Automatizzare il rilascio dei messaggi nelle quarantene PVO utilizzando l'API SMA

Introduzione

In questo documento viene descritto come automatizzare la gestione e il rilascio dei messaggi su uno SMA Cisco tramite l'API REST per elaborare grandi volumi di messaggi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze dei prodotti Cisco SMA
- Familiarità con API REST, Postman, Curl e JQ per l'elaborazione JSON
- Credenziali valide per l'accesso API SMA
- Riga di comando
- Accesso di rete all'SMA
- Strumenti installati: curl (per le richieste), JQ (per la manipolazione JSON) e un client come Postman per il test iniziale
- Ruolo utente appropriato nell'SMA per eseguire le azioni di rilascio del messaggio

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'automazione del rilascio dei messaggi è essenziale per gli ambienti con un elevato volume di e-mail. Utilizzando l'API, gli amministratori possono filtrare messaggi specifici (ad esempio, per mittente) e rilasciarli a livello di programmazione, riducendo il tempo operativo e il rischio di errore umano rispetto alla gestione manuale nell'interfaccia utente.

Test iniziale

Per gestire la quarantena, eseguire una query iniziale per verificare la connettività e confermare la struttura dei dati.

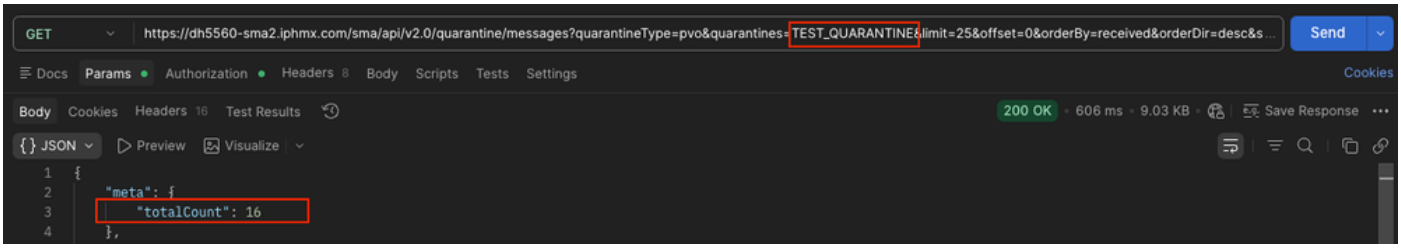
```
https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages?quarantineType=pvo&quarantines=TEST_QUARA
```

Struttura dei dati

- Endpoint API: L'URL di base per l'API SMA (ad esempio, [https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages)](https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages).
- Nome quarantena: L'identificatore di quarantena specifico di PVO (ad esempio, TEST_QUARANTINE) da cui si intende recuperare i messaggi.
- Intervallo di date: StartDate e endDate utilizzati per definire l'intervallo di tempo specifico per la ricerca.
- Limite: Numero massimo di record da restituire in una singola risposta API. In questo modo è possibile gestire le dimensioni del payload e impedire timeout durante code di grandi dimensioni.
- Scostamento: Indice iniziale del set di risultati. È usato per l'impaginazione; se ad esempio si imposta un valore di offset pari a 25, i primi 25 messaggi verranno ignorati e sarà possibile recuperare il batch di risultati successivo.

Verificare i risultati utilizzando sia la GUI che l'API

Quando si recuperano le informazioni, è possibile visualizzare la stessa quantità di messaggi nella chiamata API e nella GUI.



richiesta GET postman

TEST_QUARANTINE	Centralized Policy	16

Messaggi TEST_QUARANTINE

Test iniziale con CURL

Generare il token di autenticazione Base64 per l'intestazione dell'autorizzazione:

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

Recupera tutti i messaggi

Eseguire la richiesta curl per estrarre i messaggi in un file locale:

```
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
```

Verifica conteggio totale

Verifica il numero totale di messaggi ricevuti:

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

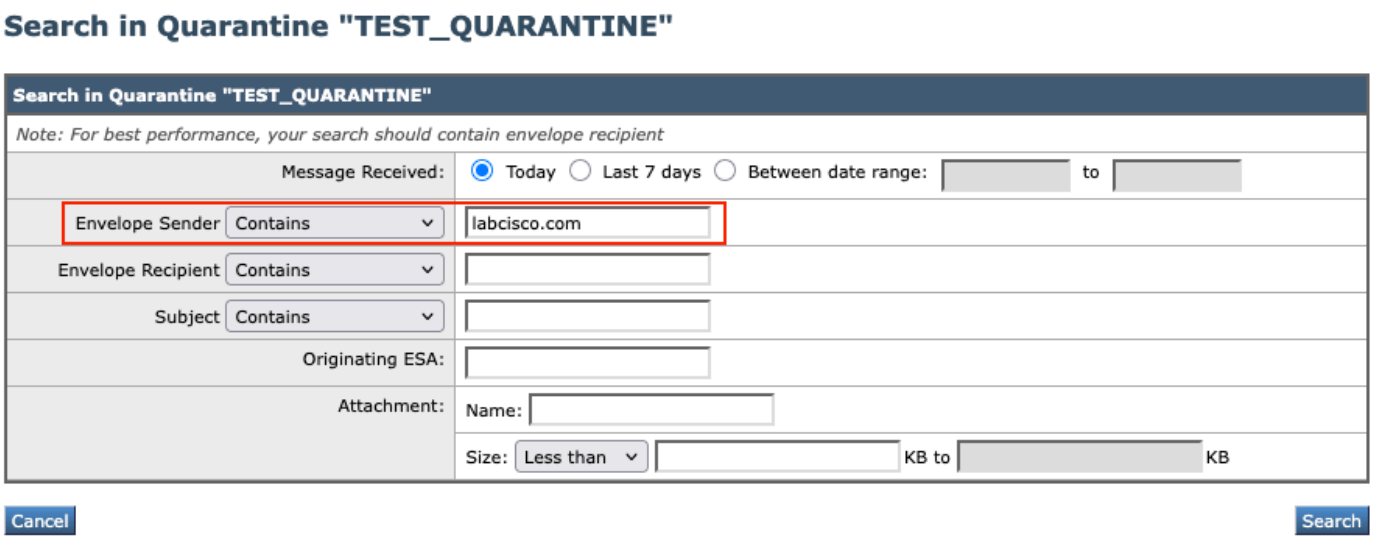
ID filtro per dominio

Utilizzare JQ per filtrare i MID dei messaggi che si desidera rilasciare (ad esempio, filtrando per dominio).

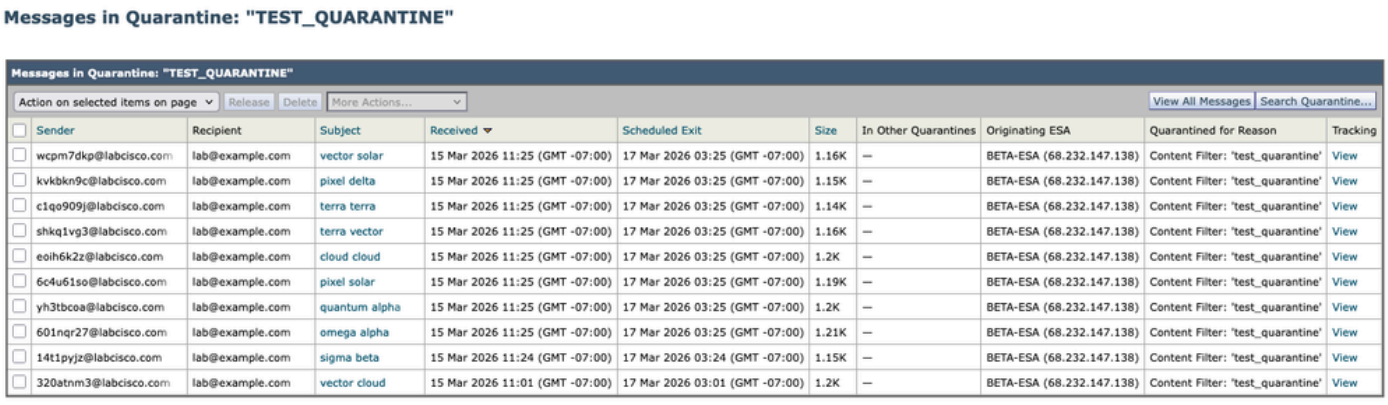
```
$ jq '[.data[] | select(.attributes.sender | endswith("@labcisco.com")) | .mid]' response.json > mids-l
$ cat mids-labcisco-domain.json
[
```

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

Il numero di MID, può corrispondere se si esegue una ricerca nella GUI TEST_QUARANTINE dell'interfaccia SMA.



ricerca quarantena



risultati quarantena

Filtra MID e crea payload

Filtrare i MID e generare il file di payload.

```
$ 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
  ]
}
```

Esecuzione della release (POST)

Inviare la richiesta di rilascio all'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}}
```

Verifica dei risultati

Controllo dei log di posta

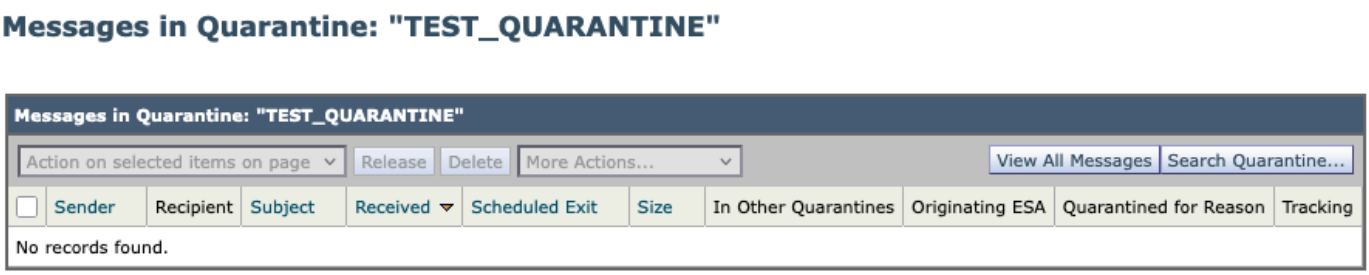
Quando si controlla mail_logs per i messaggi rilasciati, è possibile filtrare per grep "release" mail_logs e gli stessi MID filtrati in precedenza, gli stessi che sono stati rilasciati.

```
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
```

Controllo diretto nella GUI

Se si esegue la stessa ricerca per il dominio in cui sono stati rilasciati i messaggi, si noterà che la ricerca non ha alcun risultato, poiché tutti i messaggi sono stati rilasciati.

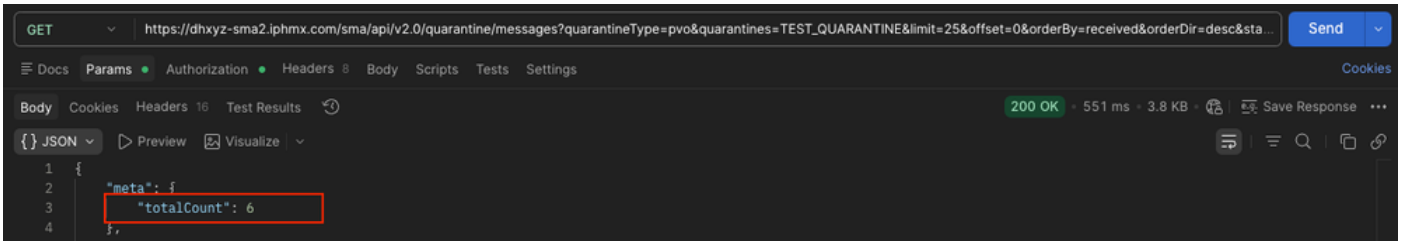


quarantena dei nuovi risultati

Controllo tramite API

Postino

Eseguire nuovamente il comando GET da Retrieve All Messages per verificare che totalCount sia diminuito o che i MID specifici non siano più presenti.



query GET postman

ARRICCIATURA

```
$ 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
[]
```

Rilascio in blocco messaggi (500 messaggi)

Per gestire in modo efficace le operazioni di massa, è necessario conoscere le modalità di gestione dei dataset di grandi dimensioni tramite l'impaginazione. Quando è necessario elaborare un numero elevato di messaggi, è necessario calcolare i parametri di limite e offset per garantire il recupero dell'insieme completo di dati senza superare i vincoli di risposta API.

Adeguamento dei parametri API per le operazioni di massa

Quando si recupera un grande volume di messaggi, utilizzare questa logica per configurare la richiesta:

- Limite: Definisce il numero di record restituiti per richiesta. Sebbene sia possibile impostare questo valore su un valore elevato (ad esempio, 500 o 1000) per acquisire più dati contemporaneamente, è importante tenere presente le prestazioni del sistema e i potenziali timeout.
- Scostamento: In questo modo viene definito il punto iniziale dell'insieme di risultati. Se il numero totale di messaggi supera il limite, è necessario eseguire più richieste, incrementando lo scostamento del valore limite in ogni chiamata successiva (ad esempio, offset=0, offset=500, offset=1000).

Ridimensionamento del flusso di lavoro

Il processo utilizzato nell'esempio di 10 messaggi precedente funge da base per tutte le operazioni di massa. Per scalare il flusso di lavoro, è sufficiente scorrere la coda incrementando sistematicamente il parametro di offset. Se si utilizzano questi valori, modificando il limite per definire le dimensioni del batch e l'offset per spostarsi nelle pagine, è possibile recuperare ed elaborare l'intera coda di quarantena, indipendentemente dal numero totale di messaggi.

Informazioni correlate

- Guida introduttiva ad AsyncOS API 16.0 per Cisco Secure Email e Web Manager - GD (General Deployment)
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).