODY></HTML>\r\n\r\
n-----_NextPart_000_000A_01C52F00.3AA3B580--\r\n'
Tue Mar 22 16:52:07 2005 Info: 411 Sent: '.\r\n'
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'
```

## 相关信息

- [思科电子邮件安全工具 最终用户指南](#)
- [ESA域调试记录配置示例](#)
- [ESA FAQ：如何分析在ESA的断断续续邮件发送问题？](#)
- [技术支持&文档 系统](#)