

# Konfigurationsbeispiel für ESA Domain Debug Logs

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie die Domänen-Debug-Protokolle auf der Cisco E-Mail Security Appliance (ESA) konfigurieren.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- AsyncOS

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf allen Versionen von AsyncOS.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Hintergrundinformationen

Das Domänen-Debug-Protokoll ist ein Systemprotokoll, das entwickelt wurde, um den gesamten SMTP-Verkehr (Simple Mail Transfer Protocol) zwischen einer bestimmten Domäne und der ESA für eine begrenzte Anzahl von Sitzungen aufzuzeichnen.

Dieser Protokolltyp kann bei Versuchen helfen, Probleme zu beheben, die sich auf eine bestimmte Empfängerdomäne oder einen bestimmten Host beziehen. Jede Sitzung wird aufgezeichnet, bis die festgelegte Anzahl der Sitzungen erreicht ist, und anschließend wird die Datensammlung beendet. Um die Datensammlung der Domänendebbugprotokolle zu beenden, bevor alle Sitzungen aufgezeichnet werden, können Sie das Protokollabonnement löschen oder bearbeiten.

## Konfigurieren

Geben Sie zum Erstellen und Konfigurieren der DomänenDebug-Protokolle den Befehl `logconfig` in die ESA-CLI ein.

**Hinweis:** Wenn Sie die Domänen-Debug-Protokolle mit der ESA-GUI konfigurieren möchten, lesen Sie den Abschnitt **Protokollabonnements** im **erweiterten Benutzerhandbuch**.

Das folgende Beispiel zeigt die Erstellung des Domain Debug Logs-Abonnements unter Verwendung der ESA-CLI:

```
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. gmail 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**

## Überprüfen

Das folgende Beispiel zeigt die Domänen-Debug-Protokolle, wenn die ESA eine Nachricht an die Empfängerdomäne **example.com** übermittelt:

```
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)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$407fa0a@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'

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

## Zugehörige Informationen

- [AsyncOS E-Mail-Benutzerhandbuch](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)