使用SMA API在PVO隔离区中自动发布消息

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

初始测试

- 数据结构
- 使用GUI和API验证结果
- 使用CURL进行初始测试
- 检索所有邮件
- 验证总计数
- 按域过滤MID
- 过滤MID和创建负载
- 执行发布(POST)
- 检查结果
  - 检查mail_logs
  - 直接在GUI中检查
- 使用API检查
  - POSTMAN
  - 卷曲

批量报文发布（500条报文）

- 调整批量操作的API参数
- 扩展工作流程

相关信息

简介

本文档介绍如何通过REST API在Cisco SMA上自动进行消息管理和释放，以便处理大量消息。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco SMA产品知识
- 熟悉REST API基础知识、用于JSON处理的Postman、curl和JQ
- SMA API访问的有效凭证
- 命令行
- 对SMA的网络访问
- 安装的工具：curl（用于请求）、JQ（用于JSON操作）和Postman等客户端用于初始测试
- 在SMA上执行消息释放操作的适当用户角色

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

自动化消息发布对于邮件量大的环境至关重要。通过使用API，管理员可以过滤特定邮件（例如，按发件人）并以编程方式释放这些邮件，与GUI中的手动管理相比，可减少操作时间并降低人为错误的风险。

初始测试

要管理隔离区，首先要执行初始查询以验证连接并确认数据结构。

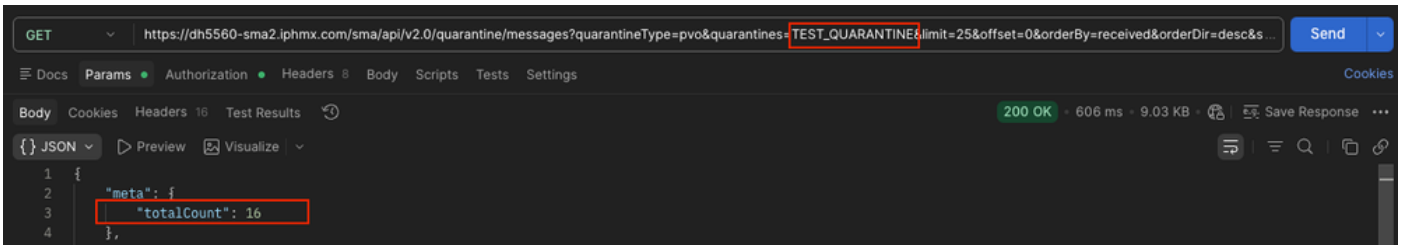
```
https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages?quarantineType=pvo&quarantines=TEST_QUARA
```

数据结构

- API终端：SMA API的基本URL(例如https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages)。
- 隔离区名称：要从中检索邮件的特定PVO隔离区标识符（例如TEST_QUARANTINE）。
- 日期范围:用于定义搜索的特定时间范围的开始日期和结束日期。
- 限制:单个API响应中返回的最大记录数。这有助于管理负载大小，并防止在处理大型队列时超时。
- 偏移：结果集的开始索引。用于分页；例如，将偏移量设置为25会跳过前25条消息，使您可以检索下一批结果。

使用GUI和API验证结果

检索信息时，您可在API调用和GUI中看到相同数量的消息。



postman GET请求

TEST_QUARANTINE	Centralized Policy	16

TEST_QUARANTINE邮件

使用CURL进行初始测试

为授权报头生成Base64身份验证令牌：

```
echo -n 'username:password' | base64
```

检索所有邮件

执行curl请求以将消息提取到本地文件中：

```
curl -X GET "https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages?quarantineType=pvo&quarantin
    -H "Authorization: Basic token-generated-in-base64" \
    -H "Accept: application/json" \
    -o response.json
```

验证总计数

检查收到的消息总数：

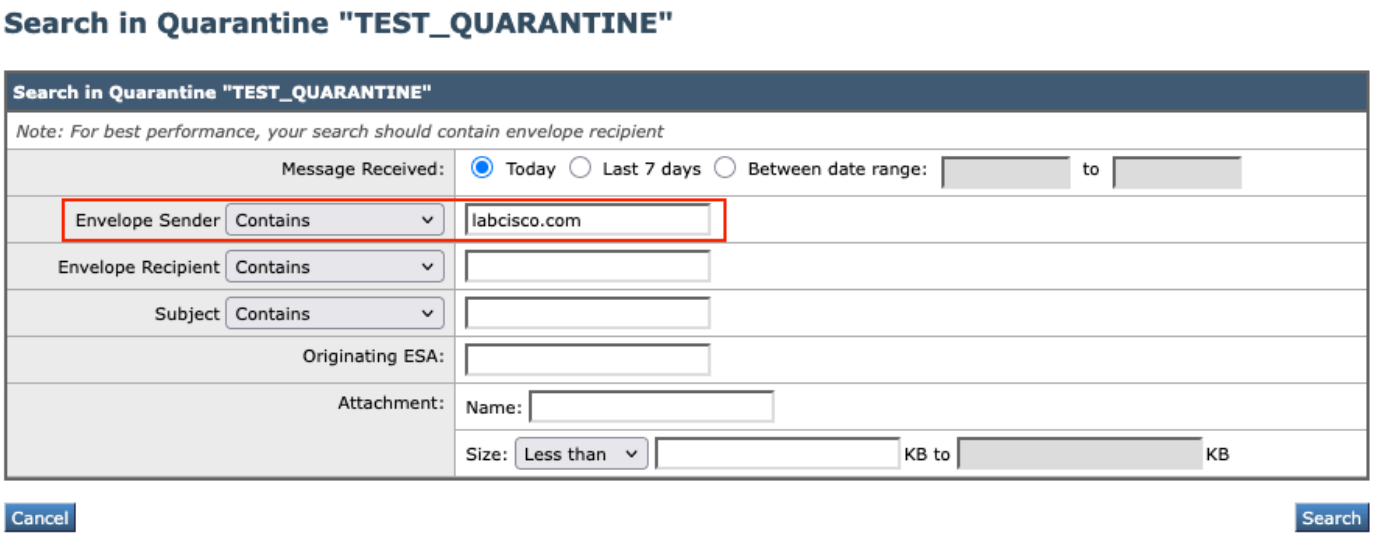
```
$ grep "totalCount" response.json | awk '{ print $2, $3}'
{"totalCount": 24},
```

按域过滤MID

使用JQ过滤要释放的邮件的MID（例如，按域过滤）。

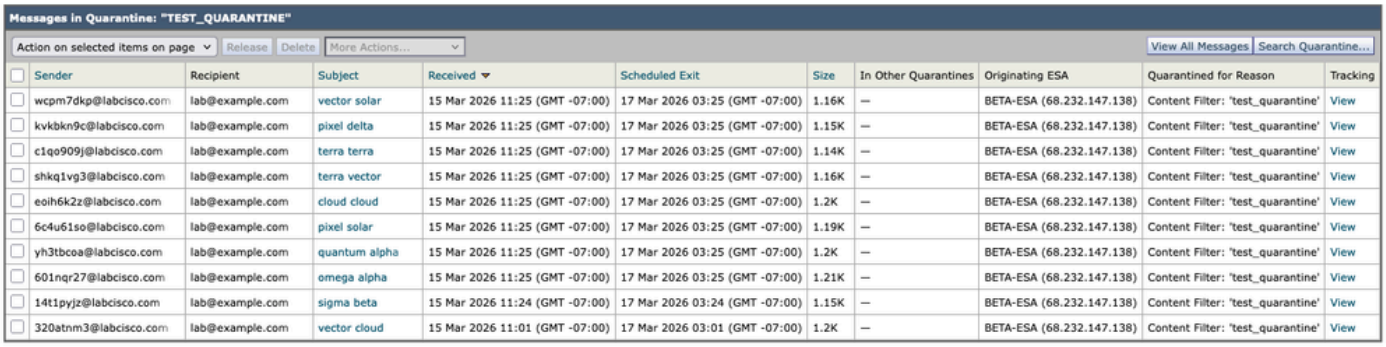
```
$ jq '[.data[] | select(.attributes.sender | endswith("@labcisco.com")) | .mid]' response.json > mids-l
$ cat mids-labcisco-domain.json
[
  440,
  439,
  438,
  437,
  436,
  435,
  434,
  433,
  425,
  414
]
```

如果您在SMA GUI的TEST_QUARANTINE中进行搜索，则可以匹配MID的数量。



隔离区搜索

Messages in Quarantine: "TEST_QUARANTINE"



Messages in Quarantine: "TEST_QUARANTINE"

Action on selected items on page | Release | Delete | More Actions... | View All Messages | Search Quarantine...

Sender	Recipient	Subject	Received	Scheduled Exit	Size	In Other Quarantines	Originating ESA	Quarantined for Reason	Tracking
wcpm7dkp@labcisco.com	lab@example.com	vector solar	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.16K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
kvkbkn9c@labcisco.com	lab@example.com	pixel delta	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.15K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
c1qo909j@labcisco.com	lab@example.com	terra terra	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.14K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
shkq1vg3@labcisco.com	lab@example.com	terra vector	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.16K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
eoih6k2z@labcisco.com	lab@example.com	cloud cloud	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.2K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
6c4u61so@labcisco.com	lab@example.com	pixel solar	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.19K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
yh3tbcoa@labcisco.com	lab@example.com	quantum alpha	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.2K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
601nqr27@labcisco.com	lab@example.com	omega alpha	15 Mar 2026 11:25 (GMT -07:00)	17 Mar 2026 03:25 (GMT -07:00)	1.21K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
14t1pyjz@labcisco.com	lab@example.com	sigma beta	15 Mar 2026 11:24 (GMT -07:00)	17 Mar 2026 03:24 (GMT -07:00)	1.15K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View
320atnm3@labcisco.com	lab@example.com	vector cloud	15 Mar 2026 11:01 (GMT -07:00)	17 Mar 2026 03:01 (GMT -07:00)	1.2K	–	BETA-ESA (68.232.147.138)	Content Filter: 'test_quarantine'	View

隔离区结果

过滤MID和创建负载

过滤MID并生成负载文件。

```
$ jq '{action:"release", quarantineType:"pvo", quarantineName:"TEST_QUARANTINE", mids:[.data[] | select
$ cat payload.json
{
  "action": "release",
  "quarantineType": "pvo",
  "quarantineName": "TEST_QUARANTINE",
  "mids": [
    440,
    439,
    438,
    437,
    436,
    435,
    434,
    433,
    425,
    414
  ]
}
```

执行发布(POST)

向SMA发送发布请求：

```
$ curl -X POST "https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages" \
        -H "Authorization: Basic token-generated-in-base64" \
        -H "Content-Type: application/json" \
        -d @payload.json
{"data": {"action": "release", "totalCount": 10}}
```

检查结果

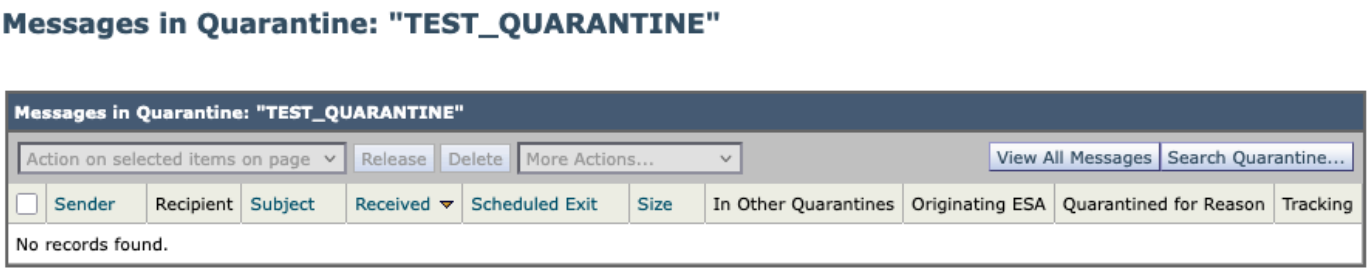
检查mail_logs

在检查mail_logs中是否存在已释放的邮件时，可以按grep "release" mail_logs和上面过滤的相同MID（与已释放的MID相同）进行过滤。

```
Sun Mar 15 11:48:21 2026 Info: MID 436 released from quarantine "TEST_QUARANTINE" (manual) t=1393
Sun Mar 15 11:48:21 2026 Info: MID 425 released from quarantine "TEST_QUARANTINE" (manual) t=1411
Sun Mar 15 11:48:21 2026 Info: MID 414 released from quarantine "TEST_QUARANTINE" (manual) t=2787
Sun Mar 15 11:48:21 2026 Info: MID 433 released from quarantine "TEST_QUARANTINE" (manual) t=1397
Sun Mar 15 11:48:21 2026 Info: MID 440 released from quarantine "TEST_QUARANTINE" (manual) t=1387
Sun Mar 15 11:48:21 2026 Info: MID 439 released from quarantine "TEST_QUARANTINE" (manual) t=1388
Sun Mar 15 11:48:21 2026 Info: MID 434 released from quarantine "TEST_QUARANTINE" (manual) t=1396
Sun Mar 15 11:48:21 2026 Info: MID 437 released from quarantine "TEST_QUARANTINE" (manual) t=1391
Sun Mar 15 11:48:21 2026 Info: MID 435 released from quarantine "TEST_QUARANTINE" (manual) t=1395
Sun Mar 15 11:48:21 2026 Info: MID 438 released from quarantine "TEST_QUARANTINE" (manual) t=1390
```

直接在GUI中检查

如果您对放行邮件的域执行相同的搜索，您会发现搜索没有结果，因为所有邮件都已放行。

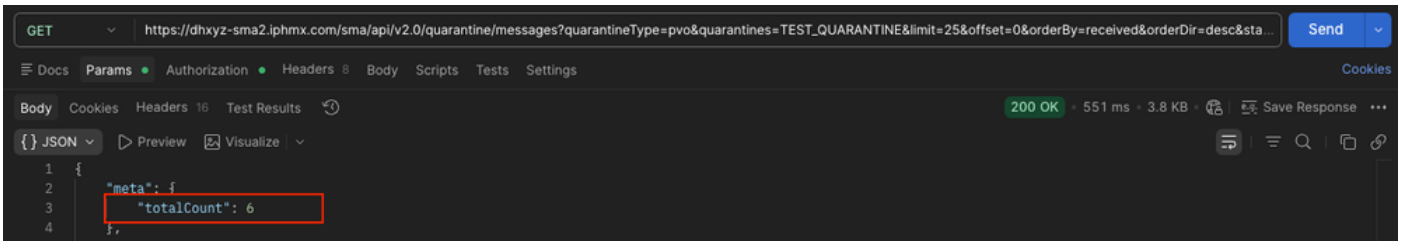


隔离新结果

使用API检查

POSTMAN

从检索所有消息中重新运行GET命令，以确认totalCount已减少或特定MID不再存在。



postman GET查询

卷曲

```
$ curl -X GET "https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages?quarantineType=pvo&quarant
          -H "Authorization: Basic token-generated-in-base64" \
          -H "Accept: application/json" \
          -o response.json
$ jq '[.data[] | select(.attributes.sender | endswith("@labcisco.com")) | .mid]' response.json > mids-l
$ cat mids-labcisco-domain.json
[]
```

批量报文发布（500条报文）

为了有效地处理批量操作，您必须了解如何使用分页管理大型数据集。当需要处理大量消息时，必须计算限制和偏移参数，以确保检索完整的数据集，而不会超过API响应限制。

调整批量操作的API参数

检索大量邮件时，请使用此逻辑配置请求：

- 限制:这定义每个请求返回的记录数。虽然可以将此值设置为较高值（例如，500或1000）以同时捕获更多数据，但请注意系统性能和可能的超时。
- 偏移：这将定义结果集的起点。如果消息总数超过限制，则必须执行多个请求，将偏移量递增到每次后续呼叫中的限制值（例如，offset=0,offset=500,offset=1000）。

扩展工作流程

上一个10条报文示例中使用的流程是所有批量操作的基础。要缩放您的工作流程，只需通过系统性地递增偏移参数来遍历队列。通过“播放”这些值（调整限制以定义批大小和页面导航的偏移量），您可以有效地检索和处理整个隔离队列，而不管邮件总数如何。

相关信息

- AsyncOS API 16.0 for Cisco Secure Email and Web Manager — 入门指南 — GD（通用部署）
- 思科技术支持和下载

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）。