

O domínio ESA debuga o exemplo de configuração dos logs

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o domínio debuga entra a ferramenta de segurança do email de Cisco (ESA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco ESA
- AsyncOS

Componentes Utilizados

A informação neste documento é baseada em todas as versões de AsyncOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O domínio debuga o log é um log de sistema que seja projetado a fim gravar todo o tráfego do Simple Mail Transfer Protocol (SMTP) entre um domínio específico e o ESA para um número finito de sessões.

Este tipo do log pode ajudar nas tentativas de pesquisar defeitos as edições que se relacionam a um domínio destinatário específico ou se hospedam. Cada sessão é gravada até que o número definido de sessões esteja alcançado, e então as paradas do levantamento de dados. A fim terminar o domínio debugar o levantamento de dados dos logs antes que todas as sessões estejam gravadas, você pode suprimir ou editar da assinatura do log.

Configurar

A fim criar e configurar o domínio debugar logs, incorporam o comando do **logconfig** no ESA CLI.

Note: Se você quer configurar o domínio debugar logs com o ESA GUI, referem a seção das assinaturas do log do guia de usuário avançado.

Está aqui um exemplo do domínio debuga a criação da assinatura dos logs com o uso do 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. "euogui_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. "reporttd_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**

Verificar

Está aqui um exemplo do domínio debuga logs quando o ESA entrega uma mensagem ao domínio destinatário **example.com**:

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. "euogui_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**

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Guia do Usuário do email de AsyncOS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)