排除DLP错误分类和扫描故障

目录

简介

重要信息

违规与无违规日志示例

检查表故障排除

- 确认DLP引擎版本
- 启用匹配的内容日志记录
  - 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
- 查看严重性等级配置
- 查看添加到过滤器发件人和收件人字段的邮件地址

相关信息

简介

本文档介绍常见方法，用于排除与ESA上的DLP相关的错误分类和扫描故障（或失败）。

重要信息

请务必注意，思科邮件安全设备(ESA)上的数据丢失防护(DLP)是即插即用的，您可以启用它、创建策略，并开始扫描敏感数据；但是，您还应注意，只有调整DLP以满足公司特定要求后，才能获得最佳效果。这将包括DLP策略的类型、策略匹配详细信息、如何调整严重性范围、过滤器和其他自定义等内容。

违规与无违规日志示例

以下是一些可在邮件日志和/或邮件跟踪中看到的DLP违规示例。日志行包括时间戳、日志级别、MID编号、违规或不违规、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 m
```

```
Thu Jul 11 16:41:50 2019 Info: MID 46 DLP violation. Severity: LOW (Risk Factor: 24). DLP policy match:
```

如果未发现违规，则邮件日志和/或邮件跟踪仅记录DLP无违规。

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

检查表故障排除

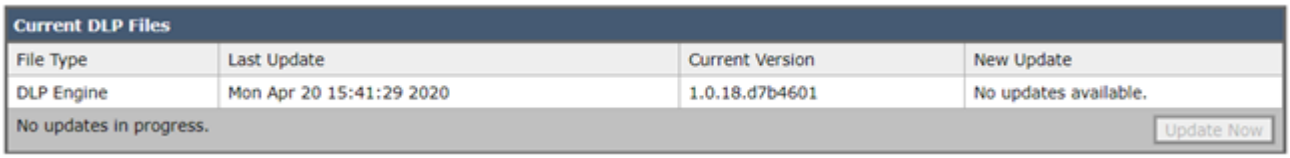
此处提供了一些常见项目，可在处理DLP错误分类或扫描失败/错误时进行审核。

注意：但这不是一个详尽列表。如果您有希望查看的项目，请联系思科TAC。

确认DLP引擎版本

默认情况下，DLP引擎更新不会自动更新，因此，确保运行包含任何最新增强功能或漏洞修复的最新版本至关重要。

您可以在GUI中的安全服务下导航到数据丢失保护，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Update Now执行更新。

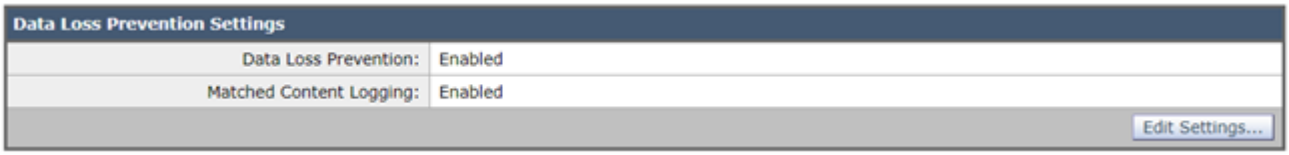


启用匹配的内容日志记录

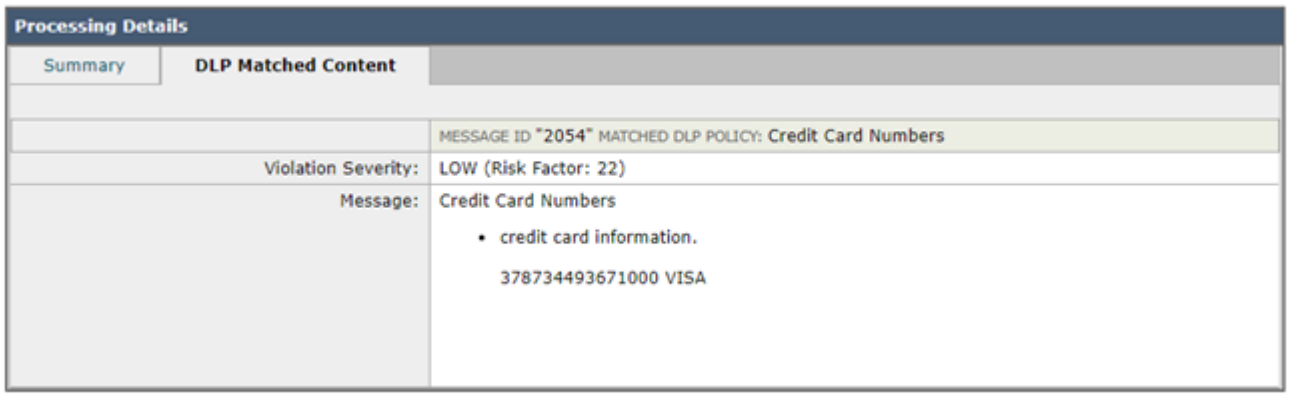
DLP提供记录违反您的DLP策略内容的选项。然后，可以在邮件跟踪中查看此数据，以帮助跟踪邮件中的哪些内容会导致特定违规。

警告：请注意，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），了解这一点非常重要。

您可以在GUI中的安全服务下导航到数据丢失保护，以查看是否已启用匹配的内容记录。



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会影响DLP后面的功能。如果以配置的最大附件扫描大小为5M的映像为例，任何较大的内容都可能导致DLP扫描丢失。此外，对具有MIME类型设置的附件的操作是另一个要审阅的常见项。这应设置为默认值Skip，以便跳过列出的MIME类型并扫描所有其他类型。如果设置为Scan，则ESA仅扫描表中列出的MIME类型。

同样，此处列出的其他设置可能会影响DLP扫描，并且应该根据附件/邮件内容予以考虑。

您可以在GUI中的安全服务下或从CLI中的scanconfig命令导航到扫描行为。

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...

查看严重性等级配置

大多数环境的默认严重性级别阈值已足够；但是，如果您需要修改它们来协助处理假阴性(FN)或假阳性(FP)匹配，则可以执行此操作。您还可以创建新的虚拟策略并进行比较，以确认DLP策略是否使用建议的默认阈值。

注意：不同的预定义策略（例如美国HIPAA与PCI-DSS）具有不同的规模

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邮件地址

检查在这些字段中输入的条目是否与发件人和/或收件人电子邮件地址的大小写匹配。Filter Senders and Recipients字段区分大小写。如果邮件客户端中的电子邮件地址类似于“TestEmail@mail.com”，且在这些字段中输入“testemail@mail.com”，则DLP策略不会触发。



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违规以测试ESA上的HIPAA策略

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。