What does the "Potential Directory Harvest Attack detected" warning message mean?

Inhalt

[Einführung](#)
[Benutzeroberfläche](#)
[CLI](#)
[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird die Fehlermeldung "Möglicher Directory-Harvest-Angriff" beschrieben, die auf der Cisco E-Mail Security Appliance (ESA) empfangen wurde.

Was bedeutet die Warnmeldung "Potenzielle Directory-Harvest-Angriffe erkannt"?

Administratoren für die ESA haben die folgende DHAP-Warnmeldung (Directory Harvest Attack Prevention) erhalten:

```
The Warning message is:

Potential Directory Harvest Attack detected. See the system mail logs for more
information about this attack.

Version: 8.0.1-023
Serial Number: XXBAD1112DYY-008X011
Timestamp: 22 Sep 2014 21:21:32 -0600
```

Diese Warnmeldungen werden als informativ angesehen und Sie sollten keine Maßnahmen ergreifen müssen. Ein externer Mailserver versuchte zu viele ungültige Empfänger und löste die DHAP-Warnung (Directory Harvest Attack Prevention) aus. Die ESA agiert wie konfiguriert, basierend auf der Konfiguration der Mail-Richtlinien.

Dies ist die maximale Anzahl ungültiger Empfänger pro Stunde, die der Listener von einem Remotehost erhält. Dieser Grenzwert stellt die Gesamtzahl der RAT-Ablehnungen und der Absagen des SMTP-Anrufvorgangs-Servers zusammen mit der Gesamtzahl der Nachrichten an ungültige LDAP-Empfänger dar, die in der SMTP-Konversation verworfen oder in der Arbeitswarteschlange abgesetzt wurden (wie im LDAP konfiguriert, werden die Einstellungen des zugeordneten Listeners akzeptiert). Weitere Informationen zum Konfigurieren von DHAP für LDAP Accept-Abfragen finden Sie im Kapitel "LDAP-Abfragen" im Email Security-Benutzerhandbuch.

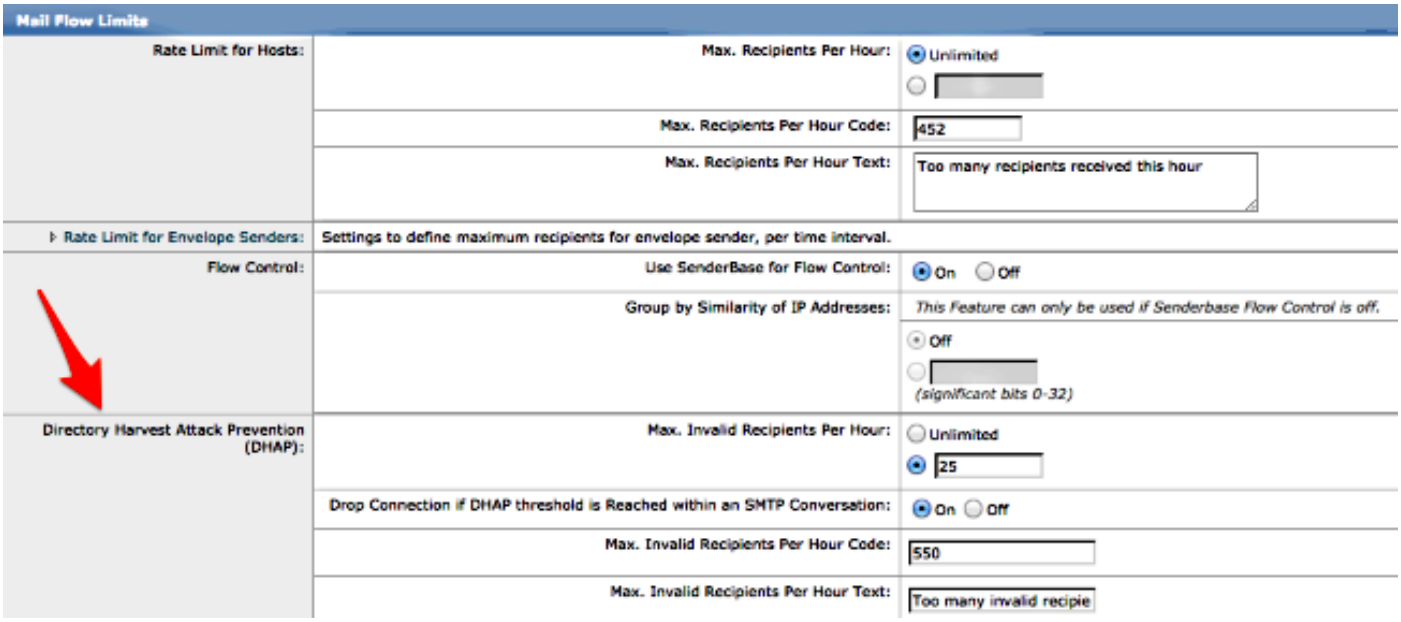
Sie können Ihr Alarmprofil mit **Warnmeldungen** anpassen, um diese herauszufiltern, wenn Sie diese Warnmeldungen nicht erhalten möchten:

```
myesa.local> alertconfig

Sending alerts to:
robert@domain.com
Class: All - Severities: All

Initial number of seconds to wait before sending a duplicate alert: 300
Maximum number of seconds to wait before sending a duplicate alert: 3600
Maximum number of alerts stored in the system are: 50

Alerts will be sent using the system-default From Address.

Cisco IronPort AutoSupport: Enabled
You will receive a copy of the weekly AutoSupport reports.

Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify alert subscription for an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> edit

Please select the email address to edit.
1. robert@domain.com (all)
[]> 1

Choose the Alert Class to modify for "robert@domain.com".
Press Enter to return to alertconfig.
1. All - Severities: All
2. System - Severities: All
3. Hardware - Severities: All
4. Updater - Severities: All
5. Outbreak Filters - Severities: All
6. Anti-Virus - Severities: All
7. Anti-Spam - Severities: All
8. Directory Harvest Attack Prevention - Severities: All
```

Oder über die GUI-**Systemverwaltung > Warnungen >** ***Empfängeradresse*** und ändern Sie den erhaltenen Schweregrad oder die gesamte Warnmeldung.

Benutzeroberfläche

Um Ihre DHAP-Konfigurationsparameter in der GUI anzuzeigen, klicken Sie durch **Mail-Policys > Mail Flow Policies (Mail-Policys) >** ***klicken Sie auf den*** **Policy Name (Name** ***der*** **Richtlinie),** ***um*** **die Standard-Policy-Parameter** ***zu bearbeiten oder*** **>** und nehmen Sie Änderungen am **Mail Flow Limits/Directory Harvest Attack Prevention (DHAP)** vor:



Senden und **bestätigen** Sie Ihre Änderungen an der GUI.

CLI

Um Ihre DHAP-Konfigurationsparameter über die CLI anzuzeigen, verwenden Sie **listenerconfig > Edit** (*wählen Sie die Nummer des zu bearbeitenden Listeners aus*) **> hostaccess > default**, um die DHAP-Einstellungen zu bearbeiten:

```
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]>
```

Wenn Sie Aktualisierungen oder Änderungen vornehmen, kehren Sie zur CLI-Hauptaufforderung zurück, und **bestätigen Sie** alle Änderungen.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems