在ESA上找到DHAP警報資訊

目錄

[簡介](#)
[從ESA查詢DHAP事件](#)
[從GUI檢視或更新DHAP配置](#)
[從CLI檢視或更新DHAP配置](#)
[相關資訊](#)

簡介

本檔案介紹如何在思科電子郵件安全裝置(ESA)上找到與目錄蒐集攻擊預防(DHAP)警報相關的資訊。

從ESA查詢DHAP事件

描述DHAP事件的條目駐留在郵件日誌中。以下是發生DHAP時的郵件日誌條目示例：

```
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
```

註：預設情況下，**在搜**索中會查詢/24網路掩碼。

在CLI中輸入此查詢以檢視郵件日誌：

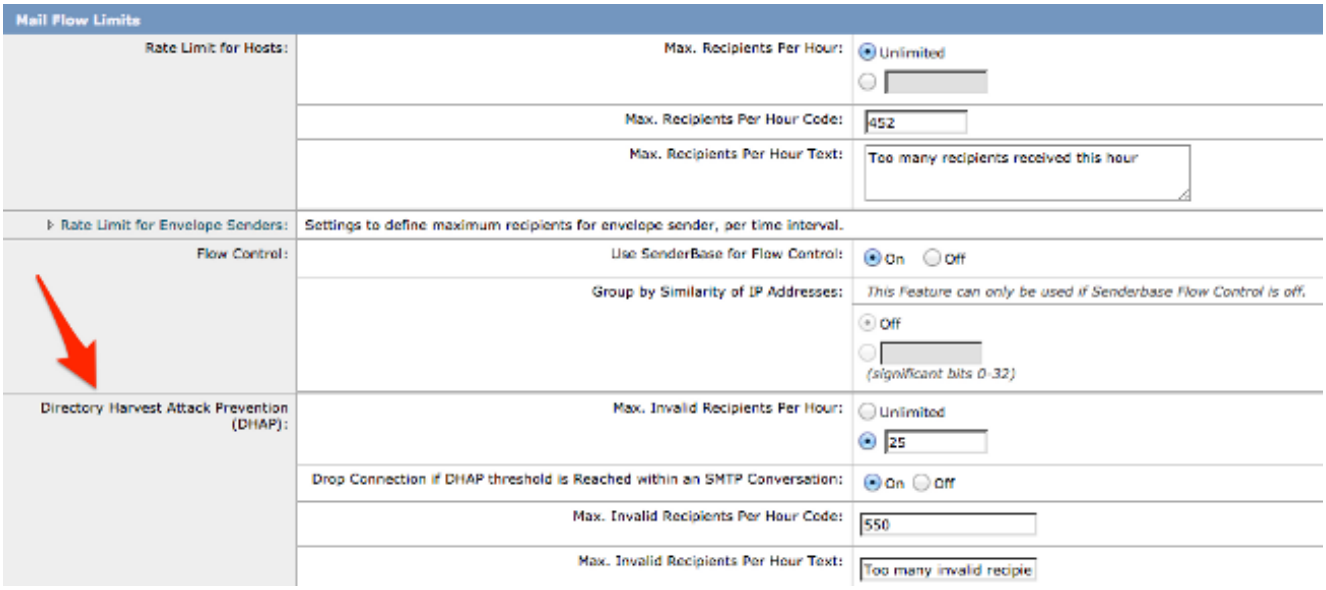
```
myesa.local> grep "dhap_limit=" mail_logs
```

DHAP計數器包括收件人訪問表(RAT)拒絕和輕型目錄訪問協定(LDAP)接受查詢拒絕。DHAP設定是在郵件流策略中配置的。

從GUI檢視或更新DHAP配置

完成以下步驟，以便從GUI檢視或編輯DHAP配置引數：

1. 導航到**Mail Policies > Mail Flow Policies**。
2. 按一下策略名稱進行編輯，或按一下**Default Policy Parameters**檢視當前DHAP配置。
3. 根據需要對**目錄收集攻擊預防(DHAP)**部分進行更改：



4. 按一下**Submit**，然後按一下**Commit**以儲存更改。

從CLI檢視或更新DHAP配置

若要從CLI檢視或編輯DHAP配置參數，請輸入**listenerconfig > edit [*listener number*] > hostaccess > default**命令：

```
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]>
```

如果選擇進行更新，請確保返回主CLI提示符並提交所有更改。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與檔案 - Cisco Systems