Prévention des pertes de données - Dépannage des erreurs de classification et d'analyse

Contenu

[Introduction](#)
[Conditions préalables](#)
[Informations importantes](#)
[Exemples de journaux de violation et d'absence de journal de violation](#)
[Liste de contrôle de dépannage](#)
[Confirmation de la version du moteur DLP](#)
[Activation de la journalisation du contenu mappé](#)
[Vérification de la configuration du comportement d'analyse](#)
[Vérification de la configuration de l'échelle de gravité](#)
[Vérification des adresses e-mail ajoutées aux champs Filtrer les expéditeurs et les destinataires](#)
[Informations connexes](#)

Introduction

Ce document décrit les méthodes courantes de dépannage des erreurs de classification et des échecs d'analyse (ou des échecs) liés à la prévention de perte de données (DLP) sur le dispositif de sécurité de la messagerie électronique (ESA).

Conditions préalables

- ESA exécutant AsyncOS 11.x ou version ultérieure.
- Clé de fonction DLP installée et utilisée.

Informations importantes

Il est essentiel de noter que DLP sur l'ESA est plug-and-play en ce sens que vous pouvez l'activer, créer une stratégie et commencer à analyser les données sensibles ; cependant, vous devez également savoir que les meilleurs résultats ne seront obtenus qu'après avoir ajusté DLP pour qu'il corresponde aux besoins spécifiques de votre entreprise. Cela inclut des éléments tels que les types de stratégies DLP, les détails de mise en correspondance des stratégies, l'ajustement de l'échelle de gravité, le filtrage et des personnalisations supplémentaires.

Exemples de journaux de violation et d'absence de journal de violation

Voici quelques exemples de violations DLP que vous pouvez voir dans les journaux de messagerie et/ou le suivi des messages. La ligne de connexion inclut un horodatage, un niveau de journalisation, un numéro MID, une violation ou aucun facteur de violation, de gravité et de risque, ainsi que la politique qui a été mise en correspondance.

```
Thu Jul 11 16:05:28 2019 Info: MID 40 DLP violation. Severity: CRITICAL (Risk Factor: 96). DLP
policy match: 'US HIPAA and HITECH'.

Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy
match: 'US State Regulations (Indiana HB 1101)'.
```

Lorsqu'aucune violation n'est détectée, les journaux de messagerie et/ou le suivi des messages enregistrent simplement *DLP sans violation*.

```
Mon Jan 20 12:59:01 2020 Info: MID 26245883 DLP no violation
```

Liste de contrôle de dépannage

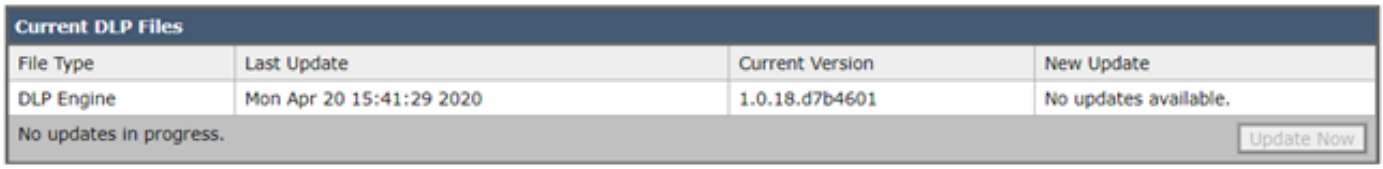
Vous trouverez ci-dessous les éléments courants qui peuvent être examinés lors de la gestion des erreurs de classification DLP ou des échecs/échecs d'analyse.

> **Note**: La liste n'est pas exhaustive. Veuillez contacter le centre d'assistance technique de Cisco si vous souhaitez voir quelque chose inclus.

Confirmation de la version du moteur DLP

Les mises à jour du moteur DLP ne sont pas automatiques par défaut, il est donc essentiel de s'assurer que vous exécutez la dernière version qui inclut des améliorations récentes ou des corrections de bogues.

Vous pouvez accéder à *Data Loss Prevention* sous *Security Services* dans l'interface utilisateur graphique pour confirmer la version actuelle du moteur et voir si des mises à jour sont disponibles. Si une mise à jour est disponible, vous pouvez cliquer sur *Mettre à jour maintenant* pour effectuer la mise à jour.

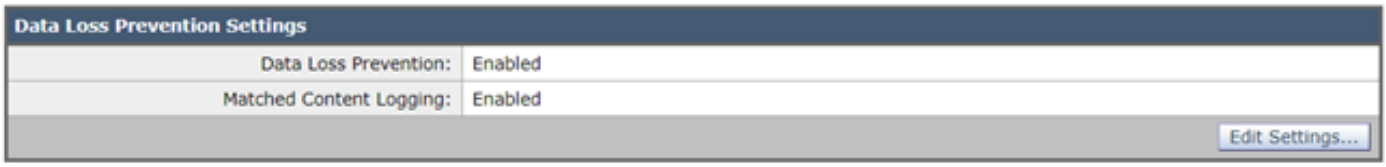


Activation de la journalisation du contenu mappé

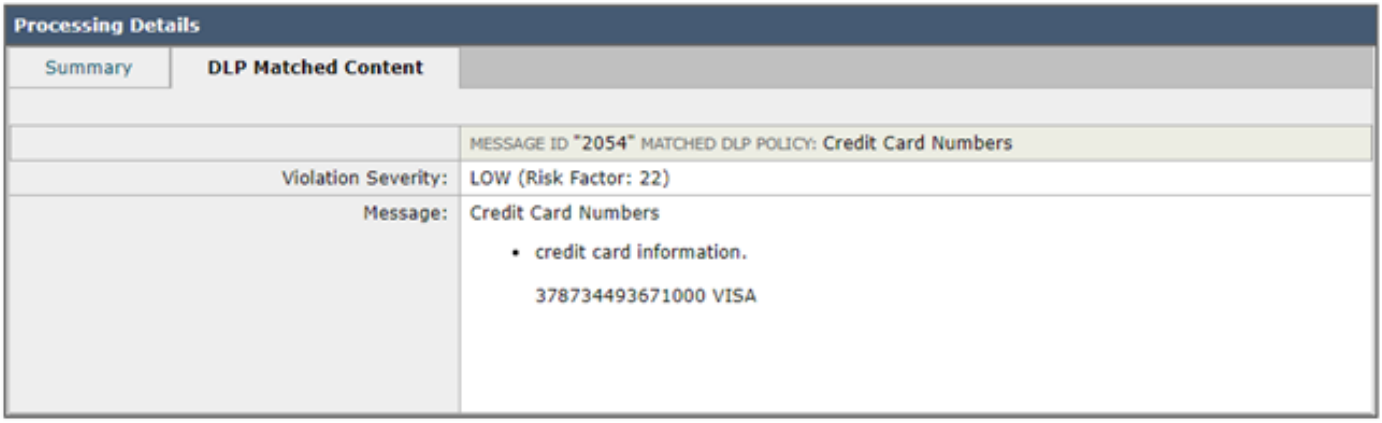
DLP offre la possibilité de consigner le contenu qui enfreint vos stratégies DLP, ainsi que le contenu environnant. Ces données peuvent ensuite être affichées dans *Suivi des messages* pour vous aider à identifier le contenu d'un e-mail qui peut causer une violation particulière.

> **Attention** : Il est important de savoir que si cette option est activée, ce contenu peut inclure des données sensibles telles que les numéros de carte de crédit et de sécurité sociale, etc.

Vous pouvez accéder à *Prévention de perte de données* sous *Services de sécurité* dans l'interface utilisateur graphique pour voir si *la journalisation de contenu correspondante* est activée.



Exemple de journalisation de contenu mappé vue dans le suivi des messages



Vérification de la configuration du comportement d'analyse

La configuration du comportement d'analyse sur le ESA aura également un impact sur la fonctionnalité de l'analyse DLP. Si vous regardez la capture d'écran ci-dessous comme exemple, qui a une **taille maximale** d'**analyse** de **pièce jointe** configurée de **5M**, tout ce qui est plus grand peut entraîner l'absence de l'analyse DLP. En outre, l'**action pour les pièces jointes avec le** paramètre **des types MIME** est un autre élément courant que vous voudrez examiner. Cette valeur doit être définie sur la valeur par défaut **Skip** afin que les types MIME listés soient ignorés et que tout le reste soit analysé. S'il est défini sur Analyser, nous *analysons uniquement les types MIME* répertoriés dans le tableau.

De même, d'autres paramètres répertoriés ici peuvent avoir un impact sur l'analyse DLP et doivent être pris en compte en fonction du contenu de la pièce jointe/de l'e-mail.

Vous pouvez naviguer jusqu'à *Scan Behavior* sous *Security Services* dans l'interface utilisateur graphique ou en exécutant la commande **scanconfig** dans l'interface de ligne de commande.

Attachment Type Mappings

Add Mapping... | Import List...

Fingerprint / MIME	Type	Edit	Delete
MIME Type	audio/*	Edit...	
MIME Type	video/*	Edit...	
MIME Type	image/*	Edit...	
Fingerprint	Media	Edit...	
Fingerprint	Image	Edit...	

Export List...

Global Settings

Action for attachments with MIME types / fingerprints in table above:	Skip
Maximum depth of attachment recursion to scan:	5
Maximum attachment size to scan:	5M
Attachment Metadata scan:	Enabled
Attachment scanning timeout:	30 seconds
Assume attachment matches pattern if not scanned for any reason:	No
Assume zip file to be unscannable if files in the archive cannot be read?	No
Action when message cannot be deconstructed to remove specified attachments:	Deliver
Bypass all filters in case of a content or message filter error:	Yes
Encoding to use when none is specified:	US-ASCII
Convert opaque-signed messages to clear-signed (S/MIME unpacking):	Disabled
Safe Print settings	Maximum File Size: 5M Maximum Page Count: 10 Document Quality: 70
Actions for Unscannable Messages due to decoding errors found during URL Filtering Actions:	Disabled
Action when a message is unscannable due to extraction failures:	Deliver As Is
Action when a message is unscannable due to RFC violations:	Disabled

Edit Global Settings...

Vérification de la configuration de l'échelle de gravité

Les seuils d'échelle de gravité par défaut seront suffisants pour la plupart des environnements ; toutefois, si vous devez les modifier pour faciliter la correspondance Faux négatif (FN) ou Faux positif (FP), vous pouvez le faire. Vous pouvez également confirmer que votre stratégie DLP utilise les seuils par défaut recommandés en créant une nouvelle stratégie factice, puis en les comparant.

> **Remarque** : les différentes politiques prédéfinies (par exemple HIPAA aux États-Unis par rapport à PCI-DSS) auront une évolutivité différente.

Severity Scale:

IGNORE	LOW	MEDIUM	HIGH	CRITICAL
0 - 34	35 - 54	55 - 72	73 - 87	88 - 100

Edit Scale...

Vérification des adresses e-mail ajoutées aux champs Filtrer les expéditeurs et les destinataires

Vérifiez que les entrées entrées dans l'un de ces champs correspondent au cas correct des adresses e-mail de l'expéditeur et/ou du destinataire. Le champ Filtrer les expéditeurs et les destinataires est **sensible à la casse**. La stratégie DLP ne se déclenchera pas si l'adresse de messagerie ressemble à "TestEmail@mail.com" dans le client de messagerie et est entrée en tant

que "testemail@mail.com" dans ces champs.

Informations connexes

- Cisco Email Security Appliance - Guides de l'utilisateur final
- Qu'est-ce que la prévention des pertes de données ?
- Déclencher une violation DLP pour tester une politique HIPAA sur l'ESA