Comment archiver les e-mails sur l'appliance de sécurité de la messagerie et la sécurité de la messagerie cloud ?

Contenu

Introduction

Ce document décrit les étapes à suivre pour archiver les e-mails sur l'appliance de sécurité de la messagerie électronique (ESA) et la sécurité de la messagerie électronique dans le cloud (CES) afin de les récupérer et de les examiner.

Informations générales

Lorsque vous archivez des courriels sur l'ESA et la CES, ils peuvent être utilisés pour répondre aux exigences de la réglementation ou pour fournir un moyen supplémentaire de données pour un diagnostic et un examen plus poussés du courrier. L'archivage des e-mails agit comme un stockage secondaire des e-mails au format de journal de boîte aux lettres dans sa source d'origine pour les administrateurs afin de récupérer et de valider.

- Il est recommandé de conserver les valeurs par défaut si vous décidez d'activer l'archivage des e-mails. Les valeurs par défaut sont 10 Mo par journal et 10 journaux maximum conservés. Les journaux continueront d'être ajoutés et restaurés en fonction de la taille du fichier journal lui-même. Les fichiers journaux de la boîte aux lettres d'archivage sont remplis en fonction du débit du trafic de messagerie électronique transitant par l'appliance. Au fur et à mesure de la création d'un plus grand nombre de journaux, les anciens journaux de la boîte de réception des archives sont supprimés dans l'espace libre pour la création du nouveau journal.
- Assurez-vous que votre périphérique dispose d'un espace disque suffisant avant d'augmenter la taille des fichiers journaux de la boîte de réception des archives et le nombre maximal de fichiers journaux conservés.
- Afin d'empêcher la génération des journaux de la boîte aux lettres d'archivage, vous devez

désactiver la fonction d'archivage par stratégie.

Note: Les journaux des boîtes aux lettres d'archivage ESA et CES ne peuvent pas être récupérés par l'appliance de gestion de la sécurité (SMA) et sont stockés localement pour chaque ESA et CES avec la fonctionnalité activée.

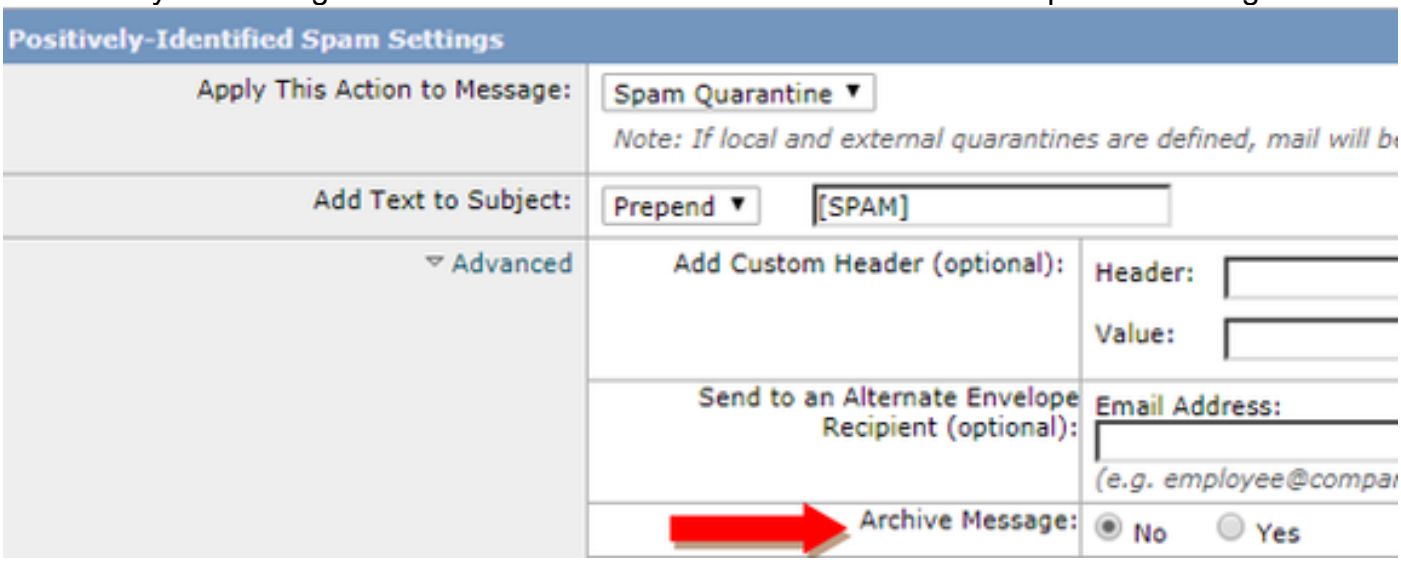
Comment archiver les e-mails sur l'ESA et la CES ?

L'archivage des e-mails est disponible avec les filtres anti-spam, anti-virus, Advanced Malware Protection, Graymail et Message. L'action d'archivage peut être configurée via l'interface utilisateur graphique (GUI) ou l'interface de ligne de commande (CLI) pour les fonctions Anti-spam, Anti-virus, Advanced Malware Protection et Graymail.

Pour les filtres de messages, l'action d'archivage peut être configurée uniquement à l'aide de l'interface de ligne de commande.

Configurer l'archive antispam

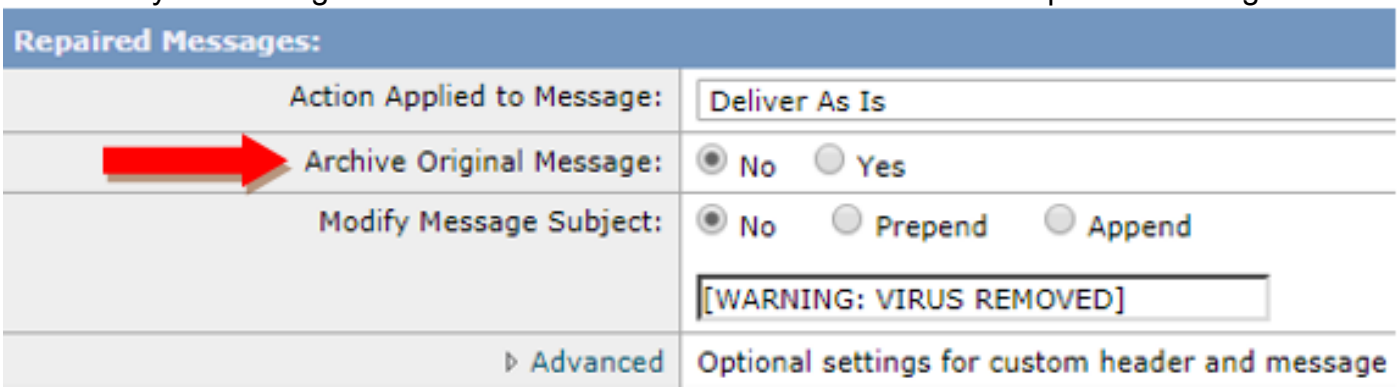
1. Accédez à l'**interface utilisateur graphique > Politiques de messagerie > Politiques de messagerie entrante/sortante**.
2. Cliquez sur les paramètres antispam de la stratégie correspondante afin de configurer l'archivage des e-mails.
3. Cliquez sur **Avancé** sur les paramètres disponibles pour les paramètres de spam d'identification positive et/ou de spam suspecté.
4. Appuyez sur la case d'option en regard de Oui afin d'archiver les e-mails avec le verdict anti-spam respectif.
5. Envoyez la configuration et confirmez ces modifications comme indiqué dans l'image.



Configurer l'archive antivirus

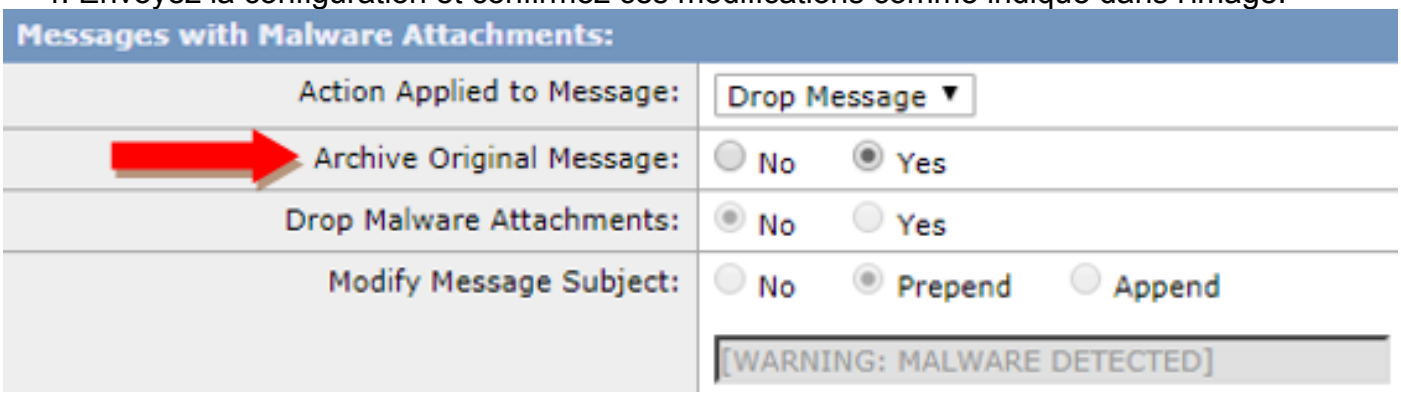
1. Accédez à l'**interface utilisateur graphique > Politiques de messagerie > Politiques de messagerie entrante/sortante**.
2. Cliquez sur les paramètres antivirus de la stratégie correspondante afin de configurer l'archivage des e-mails.
3. Sur chacun des verdicts d'analyse que vous souhaitez archiver le message d'origine,

appuyez sur la case d'option en regard de Oui afin d'archiver.
4. Envoyez la configuration et confirmez ces modifications comme indiqué dans l'image.



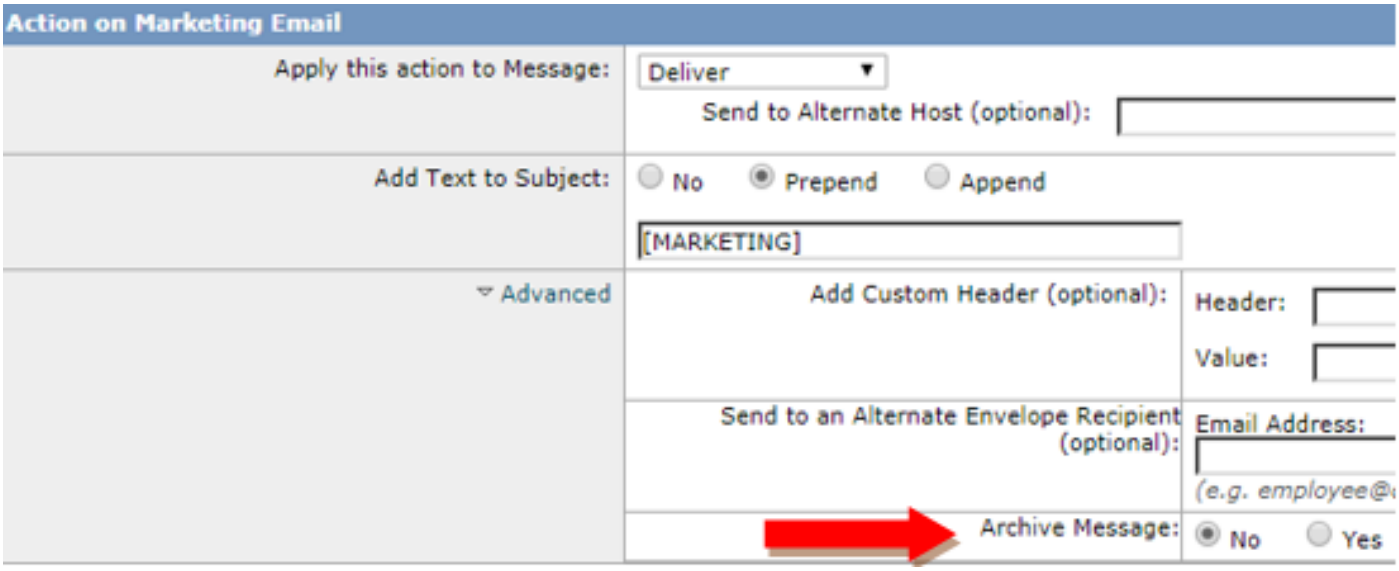
Configurer l'archive Advanced Malware Protection

1. Accédez à l'**interface utilisateur graphique > Politiques de messagerie > Politiques de messagerie entrante/sortante**.
2. Cliquez sur Advanced Malware Protectionsettings (Paramètres avancés de protection contre les programmes malveillants) dans la stratégie correspondante afin de configurer l'archivage des e-mails.
3. Sur chacun des verdicts d'analyse que vous souhaitez archiver le message d'origine, appuyez sur la case d'option en regard de Oui afin d'archiver.
4. Envoyez la configuration et confirmez ces modifications comme indiqué dans l'image.



Configurer l'archive Graymail

1. Accédez à l'**interface utilisateur graphique > Politiques de messagerie > Politiques de messagerie entrante/sortante**.
2. Cliquez sur les paramètres Graymail de la stratégie correspondante afin de configurer l'archivage des e-mails.
3. Cliquez sur Avancé dans les paramètres disponibles pour Marketing, Social, Bulk.
4. Appuyez sur la case d'option en regard de Oui afin d'archiver les courriels avec le verdict Graymail respectif.
5. Envoyez la configuration et confirmez ces modifications.



Configurer l'archivage du filtre de messages

> **Remarque** : un filtre de messages avec action d'archivage est requis pour afficher les journaux archivés. Les filtres de messages ne peuvent être créés que dans l'interface de ligne de commande.

Exemple de filtre :

```
Test_Archive:
if (mail-from == "test1@cisco.com")
{
archive("Test");
}
```

1. Connectez-vous au périphérique sur la CLI.
2. Créez un filtre de message comme indiqué dans l'exemple de filtre fourni.
3. Envoyez ce filtre et confirmez vos modifications.

Valider la disponibilité des journaux de la boîte aux lettres d'archivage

Lorsque la configuration de l'archive est validée pour les services respectifs, les e-mails archivés sont stockés dans un fichier journal au format mbox. Afin de vérifier si les journaux d'archivage sont disponibles pour la récupération, accédez à l'**interface utilisateur graphique > Administration système > Abonnements aux journaux**.

Les archives des services de sécurité créent un journal distinct avec un type de journal d'archivage, comme illustré dans l'image :

Configured Log Subscriptions

Add Log Subscription...

Log Settings	Type ▲	Log Files	Rollover Interval
amp	AMP Engine Logs	amp/	None
amparchive	AMP Archive	amparchive/	None
antispam	Anti-Spam Logs	antispam/	None
antivirus	Anti-Virus Logs	antivirus/	None
asarchive	Anti-Spam Archive	asarchive/	None
authentication	Authentication Logs	authentication/	None
avarchive	Anti-Virus Archive	avarchive/	None

Pour les filtres de messages, la configuration de l'archive est affichée à partir de l'**interface de ligne de commande uniquement** :

- **filtres > logconfig**

```
demigod.cisco.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> logconfig

Currently configured logs:
    Log Name          Log Type                  Retrieval          Interval
 ------------------------------------------------------------------------------
 1. Test              Filter Archive Logs       Manual Download    None
```

Récupérer les journaux de la boîte aux lettres

Pour les appliances autonomes, ces journaux de boîtes aux lettres peuvent être récupérés directement à partir de l'interface utilisateur graphique. Naviguez jusqu'à **l'interface utilisateur graphique > Administration système >** Abonnements aux **journaux** et cliquez sur **Fichiers journaux** pour le journal d'archives que vous allez récupérer.

Pour les appliances en cluster, les journaux de boîtes aux lettres peuvent être récupérés à l'aide de FTP/Secure Copy (SCP), comme décrit dans [cet article](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00...). (https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118315-technote-esa-00...)

Informations connexes

- [Cisco Email Security Appliance - Guides de l'utilisateur final]
- [Qu'est-ce que le format de boîte aux lettres UNIX ?]
- [Où sont stockés les journaux sur l'appliance de sécurité de la messagerie Cisco (ESA) et comment y accéder ?]

- Extraction d'un e-mail à partir des journaux de la boîte aux lettres d'archivage
- Support et documentation techniques - Cisco Systems