Automatische berichtafgifte in PVO-quarantaines met behulp van SMA API

Inleiding

In dit document wordt beschreven hoe het berichtenbeheer en de release op een Cisco SMA via de REST API kunnen worden geautomatiseerd om grote hoeveelheden berichten te verwerken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco SMA productkennis
- Bekendheid met REST API-basics, Postman, curl en JQ voor JSON-verwerking
- Geldige referenties voor SMA API-toegang
- Opdrachtregel
- Netwerktoegang tot de SMA
- Gereedschappen geïnstalleerd: curl (voor verzoeken), JQ (voor JSON-manipulatie) en een client zoals Postman voor de eerste test
- Passende gebruikersrol op de SMA om acties voor het vrijgeven van berichten uit te voeren

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het automatiseren van het vrijgeven van berichten is essentieel voor omgevingen met een hoog e-mailvolume. Door de API te gebruiken, kunnen beheerders specifieke berichten filteren (bijvoorbeeld per afzender) en deze programmatisch vrijgeven, waardoor de operationele tijd en het risico op menselijke fouten worden verminderd in vergelijking met handmatig beheer in de GUI.

eerste beproeving

Om de quarantaine te beheren, begint u met het uitvoeren van een eerste query om de connectiviteit te verifiëren en de gegevensstructuur te bevestigen.

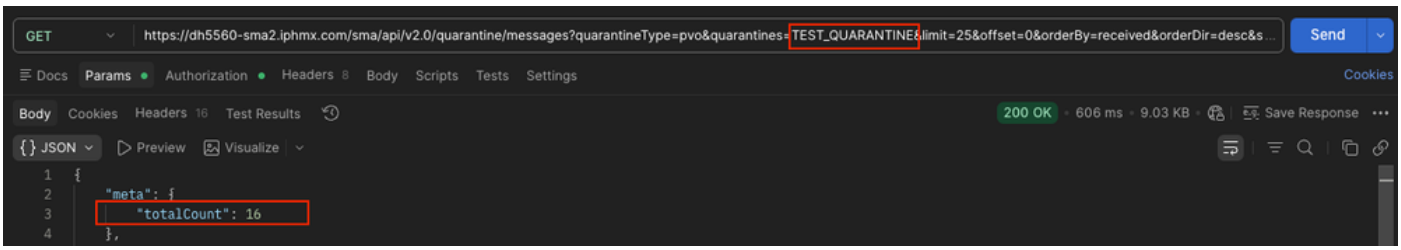
```
https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages?quarantineType=pvo&quarantines=TEST_QUARA
```

gegevensstructuur

- API-eindpunt: de basis-URL voor de SMA-API (bijvoorbeeld [https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages)](https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages).
- Quarantainenaam: De specifieke PVO-quarantaine-id (bijvoorbeeld TEST_QUARANTINE) waarvan u berichten wilt ophalen.
- Datumbereik: de startDate en endDate die worden gebruikt om het specifieke tijdsbestek voor de zoekopdracht te definiëren.
- Limiet: Het maximale aantal records dat in één API-reactie moet worden geretourneerd. Dit helpt bij het beheren van de payloadgrootte en voorkomt time-outs bij het omgaan met grote wachtrijen.
- Offset: De beginindex van de resultatenset. Dit wordt gebruikt voor paginering; bijvoorbeeld, het instellen van een offset van 25 slaat de eerste 25 berichten over, zodat u de volgende batch resultaten kunt ophalen.

Controleer de resultaten met zowel de GUI als de API

Bij het ophalen van de informatie kunt u hetzelfde aantal berichten zien in de API-oproep en in de GUI.



postbode GET-aanvraag

TEST_QUARANTINE	Centralized Policy	16

TEST_QUARANTAINE-berichten

Eerste testen met CURL

Genereer uw Base64-authenticatietoken voor de autorisatieheader:

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

Alle berichten ophalen

Voer het curl-verzoek uit om de berichten in een lokaal bestand uit te pakken:

```
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
```

Totaal aantal controleren

Controleer het totale aantal ontvangen berichten:

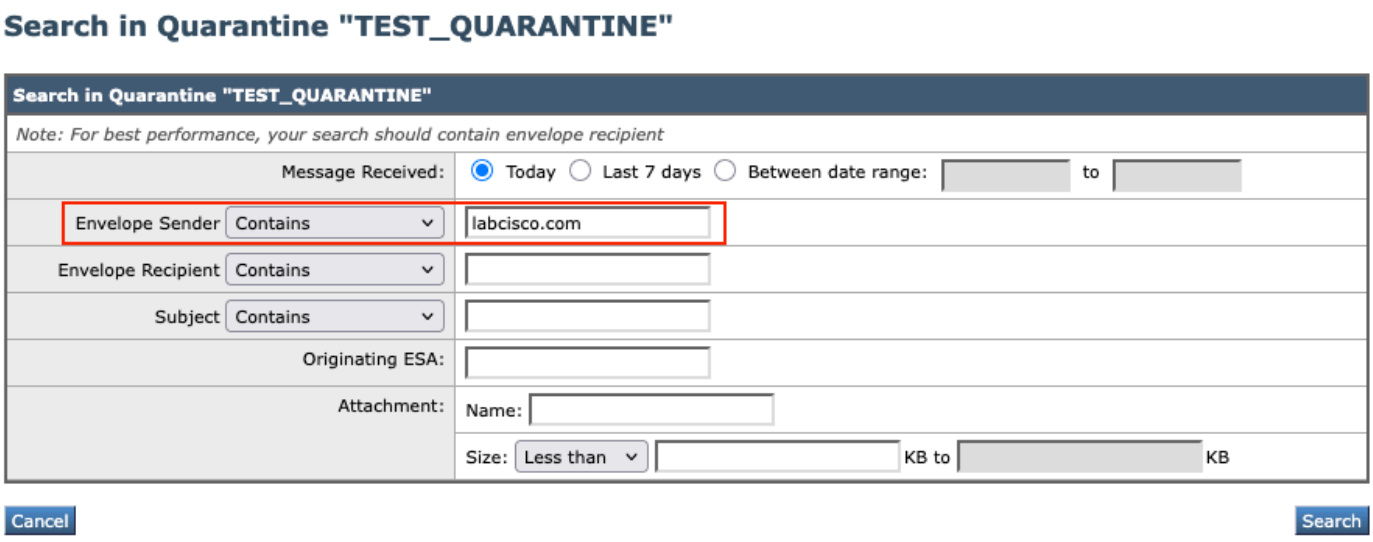
```
$ grep "totalCount" response.json | awk '{ print $2, $3}'
{"totalCount": 24},
```

MID's per domein filteren

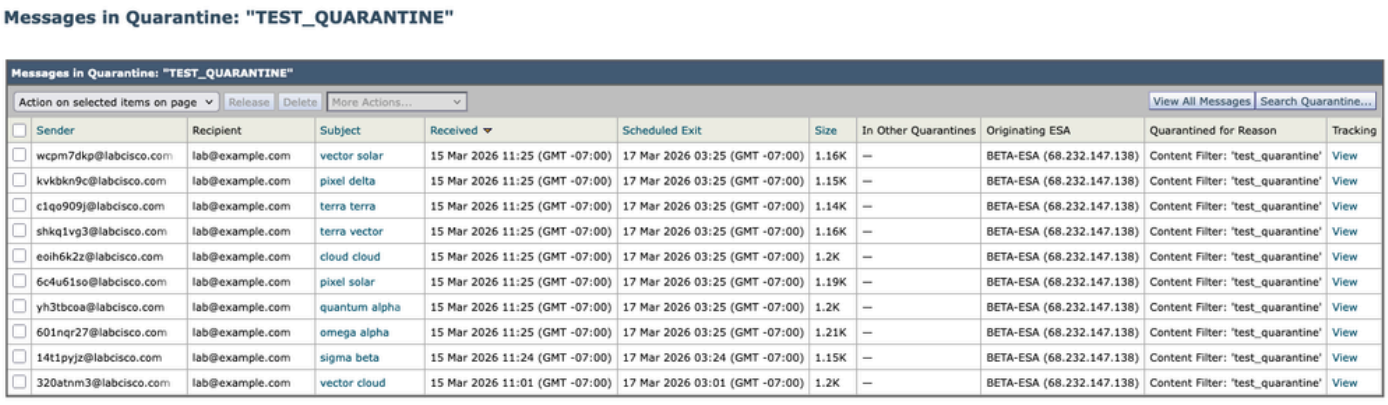
Gebruik JQ om de MID's van de berichten die u wilt vrijgeven te filteren (bijvoorbeeld filteren op domein).

```
$ 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
]
```

Het aantal MID's kan overeenkomen als u een zoekopdracht uitvoert in de TEST_QUARANTINE in de SMA GUI.



quarantaine-onderzoek



quarantaineresultaten

MID's filteren en payload maken

Filter de MID's en genereer het payload-bestand.

```
$ 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
  ]
}
```

De release uitvoeren (POST)

Stuur het vrijgaveverzoek naar de 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}}
```

Controleer de resultaten

Mail_logs controleren

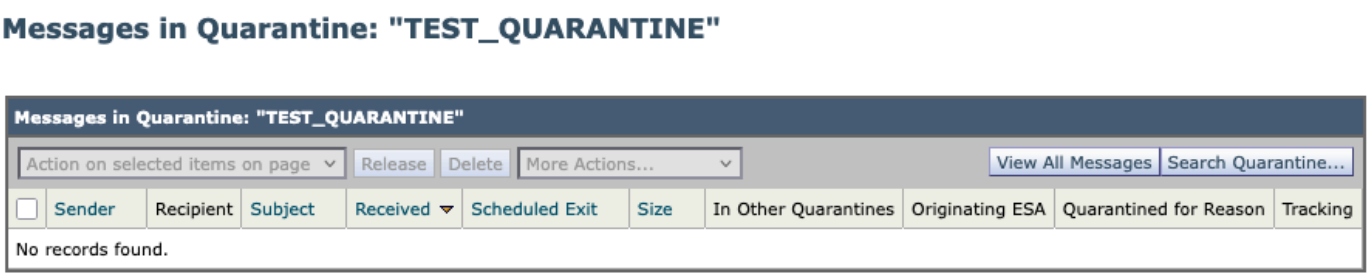
Bij het controleren van mail_logs voor vrijgegeven berichten, kunt u filteren op grep "release" mail_logs en dezelfde MID's die u hierboven filtert, dezelfde als degene die zijn vrijgegeven.

```
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
```

Rechtstreeks controleren in de GUI

Als u dezelfde zoekopdracht uitvoert voor het domein waarin u de berichten hebt vrijgegeven, ziet u dat de zoekopdracht geen resultaten heeft, omdat alle berichten zijn vrijgegeven.

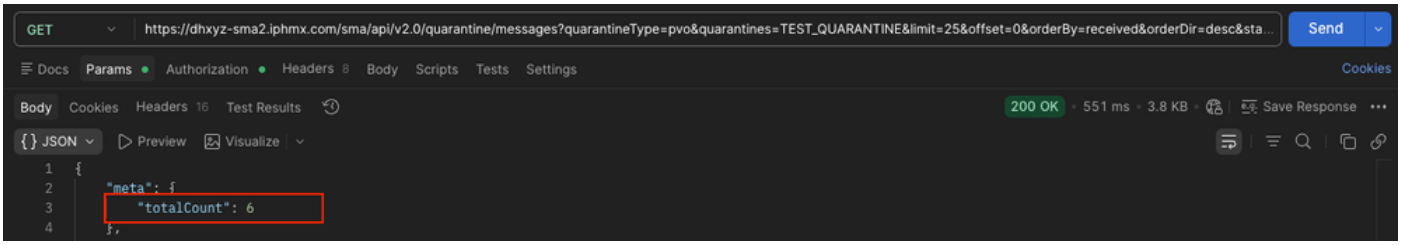


Nieuwe resultaten in quarantaine plaatsen

Controleren met behulp van API

postbode

Voer de opdracht GET opnieuw uit vanuit Alle berichten ophalen om te bevestigen dat het totaal aantal is afgenomen of dat de specifieke MID's niet langer aanwezig zijn.



postbode GET-zoekopdracht

KRULLEN

```
$ 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
[]
```

Bulkbericht vrijgeven (500 berichten)

Om bulkbewerkingen effectief af te handelen, moet u begrijpen hoe u grote datasets kunt beheren met behulp van paginering. Wanneer u een groot aantal berichten moet verwerken, moet u de limiet- en offsetparameters berekenen om ervoor te zorgen dat u de volledige set gegevens ophaalt zonder de API-responsbeperkingen te overschrijden.

API-parameters aanpassen voor bulkbewerkingen

Wanneer u een groot aantal berichten ophaalt, gebruikt u deze logica om uw verzoek te configureren:

- Limiet: Dit definieert het aantal records dat per aanvraag wordt geretourneerd. Hoewel u dit kunt instellen op een hoog aantal (bijvoorbeeld 500 of 1000) om meer gegevens tegelijk vast te leggen, moet u rekening houden met systeemprestaties en potentiële time-outs.
- Offset: hiermee wordt het beginpunt van de resultatenset bepaald. Als uw totale aantal berichten uw limiet overschrijdt, moet u meerdere verzoeken uitvoeren, waarbij de offset wordt verhoogd met de grenswaarde bij elke volgende oproep (bijvoorbeeld offset=0, offset=500, offset=1000).

Schaalbare workflow

Het proces dat in het vorige voorbeeld met 10 berichten is gebruikt, dient als basis voor alle bulkbewerkingen. Om uw workflow te schalen, herhaalt u eenvoudig door de wachtrij door de offset-parameter systematisch te verhogen. Door met deze waarden te 'spelen' - de limiet aan te passen om uw batchgrootte en de offset te definiëren om door de pagina's te navigeren - kunt u uw hele quarantainewachtrij effectief ophalen en verwerken, ongeacht het totale aantal berichten.

Gerelateerde informatie

- AsyncOS API 16.0 voor Cisco Secure Email and Web Manager-handleiding - GD (Algemene implementatie)

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.