

Que « le message d'avertissement détecté par attaque potentielle de récolte de répertoire » signifie-t-il ?

Contenu

[Introduction](#)

[GUI](#)

[CLI](#)

[Informations connexes](#)

Introduction

Ce document décrit le message d'erreur « de répertoire d'attaque potentielle de récolte » comme reçu sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Que « le message d'avertissement détecté par attaque potentielle de récolte de répertoire » signifie-t-il ?

Les administrateurs pour l'ESA ont reçu le message d'avertissement suivant de la prévention d'attaque de récolte de répertoire (DHAP) :

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
```

Ces alertes sont considérées informationnelles et vous ne devriez pas devoir ne prendre aucune mesure. Un serveur de messagerie extérieur a tenté trop de destinataires non valides et a déclenché l'alerte DHAP (prévention d'attaque de récolte de répertoire). L'ESA agit en tant que configuré basé sur la configuration de politique de messagerie.

C'est le nombre maximal de destinataires non valides par heure où l'auditeur recevra d'un serveur distant. Ce seuil représente le nombre total de rejets de serveur de rejets de RAT et d'appel-en avant de SMTP combinés avec le nombre total de messages aux destinataires non valides de LDAP abandonnés dans la conversation de SMTP ou rebondis dans la file d'attente de travail (comme configuré dans le LDAP recevez les configurations sur l'auditeur associé). Pour plus

d'informations sur configurer DHAP pour le LDAP recevez les requêtes, voient que le « LDAP questionne » le chapitre du [guide utilisateur de sécurité du courrier électronique](#).

Vous pouvez ajuster votre profil vigilant avec l'**alertconfig** pour filtrer ces derniers si vous ne souhaitez pas recevoir ces alertes :

```
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
```

Ou de l'**administration système GUI > alerte > adresse réceptive** et modifie la sévérité reçue, ou l'alerte en sa totalité.

GUI

Pour visualiser vos paramètres de configuration DHAP du GUI, clic par des **stratégies de messagerie > stratégies > clic de flux de courrier le nom de stratégie à éditer, ou paramètres de stratégie par défaut >** et à apporter des modifications aux **limites de flux de courrier/à la section de la prévention d'attaque récolte de répertoire (DHAP)** comme nécessaire :

Soumettez et commettez vos modifications au GUI.

CLI

Pour visualiser vos paramètres de configuration DHAP du CLI, le **listenerconfig** d'utilisation > **éditent** (*choisissant le nombre de l'auditeur pour éditer*) > **des hostaccess** > **par défaut** pour éditer les configurations DHAP :

```
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
```

Si vous faites n'importe quelles mises à jour ou changez, revenez à la demande principale CLI et **commettez** toutes les modifications.

[Informations connexes](#)

- [Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur](#)
- [Support et documentation techniques - Cisco Systems](#)