Automatiser la libération des messages dans les quarantaines PVO via l'API SMA

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Test initial
  - Structure des données
  - Vérifiez les résultats à l'aide de l'interface utilisateur graphique et de l'API
  - Test initial avec CURL
  - Récupérer tous les messages
  - Vérifier le nombre total
  - Filtrer les MID par domaine
  - Filtrer les MID et créer des données utiles
  - Exécution de la libération (POST)
  - Vérification des résultats
    - Vérification des journaux de messagerie
    - Vérification directe dans l'interface utilisateur graphique
  - Vérification via l'API
    - POSTMAN
    - BOUCLER
- Diffusion de messages en masse (500 messages)
  - Ajustement des paramètres API pour les opérations en bloc
  - Évolutivité de votre workflow
- Informations connexes

Introduction

Ce document décrit comment automatiser la gestion et la publication des messages sur un Cisco SMA via l'API REST afin de traiter de grands volumes de messages.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances des produits Cisco SMA
- Familiarité avec les bases de l'API REST, Postman, curl et JQ pour le traitement JSON
- Informations d'identification valides pour l'accès SMA API
- Ligne de commande
- Accès réseau au SMA
- Outils installés : curl (pour les requêtes), JQ (pour la manipulation JSON) et un client comme Postman pour le test initial
- Rôle d'utilisateur approprié sur le SMA pour effectuer des actions de libération de messages

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'automatisation de la diffusion des messages est essentielle pour les environnements à fort volume d'e-mails. Grâce à l'API, les administrateurs peuvent filtrer des messages spécifiques (par exemple, par expéditeur) et les diffuser par programme, réduisant ainsi le temps d'exploitation et le risque d'erreur humaine par rapport à la gestion manuelle dans l'interface utilisateur graphique.

Test initial

Afin de gérer la quarantaine, commencez par exécuter une requête initiale pour vérifier la connectivité et confirmer la structure des données.

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

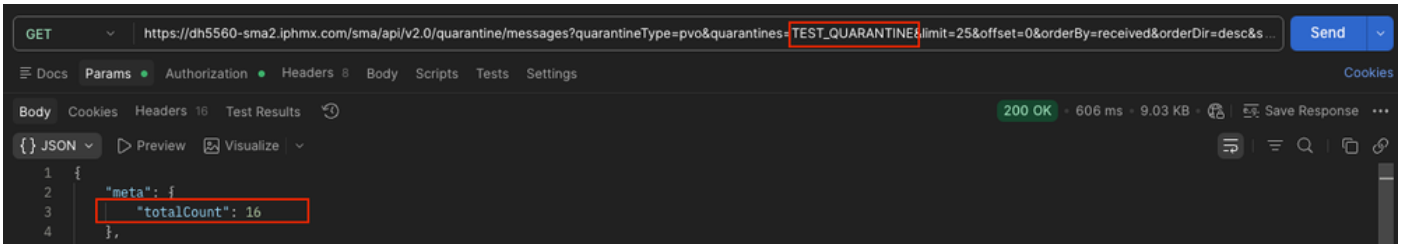
Structure des données

- Terminal API : URL de base de l'API SMA (par exemple, https://dhxyz-sma2.iphmx.com/sma/api/v2.0/quarantine/messages).

- Nom de la quarantaine : Identificateur de quarantaine PVO spécifique (par exemple, TEST_QUARANTINE) à partir duquel vous souhaitez récupérer des messages.
- Plage de dates : StartDate et endDate utilisées pour définir le délai spécifique de la recherche.
- Limite : Nombre maximal d'enregistrements à renvoyer dans une seule réponse API. Cela permet de gérer la taille de la charge utile et évite les délais d'attente lors de files d'attente volumineuses.
- Décalage : Index de début du jeu de résultats. Il est utilisé pour la pagination ; par exemple, si vous définissez un décalage de 25, les 25 premiers messages sont ignorés, ce qui vous permet de récupérer le lot de résultats suivant.

Vérifiez les résultats à l'aide de l'interface utilisateur graphique et de l'API

Lors de la récupération des informations, vous pouvez voir le même nombre de messages dans l'appel API et dans l'interface utilisateur graphique.



demande GET du facteur

TEST_QUARANTINE	Centralized Policy	16

Messages TEST_QUARANTINE

Test initial avec CURL

Générez votre jeton d'authentification Base64 pour l'en-tête d'autorisation :

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

Récupérer tous les messages

Exécutez la requête curl pour extraire les messages dans un fichier local :

```
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
```

Vérifier le nombre total

Vérifiez le nombre total de messages reçus :

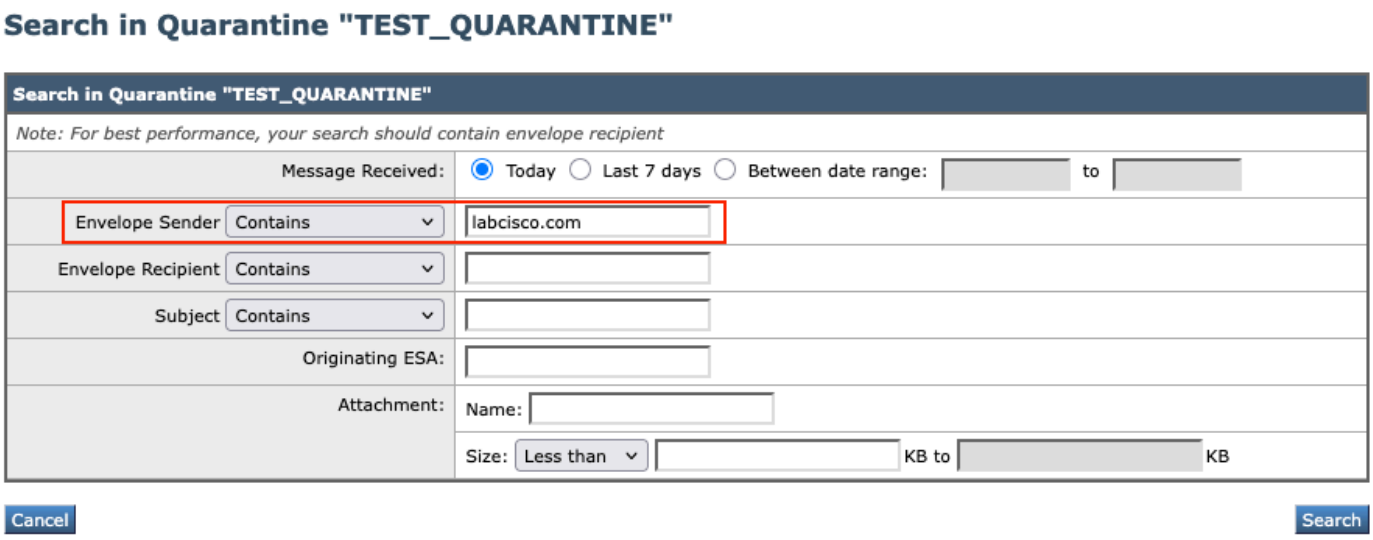
```
$ grep "totalCount" response.json | awk '{ print $2, $3}'
{"totalCount": 24},
```

Filtrer les MID par domaine

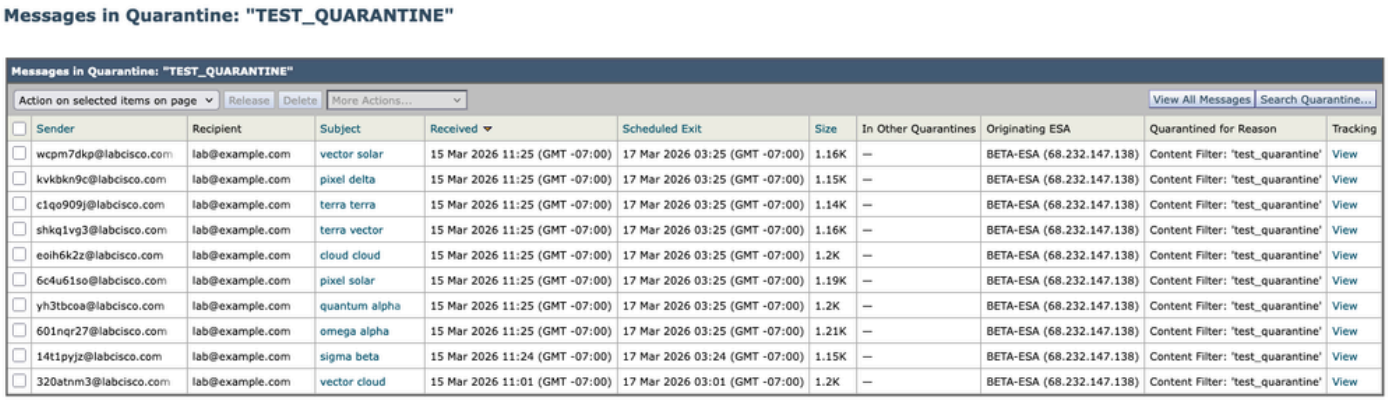
Utilisez JQ pour filtrer les MID des messages que vous souhaitez diffuser (par exemple, le filtrage par domaine).

```
$ 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
]
```

Le nombre de MID peut correspondre si vous effectuez une recherche dans TEST_QUARANTINE dans l'interface utilisateur graphique de SMA.



recherche en quarantaine



résultats de la quarantaine

Filtrer les MID et créer des données utiles

Filtrez les MID et générez le fichier de données utiles.

```
$ 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
  ]
}
```

Exécution de la libération (POST)

Envoyez la demande de libération au 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}}
```

Vérification des résultats

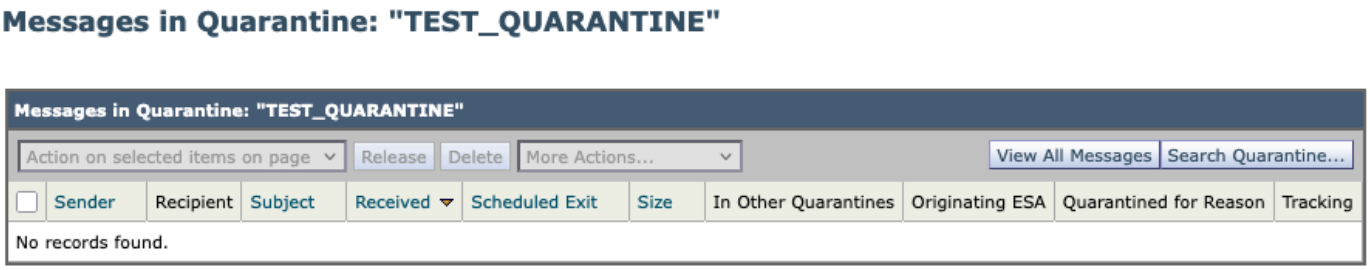
Vérification des journaux de messagerie

Lors de la vérification de mail_logs pour les messages libérés, vous pouvez filtrer par grep "release" mail_logs et les mêmes MID que vous filtrez ci-dessus, les mêmes que ceux qui ont été libérés.

```
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
```

Vérification directe dans l'interface utilisateur graphique

Si vous effectuez la même recherche pour le domaine que vous avez libéré les messages, vous voyez que la recherche n'a aucun résultat, puisque tous les messages ont été libérés.

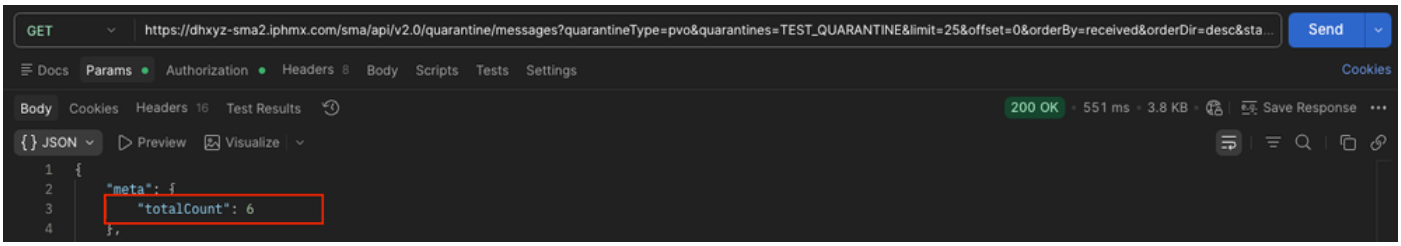


mettre en quarantaine les nouveaux résultats

Vérification via l'API

POSTMAN

Exécutez à nouveau la commande GET à partir de Retrieve All Messages afin de confirmer que le nombre totalCount a diminué ou que les MID spécifiques ne sont plus présents.



requête GET postman

BOUCLER

```
$ 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
[]
```

Diffusion de messages en masse (500 messages)

Afin de gérer efficacement les opérations en masse, vous devez comprendre comment gérer des jeux de données volumineux à l'aide de la pagination. Lorsque vous devez traiter un grand nombre de messages, vous devez calculer les paramètres de limite et de décalage pour vous

assurer de récupérer l'ensemble complet de données sans dépasser les contraintes de réponse de l'API.

Ajustement des paramètres API pour les opérations en bloc

Lorsque vous récupérez un grand volume de messages, utilisez cette logique pour configurer votre requête :

- Limite : Définit le nombre d'enregistrements renvoyés par demande. Bien que vous puissiez définir ce paramètre sur un nombre élevé (par exemple, 500 ou 1000) pour capturer plus de données à la fois, gardez à l'esprit les performances du système et les délais d'expiration potentiels.
- Décalage : Définit le point de départ de votre jeu de résultats. Si le nombre total de messages dépasse votre limite, vous devez effectuer plusieurs requêtes, en incrémentant le décalage de la valeur limite pour chaque appel suivant (par exemple, décalage=0, décalage=500, décalage=1000).

Évolutivité de votre workflow

Le processus utilisé dans l'exemple précédent de 10 messages sert de base à toutes les opérations en bloc. Afin de faire évoluer votre flux de travail, il vous suffit d'itérer dans la file d'attente en incrémentant systématiquement le paramètre de décalage. En jouant avec ces valeurs (en ajustant la limite pour définir la taille de votre lot et le décalage pour naviguer dans les pages), vous pouvez récupérer et traiter efficacement l'ensemble de votre file d'attente de quarantaine, quel que soit le nombre total de messages.

Informations connexes

- API AsyncOS 16.0 pour Cisco Secure Email and Web Manager - Guide de démarrage - GD (General Deployment)
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.