

# ESA で DHAP アラート情報を探す

## 目次

[はじめに](#)

[ESA から DHAP の発生を検出する](#)

[GUI から DHAP の構成を表示または更新する](#)

[CLI から DHAP の構成を表示または更新する](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス (ESA) のディレクトリ獲得攻撃防御 (DHAP) のアラートに関する情報を見つける方法を説明します。

## ESA から DHAP の発生を検出する

DHAP のイベントを記述するエントリはメール ログに存在します。DHAP が発生する場合のメール ログ エントリの例を次に示します。

```
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
```

注: デフォルトでは、検索で /24 のネットマスクを探します。

次のクエリを CLI に入力し、メール ログを表示します。

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

DHAP カウンタには、受信者アクセス テーブル (RAT) の拒否、Lightweight Directory Access Protocol (LDAP) 承認のクエリの拒否が含まれます。DHAP の設定は、メール フロー ポリシーで設定されます。

## GUI から DHAP の構成を表示または更新する

GUI から DHAP の構成パラメータを表示または編集するには、次の手順を実行します。

1. [Mail Policies] > [Mail Flow Policies] に移動します。
2. 編集するにはポリシー名をクリックします。また、現在の DHAP 構成を表示するには、デ

フォルトの [Policy Parameters] をクリックします。

3. 必要に応じて、[Directory Harvest Attack Prevention (DHAP)] セクションを変更します。

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: This Feature can only be used if Senderbase Flow Control is off. <input type="radio"/> Off <input type="radio"/> <input type="text"/> (significant bits 0-32)
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. [Submit] をクリックし、[Commit] をクリックして変更を保存します。

## CLI から DHAP の構成を表示または更新する

CLI から DHAP の構成パラメータを表示または編集するには、`listenerconfig > edit [listener number] > hostaccess > default` コマンドを入力します。

```
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]>

更新する場合は、メイン CLI プロンプトに戻り、すべての変更をコミットしてください。

## 関連情報

- [Cisco E メール セキュリティ アプライアンス - エンドユーザ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)