防数据丢失 — 错误分类和扫描故障故障排除

目录

简介

本文档介绍在邮件安全设备(ESA)上排除与防数据丢失(DLP)相关的错误分类和扫描失败（或未命中）的常见方法。

先决条件

- 运行AsyncOS 11.x或更高版本的ESA。
- DLP功能密钥已安装且正在使用。

重要信息

请务必注意，ESA上的DLP是即插即用的，因为您可以启用它、创建策略并开始扫描敏感数据；但是，您也应注意，只有在调整DLP以满足公司特定要求后，才能获得最佳效果。这包括DLP策略类型、策略匹配详细信息、调整严重性范围、过滤和其他自定义。

违规与无违规日志示例

以下是一些DLP违规示例，您可能在邮件日志和/或邮件跟踪中看到。日志行将包括时间戳、日志记录级别、MID #、违规或无违规、严重性和风险因素以及匹配的策略。

```
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)'.
```

如果未发现违规，邮件日志和/或邮件跟踪将只记录*DLP无违规*。

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

故障排除核对表

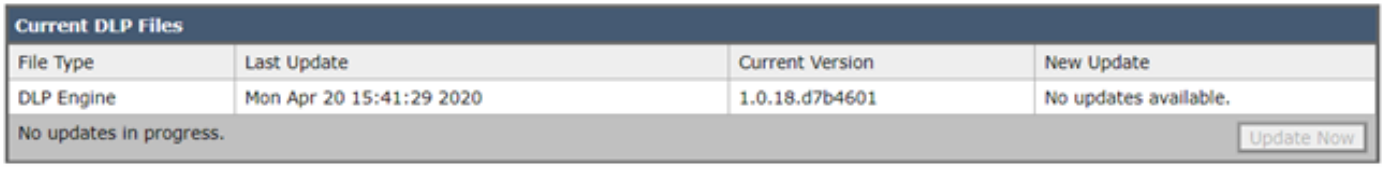
下面提供的是处理DLP错误分类或扫描失败/丢失时可以查看的常见项目。

> **注意**：但这不是一个详尽列表。如果您有希望查看的内容，请联系思科TAC。

确认DLP引擎版本

默认情况下，DLP引擎更新不是自动的，因此确保运行的最新版本包括任何最新增强功能或漏洞修复功能至关重要。

您可以导航到GUI*中"安全服务"*下的*防数据丢失*，以确认当前引擎版本并查看是否有可用的更新。如果更新可用，则可以单击"立*即更新*"以执行更新。

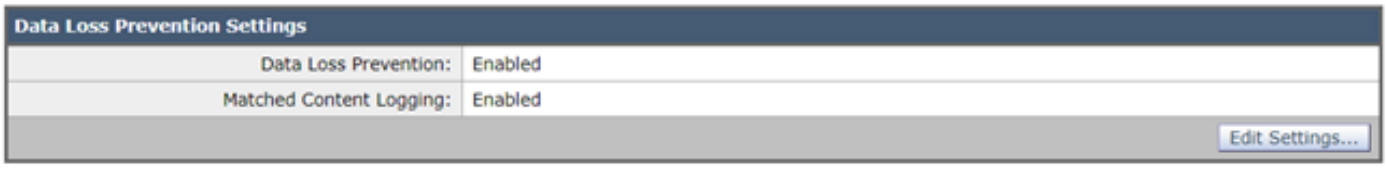


启用匹配的内容日志记录

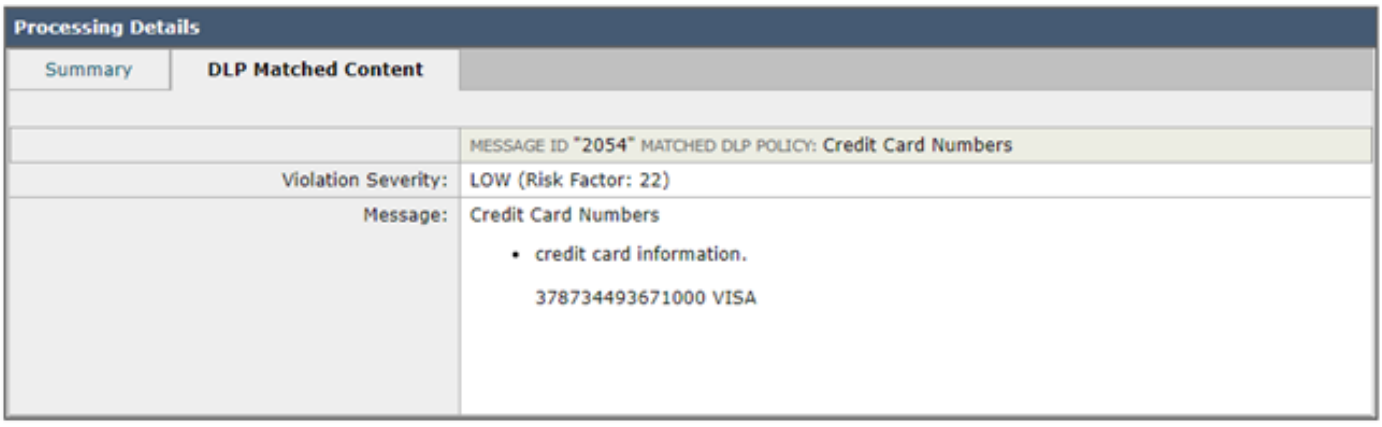
DLP提供了记录违反DLP策略的内容以及周围内容的选项。然后，可以在邮件跟踪中查*看此数*据，以帮助跟踪电子邮件中哪些内容可能导致特定违规。

> **警告**：必须知道，如果启用，此内容可能包括敏感数据，如信用卡号和社会保险号等。

您可以导航到GUI*中"安全服务"*下的"数*据丢失保护"*，查看是否启用了"匹配内容日志记录"。



在邮件跟踪中看到的匹配内容日志记录示例



检查扫描行为配置

ESA上的扫描行为配置也将影响DLP扫描的功能。以下屏幕截图为例，其配置的最大附**件扫描大**小**为5M**，任何较大的内容都可能导致DLP扫描丢失。此外，具有**MIME类型设置的附**件的操作是另一个您要查看的常见项。应将此设置为默认值**Skip**，以便跳过列出的MIME类型并扫描其他所有类型。如果设置为"扫描"，则我们只*扫描表中列出*的那些MIME类型。

同样，此处列出的其他设置可能会影响DLP扫描，应根据附件/邮件内容考虑。

您可以导航到GUI中*安全服务*下的*扫描行为(Scan Behavior)，或通过在CLI中运行***scanconfig**命令。

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...

查看严重性扩展配置

默认严重性级别阈值将足以满足大多数环境；但是，如果需要修改它们以帮助进行False Negative(FN)或False Position(FP)匹配，则可以执行此操作。您还可以通过创建新的虚拟策略并进行比较来确认您的DLP策略是否使用了建议的默认阈值。

注意：不同的预定义策略（例如，美国HIPAA与PCI-DSS）将具有不同的扩展。

Severity Scale:

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

Edit Scale...

查看添加到过滤器发件人和收件人字段的电子邮件地址

检查输入到这些字段中的任何条目是否与发件人和/或收件人电子邮件地址的正确大小写匹配。“过滤发件人和收件人”(Filter Senders and Recipients)字段区**分大小写**。如果邮件客户端中的邮件地址看起来像“TestEmail@mail.com”，并且在这些字段中输入为“testemail@mail.com”，则不会触发DLP策略。

相关信息

- [思科邮件安全设备 — 最终用户指南]
- [什么是防数据丢失？]
- [触发DLP违规以在ESA上测试HIPAA策略]