Automatisierte Nachrichtenfreigabe in PVO-Quarantänen mit SMA API

Einleitung

In diesem Dokument wird beschrieben, wie die Nachrichtenverwaltung und -freigabe auf einer Cisco SMA über die REST-API automatisiert werden kann, um große Nachrichtenmengen zu verarbeiten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco SMA-Produktkenntnisse
- Vertrautheit mit REST API-Grundlagen, Postman, Curl und JQ für JSON-Verarbeitung
- Gültige Anmeldeinformationen für SMA API-Zugriff
- Befehlszeile
- Netzwerkzugriff auf die SMA
- Installierte Tools: curl (für Anfragen), JQ (für JSON-Manipulation) und ein Client wie Postman für erste Tests
- Geeignete Benutzerrolle auf der SMA zum Durchführen von Nachrichtenfreigabeaktionen

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Die automatische Freigabe von Nachrichten ist in Umgebungen mit hohem E-Mail-Volumen unerlässlich. Mithilfe der API können Administratoren bestimmte Nachrichten (z. B. nach Absender) filtern und programmgesteuert freigeben. Dies reduziert die Betriebszeit und das Risiko menschlicher Fehler im Vergleich zur manuellen Verwaltung in der GUI.

Anfängliche Tests

Um die Quarantäne zu verwalten, führen Sie zunächst eine erste Abfrage durch, um die Verbindung zu überprüfen und die Datenstruktur zu bestätigen.

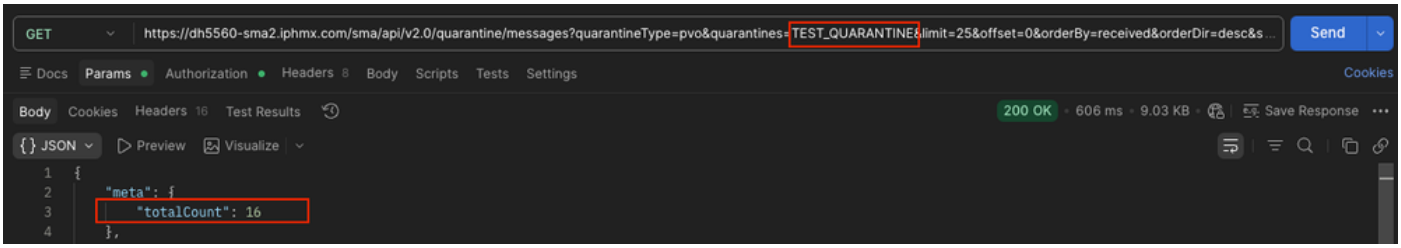
```
https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages?quarantineType=pvo&quarantines=TEST_QUARA
```

Datenstruktur

- API-Endpunkt: Die Basis-URL für die SMA-API (z. B. https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages).
- Quarantänename: Die spezifische PVO-Quarantäne-ID (z. B. TEST_QUARANTINE), von der Sie Nachrichten abrufen möchten.
- Datumsbereich: startDate und endDate, mit denen der spezifische Zeitrahmen für die Suche definiert wird.
- Grenzwert: Die maximale Anzahl von Datensätzen, die in einer einzelnen API-Antwort zurückgegeben werden. Dies erleichtert die Verwaltung der Payload-Größe und verhindert Zeitüberschreitungen bei großen Warteschlangen.
- Versatz: Der Startindex der Ergebnismenge. Dies wird für das Paginieren verwendet. Wenn Sie beispielsweise einen Offset von 25 festlegen, werden die ersten 25 Nachrichten übersprungen, sodass Sie den nächsten Stapel von Ergebnissen abrufen können.

Überprüfen der Ergebnisse mit der Benutzeroberfläche und der API

Wenn Sie die Informationen abrufen, können Sie die gleiche Anzahl an Nachrichten im API-Aufruf und in der GUI sehen.



POST GET-Anforderung

TEST_QUARANTINE	Centralized Policy	16

TEST_QUARANTINE-Meldungen

Anfängliche Tests mit CURL

Generieren Sie Ihr Base64-Authentifizierungstoken für den Autorisierungs-Header:

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

Alle Nachrichten abrufen

Führen Sie die Curl-Anforderung aus, um die Nachrichten in eine lokale Datei zu extrahieren:

```
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
```

Gesamtanzahl überprüfen

Überprüfen Sie die Gesamtzahl der empfangenen Nachrichten:

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

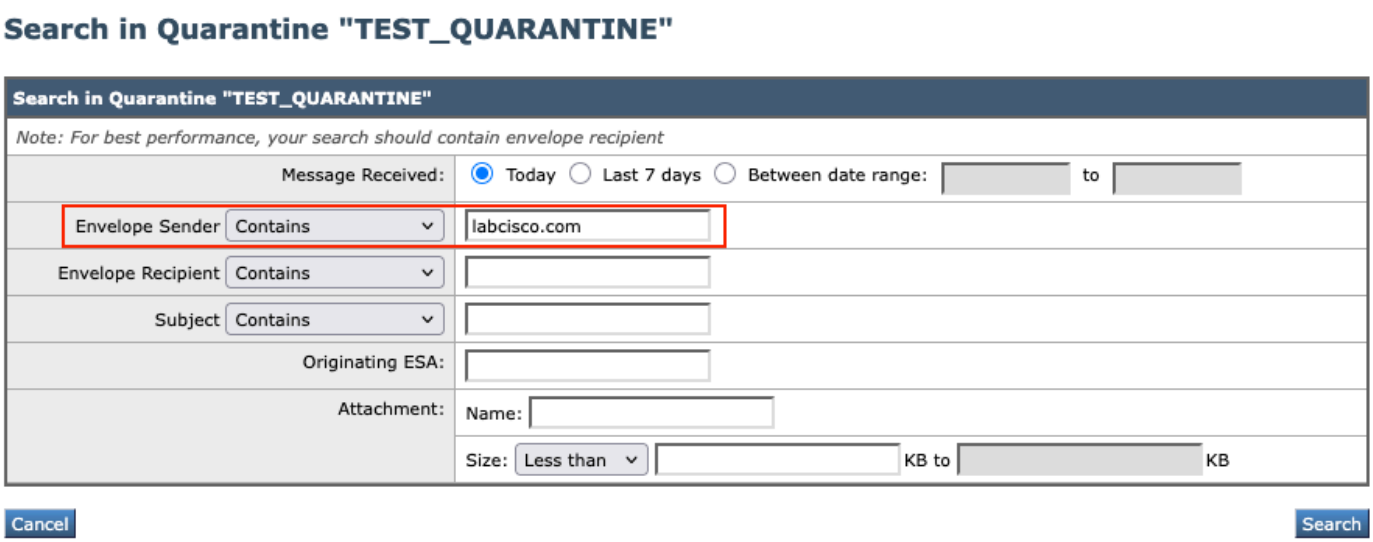
MIDs pro Domäne filtern

Verwenden Sie JQ, um die MIDs der Nachrichten zu filtern, die Sie veröffentlichen möchten (z. B. Filtern nach Domäne).

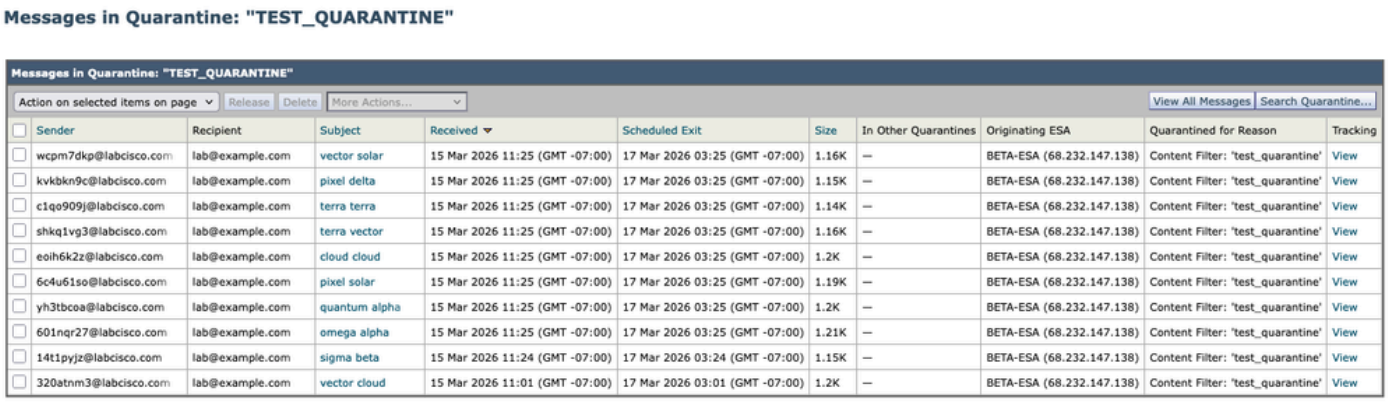
```
$ jq '[.data[] | select(.attributes.sender | endswith("@labcisco.com")) | .mid]' response.json > mids-l
$ cat mids-labcisco-domain.json
[
```

```
  440,
  439,
  438,
  437,
  436,
  435,
  434,
  433,
  425,
  414
]
```

Die Anzahl der MIDs kann übereinstimmen, wenn Sie die TEST_QUARANTINE in der SMA-GUI durchsuchen.



Quarantänesuche



Quarantäne-Ergebnisse

MIDs filtern und Payload erstellen

Filtern Sie die MIDs, und generieren Sie die Payload-Datei.

```
$ 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
  ]
}
```

Ausführen des Releases (POST)

Senden Sie die Freigabeanfrage an die SMA:

```
$ 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}}
```

Überprüfen der Ergebnisse

E-Mail-Protokolle überprüfen

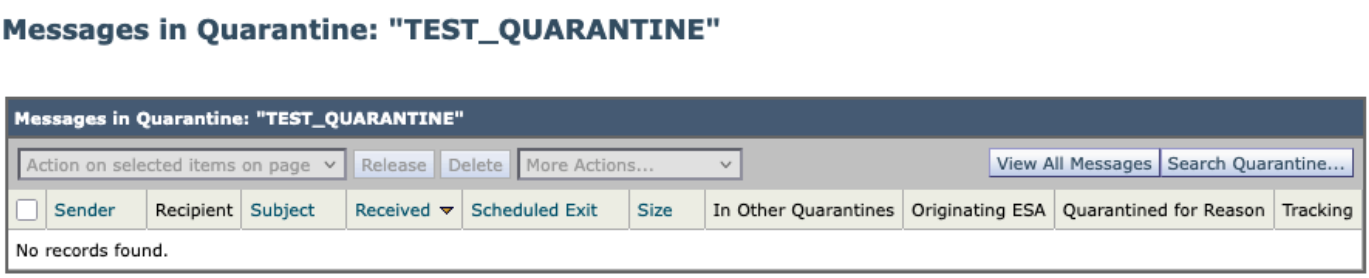
Wenn Sie mail_logs auf freigegebene Nachrichten überprüfen, können Sie nach grep "release" mail_logs und den gleichen MIDs, die Sie oben filtern, filtern, die gleichen, die freigegeben wurden.

```
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
```

Direkte Überprüfung in der Benutzeroberfläche

Wenn Sie die gleiche Suche für die Domain, die Sie die Nachrichten freigegeben, Sie sehen, dass die Suche keine Ergebnisse, da alle Nachrichten freigegeben wurden.

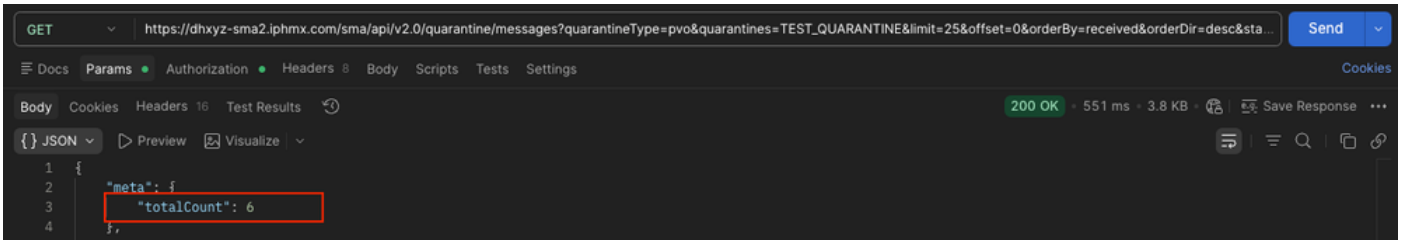


neue Ergebnisse in Quarantäne verschieben

Prüfen mit API

Postbote

Führen Sie den Befehl GET unter Retrieve All Messages (Alle Nachrichten abrufen) erneut aus, um zu bestätigen, dass totalCount abgenommen hat oder dass die spezifischen MIDs nicht mehr vorhanden sind.



Postman-GET-Abfrage

CURL

```
$ 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
[]
```

Bulk Message Release (500 Nachrichten)

Um Massenvorgänge effektiv zu verarbeiten, müssen Sie wissen, wie Sie große Datasets mithilfe von Paginierung verwalten. Wenn Sie eine große Anzahl von Meldungen verarbeiten müssen, müssen Sie die Grenzwert- und Offset-Parameter berechnen, um sicherzustellen, dass Sie den gesamten Datensatz abrufen, ohne die API-Antworteinschränkungen zu überschreiten.

Anpassen von API-Parametern für Massenvorgänge

Verwenden Sie diese Logik, um Ihre Anforderung zu konfigurieren, wenn Sie eine große Anzahl von Nachrichten abrufen:

- Grenzwert: Legt die Anzahl der pro Anforderung zurückgegebenen Datensätze fest. Sie können diesen Wert auf einen hohen Wert (z. B. 500 oder 1000) setzen, um mehr Daten auf einmal zu erfassen. Achten Sie jedoch auf die Systemleistung und mögliche Zeitüberschreitungen.
- Versatz: Dies definiert den Ausgangspunkt Ihrer Ergebnismenge. Wenn die Gesamtzahl der Nachrichten den Grenzwert überschreitet, müssen Sie mehrere Anforderungen ausführen und den Offset bei jedem nachfolgenden Aufruf um den Grenzwert erhöhen (z. B. offset=0, offset=500, offset=1000).

Workflow-Skalierung

Der im vorherigen Beispiel mit 10 Nachrichten verwendete Prozess dient als Grundlage für alle Massenvorgänge. Um Ihren Workflow zu skalieren, durchlaufen Sie einfach die Warteschlange, indem Sie den Offset-Parameter systematisch inkrementieren. Indem Sie mit diesen Werten 'spielen' - also den Grenzwert anpassen, um die Stapelgröße und den Offset zu definieren, um durch die Seiten zu navigieren - können Sie die gesamte Quarantäne-Warteschlange unabhängig von der Gesamtzahl der Nachrichten effektiv abrufen und verarbeiten.

Zugehörige Informationen

- AsyncOS API 16.0 für Cisco Secure Email und Web Manager - Erste Schritte - GD

(Allgemeine Bereitstellung)

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.