

Encontre alerta DHAP no ESA

Índice

[Introdução](#)

[Encontre ocorrências DHAP do ESA](#)

[Configuração da vista ou da atualização DHAP do GUI](#)

[Configuração da vista ou da atualização DHAP do CLI](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como encontrar com respeito aos alertas da prevenção do ataque da colheita do diretório (DHAP) em sua ferramenta de segurança do email de Cisco (ESA).

Encontre ocorrências DHAP do ESA

As entradas que descrevem o evento DHAP residem nos logs do correio. Está aqui uma entrada de registro do correio do exemplo quando DHAP ocorre:

```
Tue Oct 18 00:25:35 2005 Warning: LDAP: Dropping connection due to potential Directory Harvest Attack from host=(192.168.10.1', None), dhap_limit=4, sender_group=SUSPECTLIST
```

Note: À revelia, o netmask de /24 é procurado na busca.

Incorpore esta pergunta no CLI a fim ver os logs do correio:

```
myesa.local> grep "dhap_limit=" mail_logs
```

Os contadores DHAP incluem rejeições destinatárias da pergunta das rejeições da tabela do acesso (RATO) e da aceitação do Lightweight Directory Access Protocol (LDAP). Os ajustes DHAP são configurados na política do fluxo de correio.

Configuração da vista ou da atualização DHAP do GUI

Termine estas etapas a fim ver ou editar seus parâmetros de configuração DHAP do GUI:

1. Navegue para enviar políticas > políticas do fluxo de correio.
2. Clique o nome da política a fim fazer edita, ou clicam parâmetros da política padrão a fim ver a configuração atual DHAP.

3. Faça mudanças ao diretório colher a seção da prevenção do ataque (DHAP) como necessária:

| Mail Flow Limits | |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rate Limit for Hosts: | Max. Recipients Per Hour: <input checked="" type="radio"/> Unlimited <input type="radio"/> <input type="text"/> Max. Recipients Per Hour Code: <input type="text" value="452"/> Max. Recipients Per Hour Text: <input type="text" value="Too many recipients received this hour"/> |
| ▶ Rate Limit for Envelope Senders: | Settings to define maximum recipients for envelope sender, per time interval. |
| Flow Control: | Use SenderBase for Flow Control: <input checked="" type="radio"/> On <input type="radio"/> Off Group by Similarity of IP Addresses: <i>This Feature can only be used if Senderbase Flow Control is off.</i> <input type="radio"/> Off <input type="radio"/> <input type="text"/> <small>(significant bits 0-32)</small> |
| Directory Harvest Attack Prevention (DHAP): | Max. Invalid Recipients Per Hour: <input type="radio"/> Unlimited <input checked="" type="radio"/> <input type="text" value="25"/> Drop Connection if DHAP threshold is Reached within an SMTP Conversation: <input checked="" type="radio"/> On <input type="radio"/> Off Max. Invalid Recipients Per Hour Code: <input type="text" value="550"/> Max. Invalid Recipients Per Hour Text: <input type="text" value="Too many invalid recipie"/> |

4. O clique **submete-se**, e clica-se então **compromete** a fim salvar suas mudanças.

Configuração da vista ou da atualização DHAP do CLI

A fim ver ou editar seus parâmetros de configuração DHAP do CLI, incorpore o `listenerconfig > editam o [listener number] > os hostaccess > o comando default:`

```

Default Policy Parameters
=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
  
```

There are currently 5 policies defined.

There are currently 8 sender groups.

Choose the operation you want to perform:

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.

[> default

Enter the default maximum message size. Add a trailing k for kilobytes, M for megabytes, or no letter for bytes.

[10M]>

Enter the maximum number of concurrent connections allowed from a single IP address.

[10]>

Enter the maximum number of messages per connection.

[10]>

Enter the maximum number of recipients per message.

[50]>

Do you want to override the hostname in the SMTP banner? [N]>

Would you like to specify a custom SMTP acceptance response? [N]>

Would you like to specify a custom SMTP rejection response? [N]>

Do you want to enable rate limiting per host? [N]>

Do you want to enable rate limiting per envelope sender? [N]>

Do you want to enable Directory Harvest Attack Prevention per host? [Y]>

Enter the maximum number of invalid recipients per hour from a remote host.

[25]>

Select an action to apply when a recipient is rejected due to DHAP:

1. Drop
2. Code

[1]>

Would you like to specify a custom SMTP DHAP response? [Y]>

Enter the SMTP code to use in the response. 550 is the standard code.

[550]>

Enter your custom SMTP response. Press Enter on a blank line to finish.

Would you like to use SenderBase for flow control by default? [Y]>

Would you like to enable anti-spam scanning? [Y]>

Would you like to enable anti-virus scanning? [Y]>

Do you want to allow encrypted TLS connections?

1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify

[1]>

Would you like to enable DKIM/DomainKeys signing? [N]>

Would you like to enable DKIM verification? [N]>

Would you like to change SPF/SIDF settings? [N]>

Would you like to enable DMARC verification? [N]>

Would you like to enable envelope sender verification? [N]>

Would you like to enable use of the domain exception table? [N]>

Do you wish to accept untagged bounces? [N]>

Se você escolhe fazer atualizações, assegure-se de que você retorne à alerta principal CLI e **comprometa** todas as mudanças.

Informações Relacionadas

- [Cisco envia por correio eletrônico a ferramenta de segurança – Guias do utilizador final](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)